TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

"Auditoría con normas ISO de la familia 27000 y otros estándares para los procesos internos del H. Ayuntamiento de Tultitlán."

Informe Técnico de Residencias Profesionales
Para obtener el título de

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Especialidad
Auditoria en Seguridad Informática

Presenta(n):
Moran Diego Oscar Yahir
Santos Ramírez Ana Laura

Coacalco de Berriozábal, Noviembre de 2024.

AGRADECIMIENTOS

Quiero externar mi gratitud principalmente hacia mis padres. Gerardo Santos y Guadalupe Ramírez por brindarme estudios de forma profesional. Quienes moral y emocionalmente estuvieron y siempre estarán presentes en mi vida. Además de agradecer a mis Hermanos por brindarme su apoyo siempre, a Aaron Santos y José Santos, quienes entre risas y consejos que me ayudaron en mi camino para formarme profesionalmente. En especial a Luis Ángel Santos Ramírez quien partió de este mundo en el año 2021, a quien eternamente le estaré agradecida por siempre brindarme apoyo incondicional, y quien siempre se postraba orgulloso hacia mi persona. Este logro va por él, ya que sea donde se encuentre, espero este orgulloso y celebre quién ahora soy. A mis amigos, Brenda Gante, Eduardo Junco, Braulio Olvera, Daniel Palma, por brindarme su más sincera amistad en este camino, su apoyo moral y emocional que me brindaron ya que cuando más bajo estaba ellos me daban aliento de superación. Por último, a mí misma ya que a pesar de tener obstáculos y pérdidas he sobrellevado toda aquella situación que se me ha materializado, reconozco que durante estos 4 años con 6 meses ha sido un total reto que he logrado superar junto con mi compañero Oscar Moran, que durante este proceso nos hemos apoyado para salir y superar este último tramo de mi formación profesional.

- Ana Laura Santos Ramírez

Agradezco en primer lugar a mis padres Oscar Moran y Alejandra Diego, que me han brindado su apoyo incondicional para poder cumplir mis objetivos personales y académicos, me han impulsado a perseguir mis metas y no abandonarlas ante las adversidades, pues me han brindado el apoyo material y económico para poder concentrarme en los estudios. A mis hermanas Dulce Moran y Valeria Moran por ser un pilar emocional para continuar día con día en mi preparación. Agradezco profundamente a mi asesora Diana Prado por su dedicación y paciencia, sin sus palabras y correcciones precisas no hubiese podido llegar a esta instancia tan anhelada. Gracias por darme una visión sobre las distintas alternativas que existen aparte de la programación y por sus consejos, los llevaré grabados en mi futuro profesional. Debo agradecer al TESCo y sus docentes que me han exigido tanto, pero al mismo tiempo me han permitido terminar exitosamente esta etapa, agradezco a la Unidad de Tecnologías de la Información y Comunicación por permitirme desarrollar mi trabajo dentro de sus instalaciones y a los empleados que colaboraron y me brindaron de su ayuda. Agradezco a mi compañera Ana Santos por permitirme colaborar con ella en este

proyecto y su apoyo durante el proceso, no cabe duda de que trabajar a su lado ha sido un honor. Por último, quiero hacer una mención especial y agradecer a Fernando Reyes, amigo y compañero de la carrera quien partió en agosto del año 2022, gracias por las horas compartidas, por tantos trabajos realizados en conjunto y por el apoyo que me brindaste durante tu estadía.

- Oscar Yahir Moran Diego

RESUMEN

El siguiente trabajo escrito trata sobre la auditoría realizada al laboratorio de la Unidad de Tecnologías de la Información y Comunicación (UTIC) en el Ayuntamiento de Tultitlán, tiene como objetivo evaluar la seguridad y el rendimiento de dicho laboratorio en diversos aspectos críticos. Durante esta auditoría se llevarán a cabo pruebas exhaustivas en varios apartados clave, que incluyen la seguridad física, seguridad lógica, infraestructura, inventario y servicios. El propósito fundamental de esta auditoría es asegurar que el laboratorio de la UTIC opere de manera eficiente, segura y cumpla con las mejores prácticas establecidas. Mediante la identificación de posibles vulnerabilidades, riesgos y áreas de mejora, se buscará fortalecer la integridad y confiabilidad de las operaciones del laboratorio. A través de este proceso, se podrán ofrecer recomendaciones específicas y medidas correctivas para garantizar un entorno de laboratorio óptimo, que promueva la excelencia académica y el desarrollo de habilidades prácticas en el ámbito profesional dentro del laboratorio de la UTIC que así mismo beneficiará en conjunto a otros departamentos al Ayuntamiento de Tultitlán.

ÍNDICE DE CONTENIDOS

GENERALIDADES DEL PROYECTO 1
1.1 INTRODUCCIÓN 2
1.2 DESCRIPCIÓN DE LA EMPRESA 4
1.2.1 Nombre, razón social 4
1.2.2 Ubicación 4
1.2.3 Organigrama 4
1.2.4 Sector productivo de la empresa 5
1.2.5 Misión, Visión, Filosofía y/o Valores 5
1.2.5.1 Misión 5
1.2.5.2 Visión 5
1.2.5.3 Valores 5
1.2.6 Breve historia de la empresa 6
1.3 PROBLEMA A RESOLVER 7
1.4 OBJETIVOS 9
1.4.1 Objetivo general 9
1.4.2 Objetivos específicos 9
1.5 JUSTIFICACIÓN 10
MARCO TEÓRICO 11
2.1 Marco Teórico 12
2.2 Estado de Arte 13
2.3 Marco Conceptual 15
2.4 Marco Metodológico 18
2.5 Estándar 27002 24
DESARROLLO 29
3.1 Primer Objetivo: Planificar Auditoría 31
3.1.1 Actividades 31
3.1.1.1 Actividad 1.1 Conocer el entorno general de la dependencia 31

3.1.1.1.1 Descripción de la actividad..... 31
3.1.1.1.2 Resultado de la actividad..... 31
3.1.1.1.2.1 Nombre, razón social 31
3.1.1.1.2.2 Ubicación 31
3.1.1.1.2.3 Organigrama..... 32
3.1.1.1.2.4 Sector productivo de la empresa 32
3.1.1.1.2.5 Misión, Visión, Filosofía y/o Valores 32
3.1.1.1.2.5.1 Misión 32
3.1.1.1.2.5.2 Visión..... 33
3.1.1.1.2.5.3 Valores..... 33
3.1.1.1.2.5.4 Breve historia de la empresa..... 33
3.1.1.2 Actividad 1.2 Conocer el entorno particular dentro de la dependencia 34
3.1.1.2.1 Descripción de la actividad..... 34
3.1.1.2.2 Resultado de la actividad 35
3.1.1.3 Actividad 1.3 Establecer objetivos y alcances..... 36
3.1.1.3.1 Descripción de la actividad..... 36
3.1.1.3.2 Resultado de la actividad 37
3.1.1.3.2.1 Objetivo general..... 37
3.1.1.3.2.2 Objetivos específicos..... 37
3.1.1.3.2.3 Alcance 37
3.1.1.4 Actividad 1.4 Generar un plan de trabajo de la Auditoría detallado, como que incluya los objetivos, el cronograma y los recursos necesarios..... 37
3.1.1.4.1 Descripción de la actividad 37
3.1.1.4.2 Resultado de la actividad 38
3.1.1.5 Actividad 1.5 Comunicar el plan de Auditoría al responsable del área de la Unidad de Tecnologías de la Información y Comunicación. 41
3.1.1.5.1 Descripción de la actividad..... 41
3.1.1.5.2 Resultado de la actividad 41
3.1.1.6 Actividad 1.6 Realizar formatos para la recopilación de la información. 41

3.1.1.6.1 Actividad 1.6.1 Generar formato para la obtención de fortalezas, oportunidades, debilidades y amenazas de la UTIC (FODA). 42
3.1.1.6.1.1 Descripción de la actividad 42
3.1.1.6.1.2 Resultado de la actividad 42
3.1.1.6.2 Actividad 1.6.2 Generar los cuestionarios. 43
3.1.1.6.2.1 Descripción de la actividad 43
3.1.1.6.2.2 Resultado de la actividad 43
3.1.1.6.2.2.1 Cuestionario Seguridad Física 43
3.1.1.6.2.2.2 Cuestionario Seguridad Lógica 45
3.1.1.6.2.2.3 Cuestionario de Servicios 49
3.1.1.6.2.2.4 Cuestionario de Infraestructura 51
3.1.1.6.3 Actividad 1.6.3 Generar formato de la Matriz y el análisis de riesgos. 55
3.1.1.6.3.1 Descripción de la actividad 55
3.1.1.6.3.2 Resultado de la actividad 55
3.1.1.6.4 Actividad 1.6.4 Generar formato para la realización de pruebas. 57
3.1.1.6.4.1 Descripción de la actividad 57
3.1.1.6.4.2 Resultado de la actividad 58
3.2 Segundo Objetivo: Ejecutar Auditoría 59
3.2.1 Actividades 59
3.2.1.1 Actividad 2.1 Aplicar los cuestionarios 59
3.2.1.1.1 Descripción de la actividad 59
3.2.1.1.2 Resultado de la actividad 60
3.2.1.2 Actividad 2.2 Realizar los Análisis FODA 85
3.2.1.2.1 Descripción de la actividad 85
3.2.1.2.2 Resultado de la actividad 85
3.2.1.2.2.1 FODA de la Unidad De Tecnologías De La Información Y Comunicación 85
3.2.1.2.2.2 FODA Seguridad Física 87
3.2.1.2.2.2.1 Conclusión 89

3.2.1.2.2.3 FODA Seguridad Lógica 90
3.2.1.2.2.3.1 Conclusión 92
3.2.1.2.2.4 FODA Servicios de la UTIC 93
3.2.1.2.2.4.1 Conclusión 96
3.2.1.2.2.5 FODA Infraestructura de la UTIC 97
3.2.1.2.2.5.1 Conclusión 102
3.2.1.2.2.6 FODA del Sistema de Inventario de la UTIC 103
3.2.1.2.2.6.1 Conclusión 106
3.2.1.3 Actividad 2.3 Realizar el Análisis de Riesgos 107
3.2.1.3.1 Análisis de riesgos de la Seguridad Física de la UTIC 107
3.2.1.3.1.1 Recopilación de la situación actual de la SEGURIDAD FÍSICA por parte de los empleados de la UTIC. 111
3.2.1.3.1.1.1 Vulnerabilidades consideradas 111
3.2.1.3.1.1.2 Amenazas consideradas 114
3.2.1.3.2 Análisis de riesgos de la Seguridad Lógica de la UTIC 118
3.2.1.3.2.1 Recopilación de la situación actual sobre la SEGURIDAD LÓGICA por pare de los empleados de la UTIC 120
3.2.1.3.2.1.1 Vulnerabilidades consideradas 120
3.2.1.3.2.1.2 Amenazas consideradas 123
3.2.1.3.3 Análisis de riesgo de los Servicios de la UTIC 125
3.2.1.3.3.1 Recopilación de la situación actual sobre los SERVICIOS por parte de los empleados de la UTIC 128
3.2.1.3.3.1.1 Vulnerabilidades consideradas 128
3..2.1.3.3.1.2 Amenazas Consideradas 132
3.2.1.3.4 Análisis de riesgo de los Infraestructura de la UTIC. 136
3.2.1.3.4.1 Recopilación de la situación actual sobre los INFRAESTRUCTURA por parte de los empleados de la UTIC 141
3.2.1.3.4.1.1 Vulnerabilidades consideradas 141
3.2.1.3.4.1.2 Amenazas Consideradas 150

3.2.1.3.5 Análisis de riesgo del Sistema de Inventario de la UTIC 158
3.2.1.3.5.1 Recopilación de la situación actual sobre el sistema de INVENTARIO por parte de los empleados de la UTIC..... 163
3.2.1.3.5.1.1 Vulnerabilidades consideradas..... 163
3.2.1.3.5.1.2 Amenazas Consideradas 168
3.2.1.3.6 Clasificación de atención de acuerdo con las vulnerabilidades. 172
3.2.1.4 Actividad 2.4 Realizar Pruebas de Seguridad Física. 218
3.2.1.4.1 Descripción de la actividad..... 218
3.2.1.4.2 Resultado de la actividad 219
3.2.1.5 Actividad 2.5 Realizar Pruebas de Seguridad Lógica. 245
3.2.1.5.1 Descripción de la actividad..... 245
3.2.1.5.2 Resultado de la actividad 245
3.2.1.6 Actividad 2.6 Realizar Pruebas de Servicios. 281
3.2.1.6.1 Descripción de la actividad..... 281
3.2.1.6.2 Resultado de la actividad..... 281
3.2.1.7 Actividad 2.7 Realizar Pruebas de Infraestructura 342
3.2.1.7.1 Descripción de la actividad 342
3.2.1.7.2 Resultado de la actividad..... 342
3.2.1.8 Actividad 2.8 Realizar Pruebas del Sistema de Inventario. 419
3.2.1.8.1 Descripción de la actividad 419
3.2.1.8.2 Resultado de la actividad..... 419
RESULTADOS..... 475
4.1 Tercer Objetivo: Entregar Resultados 476
4.1.1 Actividades..... 476
4.1.1.1 Actividad 3.1 Analizar y sintetizar los hallazgos de la Auditoría en un informe final. 476
4.1.1.2 Actividad 3.2 Generar recomendaciones de acuerdo con los estándares y normas utilizados..... 476
4.1.1.2.1 Descripción de las actividades..... 476

4.1.1.2.2 Resultado de las actividades 476
IMPLEMENTACIONES 540
5.1.1.3 Actividad 3.3 Implementar las Recomendaciones 541
5.1.1.3.1 Descripción de la actividad 541
5.1.1.3.2 Resultado de la actividad 541
CONCLUSIONES 624
COMPETENCIAS DESARROLLADAS 625
FUENTES DE INFORMACIÓN 633
ANEXOS 648
Anexo 1 648
Anexo 2 650
Anexo 3 656
INICIO DE SESIÓN 658
REGISTRO DE EMPLEADOS 660
REGISTRO DE PRODUCTOS 668
CONSULTA DE MARCAS 673
CONSULTA DE CARGOS 674
REGISTRO DE ENTRADA 676
REGISTRO DE SALIDA 679
CONSULTAS DE ENTRADAS 681
Instrucciones para imprimir 682
CONSULTAS DE SALIDAS 687
Instrucciones para imprimir 689
CONSULTA DEL INVENTARIO TOTAL 692
VALE DE SALIDA 694
ADMINISTRADOR 699
CAMBIAR IMAGEN DEL LOG IN 699
CAMBIAR IMAGEN DE LAS CONSULTAS DE ENTRADAS Y SALIDAS E INVENTARIO TOTAL 700

CAMBIAR IMAGEN DEL ENCABEZADO Y PIE DE PAGINA DEL VALE DE SALIDA... 701

Índice de Figuras

Figura 1. Ubicación del H. Ayuntamiento de Tultitlán 4
Figura 2. Organigrama del Palacio Municipal 4
Figura 3. Ubicación del H. Ayuntamiento de Tultitlán 31
Figura 4. Organigrama del Palacio Municipal 32
Figura 5 Ubicación Física de la Unidad de Tecnologías de la Información y Comunicación (UTIC) 35
Figura 6. Acceso Principal al UTIC 35
Figura 7. Análisis de Riesgos, Seguridad Física Vulnerabilidad 1 111
Figura 8. Análisis de Riesgos, Seguridad Física Vulnerabilidad 2. 112
Figura 9. Análisis de Riesgos, Seguridad Física Vulnerabilidad 3 112
Figura 10. Análisis de Riesgos, Seguridad Física Vulnerabilidad 4. 112
Figura 11. Análisis de Riesgos, Seguridad Física Vulnerabilidad 5. 113
Figura 12. Análisis de Riesgos, Seguridad Física Vulnerabilidad 6. 113
Figura 13. Análisis de Riesgos, Seguridad Física Vulnerabilidad 7. 113
Figura 14. Análisis de Riesgos, Seguridad Física Amenaza 1. 114
Figura 15. Análisis de Riesgos, Seguridad Física Amenaza 2 114
Figura 16. Análisis de Riesgos, Seguridad Física Amenaza 3. 115
Figura 17. Análisis de Riesgos, Seguridad Física Amenaza 4. 115
Figura 18. Análisis de Riesgos, Seguridad Física Amenaza 5. 115
Figura 19. Análisis de Riesgos, Seguridad Física Amenaza 6. 116
Figura 20. Análisis de Riesgos, Seguridad Física Amenaza 7. 116
Figura 21. Análisis de Riesgos, Seguridad Física Amenaza 8. 116
Figura 22. Análisis de Riesgos, Seguridad Física Amenaza 9. 117
Figura 23. Análisis de Riesgos, Seguridad Física Amenaza 10. 117
Figura 24. Análisis de Riesgos, Seguridad Física Amenaza 11. 117
Figura 25. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 120
Figura 26. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 2. 120

Figura 27. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 3. 121
Figura 28. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 4. 121
Figura 29. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 5. 121
Figura 30. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 6. 122
Figura 31. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 7. 122
Figura 32. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 8. 122
Figura 33. Análisis de Riesgos, Seguridad Lógica Amenaza 1. 123
Figura 34. Análisis de Riesgos, Seguridad Lógica Amenaza 2.. 123
Figura 35. Análisis de Riesgos, Seguridad Lógica Amenaza 3. 123
Figura 36. Análisis de Riesgos, Seguridad Lógica Amenaza 4. 124
Figura 37. Análisis de Riesgos, Seguridad Lógica Amenaza 5. 124
Figura 38. Análisis de Riesgos, Seguridad Lógica Amenaza 6. 124
Figura 39. Análisis de Riesgos, Servicios Vulnerabilidad 1 128
Figura 40. Análisis de Riesgos, Servicios Vulnerabilidad 2. 128
Figura 41. Análisis de Riesgos, Servicios Vulnerabilidad 3. 129
Figura 42. Análisis de Riesgos, Servicios Vulnerabilidad 4 129
Figura 43. Análisis de Riesgos, Servicios Vulnerabilidad 5. 129
Figura 44. Análisis de Riesgos, Servicios Vulnerabilidad 6. 130
Figura 45. Análisis de Riesgos, Servicios Vulnerabilidad 7. 130
Figura 46. Análisis de Riesgos, Servicios Vulnerabilidad 8. 131
Figura 47. Análisis de Riesgos, Servicios Vulnerabilidad 9. 131
Figura 48. Análisis de Riesgos, Servicios Amenaza 1..... 132
Figura 49. Análisis de Riesgos, Servicios Amenaza 2..... 132
Figura 50. Análisis de Riesgos, Servicios Amenaza 3..... 133
Figura 51. Análisis de Riesgos, Servicios Amenaza 4..... 133
Figura 52. Análisis de Riesgos, Servicios Amenaza 5..... 134
Figura 53. Análisis de Riesgos, Servicios Amenaza 6..... 134
Figura 54. Análisis de Riesgos, Servicios Amenaza 7..... 135
Figura 55. Análisis de Riesgos, Servicios Amenaza 8..... 135

Figura 56. Análisis de Riesgos, Infraestructura Vulnerabilidad 1..... 141
Figura 57. Análisis de Riesgos, Infraestructura Vulnerabilidad 2..... 141
Figura 58. Análisis de Riesgos, Infraestructura Vulnerabilidad 3..... 142
Figura 59. Análisis de Riesgos, Infraestructura Vulnerabilidad 4..... 142
Figura 60. Análisis de Riesgos, Infraestructura Vulnerabilidad 5..... 143
Figura 61. Análisis de Riesgos, Infraestructura Vulnerabilidad 6..... 143
Figura 62. Análisis de Riesgos, Infraestructura Vulnerabilidad 7..... 144
Figura 63. Análisis de Riesgos, Infraestructura Vulnerabilidad 8..... 144
Figura 64. Análisis de Riesgos, Infraestructura Vulnerabilidad 9..... 144
Figura 65. Análisis de Riesgos, Infraestructura Vulnerabilidad 10..... 145
Figura 66. Análisis de Riesgos, Infraestructura Vulnerabilidad 11..... 145
Figura 67. Análisis de Riesgos, Infraestructura Vulnerabilidad 12..... 146
Figura 68. Análisis de Riesgos, Infraestructura Vulnerabilidad 13..... 146
Figura 69. Análisis de Riesgos, Infraestructura Vulnerabilidad 14..... 147
Figura 70. Análisis de Riesgos, Infraestructura Vulnerabilidad 15..... 147
Figura 71. Análisis de Riesgos, Infraestructura Vulnerabilidad 16..... 148
Figura 72. Análisis de Riesgos, Infraestructura Vulnerabilidad 17..... 148
Figura 73. Análisis de Riesgos, Infraestructura Vulnerabilidad 18..... 149
Figura 74. Análisis de Riesgos, Infraestructura Amenaza 1 150
Figura 75. Análisis de Riesgos, Infraestructura Amenaza 2 150
Figura 76. Análisis de Riesgos, Infraestructura Amenaza 3 151
Figura 77. Análisis de Riesgos, Infraestructura Amenaza 4 151
Figura 78. Análisis de Riesgos, Infraestructura Amenaza 5 152
Figura 79. Análisis de Riesgos, Infraestructura Amenaza 6 152
Figura 80. Análisis de Riesgos, Infraestructura Amenaza 7 153
Figura 81. Análisis de Riesgos, Infraestructura Amenaza 8 153
Figura 82. Análisis de Riesgos, Infraestructura Amenaza 9 154
Figura 83. Análisis de Riesgos, Infraestructura Amenaza 10 154
Figura 84. Análisis de Riesgos, Infraestructura Amenaza 11. 155

Figura 85. Análisis de Riesgos, Infraestructura Amenaza 12. 155
Figura 86. Análisis de Riesgos, Infraestructura Amenaza 13. 156
Figura 87. Análisis de Riesgos, Infraestructura Amenaza 14. 156
Figura 88. Análisis de Riesgos, Infraestructura Amenaza 15. 157
Figura 89. Análisis de Riesgos, Inventario Vulnerabilidad 1. 163
Figura 90. Análisis de Riesgos, Inventario Vulnerabilidad 2. 163
Figura 91. Análisis de Riesgos, Inventario Vulnerabilidad 3. 164
Figura 92. Análisis de Riesgos, Inventario Vulnerabilidad 4. 164
Figura 93. Análisis de Riesgos, Inventario Vulnerabilidad 5. 164
Figura 94. Análisis de Riesgos, Inventario Vulnerabilidad 6 165
Figura 95. Análisis de Riesgos, Inventario Vulnerabilidad 7 165
Figura 96. Análisis de Riesgos, Inventario Vulnerabilidad 8 165
Figura 97. Análisis de Riesgos, Inventario Vulnerabilidad 9 166
Figura 98. Análisis de Riesgos, Inventario Vulnerabilidad 10 166
Figura 99. Análisis de Riesgos, Inventario Vulnerabilidad 11 166
Figura 100. Análisis de Riesgos, Inventario Vulnerabilidad 12 167
Figura 101. Análisis de Riesgos, Inventario Vulnerabilidad 13 167
Figura 102. Análisis de Riesgos, Inventario Vulnerabilidad 14 167
Figura 103. Análisis de Riesgos, Inventario Amenaza 1 168
Figura 104. Análisis de Riesgos, Inventario Amenaza 2 168
Figura 105. Análisis de Riesgos, Inventario Amenaza 3 169
Figura 106. Análisis de Riesgos, Inventario Amenaza 4) 169
Figura 107. Análisis de Riesgos, Inventario Amenaza 5 169
Figura 108. Análisis de Riesgos, Inventario Amenaza 6 170
Figura 109. Análisis de Riesgos, Inventario Amenaza 7 170
Figura 110. Análisis de Riesgos, Inventario Amenaza 8 170
Figura 111. Análisis de Riesgos, Inventario Amenaza 9 171
Figura 112. Acceso a la UTIC. 220
Figura 113. Vista trasera al Acceso a la UTIC..... 221

Figura 114. Vista de la Cerradura del Acceso Principal a la UTIC..... 221
Figura 115. Segunda Vista de la Cerradura del Acceso Principal a la UTIC 222
Figura 116. Tercera Vista de la Cerradura del Acceso Principal a la UTIC 222
Figura 117. Oficina de la UTIC..... 223
Figura 118. Cerraduras de la puerta de la UTIC 223
Figura 119. Segundo acceso hacia la UTIC..... 224
Figura 120. Equipo de Impresión Multifuncional..... 228
Figura 121. Cámara Interna de la UTIC. 242
Figura 122. Imagen de la Cámara de Videovigilancia. 243
Figura 123. Equipo 1 con contraseña. 247
Figura 124. Equipo 2 sin contraseña..... 248
Figura 125. Equipo 3 sin contraseña..... 248
Figura 126. Equipo 4 sin contraseña..... 249
Figura 127. Equipo 5 con contraseña. 249
Figura 128. Lista de aplicaciones que contiene el equipo. 261
Figura 129. Actualización Postergada..... 274
Figura 130. Actualización Postergada en otro equipo. 274
Figura 131. Vista 1 de los contactos eléctricos. 283
Figura 132. Vista 2 de los contactos eléctricos. 284
Figura 133. Vista 3 de los contactos eléctricos. 284
Figura 134. Bajada del contacto eléctrico. 286
Figura 135. Bajada del contacto eléctrico. 286
Figura 136. Extensiones eléctricas 287
Figura 137. Extensiones eléctricas 287
Figura 138. Extensiones eléctricas. 288
Figura 139. Extintor 1..... 295
Figura 140. Extintor 2..... 296
Figura 141. Archivos Físicos bajo la corriente alterna de la UTIC. 297
Figura 142. Extintor fuera de la UTIC..... 298

Figura 143. Acceso al botiquín médico 305
Figura 144. Acceso al botiquín médico. 306
Figura 145. Vendas del botiquín médico. 307
Figura 146. Gasas del botiquín médico. 307
Figura 147. Tela Adhesiva del botiquín médico 308
Figura 148. Abatelenguas del botiquín médico. 308
Figura 149. Agua Oxigenada del botiquín médico. 309
Figura 150 Jabón Germicida Líquido del botiquín médico 310
Figura 151. Tijeras de botón sin empaque del botiquín médico. 311
Figura 152 Termómetro digital del botiquín médico 312
Figura 153. Pinzas de Kelly rectas del botiquín médico. 312
Figura 154 Gafas de Protección del botiquín médico. 313
Figura 155. Lampara de Diagnóstico. del botiquín médico. 313
Figura 156. Glucómetro del botiquín médico 314
Figura 157. Isopos de algodón del botiquín médico. 314
Figura 158. Oxímetro de Pulso del botiquín médico. 315
Figura 159. Cubrebocas KNY-95 del botiquín médico 315
Figura 160. Activos ubicados en el suelo. 323
Figura 161. Activos ubicados en el suelo. 324
Figura 162. Materiales ubicados en el suelo. 325
Figura 163. Vista 1 del Aire Acondicionado. 330
Figura 164. Vista 2 del Aire Acondicionado. 330
Figura 165. Vista 3 del Aire Acondicionado. 331
Figura 166. Señalamiento de Salida de Emergencia. 336
Figura 167. Señalamiento de Ruta de Evacuación. 336
Figura 168. Señalamiento de Ruta de Evacuación. 337
Figura 169. Señalamiento del Extintor. 338
Figura 170. Etiquetado 1. 344
Figura 171. Etiquetado 2. 345

Figura 172. Etiquetado 3. 345
Figura 173. Etiquetado 4. 345
Figura 174. Etiquetado 5. 346
Figura 175. Vista General de la UTIC. 350
Figura 176. Vista del escritorio 1. 351
Figura 177. Vista del escritorio 2. 351
Figura 178. Vista del escritorio principal. 352
Figura 179. Activos situados en el suelo. 355
Figura 180. Activos, Materiales, Archivos de la UTIC. 356
Figura 181. Activos, Materiales, Archivos de la UTIC. 356
Figura 182. Activos, Materiales, Archivos de la UTIC. 357
Figura 183. Activos, Materiales, Archivos, Equipos de Impresión. 357
Figura 184. Activos sobre el pasillo 358
Figura 185. Cableado 1 360
Figura 186. Cableado 2. 361
Figura 187. Cableado 3. 361
Figura 188. Cableado 4. 362
Figura 189. Cableado 5. 362
Figura 190. Cableado 6. 363
Figura 191. Cableado 7. 363
Figura 192. Cableado 8. 364
Figura 193. Cableado 9. 364
Figura 194. Cableado 10. 365
Figura 195. Cableado 11. 365
Figura 196. Reparación de equipos fuera de la UTIC. 369
Figura 197. Reparación de equipos fuera de la UTIC. 370
Figura 198. Equipo en proceso de reparación. 370
Figura 199. Vista 1 del techo falso de la UTIC. 374
Figura 200. Vista 2 del techo falso de la UTIC. 375

Figura 201. Vista 3 del techo falso de la UTIC. 375
Figura 202. Vista del Drenaje..... 378
Figura 203. "Remachado" del tubo de drenaje. 379
Figura 204. Protección de la puerta principal de la UTIC. 379
Figura 205. Dispositivos de telecomunicaciones. 382
Figura 206. Dispositivos de telecomunicaciones. 383
Figura 207. Vista interior 1 del rack..... 388
Figura 208. Vista del cableado. 389
Figura 209. Vista del Servidor. 389
Figura 210. Cableado 1 del Rack. 393
Figura 211. Cableado 2 del Rack. 394
Figura 212. Cableado 3 del Rack. 395
Figura 213. Cableado 4 del Rack. 396
Figura 214. Cableado 5 del Rack. 396
Figura 215. Cableado 6 del Rack. 397
Figura 216. Asientos de la UTIC. 404
Figura 217. Formato 1 de Vale de Salida. 408
Figura 218. Formato 1 de Vale de Entrega. 409
Figura 219. Formato 2 de Vale de Entrega. 409
Figura 220. Función Ejecutar de Windows. 421
Figura 221. Carpetas en Red. 421
Figura 222. Archivos de la Carpeta UTIC 2022-2024..... 422
Figura 223. Vista del Sistema de Inventario de la UTIC. 422
Figura 224. Vista del Sistema de Inventario..... 426
Figura 225. Función de Ejecutar de Windows. 436
Figura 226. Vista 1 del Sistema de Inventario. 440
Figura 227. Vista 2 del Sistema de Inventario..... 441
Figura 228. Vista 3 del Sistema de Inventario. 441
Figura 229. Partidas de la UTIC. 445

Figura 230. Oficina de la UTIC sin vigilancia. 542
Figura 231. Formato de Asignación de Cierre. 543
Figura 232. Formato de llenado de la Asignación de Cierre. 544
Figura 233. Escrito firmado de la asignación del encargado de la UTIC. 545
Figura 234. Formato de Bitácora. Fuente: Elaboración propia. 546
Figura 235. Formato de llenado de la Bitácora. 547
Figura 236. Bitácora del uso de la impresora en uso. 547
Figura 237. Caratula de la política. 549
Figura 238. Política aprobada. 550
Figura 239. Compromiso Firmado de Implementación de Recomendaciones de Auditoría Interna. 551
Figura 240. Compromiso de uso de contraseñas seguras. 553
Figura 241. Datos de Inicio de sesión con contraseñas seguras. 553
Figura 242. Compromiso firmado de uso de contraseñas seguras. 554
Figura 243. Equipo mostrando mensaje de actualización. 556
Figura 244. Equipo aleatorio mostrando mensaje de actualización. 556
Figura 245. Compromiso de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC. 557
Figura 246. Compromiso firmado de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC. 558
Figura 247. Compromiso de asignación de encargado para el correcto cierre de la UTIC 559
Figura 248. Respaldo en la nube de datos de la UTIC. 561
Figura 249. Uso de extensiones en la UTIC. 562
Figura 250. Uso de extensiones en la UTIC. 562
Figura 251. Cambio de extensiones por sistemas de alimentación ininterrumpidas. 563
Figura 252. Vista frontal del sistema de alimentación ininterrumpida. 564
Figura 253. Vista del No Break con código QR para saber sus características. 565
Figura 254. Caja de los No Break implementados en la UTIC. 565

Figura 255. Características de los No Break implementados en la UTIC. 566
Figura 256. Archivo debajo de interruptores eléctricos principales de la UTIC. 567
Figura 257. Extintor mal ubicado dentro del site. 568
Figura 258. Interruptores eléctricos despejados de archivos. 569
Figura 259. Extintor mejor ubicado dentro del site. 570
Figura 260. Activos situados en el piso. 572
Figura 261. Activos obstruyendo el acceso principal de la UTIC. 573
Figura 262. Espacio del pasillo libre de activos. 574
Figura 263. Acceso principal a la UTIC despejado. 575
Figura 264. Señalamiento de emergencia. 576
Figura 265 Señalamiento de emergencia. 577
Figura 266 Señalamiento de emergencia. 577
Figura 267 Compromiso firmado de implementación de recomendaciones de auditoría interna. 578
Figura 268 Activos situados en el piso. 579
Figura 269 Activos situados en el piso. 580
Figura 270 Activos situados en el piso. 580
Figura 271 Activos situados en el piso. 581
Figura 272 Reubicación de los activos situados en el piso. 581
Figura 273 Reubicación de activos. 582
Figura 274 Reubicación de activos. 583
Figura 275 Reubicación de activos. 584
Figura 276 Cableado desordenado. 585
Figura 277 Cableado desordenado. 586
Figura 278 Identificación del cableado. 587
Figura 279 Identificación del cableado. 587
Figura 280 Identificación de cableado. 588
Figura 281 Identificación de cableado. 588
Figura 282 Identificación de cableado. 589

Figura 283 Identificación de cableado. 589
Figura 284 Parte de la Política (revisar anexo 2). 591
Figura 285 Capitulo V de la política (revisar anexo 2). 592
Figura 286 Política firmada por los empleados de la UTIC 593
Figura 287 Contenido de la política (revisar anexo 2). 594
Figura 288 Capitulo V de la política (revisar anexo 2). 595
Figura 289 Contenido de la política (revisar anexo 2). 596
Figura 290 Artículo 15 de la política (revisar anexo 2). 596
Figura 291 Política firmada por los empleados de la UTIC. 597
Figura 292 Compromiso firmado de implementación de recomendaciones de auditoría interna. 598
Figura 293 Acceso al inventario desde la herramienta 'Ejecutar'. 599
Figura 294 Carpetas en red donde se encuentra el inventario. 600
Figura 295 Inventario de la UTIC en hojas de cálculo. 600
Figura 296 Lista de programas a instalar para la implementación del Sistema de Inventario. 601
Figura 297 Instalación del JDK para NetBeans. 602
Figura 298 Instalación del JDK para NetBeans. 602
Figura 299 Instalación del lenguaje de programación Apache NetBeans. 603
Figura 300 Instalación del JDK para NetBeans. 603
Figura 301 Instalación del Gestor de Base de Datos SQL Server. 604
Figura 302 Instalación del Gestor de Base de Datos SQL Server. 604
Figura 303 Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC. 605
Figura 304 Interfaz Principal del Sistema de Inventario. 606
Figura 305 Interfaz de Registro de Empleados. 607
Figura 306 Interfaz de Cargos de los Empleados. 607
Figura 307 Interfaz de Registro de Entradas. 608
Figura 308 Interfaz de Registro de Productos. 608
Figura 309 Interfaz de las Marcas manejadas de la UTIC. 609

Figura 310 Interfaz de Registro de Salidas. 609
Figura 311 Interfaz de Consulta de las Entradas del Inventario. 610
Figura 312 Interfaz de Consulta de las Salidas del Inventario. 610
Figura 313 Interfaz del llenado del Vale de Salida. 611
Figura 314 Mensaje de Advertencia si no se llena el Vale de Salida. 611
Figura 315 Vista preliminar de impresión del inventario total de la partida que se seleccione 612
Figura 316 Inventario de la UTIC en hojas de cálculo 613
Figura 317 Consulta directa en la Base de Datos 614
Figura 318 Carpetas en red donde se encuentra el inventario. 616
Figura 319 Inventario de la UTIC en hojas de cálculo 616
Figura 320 Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC 617
Figura 321 Inventario de la UTIC en hojas de cálculo 618
Figura 322 Interfaz Principal del Sistema de Inventario) 619
Figura 323 Tablas de la base de datos. 619
Figura 324 Tablas de la base de datos. 620
Figura 325 Tablas de la base de datos 620
Figura 326 Tablas de la base de datos. 621
Figura 327 Interfaz de Consulta de las Entradas del Inventario 623

Índice de Tablas

Tabla 1. Estado de Arte 13
Tabla 2. Marco Metodológico. 18
Tabla 3. Cuadro de Normas y Estándares a Utilizar. 24
Tabla 4. Personal de la UTIC con su respectivo Cargo y Privilegio. 36
Tabla 5. Plan de Trabajo de la Auditoría Informática del H. Ayuntamiento de Tultitlán. ... 38
Tabla 6. Maquetado del FODA. 42
Tabla 7. Matriz de Riesgos. 55
Tabla 8. Catálogo de Riesgos. 56
Tabla 9. Análisis de Riesgos. 56
Tabla 10. Análisis de Amenazas. 56
Tabla 11. Análisis de Riesgos Enfocada a Vulnerabilidades. 57
Tabla 12. Formato de Pruebas. 58
Tabla 13. Cuestionario de Seguridad Física. 60
Tabla 14. Cuestionario de Seguridad Lógica. 64
Tabla 15. Cuestionario de Servicios. 69
Tabla 16. Cuestionario de Infraestructura. 75
Tabla 17. Cuestionario del Sistema de Inventario. 81
Tabla 18. FODA general de la UTIC. 85
Tabla 19. FODA de Seguridad Física. 87
Tabla 20. FODA de Seguridad Lógica. 90
Tabla 21. FODA de Servicios 93
Tabla 22. FODA de Infraestructura. 97
Tabla 23. FODA del Sistema de Inventario. 103
Tabla 24. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Seguridad Física. ... 107
Tabla 25. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Seguridad Lógica. .. 118
Tabla 26. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Servicios. 125
Tabla 27. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Infraestructura. 136

Tabla 28. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Inventario. 158
Tabla 29. Catálogo de Clasificación de atención de Seguridad Física. 172
Tabla 30. Catálogo de Clasificación de atención de Seguridad Lógica. 180
Tabla 31. Catálogo de Clasificación de atención de Servicios. 188
Tabla 32. Catálogo de Clasificación de atención de Infraestructura. 197
Tabla 33. Prueba 1 de Seguridad Física. 219
Tabla 34. Prueba 2 de Seguridad Física. 227
Tabla 35. Prueba 3 de Seguridad Física. 230
Tabla 36. Prueba 4 de Seguridad Física. 236
Tabla 37. Prueba 5 de Seguridad Física. 241
Tabla 38. Prueba 1 de Seguridad Lógica. 245
Tabla 39. Prueba 2 de Seguridad Lógica. 254
Tabla 40. Prueba 3 de Seguridad Lógica. 259
Tabla 41. Prueba 4 de Seguridad Lógica. 263
Tabla 42. Prueba 5 de Seguridad Lógica. 268
Tabla 43. Prueba 6 de Seguridad Lógica. 272
Tabla 44. Prueba 7 de Seguridad Lógica. 277
Tabla 45. Prueba 1 de Servicios. 281
Tabla 46. Prueba 2 de Servicios. 293
Tabla 47 Prueba 3 de Servicios. 303
Tabla 48. Prueba 4 de Servicios. 321
Tabla 49. Prueba 5 de Servicios. 328
Tabla 50 Prueba 6 de Servicios. 334
Tabla 51 Prueba 1 de Infraestructura. 342
Tabla 52. Prueba 2 de Infraestructura. 349
Tabla 53. Prueba 3 de Infraestructura. 354
Tabla 54. Prueba 4 de Infraestructura. 359
Tabla 55. Prueba 5 de Infraestructura. 368
Tabla 56. Prueba 6 de infraestructura. 373

Tabla 57. Prueba 7 de infraestructura. 377
Tabla 58. Prueba 8 de infraestructura. 381
Tabla 59. Prueba 9 de infraestructura. 387
Tabla 60. Prueba 10 de Infraestructura. 392
Tabla 61. Prueba 11 de Infraestructura. 399
Tabla 62. Prueba 12 de Infraestructura. 403
Tabla 63. Prueba 13 de Infraestructura. 407
Tabla 64. Prueba 14 de Infraestructura. 411
Tabla 65. Prueba 15 de Infraestructura. 415
Tabla 66. Prueba 1 del Sistema de Inventario..... 419
Tabla 67. Prueba 2 del Sistema de Inventario. 425
Tabla 68. Prueba 3 del Sistema de Inventario. 429
Tabla 69. Prueba 4 del Sistema de Inventario. 435
Tabla 70. Prueba 5 del Sistema de Inventario. 439
Tabla 71. Prueba 6 del Sistema de Inventario. 444
Tabla 72. Prueba 7 del Sistema de Inventario. 447
Tabla 73. Prueba 8 del Sistema de Inventario. 451
Tabla 74. Prueba 9 del Sistema de Inventario. 457
Tabla 75. Prueba 10 del Sistema de Inventario. 463
Tabla 76. Prueba 11 del Sistema de Inventario. 470
Tabla 77 Competencias Desarrolladas. 625
Tabla 78. Anexo 1. Cronograma de Reuniones. 648

CAPÍTULO I
GENERALIDADES DEL PROYECTO

1.1 INTRODUCCIÓN

El desarrollo de esta Auditoría es principalmente enfocado a revisar los procedimientos que utilizan dentro de la dependencia y que han sido utilizados durante un largo periodo de tiempo, para encontrar posibles errores o deficiencias e implementar respectivamente mejoras o correcciones que maximicen el desarrollo de sus actividades.

Para esto es necesario comprender la naturaleza, las operaciones, las actividades y la estructura en sí de la dependencia ya que estos puntos proporcionan un contexto sobre la función de esta, los productos y los servicios que ofrece, además del desempeño del personal.

Una vez identificado lo anterior se comienza con la planeación de dicha Auditoría, tomando en cuenta todas las herramientas y técnicas con las que se disponen y la forma de trabajo del lugar, permitiendo así organizar tiempos, actividades, diseñar y desarrollar los recursos necesarios que se necesitaron a lo largo del proceso de esta auditoría.

A partir de este momento y en adelante la dependencia donde se realizó esta Auditoría llamada Unidad de Tecnologías de la Información y Comunicación dentro del H. Ayuntamiento de Tultitlán se le conocerá con el nombre de UTIC, el cual serán las siglas correspondientes o abreviación del nombre inicial.

Conocida la forma de trabajo y el espacio por auditar, se comenzó a evaluar distintos puntos que se consideran críticos y que abordan a su vez temas de formas específicas, dichos puntos son: Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y Sistema de Inventario. Para ello fue necesario recabar información sobre la forma en que desempeñan sus actividades, existencia de procesos, activos, información relevante ya que con esto se pudo analizar en qué situación estaban al inicio del proceso de auditoría.

Seguido de esto fue crucial identificar 4 puntos esenciales de cada uno de los apartados mencionados (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y Sistema de Inventario.), los cuales consistían en sus Fortalezas,

Debilidades, Amenazas y Oportunidades, respectivamente ya que al tener esta información se pudieron detectar las vulnerabilidades que requerían ser atendidas y un enfoque de las mejoras que se podrían implementar en su momento. Realizados cada uno de los análisis FODA y ubicadas todas las debilidades se dio paso a desarrollar un análisis de riesgos el cual consistió en identificar todos los posibles riesgos de acuerdo a cada uno de los puntos inspeccionados y tomando como base las debilidades y amenazas de cada uno de los FODAS dando como resultado un catálogo donde se especifica los posibles escenarios y su respectivos factores, además se evaluaron los puntos conforme a las opiniones de los empleados usando una métrica entre probabilidad e impacto, y con ello priorizar las vulnerabilidades acuerdo a su clasificación de atención.

Como parte del proceso de la Auditoría es indispensable poner a prueba los procedimientos, equipos y medidas de prevención con los que cuentan para la seguridad de la información, de los activos y el personal, es por ello que se adecuaron una serie de pruebas que con ayuda de una métrica se pudo obtener la condición en la que se encontraban los temas puestos a prueba evidenciando dichas situaciones a partir de la identificación de la condición se pudo localizar normas o estándares que regulan dichos aspectos negativos encontrados y en base a ello se dio una recomendación para atender la(s) necesidad(es) que en su defecto en caso de ser implementadas se garantiza un mejor rendimiento en todos los procesos desarrollados en la UTIC.

Por último, se entrega un informe ejecutivo que contiene la extracción de los puntos atendidos (vulnerabilidades) y los posibles riesgos que existen, su nivel de atención y las recomendaciones específicas por cada una de las pruebas realizadas, y se muestra en el apartado de resultado como se implementaron dentro de la dependencia distintas estrategias diseñadas para la resolución de diversas problemáticas.

1.2 DESCRIPCIÓN DE LA EMPRESA

1.2.1 Nombre, razón social

H. Ayuntamiento de Tultitlán

1.2.2 Ubicación

Av. San Antonio 22, San Bartolo, 54900 Tultitlán de Mariano Escobedo, Estado de México.



Figura 1. Ubicación del H. Ayuntamiento de Tultitlán. Fuente: Google Maps. (Maps, 2023)

1.2.3 Organigrama



Figura 2. Organigrama del Palacio Municipal. Fuente: Dirección del H. Ayuntamiento de Tultitlán. (Tultitlán, 2023)

1.2.4 Sector productivo de la empresa

Pertenece al Sector Terciario porque se enfoca a satisfacer a las necesidades operativas, comerciales o de cualquier naturaleza de la ciudadanía o industria.

1.2.5 Misión, Visión, Filosofía y/o Valores

1.2.5.1 Misión

Ser la Administración Pública Municipal que brinde continuidad al proceso de transformación de Tultitlán, que posibilite impulsar el bienestar social para las y los habitantes, por medio de servicios públicos oportunos y de calidad, que consoliden el desarrollo general del municipio, con el fin de mejorar la calidad de vida de las y los tultitlenses.

1.2.5.2 Visión

Hacer del gobierno municipal de Tultitlán, el régimen de la consolidación transformativa, bajo un mandato garante del respeto a la Ley y los Derechos Humanos de todas y todos, tutelados en los principios de austeridad, eficacia y eficiencia, promotor de políticas públicas innovadoras en materia de servicios públicos, de rehabilitación y mejora de la infraestructura urbana, preservando y protegiendo el medio ambiente, además de recuperar espacios públicos que permita recobrar la paz y seguridad de las y los habitantes e impulsar su bienestar.

1.2.5.3 Valores

Dentro del Ayuntamiento de Tultitlán se emplean distintos valores los cuales a través de sus actividades se encargan de transmitirlos a la sociedad para tener un impacto positivo en su comunidad, entre ellos están: respeto, compromiso, profesionalismo, responsabilidad confianza y equidad, todos dirigidos a cada uno de los integrantes de su comunidad y visitantes.

1.2.6 Breve historia de la empresa

Tultitlán es un municipio ubicado en el Estado de México, México, con una rica historia que se remonta a la época prehispánica. A continuación, se proporciona una breve reseña de la historia del Ayuntamiento de Tultitlán:

Época Prehispánica: Antes de la llegada de los españoles, la región que hoy comprende Tultitlán estaba habitada por grupos indígenas, principalmente otomíes y mazahuas. La zona era conocida como Tultitlán, que en náhuatl significa "entre las cañas".

Conquista y Colonia: Tras la conquista de México por los españoles en el siglo XVI, la región de Tultitlán se incorporó al sistema de encomiendas y fue evangelizada por misioneros. Durante la colonia, la agricultura y la ganadería fueron actividades económicas importantes.

Siglo XIX: Durante la época de la independencia de México y la posterior Guerra de Reforma, Tultitlán fue escenario de diversos eventos históricos. El 11 de enero de 1861, Benito Juárez emitió el Decreto de Nacionalización de los Bienes Eclesiásticos, que tuvo un impacto significativo en la región.

Siglo XX: En el siglo XX, Tultitlán experimentó un crecimiento demográfico y económico considerable debido a su proximidad a la Ciudad de México. Se desarrolló como un municipio industrial y residencial.

Siglo XXI: Tultitlán sigue siendo un municipio importante en el Estado de México y forma parte de la Zona Metropolitana del Valle de México. A lo largo de los años, ha experimentado un crecimiento urbano y una expansión industrial significativos.

La historia del Ayuntamiento de Tultitlán está intrínsecamente ligada a la evolución de la región a lo largo de los siglos. A medida que la población y la economía han cambiado, también lo han hecho las prioridades y los desafíos que enfrenta el gobierno local.

1.3 PROBLEMA A RESOLVER

En el H. Ayuntamiento de Tultitlán, quien se dedica al sector terciario, donde abarca una amplia gama de actividades que van desde el comercio hasta la administración, pasando por el transporte y las comunicaciones. Al pasar de los años los avances tecnológicos también formaron parte del crecimiento del municipio y con ello se conlleva a que las Tecnologías de la Información (TI) se integren con todo el personal que labora en las distintas áreas del palacio municipal.

Es por esto, por lo que las TI son fundamentales en todas las áreas y sobre todo que se haga un correcto uso acorde a sus políticas, normas y/o estándares tanto nacionales como internacionales. Tal es el caso de la Unidad del Tecnologías de la Información y Comunicaciones (UTIC) que busca gestionar con eficacia los recursos tecnológicos y de comunicación para apoyar y mejorar los procesos y servicios de la institución, realizando actividades como soporte a los equipos de cómputo de otras unidades y la gestión de activos del mismo departamento hacia otros; actualmente dar soporte a otros equipos que no están dentro del área resulta difícil, cuando son reportes internos, los cuales se concentran en asistir al área/departamento que solicita la intervención, se piden detalles sobre la situación verbalmente y en caso de ser necesario se procede a retirar el quipo y trasladarlo a la UTIC para una mejor revisión y no afectar el rendimiento de los empleados dentro de dicho departamento, una vez realizado el servicio o resuelta la problemática que se haya surgido, se regresa el equipo a la instancia original, se instala y se dan recomendaciones por parte de los ingenieros que dieron soporte.

El caso anterior tiene puntos negativos o bien etapas que no se desarrollan de manera correcta, iniciando por la visita al área/departamento donde se solicita el soporte, ya que no se levanta una bitácora o un reporte escrito sobre lo sucedido o la problemática que presenta el equipo, al ser verbal esto ocasiona que durante el trayecto de la reparación datos o información específica sobre el comportamiento actual o la problemática que se está atendiendo sean olvidados y no se resuelva correctamente o por completo, dando así entrada a nuevas fallas o continuar con las fallas reportadas, otro punto en desventaja es el traslado del equipo desde el área o departamento solicitante hasta la UTIC para su mantenimiento, pueden suceder accidentes, en donde puede haber daños físicos hasta la pérdida total del equipo en el que el causante del accidente no intencional se deslinda de

toda responsabilidad al no contar con un oficio que responsabilice cualquier daño durante el traslado de este.

Otra de las debilidades de la UTIC es en la gestión de activos ya que no se cuenta con un sistema específico para el control de estos, pues actualmente se tienen unas hojas de cálculo realizando la función de un gestor de base de datos, que a su vez está dividido en varios archivos clasificados por categorías de activos, esto trae como consecuencia que no puedan acceder varios usuarios a la información actualizada en tiempo real, que la base de datos sea más propensa a volverse lenta y a dañarse conforme crezca la misma, sin mencionar que no se tiene un control sobre los usuarios que acceden, así como no se tienen ningún nivel de seguridad que la proteja de alguna manipulación.

Por otro lado, en el caso de los servicios con los que cuenta la UTIC hay algunas irregularidades, entre ellas el aire acondicionado, prevención de incendios, servicio médico, conexión eléctrica.

Es por ello por lo que se requiere una solución que permita conocer con detalle cada una de estas situaciones y pueda mejorar el contexto actual de los procesos y la TI dentro de la UTIC.

1.4 OBJETIVOS

1.4.1 Objetivo general

Realizar una Auditoría con Normas ISO de la familia 27000 y otros estándares para los procesos internos del H. Ayuntamiento de Tultitlán.

1.4.2 Objetivos específicos

1) Planificar la auditoría mediante el análisis del entorno, la definición de objetivos y alcances, y la creación de herramientas y formatos necesarios para garantizar un proceso estructurado y comunicado.
2) Ejecutar la auditoría mediante la aplicación de cuestionarios, análisis FODA, inspección de infraestructura, evaluación de servicios, medidas de seguridad y estado de activos, garantizando un diagnóstico integral de la UTIC.
3) Entregar los resultados de la auditoría mediante un informe final que sintetice los hallazgos, incluya recomendaciones basadas en estándares y norme su implementación.

1.5 JUSTIFICACIÓN

Las TI en la Unidad de Tecnologías de la Información y Comunicaciones desempeñan un rol primordial para optimizar los procesos y servicios gubernamentales, garantizar la disponibilidad de información vital para los ciudadanos y empleados municipales, y salvaguardar la seguridad de los datos confidenciales. Sin embargo, la carencia de sistemas efectivos para la gestión de activos, la falta de un registro documentado para dar soporte y soluciones están afectando negativamente la eficiencia operativa y la calidad de los servicios prestados, además de documentos oficiales que asignen un nivel de responsabilidad a los que trasladan dichos equipos de soporte.

Es indispensable destacar que la transparencia y la responsabilidad gubernamental son valores fundamentales en la gestión pública, y una vez implementada la documentación adecuada y el seguimiento de incidentes de TI pueden evitar o bien minimizar el impacto de daño de estos procesos. Además, la implementación de un protocolo formal para el traslado de equipos de TI puede minimizar grandes pérdidas, o bien lo que pueden ser riesgos financieros y operativos significativos para la institución.

En este contexto, se busca abordar estas deficiencias críticas en la gestión de TI mediante la implementación de sistemas de gestión de activos y protocolos de registro de incidentes y traslado de equipos. Esto no solo mejorará la eficiencia operativa y la calidad de los servicios, sino que también garantizará la seguridad de datos, promoverá la transparencia y responsabilidad institucional, y optimizará la asignación de recursos. En última instancia, estas mejoras que bien serán características resultantes de una Auditoría desarrollada correctamente contribuirán a un gobierno municipal más eficiente y confiable, en línea con las expectativas y necesidades de los ciudadanos y empleados municipales.

Recordando que el carácter de una Auditoría es totalmente preventivo por lo que, si bien no se buscará eliminar totalmente los riesgos que pueden existir dentro de estos procesos/actividades, se enfocara en tratar de evitar estas debilidades o bien disminuir el nivel de impacto que tendrían dentro del espacio de trabajo.

CAPÍTULO II
MARCO TEÓRICO

2.1 Marco Teórico

El Marco teórico es el resultado de los dos primeros pasos de una investigación (la idea y planteamiento del problema), ya que una vez que se tiene claro que se va a investigar, es el “manos a la obra” de la investigación. Consiste en analizar y presentar las teorías que existen sobre el problema a investigar, dentro de ello se tendrá el Estado de Arte que incluye trabajos e investigaciones que existen y algunos antecedentes de los últimos años sobre lo que se va a desarrollar como investigación con el detalle de que sea en un periodo de tiempo no muy lejano a la fecha. Asimismo dentro del marco conceptual que básicamente es la justificación de por qué debe realizarse el estudio mencionado, también describe el estado de los conocimientos conocidos, normalmente a través de una revisión bibliográfica; identifica las lagunas en nuestra comprensión de un fenómeno o problema. Por último, se mencionará la descripción de los pasos, etapas, fases, y actividades que se llevarán a cabo para solucionar el problema mencionado, de acuerdo con el tipo de investigación que se asume en el momento en que se inicia la identificación del problema, todo esto dentro del Marco Metodológico. El siguiente marco teórico se refiere a todas las fuentes de consulta teórica de que se puede disponer sobre el problema a resolver.

2.2 Estado de Arte

La siguiente tabla presenta una serie de investigaciones que tratan de mostrar el panorama de resolución de diversas auditorías, a fin de tener un contexto histórico de las posibles aplicaciones y resoluciones en el tiempo, además de conocer las técnicas y herramientas usadas.

Tabla 1. Estado de Arte. Fuente: Elaboración propia.

Fuente	Titulo	Estrategias/Técnicas	Resultados Obtenidos
Ramírez, 2015	Plan de Auditoría Informática para el Departamento de Sistemas Informáticos en el Municipio del Cantón Ventanas	Se opta por una investigación a fondo sobre el tema de una Auditoría enfocada a los sistemas información, realización de encuestas, checklist y el uso de la Norma 27001 para la seguridad de los sistemas de Información	Se concluye que no cuentan con normas ni regulaciones para el departamento de sistemas, falta de implementación de sistemas de seguridad (servicio de vigilancia, cámaras, alarmas etc.), No se reciben capacitaciones ni seminarios para la mejora de procesos sobre la seguridad de los sistemas de información, los administradores no cuentan con controles generales (manual de equipos informáticos) y operativos de software (manual del sistema o de usuario)

Tabla 1 (continuación)

Márquez, 2021	Informe final Auditoría de Cumplimiento para el Fideicomiso Museo de la Ciudad del Ayuntamiento de León	Principalmente el análisis de rubros sobre los procesos de control internos, además de encuestas para obtener resultados plasmados en graficas de barra, por último, la observación e inspección de los sistemas de información	El Fideicomiso Museo de la Ciudad no cuenta con un programa de comunicación, Figura y difusión. No cuentan con un expediente de auditorías sin embargo la evidencia contenida no es suficiente para acreditar el seguimiento a las observaciones y recomendaciones emitidas por los órganos fiscalizadores y de control interno y externos de la Entidad. Cuentan con un inventario que no se mantiene actualizado en los números de los bienes muebles e inmuebles.

De estas investigaciones se puede observar el punto en común que las relaciona, en este caso es la falta de normativas o regulaciones que estén a cargo de los sistemas de información y de los servicios, así como los activos de TI.

2.3 Marco Conceptual

A continuación, se presentan algunos temas y conceptos que ayudaran a entender mejor este trabajo, ya que existe relación entre algunos y facilita si comprensión para el lector, por supuesto no dejando atrás el hecho de ser un apartado específico para mostrar información relevante para la interpretación total del trabajo.

En el contexto de una **Auditoría** se abordan diversos conceptos fundamentales, principalmente la definición de auditoría que habla sobre ser un proceso sistemático y objetivo de evaluar la evidencia obtenida de eventos o sucesos, asimismo en este caso al tocar temas de una **Auditoría informática** ya que se determina si el sistema que está en uso actualmente dentro del departamento de la UTIC es Integro y eficaz además de eficiente y cumple con las leyes y regulaciones que debería tener se estarán realizando actividades correspondientes a las responsabilidades que tiene un **auditor informático** ya que se estará evaluando la integridad, confidencialidad y disponibilidad de los datos así como los sistemas de dicha organización. (ibaiscanbit.com, 2022)

La **seguridad** se vuelve fundamental si hablamos de un sistema de información o bien como tal un departamento en general, ya que si se habla se seguridad se dice que es todo aquello que no corre riesgos ni amenazas y que está libre de vulnerabilidades, pero es de saberse que nada está completamente seguro en su totalidad (Pérez Porto & Gardey, Definición.de, 2021), por eso la **seguridad física** (Vélez Martínez, s.f.) es el primer paso a revisar si hablamos del entorno en el que se desarrollan las actividades, asegurar que sea óptimo para los equipos de cómputo en particular, mencionando estos equipos de cómputo se tienen todos los componentes físicos de un sistema informático, mejor conocidos como **hardware** (Desconocido, Universidad Europea, 2021), así como en la **seguridad lógica** contar con opciones de protección eficaces para mantener la información de los equipos a salvo, que a su vez todos los programas, aplicaciones y sistemas operativos que se ejecutan y proporcionan instrucciones para el hardware (Segura Martínez, 2012) son conocidos como **software** (Pérez Porto & Gardey, Definicion.de, 2024), de igual manera se debe

inspeccionar la parte de las instalaciones, servicios y medios técnicos que se vean implicados en el desarrollo de las actividades interinas refiriéndose a la **infraestructura** (Equipo editorial, Concepto.de, 2020).

Cabe mencionar que en este contexto es fundamental comprender lo que son las **tecnologías de la información** , ya que son las que se encargan de gestionar la información, incluyendo hardware, software, redes, sistemas de comunicación y los procedimientos para recopilar, procesar y distribuirla, estos aspectos son fundamentales (ISEC, 2022) si hablamos de un **sistema de información** ya que es el encargado de recibir directrices por parte de los trabajadores para ejecutarlas y optimiza diversas actividades dentro de una institución.

Generalmente una Auditoría se divide en dos ámbitos, **auditoría externa** la cual se encarga de evaluar la veracidad y el control de los activos, funciones y desempeño de una organización y entidad proviniendo de afuera (UCSP, s.f.), es decir un auditor externos a la institución, mientras que la **auditoría interna** se encarga de lo mismo, pero a través de empleados provenientes de la misma empresa es decir internos, por este motivo en este caso la Auditoría que se está realizando es externa, y del mismo modo se buscara encontrar áreas de mejora y brindar recomendaciones que cumplan con algunas **normas y estándares** (Desconocido, idc Online, 2021) oficiales entre ellas ISO 27002 para un sistema de gestión de activos, COBIT para gestionar y controlar los sistemas de información de manera efectiva todo esto mediante la aplicación de **procesos** los cuales son un conjunto de actividades que toman información y la procesan arrojando resultados, así mismo también se ejecutaran **pruebas** en los sistemas, servicios e infraestructura ya que estas son esencialmente implementadas y puestas en práctica para la obtención de defectos, que bien pueden ser mediante la **inspección** que consiste en identificar vulnerabilidades o posibles riesgos a simple vista (Pérez Porto & Merino, Definición.de, 2021), ya que el contar con una **vulnerabilidad** básicamente es una debilidad o fallo en un sistema que puede ser explotado por una amenaza para causar daño, pérdida o interrupción en una organización, a su vez un **riesgo** es la probabilidad de que ocurra un evento no deseado.

Todo esto es parte fundamental para poder llegar a la evaluación del **control interno**, el cual se basa en identificar, analizar y diagnosticar la utilidad de los procesos, políticas y procedimientos diseñados para salvaguardar los activos de una organización, garantizar la precisión y confiabilidad de la información que promueve la eficiencia operativa y el cumplimiento de las leyes.

Es indispensable abordar herramientas que brinden la identificación de información clave, como el análisis **FODA** el cual se encarga de identificar las **fortalezas** dentro de una organización las cuales se concentran en los puntos positivos y fuertes que contiene la misma internamente, de la misma forma las **debilidades** que es básicamente lo contrario es decir la deficiencias que tiene la empresa en general, por otro lado logra identificar las **oportunidades** o áreas de mejora en las que podría haber cambios dentro de la institución siempre y cuando sea del ámbito externo, y por ultimo las **amenazas** que son todos aquellos riesgos de índole natural o humano que puedan afectar directamente a la empresa.

El **plan de auditoría** se elabora con el propósito de obtener información objetiva sobre el sistema, los procesos y los controles de una organización. Este plan se compara con las normas y estándares establecidos, para determinar si se cumplen los requisitos y para identificar posibles áreas de mejora o incumplimientos (Gabarró Sust, s.f.) esto con ayuda de un **análisis** profundo el cual se realiza para comprender los fundamentos y las causas que pueden afectar la integridad de la información y la disponibilidad de los sistemas. Esto implica investigar y examinar detenidamente los factores que pueden influir en la confiabilidad y la precisión de los datos (Martínez, 2023), recordando que la **confidencialidad** es un aspecto crítico en una auditoría, ya que implica la protección de la información sensible y restringe su acceso a personas no autorizadas. Esto se logra mediante la implementación de controles de seguridad y la aplicación de políticas de acceso y divulgación de información (Ávila Funes, 2013), así como tener acceso a los datos y aplicaciones cuando sea requerido a lo cual se le llama **disponibilidad** (IBM, 2021), y garantizar la confiabilidad de la información evitando que haya manipulación o alteración de esta como lo marca la **integridad** (Acronis, s.f.)**.**

Por último, **la gestión de activos** es un proceso que evalúa el valor y el rendimiento de los recursos de una organización (valuekeep, s.f.). Esto implica identificar oportunidades, evaluar riesgos y establecer prioridades en cuanto al uso y mantenimiento de los activos. La gestión eficiente de los activos contribuye a optimizar el desempeño y la rentabilidad de la organización.

2.4 Marco Metodológico

La siguiente tabla es la descripción de las actividades, técnicas, herramientas y los posibles resultados o bien lo que se espera lograr, que se lleva a cabo para solucionar el problema abordado, con la intención de brindar una mayor visión del cómo se desarrolla este proyecto.

Tabla 2. Marco Metodológico. Fuente: Elaboración propia.

Cuadro Metodológico				
N°	Actividades	Técnicas	Herramientas	Resultados Esperados
1.1	Conocer el Entorno General de la dependencia	-Investigación -Observación	-Libros, sitios oficiales.	Tener conocimiento del giro y las funciones que realiza
1.2	Conocer el entorno particular dentro de la dependencia	-Entrevista	-Preguntas sobre el entorno y procesos	Tener conocimiento de los procesos, personas y activos que lo componen.
1.3	Establecer objetivos y alcances	-Analizar el espacio a Auditar -Redacción de los objetivos y alcance	- Computadora, Editor de Texto	Conocer las metas a alcanzar y hasta donde llegara la investigación al final del proyecto
1.4	Generar un plan de Auditoría detallado, que incluya los objetivos, el cronograma y los recursos necesarios	- Analizando - Redactando - Planificación	Computadora, editores de texto, programas para planificar el cronograma	Una visualización de tiempos y actividades de todo el transcurso del proyecto

Tabla 2 (continuación)

1.5	Comunicar el plan de Auditoría al responsable del área de la unidad de tecnologías de la información y comunicación	- Comunicación verbal o escrita	Correo electrónico, junta presencial	Obtener la aprobación del responsable de la UTIC
1.6	Realizar formatos para la recopilación de información	- Diseñar - Estructurar	Gestores de texto	Obtener los formatos para plasmar y recopilar la información que se obtenga
1.6.1	Generar formato para la obtención de Fortalezas, Oportunidades, Debilidades y Amenazas de la UTIC (FODA).	- Diseñar - -Estructurar	Gestores de texto	Obtener los formatos para plasmar y recopilar la información que se obtenga
1.6.2	Generar los cuestionarios	- Diseñar - -Estructurar	Gestores de texto	Obtener los formatos para plasmar y recopilar la información que se obtenga
1.6.3	Generar Formato para el análisis de riesgos.	- Diseñar - Estructurar	Gestores de texto	Obtener los formatos para plasmar y recopilar la información que se obtenga
2.1	Aplicar los cuestionarios	-Entrevistas	Cuestionarios, computadora, dispositivo móvil, papel.	Obtener información sobre la dependencia, sobre los activos y servicios que manejan

Tabla 2 (continuación)

2.2	Realizar los análisis FODA	-Análisis -Observación - Investigación	Computadora, documentos, cuestionarios.	Identificar los puntos clave para el área de mejora del entorno particular
2.3	Inspeccionar la Infraestructura de la Unidad (Inmobiliario, cableado, distribución).	-Inspección -Observación	Reunión física y presencial en el área,	Conocer el estado actual de la infraestructura del entorno particular
2.4	Evaluar el funcionamiento de los servicios	Inspección Observación Evaluación	Listas, métricas, reunión física, pruebas de campo	Conocer el estado del funcionamiento actual de los servicios que ofrece el entorno particular
2.4.1	Probar Servicios de Computación y comunicación (HW, Sw, Soporte).	Inspección Observación Evaluación	Listas, métricas, reunión física, pruebas de campo	Conocer el estado del funcionamiento actual de los servicios que ofrece el entorno particular
2.4.2	Evaluar servicios generales (calefacción, iluminación, energía y aire acondicionado).	Inspección Observación Evaluación	Listas, métricas, reunión física, pruebas de campo	Conocer el estado del funcionamiento actual de los servicios que ofrece el entorno particular
2.5	Evaluar las medidas de seguridad lógica	Inspección Observación Evaluación Pruebas de Seguridad	Pruebas de campo, aplicaciones de inspección	Las posibles vulnerabilidades o debilidades que tengan los equipos de cómputo.

Tabla 2 (continuación)

2.5.1	Consultar Privilegios de usuarios y sesiones	Inspección Observación	Computadoras	Conocer las distintas cuentas o usuarios y los roles con los que funcionan además de las restricciones que puedan tener.
2.5.2	Inspeccionar la instalación de aplicaciones.	Inspección Observación	Computadora, historial	Identificar los sitios de descarga, así como aplicaciones maliciosas
2.5.3	Consultar la existencia de licencias	Investigación, Inspección Observación	Computadora, programas instalados y en uso	Saber si los programas son legítimos o son versiones desactualizadas o simplemente piratas
2.5.4	Examinar el uso y/o tipos de software	Inspección Observación	Computadora, programas instalados y en uso	Conocer si el sistema operativo que usan es adecuado a sus necesidades
2.5.5	Realizar un análisis en busca de malware.	Análisis	Computadora, antivirus	Identificar algún tipo de malware dentro de los equipos en uso.
2.6	Conocer las medidas de seguridad física	Observación Consulta	Accesos físicos, políticas o reglamentos que posean	Saber si cuentan con algunas medidas de seguridad y que tan eficaces son al momento de resguardar la seguridad física de los equipos

Tabla 2 (continuación)

2.6.1	Examinar el estado físico de los activos tales como computadoras, Routers y switches.	Observación Consulta	Computadoras, routers, switches	Conocer el estado físico actual de los componentes mencionados
2.6.2	Examinar los diferentes accesos a la UTIC	Observación Análisis Evaluación	Puertas, ventanas, candados, cerraduras	Saber si los accesos son seguros y protegen los activos del entorno particular
2.7	Poner a prueba las medidas de seguridad física	Pruebas Análisis Observación	Pruebas de campo	Asegurarse que las medidas de seguridad física sean las adecuadas para la protección de los activos
2.8	Obtener las características de hardware de los activos	Análisis	Lista de verificación, computadoras, periféricos,	Conocer el estado actual físico de los activos
2.9	Evaluar en qué estado se encuentran los periféricos (monitores, teclados, ratones).	Análisis Inspección Evaluación	Lista de verificación, computadoras, periféricos,	Conocer el estado actual físico de los periféricos
3.1	Analizar y sintetizar los hallazgos de la Auditoría en un informe final	Análisis de datos Redacción Síntesis	Computadora, datos obtenidos, papel, informes	Observar y plasmar la información obtenida y más relevante en el informe final

Tabla 2 (continuación)

3.2	Generar Recomendaciones de acuerdo con los estándares y normas utilizados	Redacción Síntesis Comparación	Computadora, papel, gestores de texto, Estándares y Normas	Proponer soluciones para abordar los hallazgos y mejorar las áreas
3.3	Implementar las recomendaciones	Aplicar las soluciones de los hallazgos	Normas, estándares, informes anteriores, computadora	Mejorar los procesos y esperar que se lleven a cabo las recomendaciones

2.5 Estándar 27002

El siguiente cuadro muestra un resumen general de la norma que se utiliza dentro de la implementación del proyecto, además se incluye un breve resumen de los apartados que en particular serán empleados para las recomendaciones de esta auditoría.

Tabla 3. Cuadro de Normas y Estándares a Utilizar. Fuente: Elaboración propia.

Nombre: ISO/IEC 27002
Descripción: Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. **Uso:** <u>Política de Seguridad:</u> El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El documento de la política debiera contener enunciados relacionados con: a) una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información (ver introducción); b) un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales; c) un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;

Tabla 3 (continuación)

d) una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo: 1. conformidad con los requerimientos legislativos, reguladores y restrictivos, 2. educación, capacitación y conocimiento de seguridad, 3. gestión de la continuidad del negocio, 4. consecuencias de las violaciones de la política de seguridad de la información; e) una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información, f) referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar. Esta política de seguridad de la información se debiera comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector objetivo.
Lo que se espera: En caso de que la dependencia no cuente con políticas o normativas internas, se deberá seguir las regulaciones mencionadas para crear una Política de Seguridad que se enfoque y proteja el entorno particular, en caso de que ya se cuente con dichas normativas, se corroborara si cumple con los puntos mencionados.
Gestión de Activos: Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales. Todos los activos debieran ser inventariados y contar con un propietario nombrado. Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

Tabla 3 (continuación)

Uso: Una organización debiera identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado.
Lo que se espera: Evaluar el funcionamiento y control del sistema gestor de activos con el que se cuenta actualmente, verificando que cumpla con los puntos mencionados y sea adecuado para la realización de actividades dentro de la dependencia. Obteniendo así un diagnóstico que mencione las debilidades o puntos de mejora de dicho sistema.
Control de Acceso: Objetivo: Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad. Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información. Uso: • Las políticas para la divulgación y autorización de la información; por ejemplo, la necesidad de conocer el principio y los niveles de seguridad, y la clasificación de la información. • Los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización; • Segregación de roles del control del acceso; por ejemplo, solicitud de acceso, autorización de acceso, administración del acceso; • Requerimientos para la autorización formal de las solicitudes de acceso;
Lo que se espera: Analizar el control de acceso a la información y a los procesadores de esta de acuerdo con los puntos mencionados y verificar que se cuenten con cada uno de ellos, o bien buscar alternativas para su elaboración y puesta en práctica mejorando de esta manera la seguridad al querer tener acceso a la información.

Tabla 3 (continuación)

Seguridad Física: Objetivo áreas seguras: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia. Uso áreas seguras Controles de ingreso físico: Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado. Asegurar las oficinas, habitaciones y medios: Se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios. Protección contra amenazas externas e internas: Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre. Objetivo Equipo de Seguridad: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización. Se debiera proteger el equipo de amenazas físicas y ambientales. La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-autorizado a la información y proteger contra pérdida o daño. Esto también debiera considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

Tabla 3 (continuación)

Uso Equipo de Seguridad: Ubicación y protección del equipo: Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado. Seguridad del cableado: El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño. Mantenimiento de equipo: Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad. Seguridad del equipo fuera del local: Se debiera aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
Lo que se espera: Verificar que el espacio de trabajo este preparado para circunstancias físicas y ambientales externas o internas que pongan en peligro los sistemas de información, así como también analizar la seguridad física de los activos buscando puntos débiles o de mejora que eviten el mayor índice de impacto posible en caso de un accidente, todo esto de acuerdo con las normativas mencionadas.

CAPÍTULO III

DESARROLLO

A continuación, se presenta el listado de las actividades del proyecto en orden cronológico, mostrando el desarrollo de estas y sus resultados, dando consigo una visión más clara del desarrollo de la Auditoría paso a paso.

Un plan de auditoría es un documento detallado que establece el enfoque, el alcance, los objetivos y los procedimientos que se seguirán durante una auditoría. Es elaborado por el auditor o el equipo de auditoría antes de iniciar el proceso de auditoría y sirve como guía para llevar a cabo la evaluación de la información, los controles internos u otros aspectos de una organización o proceso, es importante dar a conocer el plan de Auditoría porque promueve la transparencia, la confianza y la colaboración entre el auditor y la organización, lo que contribuye a un proceso de auditoría más efectivo y significativo.

En este caso para establecer los objetivos y el alcance del proyecto se acudió a la dependencia Unidad de Tecnologías de la Información Comunicaciones en forma de reunión se propone el proyecto mostrando el plan de Auditoría establecido previamente para que los trabajadores y Jefes Inmediatos decidan si es favorable aceptarlo y ponerlo en marcha, por lo que en este caso se sugiere una Auditoría a los procesos internos del Ayuntamiento de Tultitlán, sin embargo los superiores mencionan que no es posible ya que son diversas áreas con las que cuentan y no todas brindaran acceso, por lo que se canalizó específicamente a una sola Unidad dentro del Ayuntamiento, la cual es la Unidad de Tecnologías de la Información y Comunicaciones (UTIC), una vez establecido el alcance se definieron los puntos que abarcara dicha Auditoría, (seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario) dentro de la UTIC, al final solo se ajustó dicho plan de Auditoría en base a la unidad asignada.

3.1 Primer Objetivo: Planificar Auditoría

3.1.1 Actividades

3.1.1.1 Actividad 1.1 Conocer el entorno general de la dependencia

3.1.1.1.1 Descripción de la actividad

Lo primero que se realiza para el desarrollo de esta actividad fue una investigación donde se ingresa al portal oficial del gobierno municipal de Tultitlán, consiguiendo datos relevantes como su propósito, objetivo y sus principios y creencias (misión, visión y valores) mejor conocidos como su identidad corporativa, además, se ha obtenido el croquis, ubicación y dirección de la dependencia. Otros datos adicionales que se han recabado son: la historia, para conocer la evolución de dicha gobernatura y su organización. A fin de complementar el conocimiento general y particular de la institución a evaluar se realiza una visita presencial a la institución para solicitar el organigrama de la dependencia, además de corroborar la información que se obtuvo de la indagación en internet y en su sitio oficial.

3.1.1.1.2 Resultado de la actividad

3.1.1.1.2.1 Nombre, razón social

Honorable Ayuntamiento de Tultitlán

3.1.1.1.2.2 Ubicación

Av. San Antonio 22, San Bartolo, 54900 Tultitlán de Mariano Escobedo, Méx.



Figura 3. Ubicación del H. Ayuntamiento de Tultitlán. Fuente Google Maps. (Maps, 2023)

3.1.1.1.2.3 Organigrama



Figura 4. Organigrama del Palacio Municipal. Fuente: Dirección del H. Ayuntamiento de Tultitlán. (Tultitlán, 2023)

3.1.1.1.2.4 Sector productivo de la empresa

Pertenece al Sector Terciario por que se enfoca a satisfacer a las necesidades operativas, comerciales o de cualquier naturaleza de la ciudadanía o industria

3.1.1.1.2.5 Misión, Visión, Filosofía y/o Valores

3.1.1.1.2.5.1 Misión

Ser la Administración Pública Municipal que brinde continuidad al proceso de transformación de Tultitlán, que posibilite impulsar el bienestar social para las y los habitantes, por medio de servicios públicos oportunos y de calidad, que consoliden el desarrollo general del municipio, con el fin de mejorar la calidad de vida de las y los tultitlenses.

3.1.1.1.2.5.2 Visión

Hacer del gobierno municipal de Tultitlán, el régimen de la consolidación transformativa, bajo un mandato garante del respeto a la Ley y los Derechos Humanos de todas y todos, tutelados en los principios de austeridad, eficacia y eficiencia, promotor de políticas públicas innovadoras en materia de servicios públicos, de rehabilitación y mejora de la infraestructura urbana, preservando y protegiendo el medio ambiente, además de recuperar espacios públicos que permita recobrar la paz y seguridad de las y los habitantes e impulsar su bienestar.

3.1.1.1.2.5.3 Valores

Dentro del Ayuntamiento de Tultitlán se emplean distintos valores los cuales a través de sus actividades se encargan de transmitirlos a la sociedad para tener un impacto positivo en su comunidad, entre ellos están: respeto, compromiso, profesionalismo, responsabilidad confianza y equidad, todos dirigidos a cada uno de los integrantes de su comunidad y visitantes.

3.1.1.1.2.5.4 Breve historia de la empresa.

Tultitlán es un municipio ubicado en el Estado de México, México, con una rica historia que se remonta a la época prehispánica. A continuación, se proporciona una breve reseña de la historia del Ayuntamiento de Tultitlán:

Época Prehispánica: Antes de la llegada de los españoles, la región que hoy comprende Tultitlán estaba habitada por grupos indígenas, principalmente otomíes y mazahuas. La zona era conocida como Tultitlán, que en náhuatl significa "entre las cañas".

Conquista y Colonia: Tras la conquista de México por los españoles en el siglo XVI, la región de Tultitlán se incorporó al sistema de encomiendas y fue evangelizada por misioneros. Durante la colonia, la agricultura y la ganadería fueron actividades económicas importantes.

Siglo XIX: Durante la época de la independencia de México y la posterior Guerra de Reforma, Tultitlán fue escenario de diversos eventos históricos. El 11 de enero de 1861,

Benito Juárez emitió el Decreto de Nacionalización de los Bienes Eclesiásticos, que tuvo un impacto significativo en la región.

Siglo XX: En el siglo XX, Tultitlán experimentó un crecimiento demográfico y económico considerable debido a su proximidad a la Ciudad de México. Se desarrolló como un municipio industrial y residencial.

Siglo XXI: Tultitlán sigue siendo un municipio importante en el Estado de México y forma parte de la Zona Metropolitana del Valle de México. A lo largo de los años, ha experimentado un crecimiento urbano y una expansión industrial significativos.

La historia del Ayuntamiento de Tultitlán está intrínsecamente ligada a la evolución de la región a lo largo de los siglos. A medida que la población y la economía han cambiado, también lo han hecho las prioridades y los desafíos que enfrenta el gobierno local.

3.1.1.2 Actividad 1.2 Conocer el entorno particular dentro de la dependencia

3.1.1.2.1 Descripción de la actividad

Una vez que se realiza la investigación digital, se visita la dependencia específicamente el departamento donde se aplica la Auditoría, ya que la información que se requiere conocer más información específica sobre el funcionamiento de éste. Es indispensable acudir de forma presencial para conocer la condición en la que se encuentra dicho departamento, además presentarse con el personal.

Con esta actividad, se conoce la ubicación particular del departamento dentro de la dependencia, la una visión general de su área de trabajo, los encargados y su equipo de trabajo, así como los roles de cada uno de ellos tienen; también, se identifica los activos de Tecnologías de Información (TI) con los que trabaja.

3.1.1.2.2 Resultado de la actividad



Figura 5 Ubicación Física de la Unidad de Tecnologías de la Información y Comunicación (UTIC). Fuente: Instalaciones de la UTIC en el Ayuntamiento de Tultitlán. (Tultitlán. I. d., 2023)



Figura 6. Acceso Principal al UTIC. Fuente: Elaboración propia. (propia., Acceso Principal a UTIC, 2023)

La siguiente tabla muestra el personal que compone la Unidad de Tecnologías de la Información y Comunicación (UTIC), y sus respectivos cargos y los privilegios con los que cuentan.

Tabla 4. Personal de la UTIC con su respectivo Cargo y Privilegio. Fuente. Ing. Jonathan Rodrigo Pérez Del Río.

NOMBRE	CARGO	CREDENCIALES O PRIVILEGIOS DE ACCESO
Marlene Méndez Estrada	AUXILIAR	CAPTURISTA Y CONSULTA
José Luis Maldonado Jiménez	CAPTURISTA	CAPTURISTA Y CONSULTA
José Ángel Hernández Tovar	CAPTURISTA	CAPTURISTA Y CONSULTA
Gerardo Hernández Cañas	AUXILIAR	CONSULTA
Jonathan Rodrigo Pérez Del Río	JEFE DE UNIDAD	ADMINISTRADOR
María Olga Mota de la Cruz	SECRETARÍA	CONSULTA

3.1.1.3 Actividad 1.3 Establecer objetivos y alcances

3.1.1.3.1 Descripción de la actividad

Una vez que se dispone de información general y específica del lugar a auditar, es fundamental definir con precisión las dimensiones de la evaluación y el diagnóstico, así como los elementos que serán objeto de auditoría. Por este motivo, se establece un objetivo general que señala la meta del proyecto, en este caso, la auditoría, junto con los objetivos específicos, los cuales representan las fases o submetas planificadas estratégicamente para abarcar la totalidad de la Auditoría.

Asimismo, se determina el alcance, indicando los límites de la auditoría, asegurando los puntos de enfoque y el entorno en el que se implementa el proyecto.

3.1.1.3.2 Resultado de la actividad

3.1.1.3.2.1 Objetivo general

Realizar una Auditoría con Normas ISO de la familia 27000 y otros estándares para los procesos internos del H. Ayuntamiento de Tultitlán.

3.1.1.3.2.2 Objetivos específicos

1) Planificar la Auditoría
2) Ejecutar la Auditoría
3) Entregar resultados

3.1.1.3.2.3 Alcance

Revisar las medidas de control interno de las Tecnologías de la Información que intervienen en la UTIC del H. Ayuntamiento de Tultitlán (seguridad física y lógica, servicios, infraestructura, inventario).

3.1.1.4 Actividad 1.4 Generar un plan de trabajo de la Auditoría detallado, como que incluya los objetivos, el cronograma y los recursos necesarios.

3.1.1.4.1 Descripción de la actividad

Se elabora un plan de trabajo para la Auditoría, considerando el período de tiempo disponible, que en este caso es de 4 meses. En dicho plan, se especifican las fechas de inicio y término, así como las actividades que se ejecutan para cada objetivo establecido. Adicionalmente, se genera un calendario de reuniones que define la periodicidad con la que se reúnen los involucrados, y se establece un acuerdo de confidencialidad que detalla las condiciones y el uso de la información relacionada con la dependencia involucrada en la Auditoría

3.1.1.4.2 Resultado de la actividad

La siguiente tabla muestra el plan de trabajo de la Auditoría presentado ante la dependencia y el cual especifica lo antes ya mencionado en la actividad 1.4

Tabla 5. Plan de Trabajo de la Auditoría Informática del H. Ayuntamiento de Tultitlán. Fuente: Elaboración propia.

PLAN DE TRABAJO DE LA AUDITORÍA EN INFORMÁTICA DEL H. AYUNTAMIENTO DE TULTITLÁN		
	FECHAS ESTIMADAS	
	INICIO: 02 de octubre de 2023	TÉRMINO: 02 de febrero de 2024
OBJETIVO GENERAL	Realizar una Auditoría con Normas ISO de la familia 27000 y otros estándares para los procesos internos del H. Ayuntamiento de Tultitlán	
OBJETIVOS ESPECÍFICOS	1.- Planificar la Auditoría 1.1. Conocer el entorno general de la dependencia 1.2. Conocer el entorno particular dentro de la dependencia 1.3. Establecer objetivos y alcances 1.4. Generar un Plan de Auditoría detallado, que incluya los objetivos, el cronograma y los recursos necesarios. 1.5. Comunicar el plan de Auditoría al responsable del área de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC) 1.6. Realizar formatos para la recopilación de información 1.6.1. Generar formato para la obtención de Fortalezas, Oportunidades, Debilidades y Amenazas de la UTIC (FODA) 1.6.2. Generar los cuestionarios 1.6.3. Generar formato para el análisis de riesgos	

Tabla 5 (continuación)

	2.- Ejecutar la Auditoría 2.1. Aplicar los cuestionarios 2.2. Realizar los análisis FODA 2.3. Inspeccionar la infraestructura de la Unidad (Inmobiliario, cableado, distribución. 2.4. Evaluar el funcionamiento de los servicios 2.4.1. Probar servicios de computación y comunicación (HW, SW, Soporte 2.4.2. Evaluar servicios generales (calefacción, iluminación, energía y aire acondicionado) 2.5. Evaluar las medidas de seguridad lógica 2.5.1. Consultar Privilegios de usuarios y sesiones 2.5.2. Inspeccionar la instalación de aplicaciones 2.5.3. Consultar la existencia de licencias 2.5.4. Examinar el uso y/o tipos de software 2.5.5. Realizar un análisis en busca de malware 2.6. Conocer las medidas de seguridad física 2.6.1. Examinar el estado físico de los activos tales como computadoras, Routers y Switches 2.6.2. Examinar los diferentes accesos a la UTIC 2.7. Poner a prueba las medidas de seguridad física 2.8. Obtener las características de hardware de los activos 2.9. Evaluar en qué estado se encuentran los periféricos (monitores, teclados, ratones) 3.- Entregar Resultados 3.1 Analizar y sintetizar los hallazgos de la auditoría en un informe final. 3.2 Generar recomendaciones de acuerdo con los estándares y normas utilizados 3.3 Implementar las recomendaciones

Tabla 5 (continuación)

ALCANCES	Revisar las medidas de control interno de las Tecnologías de la Información que intervienen en la UTIC del H. Ayuntamiento de Tultitlán (seguridad física y lógica, servicios, infraestructura, inventario).
MIEMBROS DEL EQUIPO AUDITOR Y PERSONAS INVOLUCRADAS	Cargo de los Involucrados: Jonathan Rodrigo Pérez Del Río (Jefe de la UTIC) Moran Diego Oscar Yahir (Auditor Externo) Santos Ramírez Ana Laura (Auditor Externo)
PROGRAMAR LAS REUNIONES CON EL DEPARTAMENTO	Revisar Anexo 1 sobre las “Reuniones” con cronograma de cada una de las reuniones programadas para el desarrollo de la Auditoría.
REQUERIMIENTOS DE CONFIDENCIALIDAD	Información Pública
DISTRIBUCIÓN DEL INFORME DE AUDITORÍA FECHA DE EMISIÓN	El informe final resultante de la Auditoría realizada para la Unidad de Tecnologías de la Información y Comunicación del H. Ayuntamiento de Tultitlán será entregado al Ingeniero Jonathan Rodrigo Pérez del Rio, Jefe de la UTIC, 02 de febrero del año 2024 a las 12:00 hrs en la Unidad de Tecnologías de la Información y Comunicación.

3.1.1.5 Actividad 1.5 Comunicar el plan de Auditoría al responsable del área de la Unidad de Tecnologías de la Información y Comunicación.

3.1.1.5.1 Descripción de la actividad

Se lleva a cabo una reunión en el ayuntamiento con el personal involucrado de la UTIC, donde se presenta el plan de trabajo, diseñado con el propósito de mostrar al jefe de la Unidad y a sus empleados la metodología de trabajo prevista para el desarrollo del proyecto. Este plan incluye aspectos clave como las fechas y el lugar de trabajo, indicando específicamente dónde se realizarán las actividades, los días y las horas que se dedicarán al desarrollo de la Auditoría. Además, se detallan las etapas en las que se divide el proyecto, cada una de ellas compuesta por actividades propuestas que contribuyen al cumplimiento de los objetivos previamente establecidos. De este modo, el equipo de la UTIC estará informado sobre las acciones a ejecutar, así como sobre las herramientas y técnicas que se requerirán a lo largo del proceso.

3.1.1.5.2 Resultado de la actividad

La forma de trabajo presentada en el plan se aprueba verbalmente el mismo día de la reunión previamente mencionada.

3.1.1.6 Actividad 1.6 Realizar formatos para la recopilación de la información.

Se diseñan diversos formatos con el fin de facilitar la recolección y comprensión de la información por parte de los lectores. Cada uno de estos formatos tiene como objetivo centralizar diferentes secciones de la información recolectada. De esta manera, los formatos funcionan de manera complementaria, permitiendo una interpretación más eficiente de los datos obtenidos una vez aplicados.

3.1.1.6.1 Actividad 1.6.1 Generar formato para la obtención de fortalezas, oportunidades, debilidades y amenazas de la UTIC (FODA).

3.1.1.6.1.1 Descripción de la actividad

Se realizo un formato específico para el análisis FODA, el cual identifica los puntos clave del área en el que se está trabajando, esto con el fin de identificar los puntos positivos y negativos de la misma abarcando los puntos que se inspeccionaran: (seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario). En el color verde se ubicarán las fortalezas, de color rojo las debilidades, de amarillo las amenazas y de color azul las oportunidades de cada uno de los puntos que se inspeccionarán ya mencionados anteriormente: (seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario).

3.1.1.6.1.2 Resultado de la actividad

Tabla 6. Maquetado del FODA. Fuente: Elaboración propia.

FORTALEZAS	**DEBILIDADES**
En este apartado se identifican las características que destacan positivamente de acuerdo con cada punto de estudio (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y sistema de inventario).	En este apartado se determinan los puntos negativos y aquellas características que necesitan mejorar de acuerdo con cada uno de los puntos de estudio (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y sistema de inventario).
OPORTUNIDADES	**AMENAZAS**
En este apartado se colocan los elementos externos, cambios y/o propuestas que pueden sacar una ventaja o beneficio de acuerdo con los puntos de estudio (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y sistema de inventario).	En este apartado se detectan y se colocan aquellas situaciones o acontecimientos que impiden o ponen en peligro los elementos, bienes y procesos de cada uno de los puntos de estudio (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y sistema de inventario).

3.1.1.6.2 Actividad 1.6.2 Generar los cuestionarios.

3.1.1.6.2.1 Descripción de la actividad

Se diseñan reactivos de preguntas abiertas y de opción múltiple para conformar los cuestionarios que se aplicaran para cada uno de los rubros a evaluar construir los cuestionarios adecuados de acuerdo con cada uno de los puntos a tratar (seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario) dentro de la UTIC, dichas preguntas permiten conocer una visión más clara sobre el estado actual de los procesos que realizan internamente.

3.1.1.6.2.2 Resultado de la actividad

A continuación, se presentan las preguntan que se van a emplear para la obtención de información directamente con el Jefe de la Unidad de Tecnologías de la Información y Comunicación.

3.1.1.6.2.2.1 Cuestionario Seguridad Física

1. ¿Cuenta con personal de recepción?
2. ¿Cuenta con personal de vigilancia? En caso de ser Si describa.
3. ¿Cuenta con cámaras de seguridad? En caso de ser Si anotar el número de cámaras de vigilancia.
4. ¿El sitio es completamente cerrado?
5. ¿Qué asegura el perímetro donde se encuentra el sitio?
6. ¿Cuál es la altura de las paredes, rejas o barreras?
7. ¿Cuántos accesos hay al sitio? Mencione cuales son los accesos
8. ¿Cómo identifica quienes tienen acceso autorizado?
9. ¿Qué sucede en caso de un acceso no autorizado?
10. ¿Hay un periodo de acceso al sitio? En caso de ser Si, mencione el horario.
11. ¿Cuándo el sitio no está siendo utilizado se cierran los accesos?

12. ¿El cableado cuenta con alguna medida de seguridad? Como separar los cables de energía de los de comunicaciones

13. ¿Clasifica los cables y equipos del sitio? En caso de ser Si mencione la clasificación.

14. ¿Cada cuánto tiempo realiza un inventario del equipo?

15. ¿Cuenta con un sistema de protección de intrusos?

16. ¿Se ha establecido un programa de gestión de riesgos para identificar y evaluar los riesgos asociados a la seguridad física?

17. ¿Se realizan evaluaciones periódicas de la seguridad física en la unidad?

18. ¿Se lleva a cabo una revisión periódica de los controles de seguridad implementados en relación con el acceso físico, tales como cámaras de seguridad, cerraduras, protecciones, entre otros?

19. ¿Se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física? En caso de ser Sí mencione cuales.

20. ¿Se proporciona capacitación y concientización sobre seguridad física?

21. ¿Se realizan pruebas de seguridad física de forma periódica en el sitio?

22. ¿Se documentan y mantienen registros de los incidentes de seguridad física ocurridos en el sitio? En caso de ser Si, mencione el Como.

3.1.1.6.2.2.2 Cuestionario Seguridad Lógica

1. ¿Se realiza un seguimiento de las acciones tomadas para garantizar la seguridad lógica en el sitio? En caso de ser Sí, Mencione cuales
2. ¿Se siguen procedimientos para la creación, modificación y eliminación de cuentas de usuario? En caso de ser Sí, mencione cuales
3. ¿Se utilizan contraseñas seguras y se requiere que los usuarios las cambien periódicamente? En caso de ser Sí, mencione la frecuencia
4. ¿Se emplea autenticación de dos factores para acceder a los sistemas o servicios sensibles?
5. ¿Se implementa un sistema de control de acceso que limite el acceso a los recursos y datos según los roles y permisos asignados?
6. ¿Se revisan regularmente los privilegios de acceso y se eliminan los innecesarios o inactivos?
7. ¿Se utilizan registros de auditoría para rastrear las actividades de los usuarios y detectar posibles brechas de seguridad?
8. ¿Se realiza una copia de seguridad periódica de los datos almacenados en el sitio? En caso de ser si mencione la frecuencia.
9. ¿Se utilizan herramientas de detección de malware y antivirus en los sistemas del sitio? En caso de ser Sí mencione las herramientas
10. ¿Se realizan actualizaciones de seguridad de forma regular en los sistemas operativos y aplicaciones del sitio? En caso de ser Sí mencione la frecuencia
11. ¿Se utiliza un sistema de cifrado para proteger los datos sensibles almacenados en los sistemas del sitio?
12. ¿Se realizan pruebas de penetración o auditoras de seguridad de forma periódica en los sistemas del sitio? En caso de ser Sí, mencione cuales pruebas
13. ¿Se cuenta con un plan de respuesta a incidentes para abordar y mitigar posibles brechas de seguridad?

14. ¿Se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas para resolverlos?
15. ¿Se implementan medidas de protección de datos, como el uso de firewalls y sistemas de detección y prevención de intrusiones?
16. ¿Se implementan medidas de protección de datos, como el uso de firewalls y sistemas de detección y prevención de intrusiones? En caso de ser Sí, mencione la frecuencia
17. ¿Se brinda capacitación regular a los usuarios sobre las mejores prácticas de seguridad lógica, como el uso de contraseñas seguras y la identificación de correos electrónicos de phishing?
18. ¿Se realizan copias de seguridad de los sistemas y datos del sitio en un lugar externo seguro?
19. ¿Se requiere una contraseña para acceder a los equipos del departamento?
20. ¿Los usuarios tienen cuentas de usuario individuales para acceder a los equipos?
21. ¿Se realizan regularmente actualizaciones de seguridad en los sistemas operativos y software utilizado en el departamento? En caso de ser Sí mencione la frecuencia.
22. ¿Existen políticas o restricciones para la instalación de software adicional en los equipos del departamento?
23. ¿Se realizan copias de seguridad periódicas de los datos almacenados en los equipos de la unidad? En caso de ser Sí mencione la frecuencia
24. ¿Se utilizan soluciones de antivirus y antimalware actualizadas en los sistemas del sitio? En caso de ser Sí mencione los programas utilizados
25. ¿Se brinda capacitación o información a los usuarios sobre prácticas de seguridad informática y protección de datos? En caso de ser Sí mencione la frecuencia.
26. ¿Se monitorea y registra el acceso a los sistemas del sitio para detectar posibles actividades sospechosas? En caso de ser Sí mencione como se monitorea.
27. ¿Se cuenta con un plan de respuesta a incidentes de seguridad en caso de una brecha o ataque informático? En caso de ser Sí mencione el cómo se implementan

28. ¿Se realiza un seguimiento de las acciones tomadas para garantizar la seguridad lógica en la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
29. ¿Se siguen procedimientos para la creación, modificación y eliminación de cuentas de usuario? Especifique.
30. ¿Se utilizan contraseñas seguras y se requiere que los usuarios las cambien periódicamente? Especifique.
31. ¿Se utiliza autentificación de los factores para acceder a los sistemas o servicios sensibles? Especifique.
32. ¿Se implementa un sistema de control de acceso que limite el acceso a los recursos y datos según los roles u permisos asignados? Especifique.
33. ¿Se revisan regularmente los privilegios de acceso y se eliminan los innecesarios o inactivos? Especifique.
34. ¿Se realiza una copia de seguridad periódica de los datos almacenados en la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
35. ¿Se utilizan herramientas de detección de malware y antivirus en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
36. ¿Se realizan actualizaciones de seguridad de forma regular en los sistemas operativos y aplicaciones de la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
37. ¿Se utiliza un sistema de cifrado para proteger los datos sensibles almacenados en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
38. ¿Se realizan pruebas de penetración o Auditorías de forma periódica en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones? Especifique.
39. ¿Se cuenta con un plan de respuesta a incidentes para abordar y mitigar posibles brechas de seguridad? Especifique.
40. ¿Se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas para resolverlos? Especifique.

41. ¿Se implementan medidas de retención de datos, como el uso de firewalls y sistemas de detección y prevención de intrusiones? Especifique.

42. ¿Se realizan auditorías internas o externas para evaluar el cumplimiento de las políticas de seguridad lógica? Especifique.

43. ¿Se brinda capacitación regular a los usuarios sobre las mejores prácticas de seguridad lógica como el uso de contraseñas seguras y la identificación de correos electrónicos de phishing? Especifique.

44. ¿Se realizan copias de seguridad de los sistemas y datos del laboratorio en un lugar externo seguro? Especifique.

3.1.1.6.2.2.3 Cuestionario de Servicios

1. ¿Qué actividades o tareas se ven afectadas cuando hay falta o falla del servicio de aire acondicionado?
2. ¿Qué actividades se realizan al momento de generar el mantenimiento al servicio de aire acondicionado?
3. ¿Qué actividades deben realizarse para el correcto uso del servicio de aire acondicionado?
4. ¿Tienes alguna sugerencia o conflicto adicional para el servicio de Internet con el que cuenta la Unidad de Tecnologías de la Información y Comunicación?
5. ¿Se ha notado alguna diferencia en el rendimiento del sistema del aire acondicionado?
6. ¿Qué actividades se deben realizar para el buen uso del servicio de Internet?
7. ¿Qué actividades deben realizarse en caso de presentar una falla de energía dentro de la Unidad de Tecnologías de la Información y Comunicación?
8. ¿Qué actividades o tareas se ven afectadas cuando hay falla en el servicio Internet?
9. ¿Qué actividades o tareas se ven afectadas cuando hay falla o falta del servicio de electricidad?
10. ¿A qué autoridad se debe acudir en caso de un accidente en el servicio de Internet?
11. ¿A qué autoridad se debe acudir en caso de un accidente en el servicio eléctrico?
12. ¿A qué autoridad se debe acudir en caso de un accidente con el servicio de aire acondicionado?
13. ¿Cuál es el proceso de supervisión y monitorización del rendimiento de la red y los sistemas dentro de la Unidad de Tecnologías de la Información y Comunicación?
14. ¿Existe prácticas y/o procedimientos claros para el control de acceso lógico, tales como la autenticación, autorización y control de privilegios dentro de la Unidad de Tecnologías de la Información y Comunicación?
15. ¿Se implementan medidas de seguridad adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas dentro de la Unidad de Tecnologías de la Información y Comunicaciones?

16. ¿Se realizan evaluaciones de riesgos de manera periódica para identificar amenazas y vulnerabilidades en los servicios de la Unidad de Tecnologías de la Información y Comunicación?
17. ¿Cada cuánto se realizan evaluaciones de los servicios en la Unidad de Tecnologías de la Información y Comunicación?
18. ¿La Unidad de Tecnologías de la Información y Comunicación cuenta con algún servicio en caso de un incendio?
19. En caso de que sea afirmativa la respuesta, ¿El servicio con el que cuentas, crees que es el adecuado para usarse en caso de un incendio?
20. ¿Hay algún proceso que se realice para dar mantenimiento a los equipos de redes que se encuentran en la UTIC?
21. ¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Internet que brinda la organización?
22. ¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Aire Acondicionado que brinda la organización?
23. ¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Redes que brinda la organización?
24. ¿Existen capacitaciones para el uso de alguno de los servicios disponibles dentro de la UTIC? Especifique
25. ¿Cuentan con botiquín medico dentro de la UTIC?
26. En caso de que sea afirmativa la respuesta, ¿cada cuando se le da mantenimiento o chequeo a este servicio médico?

3.1.1.6.2.2.4 Cuestionario de Infraestructura

1. ¿En qué estado consideras que se encuentra la infraestructura del sitio?
2. ¿Consideras que la ventilación del sitio es suficiente? (Ventanas).
3. ¿En qué estado consideras que se encuentra la ventilación?
4. ¿En qué estado consideras que se encuentra la iluminación del sitio?
5. ¿Con cuántos Racks cuenta el departamento?
6. ¿Consideras que los racks están correctamente instalados?
7. ¿Los racks están ubicados en un sitio con condiciones adecuadas de temperatura y humedad?
8. ¿Los racks están organizados ordenadamente y etiquetados correctamente?
9. ¿Existe alguna regla acerca de la gestión de cables para mantener el orden y la limpieza en los racks? Si la respuesta es positiva anotar que procedimientos o regla se sigue, del caso contrario solo anote No.
10. ¿En qué estado consideras que se encuentra el cableado de manera general?
11. ¿Cuántos Routers, Switches y Servidores cuenta el departamento? Mencione cada uno
12. ¿Cuál es la marca y modelo de los Routers, switches y servidores utilizados?
13. ¿Los Routers, switches y servidores cuentas con reglas específicas para su uso? En caso de ser Si mencione la regla, de lo contrario responda No.
14. ¿Los Routers, switches y servidores tienen un mantenimiento frecuente? En caso de ser Si, mencione la frecuencia, de lo contrario responda No.
15. ¿Cómo calificaras la condición de los Routers, switches y servidores?
16. ¿Consideras que los racks están en una ubicación accesible del sitio?
17. ¿En qué estado consideras que se encuentran los equipos de cómputo?
18. ¿En qué estado consideras que se encuentran los monitores?
19. ¿Cómo crees que están los Routers en términos de su funcionamiento y estado físico?
20. ¿Cómo crees que están los Switches en términos de su funcionamiento y estado físico?
21. ¿Cómo crees que están los Servidores en términos de su funcionamiento y estado físico?
22. ¿Consideras que los escritorios sean las adecuadas? En caso de que la respuesta sea negativa menciona porque, de lo contrario responda Si.
23. ¿Consideras que los enchufes de corriente están instalados en el lugar adecuado? En caso de que la respuesta sea negativa mencione porque no, de lo contrario responda Si.

24. ¿Has notado alguna grieta o ruptura en el techo del departamento? En caso de que la respuesta sea positiva mencionar donde, de lo contrario responda que No.
25. ¿Ha notado alguna grieta o ruptura en el piso del departamento? En caso de que la respuesta sea positiva mencionar donde, de lo contrario responda que No.
26. ¿Qué aspectos consideras ms importantes en la infraestructura de la unidad? y por qué?
27. ¿Cómo describirías la calidad y disponibilidad de los equipos de cómputo en la unidad?
28. ¿Qué mejoras o actualizaciones sugieres para optimizar el rendimiento de los equipos?
29. ¿Cuál es tu opinión sobre la conectividad de red en el departamento?
30. ¿Existen problemas de velocidad o estabilidad dentro del departamento? Si la respuesta es positiva en Otra... Mencione la frecuencia del problema y como da solución
31. ¿Qué medidas de seguridad consideras que se deben implementar para proteger la infraestructura y los datos en el sitio?
32. ¿Cuál es tu evaluación de la distribución del espacio físico en el departamento?
33. ¿Hay suficiente espacio para los usuarios?
34. ¿Crees que se proporciona un ambiente adecuado en términos de iluminación y ventilación en el sitio?
35. ¿Cómo evaluarías la disponibilidad de recursos adicionales, como cables de red, cables de consola, cables seriales, u otros dispositivos periféricos en el sitio?
36. De acuerdo con la pregunta anterior, si un integrante fuera o dentro del departamento requiere un recurso adicional, ¿hay algún procedimiento de salida del recurso?
37. ¿Consideras que el mobiliario y los asientos son cómodos y ergonómicos para los usuarios del sitio?
38. ¿Existe alguna otra sugerencia o comentario que te gustara hacer respecto a la infraestructura del departamento?

3.1.1.6.2.2.5 Cuestionario de Inventario

1. ¿Se cuenta con un registro detallado de los dispositivos? Si / No_____Especifique
2. ¿Existe un sistema de etiquetado e identificación para cada dispositivo? Si / No _____Especifique
3. ¿Existe un procedimiento para dar de baja dispositivos obsoletos o fuera de servicio? Si / No__Especifique
4. ¿Existen políticas y controles para actualizar o manejar la información dentro de su inventario? Si / No.Especifique
5. ¿Cuenta con un historial de reparaciones, mantenimientos, actualizaciones realizadas en cada dispositivo? Si / No_Especifique
6. ¿Se registran las fechas de adquisición de cada equipo además del rol de trabajo de este? Si / No__Especifique
7. ¿Se realizan verificaciones periódicas para asegurarse que los dispositivos están siendo utilizados sin autorización? Si / No_____Especifique
8. ¿Existen un respaldo actualizado del inventario en caso de pérdida de datos? Si / No _____Especifique
9. ¿Se registran los cambios en el inventario? Si / No____Especifique
10. ¿Existe un registro de los softwares y licencias instaladas? Si / No___Especifique
11. ¿Se realiza un respaldo regular de los datos almacenados en los dispositivos de la UTIC? Si / No_Especifique
12. ¿Se realizan inspecciones regulares de los equipos para detectar daños o problemas de funcionamiento? Si, ¿Quién las realiza? _/ No
13. ¿Se registran regularmente los cables, conexiones y otros componentes físicos? Si / No Especifique
14. Si algo está mal en el inventario o simplemente no coinciden los componentes con lo registrado ¿a quién y cómo se le reporta? _____Especifique
15. ¿Existe un inventario separado para periféricos como cables, pantallas, teclados, mouse y memorias flash? Si / No_____Especifique
16. ¿Se lleva un registro de los incidentes de seguridad relacionado con los dispositivos? Si / No_____Especifique
17. ¿El inventario que tienen actualmente está protegido por sesiones y roles de los usuarios que lo manejan? Si / No_____Especifique

18. ¿El inventario con el que cuentan actualmente integra todo los componentes o activos de la UTIC en uno solo? _____Especifique
19. ¿El inventario con el que cuentan actualmente está desarrollado en un sistema gestor de base de datos oficial o en hojas de cálculo u otra aplicación de almacenamiento? Especifique
20. ¿El inventario con el que cuenta maneja conexiones de tablas y campos con el que se puedan hacer consultas compuestas o es más un checklist? _____Especifique.

3.1.1.6.3 Actividad 1.6.3 Generar formato de la Matriz y el análisis de riesgos.

3.1.1.6.3.1 Descripción de la actividad

La tabla a continuación presenta el diseño elaborado para el análisis de riesgos de la UTIC, enfocado en evaluar y promediar los riesgos según su nivel de impacto y probabilidad. El propósito de este análisis es identificar aquellos riesgos que presentan un mayor potencial de desastre dentro del área.

3.1.1.6.3.2 Resultado de la actividad

Tabla 7. Matriz de Riesgos. Fuente: Elaboración propia.

			IMPACTO				
PROBABILIDAD			INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	PELIGROSO (4)	CATASTRÓFICO (5)
	FRECUENTE	5	5	10	15	20	25
	PROBABLE	4	4	8	12	16	20
	OCASIONAL	3	3	6	9	12	15
	POSIBLE	2	2	4	6	8	10
	IMPROBABLE	1	1	2	3	4	5

Además, los siguientes formatos complementarán la matriz en la identificación de riesgos a través de las amenazas y vulnerabilidades, clasificándolos según su impacto. El primer formato es un catálogo que recoge los posibles riesgos en cada escenario, tomando en cuenta las amenazas y vulnerabilidades identificadas en los análisis FODA previos. El segundo formato proporciona una perspectiva adicional basada en la percepción de los empleados internos, permitiendo considerar sus puntos de vista sobre las amenazas y vulnerabilidades previamente organizadas en el catálogo de riesgos.

Tabla 8. Catálogo de Riesgos. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo

Tabla 9. Análisis de Riesgos. Fuente: Elaboración propia.

	Vulnerabilidad				
	Improbable / Insignificante	Posible / Menor	Ocasional / Moderado	Probable / Peligroso	Frecuente / Catastrófico
Pregunta de impacto					
Pregunta de Probabilidad					

Tabla 10. Análisis de Amenazas. Fuente: Elaboración propia.

	Amenaza				
	Improbable / Insignificante	Posible / Menor	Ocasional / Moderado	Probable / Peligroso	Frecuente / Catastrófico
Pregunta de impacto					
Pregunta de Probabilidad					

Por último, este formato también contribuye al análisis de riesgos, ya que, con base en las tablas anteriores y en las valoraciones obtenidas de las respuestas de los empleados internos, se utiliza la matriz de riesgos para determinar la posición de cada valoración. En este formato, se registra la vulnerabilidad y se explica el cálculo correspondiente en la columna de conclusiones, utilizando los valores obtenidos. Esto se realiza para cada vulnerabilidad en los temas de interés (seguridad física, seguridad lógica, servicios,

infraestructura y sistema de inventario), respetando el esquema de colores de la matriz de riesgos según la categorización, lo que facilita la interpretación de los resultados. El objetivo es identificar y priorizar las vulnerabilidades con el mayor índice de impacto.

Tabla 11. Análisis de Riesgos Enfocada a Vulnerabilidades. Fuente: Elaboración propia.

Tema especifico	
Vulnerabilidad	**Conclusión**
	MUY ALTA
Vulnerabilidad	**Conclusión**
	ALTA
Vulnerabilidad	**Conclusión**
	MEDIA
Vulnerabilidad	**Conclusión**
	BAJA

3.1.1.6.4 Actividad 1.6.4 Generar formato para la realización de pruebas.

3.1.1.6.4.1 Descripción de la actividad

Por último, se elabora un formato para analizar los riesgos o los puntos negativos que presentan un mayor impacto, utilizando diversas herramientas, estrategias y habilidades. Este formato permite evaluar el estado o la situación actual en función de los resultados del análisis de riesgos. En él, se especifica el tipo de prueba realizada, se documenta la evidencia de la situación actual, se registra el valor obtenido y se proporcionan recomendaciones basadas en los dictámenes del estándar o norma aplicable según el caso.

3.1.1.6.4.2 Resultado de la actividad

Tabla 12. Formato de Pruebas. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "X"	
OBJETIVO DE PRUEBA	
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	
TÉCNICA	
ACTIVIDADES DE LA PRUEBA	
PROCESO DE MEDICIÓN	
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	
CONSIDERACIONES ESPECIALES	
INTERPRETACIÓN DE RESULTADOS	
RECOMENDACIONES	

3.2 Segundo Objetivo: Ejecutar Auditoría

3.2.1 Actividades

3.2.1.1 Actividad 2.1 Aplicar los cuestionarios

3.2.1.1.1 Descripción de la actividad

Una vez diseñadas las preguntas, se procede a aplicar los cuestionarios en la Unidad de Tecnologías de la Información y Comunicación (UTIC). Dichos cuestionarios serán respondidos exclusivamente por el jefe de la unidad, el Ingeniero Jonathan Rodrigo Pérez Del Río, quien, al estar a cargo del área, posee una visión más amplia sobre la situación actual del departamento. Los cuestionarios abordan temas específicos de manera individual, lo que permite recopilar información de manera más ordenada y clara. Los aspectos tratados incluyen Seguridad Física, Seguridad Lógica, Infraestructura, Servicios e Inventario.

La aplicación de estos cuestionarios se realiza de forma presencial en la Unidad de Tecnologías de la Información y Comunicación, con el objetivo de obtener detalles precisos sobre la situación actual en relación con los puntos de estudio mencionados. Además, se busca garantizar que las respuestas se alineen con las observaciones directas, ya que a simple vista se pueden identificar anomalías en cuanto a los equipos, su organización y el espacio de trabajo, lo que evidencia una falta de acoplamiento entre los usuarios y alerta sobre el uso o control de los sistemas.

3.2.1.1.2 Resultado de la actividad

Con base en las respuestas del cuestionario de seguridad física aplicado al jefe de la unidad, se puede concluir de manera preliminar que la Unidad de Tecnologías de la Información y Comunicación (UTIC) cuenta con alguna forma de seguridad física que protege el área; sin embargo, esta no es adecuada para garantizar el resguardo y la seguridad de los activos y la información. Esto se debe a la falta de protección en los accesos, así como a la ausencia de vigilancia o medidas de seguridad que resguarden el perímetro del departamento en su totalidad.

Tabla 13. Cuestionario de Seguridad Física. Fuente: Elaboración propia.

CUESTIONARIO DE SEGURIDAD FÍSICA APLICADO AL JEFE DE LA UTIC			
Objetivo:	Recopilar información acerca sobre la seguridad física de la UTIC		
Fecha:	2023/10/23		
Entrevistado:	Jonathan Rodrigo Pérez Del Río	Entrevistador:	Moran Diego Oscar Yahir Santos Ramírez Ana Laura
Cargo:	Jede de la UTIC		
N°	Preguntas	Respuestas	Observación
1	¿Cuenta con personal de recepción?	SI (X) NO ( )	
2	¿Cuenta con personal de vigilancia? En caso de ser Si describa.	SI (X) NO ( )	Además del departamento, la vigilancia se encuentra en todo el municipio
3	¿Cuenta con cámaras de seguridad? En caso de ser Si anotar el número de cámaras de vigilancia.	SI (X) NO ( )	Cuenta con 2 cámaras, una dentro del departamento, la otra en el pasillo donde se encuentra el departamento
Otra respuesta:			

Tabla 13 (continuación)

4	¿El sitio es completamente cerrado?	SI (X) NO ( )	
5	¿Qué asegura el perímetro donde se encuentra el sitio?	SI ( ) NO ( )	
Otra respuesta: Bardas			
6	¿Cuál es la altura de las paredes, rejas o barreras?	SI ( ) NO ( )	
Otra respuesta: 2 mts			
7	¿Cuántos accesos hay al sitio? Mencione cuales son los accesos	SI ( ) NO ( )	
Otra respuesta: por lector de huella y por chip			
8	¿Cómo identifica quienes tienen acceso autorizado?	SI ( ) NO ( )	
Otra respuesta: Listado de alta de lector de huella exclusivo del personal de TIC			
9	¿Qué sucede en caso de un acceso no autorizado?	SI ( ) NO ( )	
Otra respuesta: la puerta del SITE no se abre			
10	¿Hay un periodo de acceso al sitio? En caso de ser Si, mencione el horario.	SI ( ) NO (X)	
11	¿Cuándo el sitio no está siendo utilizado se cierran los accesos?	SI (X) NO ( )	

Tabla 13 (continuación)

12	¿El cableado cuenta con alguna medida de seguridad? Como separar los cables de energía de los de comunicaciones	SI (X) NO ( )	
13	¿Clasifica los cables y equipos del sitio? En caso de ser Si mencione la clasificación.	SI ( ) NO ( )	
Otra respuesta: Cable de par trenzado sin apantallar etiquetados de cada nodo en el patch panel y switch, etiquetado del servicio de red entre de enlaces de comunicación entre gabinetes identificado por nombre del área			
14	¿Cada cuánto tiempo realiza un inventario del equipo?	SI ( ) NO ( )	
Otra respuesta: Bimestral			
15	¿Cuenta con un sistema de protección de intrusos?	SI (X) NO ( )	
16	¿Se ha establecido un programa de gestión de riesgos para identificar y evaluar los riesgos asociados a la seguridad física?	SI ( ) NO (X)	
17	¿Se realizan evaluaciones periódicas de la seguridad física en la unidad?	SI ( ) NO ( )	
Otra respuesta: Trimestral			

Tabla 13 (continuación)

18	¿Se lleva a cabo una revisión periódica de los controles de seguridad implementados en relación con el acceso físico, tales como cámaras de seguridad, cerraduras, protecciones, entre otros?	SI ( ) NO ( )	
Otra respuesta: Semestral			
19	¿Se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física? En caso de ser Sí mencione cuales.	SI ( ) NO (X)	
Otra respuesta:			
20	¿Se proporciona capacitación y concientización sobre seguridad física? No	SI ( ) NO (X)	
21	¿Se realizan pruebas de seguridad física de forma periódica en el sitio?	SI ( ) NO (X)	
Otra respuesta: No se realizan pruebas			
22	¿Se documentan y mantienen registros de los incidentes de seguridad física ocurridos en el sitio? En caso de ser Si, mencione el Como.	SI ( ) NO (X)	
Otra respuesta:			

Con base en las respuestas obtenidas del cuestionario de seguridad lógica, se puede concluir de manera preliminar que la Unidad de Tecnologías de la Información y Comunicación (UTIC) dispone de programas que contribuyen a mantener los equipos de cómputo y su información relativamente seguros. Sin embargo, se han registrado ataques o intentos de intrusión a la información. Aunque estos incidentes han sido resueltos y evitados, no existe un registro de estos que sirva como referencia en caso de que se repitan. Además, se observa la falta de capacitación para los nuevos empleados o usuarios que comienzan a desempeñar actividades internamente, lo que puede dar lugar a incidentes. A pesar de estas deficiencias, la unidad cuenta con un antivirus completamente funcional llamado ESET NOD 32, que permite la administración y verificación de la información, archivos y correos, así como de los equipos utilizados, para prevenir la corrupción de archivos

Tabla 14. Cuestionario de Seguridad Lógica. Fuente: Elaboración propia.

CUESTIONARIO DE SEGURIDAD LÓGICA APLICADO AL JEFE DE LA UTIC			
Objetivo:	Recopilar información acerca sobre la seguridad lógica de la UTIC		
Fecha:	2023/10/25		
Entrevistado:	Jonathan Rodrigo Pérez Del Río	Entrevistador:	Moran Diego Oscar Yahir Santos Ramírez Ana Laura
Cargo:	Jefe de la UTIC		
N°	Preguntas	Respuestas	Observación
1	¿Se realiza un seguimiento de las acciones tomadas para garantizar la seguridad lógica en el sitio? En caso de ser Sí, Mencione cuales	SI ( ) NO (X)	
Otra respuesta:			
2	¿Se siguen procedimientos para la creación, modificación y eliminación de cuentas de usuario? En caso de ser Sí, mencione cuales	SI (X) NO ( )	Mediante Oficio de solicitud y se generan responsivas para las cuentas creadas

Tabla 14 (continuación)

3	¿Se utilizan contraseñas seguras y se requiere que los usuarios las cambien periódicamente? En caso de ser Sí, mencione la frecuencia	SI ( ) NO (X)	
4	¿Se emplea autenticación de dos factores para acceder a los sistemas o servicios sensibles?	SI (X) NO ( )	
5	¿Se implementa un sistema de control de acceso que limite el acceso a los recursos y datos según los roles y permisos asignados?	SI ( ) NO (X)	
6	¿Se revisan regularmente los privilegios de acceso y se eliminan los innecesarios o inactivos?	SI (X) NO ( )	
7	¿Se utilizan registros de auditoría para rastrear las actividades de los usuarios y detectar posibles brechas de seguridad?	SI ( ) NO (X)	
8	¿Se realiza una copia de seguridad periódica de los datos almacenados en el sitio? En caso de ser si mencione la frecuencia.	SI ( ) NO ( )	
Otra respuesta: Mensual			
9	¿Se utilizan herramientas de detección de malware y antivirus en los sistemas del sitio? En caso de ser Sí mencione las herramientas	SI ( ) NO ( )	
Otra respuesta: Antivirus			

Tabla 14 (continuación)

10	¿Se realizan actualizaciones de seguridad de forma regular en los sistemas operativos y aplicaciones del sitio? En caso de ser Sí mencione la frecuencia	SI ( ) NO (X)	
11	¿Se utiliza un sistema de cifrado para proteger los datos sensibles almacenados en los sistemas del sitio?	SI (X) NO ( )	
12	¿Se realizan pruebas de penetración o auditorías de seguridad de forma periódica en los sistemas del sitio? En caso de ser Sí, mencione cuales pruebas	SI ( ) NO (X)	
13	¿Se cuenta con un plan de respuesta a incidentes para abordar y mitigar posibles brechas?	SI ( ) NO (X)	
14	¿Se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas para resolverlos?	SI ( ) NO (X)	
15	¿Se implementan medidas de protección de datos, como el uso de firewalls y sistemas de detección y prevención de intrusiones?	SI (X) NO ( )	
16	¿Se brinda capacitación regular a los usuarios sobre las mejores prácticas de seguridad lógica, como el uso de contraseñas seguras y la identificación de correos electrónicos de phishing?	SI ( ) NO (X)	

Tabla 14 (continuación)

17	¿Se realizan copias de seguridad de los sistemas y datos del sitio en un lugar externo seguro?	SI ( ) NO (X)	
18	¿Se requiere una contraseña para acceder a los equipos del departamento?	SI (X) NO ( )	
19	¿Se brinda capacitación o información a los usuarios sobre prácticas de seguridad informática y protección de datos? En caso de ser Sí mencione la frecuencia.	SI ( ) NO (X)	
20	¿Los usuarios tienen cuentas de usuario individuales para acceder a los equipos?	SI (X) NO ( )	
21	¿Se realizan regularmente actualizaciones de seguridad en los sistemas operativos y software utilizado en el departamento? En caso de ser Sí mencione la frecuencia.	SI ( ) NO (X)	
22	¿Existen políticas o restricciones para la instalación de software adicional en los equipos del departamento?	SI (X) NO ( )	
23	¿Se realizan copias de seguridad periódicas de los datos almacenados en los equipos de la unidad? En caso de ser Sí mencione la frecuencia	SI ( ) NO (X)	

Tabla 14 (continuación)

24	¿Se utilizan soluciones de antivirus y antimalware actualizadas en los sistemas del sitio? En caso de ser Sí mencione los programas utilizados	SI ( ) NO ( )	
Otra respuesta: ESET NOD 32			
25	¿Se monitorea y registra el acceso a los sistemas del sitio para detectar posibles actividades sospechosas? En caso de ser Sí mencione como se monitorea.	SI ( ) NO (X)	
26	¿Se cuenta con un plan de respuesta a incidentes de seguridad en caso de una brecha o ataque informática? En caso de ser Sí mencione el cómo se implementan	SI ( ) NO (X)	

Con base en las respuestas obtenidas, se puede adquirir un conocimiento más amplio sobre la situación actual de los servicios disponibles en la Unidad de Tecnologías de la Información y Comunicación (UTIC). Se consideraron los siguientes servicios: médico, eléctrico, contra incendios, aire acondicionado, internet y redes.

A partir del cuestionario y de visitas previas para la inspección personal del área, se concluye que la mayoría de los servicios que posee la UTIC son relativamente nuevos; por ejemplo, el servicio de redes, para el cual se instaló el rack hace apenas 3 meses. Además, el contrato de internet se ha renovado y corresponde a un plan actualizado que satisface las necesidades de la unidad. Sin embargo, los resultados también indican que no se cuenta con servicio médico para atender lesiones o accidentes de primer grado que puedan presentarse internamente. Asimismo, se observa una notable falta de procesos y actividades que aún no se han implementado para maximizar el estado de dichos servicios.

Tabla 15. Cuestionario de Servicios. Fuente: Elaboración propia.

CUESTIONARIO DE SERVICIOS APLICADO AL JEFE DE LA UTIC			
Objetivo:	Recopilar información acerca de los servicios con los que cuenta la UTIC		
Fecha:	2023/10/25		
Entrevistado:	Jonathan Rodrigo Pérez Del Río	Entrevistador:	Moran Diego Oscar Yahir Santos Ramírez Ana Laura
Cargo:	Jefe de la UTIC		
N°	Preguntas	Respuestas	Observación
1	¿Qué actividades o tareas se ven afectadas cuando hay falta o falla del servicio de aire acondicionado?	SI (X) NO ( )	
Otra respuesta: afecta la calidad del aire interior, lo que afecta en la ventilación adecuada de los servidores			
2	¿Qué actividades se realizan al momento de generar el mantenimiento al servicio de aire acondicionado?	SI ( ) NO ( )	Mediante Oficio de solicitud y se generan responsivas para las cuentas creadas
Otra respuesta: Cortar el suministro eléctrico, desconectar el equipo, para evitar algún daño, revisar la estructura física del componente y visualizar si hay fallos notorios, limpiarlo a profundidad y colocarlo nuevamente en el lugar asignado.			
3	¿Qué actividades deben realizarse para el correcto uso del servicio de aire acondicionado?	SI ( ) NO ( )	
Otra respuesta: Limpia de los filtros de la unidad interna, revisar que no cuente con fuga o escape del gas refrigerante			
4	¿Tienes alguna sugerencia o conflicto adicional para el servicio de Internet con el que cuenta la Unidad de Tecnologías de la Información y Comunicación?	SI ( ) NO (X)	

Tabla 15 (continuación)

5	¿Se ha notado alguna diferencia en el rendimiento del sistema del aire acondicionado?	SI ( ) NO (X)	
6	¿Qué actividades se deben realizar para el buen uso del servicio de Internet?	SI ( ) NO ( )	
Otra respuesta: Tener el control de los equipos que se conectan a la red general, monitoreo con aplicativos			
7	¿Qué actividades deben realizarse en caso de presentar una falla de energía dentro de la Unidad de Tecnologías de la Información y Comunicación?	SI ( ) NO ( )	
Otra respuesta: realizar las pruebas de restauración de hardware y software en línea de emergencia			
8	¿Qué actividades o tareas se ven afectadas cuando hay falla en el servicio Internet?	SI ( ) NO ( )	
Otra respuesta: actividades administrativas, tareas de cobro en oficinas foráneas y tareas que dependan de la comunicación con oficinas externas, lejanas o foráneas.			
9	¿Qué actividades o tareas se ven afectadas cuando hay falla o falta del servicio de electricidad?	SI ( ) NO ( )	
Otra respuesta: actividades administrativas, tareas de cobro en oficinas foráneas, podría decirse que un 80% de las actividades			

Tabla 15 (continuación)

10	¿A qué autoridad se debe acudir en caso de un accidente en el servicio de Internet?	SI ( ) NO ( )	
Otra respuesta: La Unidad de Tecnologías de la Información y Comunicación realiza la inspección del servicio de internet en cada gabinete y en el enlace dedicado principal, de existir falla desde el enlace, se envía ticket al ejecutivo de cuenta de Teléfonos de México para que levante el servicio y acuda un técnico para revisar la configuración del Router			
11	¿A qué autoridad se debe acudir en caso de un accidente en el servicio eléctrico?	SI ( ) NO ( )	
Otra respuesta: a la Subdirección de Servicios Generales del Ayuntamiento de Tultitlán, para que realicen la inspección.			
12	¿A qué autoridad se debe acudir en caso de un accidente con el servicio de aire acondicionado?	SI ( ) NO ( )	
Otra respuesta: a la Dirección de Administración y a la Subdirección de Servicios Generales del Ayuntamiento de Tultitlán, para que realicen la inspección y se solicite el servicio de mantenimiento a una empresa externa.			
13	¿Cuál es el proceso de supervisión y monitorización del rendimiento de la red y los sistemas dentro de la Unidad de Tecnologías de la Información y Comunicación?	SI ( ) NO ( )	
Otra respuesta: No hay ningún proceso de supervisión por el momento, solo monitoreamos que la red no tenga dispositivos foráneos de los ya registrados.			

Tabla 15 (continuación)

14	¿Existe prácticas y/o procedimientos claros para el control de acceso lógico, tales como la autenticación, autorización y control de privilegios dentro de la Unidad de Tecnologías de la Información y Comunicación?	SI (X) NO ( )	
15	¿Se implementan medidas de seguridad adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas dentro de la Unidad de Tecnologías de la Información y Comunicaciones?	SI (X) NO ( )	
16	¿Se realizan evaluaciones de riesgos de manera periódica para identificar amenazas y vulnerabilidades en los servicios de la Unidad de Tecnologías de la Información y Comunicación?	SI ( ) NO (X)	
17	¿Cada cuánto se realizan evaluaciones de los servicios en la Unidad de Tecnologías de la Información y Comunicación?	SI ( ) NO (X)	

Tabla 15 (continuación)

18	¿La Unidad de Tecnologías de la Información y Comunicación cuenta con algún servicio en caso de un incendio? En caso de que sea afirmativa la respuesta, ¿El servicio con el que cunetas, crees que es el adecuado para usarse en caso de un incendio?	SI (X) NO ( )	
Otra respuesta: Claro ya que es de un material específico para evitar daños mayores en caso de que se presente un incendio que implique corriente eléctrica y los equipos de cómputo.			
19	¿Hay algún proceso que se realice para dar mantenimiento a los equipos de redes que se encuentran en la UTIC	SI ( ) NO (X)	
20	¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Internet que brinda la organización?	SI ( ) NO ( )	
Otra respuesta: El Ing. Jonathan Rodrigo Pérez Del Río y José Luis Maldonado, los demás solo tienen acceso al internet por medio de los equipos de la UTIC para actividades laborales.			
21	¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Aire Acondicionado que brinda la organización?	SI ( ) NO ( )	
Otra respuesta: Personal Exclusivo de la Unidad de Tecnologías de la Información y comunicación			

Tabla 15 (continuación)

22	¿Quiénes dentro de la UTIC pueden hacer uso de los servicios de Redes que brinda la organización?	SI ( ) NO ( )	
Otra respuesta: Todo el personal interno de la UTIC puede tener acceso y usar esos servicios.			
23	¿Existen capacitaciones para el uso de alguno de los servicios disponibles dentro de la UTIC?	SI ( ) NO (X)	
24	¿Cuentan con botiquín medico dentro de la UTIC?	SI ( ) NO (X)	
25	¿En caso de que sea afirmativa la respuesta, cada cuando se le da mantenimiento o chequeo a este servicio médico?	SI ( ) NO ( )	

De acuerdo con las respuestas obtenidas en el cuestionario de infraestructura, se puede deducir que las instalaciones son adecuadas para el desempeño de las actividades, aunque no son las óptimas. Se presentan problemas notables en los espacios de trabajo, ya que los usuarios no pueden moverse con libertad. Además, se observa un cableado desordenado detrás de los equipos de cómputo debido a la falta de suficientes contactos eléctricos, lo que obliga a utilizar extensiones para el enchufado de estos. También se identifican repuestos y equipos ubicados en el piso, ya que no se dispone de un área adecuada para su almacenamiento.

Tabla 16. Cuestionario de Infraestructura. Fuente: Elaboración propia.

CUESTIONARIO DE INFRAESTRUCTURA APLICADO AL JEFE DE LA UTIC			
Objetivo:	Conocer la situación actual de los procesos, equipos y actividades que realiza la UTIC de acuerdo con su seguridad lógica.		
Fecha:	2023/11/30		
Entrevistado:	Jonathan Rodrigo Pérez Del Río	Entrevistador:	Oscar Yahir Moran Diego Ana Laura Santos Ramírez
Cargo:	Jefe de la Unidad		
N°	Preguntas	Respuestas	Observación
1	¿Se realiza un seguimiento de las acciones tomadas para garantizar la seguridad lógica en la Unidad de Tecnologías de la Información y Comunicaciones?	Si ( ) No (X)	Un seguimiento facilita la identificación de quien la implemento y si es óptima dicha acción o perjudica a los equipos.
2	¿Se siguen procedimientos para la creación, modificación y eliminación de cuentas de usuario?	Si (X) No ( )	El contar con una responsiva para notificar dicha acción independiente de cual sea, da una mayor seguridad ya que respalda la decisión tomada y se mantiene actualizado el estatus de las cuentas.
¿Cuáles?: Mediante oficio para la modificación y/o eliminación de alguna cuenta de usuario, todo se maneja vía responsiva y se entrega en las manos del usuario.			

Tabla 16 (continuación)

3	¿Se utilizan contraseñas seguras y se requiere que los usuarios las cambien periódicamente?	Si ( ) No (X)	Los usuarios cuentan con contraseñas personales que bien pueden poner en riesgo los equipos al no tener parámetros o criterios de seguridad ni actualizaciones constantes.
4	¿Se utiliza autentificación de los factores para acceder a los sistemas o servicios sensibles?	Si (X) No ( )	Estas credenciales solo son para acceder al cuarto donde se aloja el rack, aun así, los cristales no cuentan con seguridad y podría ser de fácil acceso si se llegan a quebrar.
¿Cuáles?: Vía credenciales de los servidores donde se alojan los sistemas			
5	¿Se implementa un sistema de control de acceso que limite el acceso a los recursos y datos según los roles u permisos asignados?	Si ( ) No (X)	Todos los integrantes del área pueden acceder a los recursos y datos, pero tener roles causaría un mejor rol de cada uno de ellos y se solicitaría permiso para la información sensible.
6	¿Se revisan regularmente los privilegios de acceso y se eliminan los innecesarios o inactivos?	Si ( ) No (X)	Eliminar los usuarios inactivos garantiza que no puedan acceder o modificar los datos desde equipos o cuentas externas.

Tabla 16 (continuación)

7	¿Se realiza una copia de seguridad periódica de los datos almacenados en la Unidad de Tecnologías de la Información y Comunicaciones?	Si ( ) No (X)	El no tener una copia de seguridad es de alto riesgo ya que en caso de un desastre o perdida, datos relevantes no se recuperarían y solo podrán continuar con las actividades recientes o que estaban en proceso.
8	¿Se utilizan herramientas de detección de malware y antivirus en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones?	Si (X) No ( )	Contar con un solo programa para la protección de todos los equipos puede ser vulnerable ya que no garantiza la seguridad máxima que podría obtener si implementa otro tipo de programas en conjunto.
¿Cuáles?: Antivirus, un scanner para correo malicioso, entre ellos Avast Free Antivirus			
9	¿Se realizan actualizaciones de seguridad de forma regular en los sistemas operativos y aplicaciones de la Unidad de Tecnologías de la Información y Comunicaciones?	Si (X) No ( )	Mantener actualizados los sistemas operativos y las aplicaciones garantiza un mayor nivel de seguridad que dejándolos obsoletos.

Tabla 16 (continuación)

10	¿Se utiliza un sistema de cifrado para proteger los datos sensibles almacenados en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones?	Si (X) No ( )	Cuando se tiene un sistema de cifrado se debe asegurar que sea uno de clave privada ya que es de mayor confidencialidad que los de clave pública.
11	¿Se realizan pruebas de penetración o Auditorías de forma periódica en los sistemas de la Unidad de Tecnologías de la Información y Comunicaciones?	Si ( ) No (X)	El no realizar auditorías periódicamente de los sistemas da pie a contar con actividades sospechosas u operaciones maliciosas sin ser detectadas y que ponen en riesgo los equipos y la información que se maneja en el área.
12	¿Se cuenta con un plan de respuesta a incidentes para abordar y mitigar posibles brechas de seguridad?	Si ( ) No (X)	No contar con un plan a la hora de identificar brechas solo garantiza una perdida de tiempo y mayor riesgo de quiebre mientras se intenta encontrar una solución para el tipo de brecha que se tiene.

Tabla 16 (continuación)

13	¿Se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas para resolverlos?	Si (X) No ( )	Tener un registro ayudaría demasiado si implementaran un plan para abordar brechas o situaciones de riesgo ya que tienen historial que pueden consultar si es un caso similar a los ya resueltos.
14	¿Se implementan medidas de retención de datos, como el uso de firewalls y sistemas de detección y prevención de intrusiones?	Si (X) No ( )	Contar con firewalls es una medida segura que garantiza el bloqueo de información que no sea pertinente o bien solicitada por los integrantes del área.
15	¿Se realizan auditorías internas o externas para evaluar el cumplimiento de las políticas de seguridad lógica?	Si ( ) No (X)	Esto da pie a tener una revisión por parte de autoridades y que sean acreedores a multas por no respetar las normativas como marcan algunos estándares ya que son una institución oficial.

Tabla 16 (continuación)

16	¿Se brinda capacitación regular a los usuarios sobre las mejores prácticas de seguridad lógica como el uso de contraseñas seguras y la identificación de correos electrónicos de phishing?	Si ( ) No (X)	No capacitar a los nuevos usuarios en estos temas provocaría un caso de infección no deseado o bien una brecha en la seguridad por una mala identificación de virus.
17	¿Se realizan copias de seguridad de los sistemas y datos del laboratorio en un lugar externo seguro?	Si ( ) No (X)	No tener un respaldo seguro de la información o datos de los sistemas en un lugar externo puede provocar que si atacan el área de trabajo sea pérdida total.

De acuerdo con las respuestas obtenidas en el cuestionario y tras realizar visitas previas a la Unidad de Tecnologías de la Información y Comunicación (UTIC), se puede deducir y observar que existe una notable ausencia de un sistema formal de inventario en la UTIC. Las consultas, entradas, salidas y bajas de los activos se monitorean y registran en hojas de cálculo que simulan las funciones de un inventario. Además, todos los equipos dentro de la unidad operan con cuentas de administrador, lo que implica que no se rigen mediante una cadena de mando con roles y privilegios, los cuales suelen prevenir la manipulación de información y mejorar su seguridad. Sin embargo, el método que se emplea parece resultar útil internamente, ya que son los propios empleados quienes han desarrollado este sistema y, con el tiempo, han perfeccionado sus actividades de acuerdo con este enfoque ambiguo.

Tabla 17. Cuestionario del Sistema de Inventario. Fuente: Elaboración propia.

CUESTIONARIO DE INVENTARIO APLICADO AL JEFE DE LA UTIC			
Objetivo:	Recopilar información acerca del sistema de inventario que usan dentro de la UTIC		
Fecha:	2023/10/25		
Entrevistado:	Jonathan Rodrigo Pérez Del Río	Entrevistador:	Moran Diego Oscar Yahir Santos Ramírez Ana Laura
Cargo:	Jefe de la UTIC		
N°	Preguntas	Respuestas	Observación
1	¿Se cuenta con un registro detallado de los dispositivos?	SI (X) NO ( )	
Otra respuesta: si por parte de la UTIC en un sistema, y con patrimonio municipal en su plataforma de IDESOFT			
2	¿Existe un sistema de etiquetado e identificación para cada dispositivo?	SI (X) NO ( )	
Otra respuesta: si en conjunto con patrimonio municipal se lleva la relación de cada dispositivo en su sistema de IDESOFT el cual arroja el etiquetado para llevar el control de bien patrimonial			
3	¿Existe un procedimiento para dar de baja dispositivos obsoletos o fuera de servicio?	SI (X) NO ( )	
Otra respuesta: cada departamento genera un oficio de solicitud a la Jefatura de la UTIC solicitando el Estudio Técnico de Obsolescencia, se acude a revisar el equipo o se lleva al departamento de UTIC para inspección detallada, se toma prueba fotográfica del equipo, se toma número de inventario, marca, modelo. Se contesta al oficio se adjunta el Estudio Técnico de Obsolescencia el cual contiene información sobre el departamento, el dispositivo y una descripción del motivo por el cual se debe emitir la baja del dispositivo. esto es para que el área pueda enviar la documentación elaborada por la UTIC al departamento de Patrimonio Municipal, para que pueda recoger los aparatos y llevarlos a implementar las medidas oportunas para retirarlos.			

Tabla 17 (continuación)

4	¿Existen políticas y controles para actualizar o manejar la información dentro de su inventario?	SI ( ) NO (X)	
5	¿Cuenta con un historial de reparaciones, mantenimientos, actualizaciones realizadas en cada dispositivo?	SI (X) NO ( )	
Otra respuesta: este historial de reparaciones es totalmente independiente ya que se genera una carpeta con las solicitudes que se atienden por cada uno de los casos.			
6	¿Se registran las fechas de adquisición de cada equipo además del rol de trabajo de este?	SI (X) NO ( )	
7	¿Se realizan verificaciones periódicas para asegurarse que los dispositivos no están siendo utilizados sin autorización?	SI ( ) NO (X)	
8	¿Existen un respaldo actualizado del inventario en caso de pérdida de datos? De ser afirmativa la respuesta ¿cada cuando realizan el respaldo?	SI (X) NO ( )	
Otra respuesta: cada 3 meses			
9	¿Se registran los cambios en el inventario? Es decir, un historial de quien modifico los cambios	SI ( ) NO (X)	
10	¿Existe un registro de los softwares y licencias instaladas?	SI (X) NO ( )	

Tabla 17 (continuación)

11	¿Se realiza un respaldo regular de los datos almacenados en los dispositivos de la UTIC? De ser afirmativa la respuesta, ¿en dónde se realiza el respaldo?	SI (X) NO ( )	
Otra respuesta: en el servidor de la UTIC			
12	¿Se realizan inspecciones regulares de los equipos para detectar daños o problemas de funcionamiento? De ser afirmativa la respuesta, ¿Quién las realiza?	SI (X) NO ( )	
Otra respuesta: personal de UTIC			
13	¿Se registran regularmente los cables, conexiones y otros componentes físicos?	SI ( ) NO (X)	
14	Si algo está mal en el inventario o simplemente no coinciden los componentes con lo registrado ¿a quién y cómo se le reporta?	SI (X) NO ( )	
Otra respuesta: al Jefe de La Unidad en conjunto con la Jefa del Departamento de Almacén			
15	¿Existe un inventario separado para periféricos como cables, pantallas, teclados, mouse y memorias flash?	SI (X) NO ( )	
16	¿Se lleva un registro de los incidentes de seguridad relacionado con los dispositivos?	SI ( ) NO (X)	
17	¿El inventario que tienen actualmente está protegido por sesiones y roles de los usuarios que lo manejan?	SI ( ) NO (X)	

Tabla 17 (continuación)

18	¿El inventario con el que cuentan actualmente integra todo los componentes o activos de la UTIC en uno solo o son archivos independientes?	SI ( ) NO ( )	
Otra respuesta: son archivos separados, pero funcionan en conjunto			
19	¿El inventario con el que cuentan actualmente está desarrollado en un sistema gestor de base de datos oficial o en hojas de cálculo u otra aplicación de almacenamiento?	SI (X) NO ( )	
Otra respuesta: en hojas de cálculo			
20	¿El inventario con el que cuenta maneja conexiones de tablas y campos con el que se puedan hacer consultas compuestas o es más un checklist?	SI ( ) NO ( )	
Otra respuesta: Checklist			

3.2.1.2 Actividad 2.2 Realizar los Análisis FODA

3.2.1.2.1 Descripción de la actividad

Con base en la información obtenida en los cuestionarios y mediante observación e inspección, se lleva a cabo un análisis FODA para categorizar la información más relevante de la Unidad de Tecnologías de la Información y Comunicación (UTIC). Este análisis comienza con una evaluación general del estado del departamento, proporcionando una visión amplia de los temas de interés mencionados anteriormente. El objetivo es evaluar el uso y el control de los sistemas y tecnologías disponibles, al mismo tiempo que se identifican las debilidades y riesgos presentes en el área. Se destaca, por un lado, la notable falta de organización interna en el departamento, tanto en la gestión de activos como en el mobiliario. Por otro lado, se evidencian brechas externas y la exposición de la unidad, lo que contribuye a un aumento de los riesgos asociados.

3.2.1.2.2 Resultado de la actividad

3.2.1.2.2.1 FODA de la Unidad De Tecnologías De La Información Y Comunicación

El desarrollo de este análisis FODA es principalmente para la obtención de información acerca de las Fortalezas, Oportunidades, Debilidades y Amenazas con las que cuenta la Unidad de Tecnologías de Información y Comunicación, con el fin de identificar información clave para desarrollar un plan de mejora del área mismo.

Tabla 18. FODA general de la UTIC. Fuente: Elaboración propia.

FORTALEZAS	**DEBILIDADES**
1. La UTIC cuenta con equipos de cómputo adecuados y actualizados a sus posibilidades para el desarrollo de sus actividades. 2. La UTIC tiene personal capacitado y preparado para la realización de las diversas actividades o problemáticas que se presenten.	1. Falta de espacio para el mobiliario en general dentro de la UTIC. 2. Deficiencia en los servicios con los que cuenta la UTIC (Aire Acondicionado, Seguridad física, Lógica, Software, Hardware, Medico, Infraestructura, Incendios). 3. Uso compartido de equipo de oficina como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.

Tabla 18 (continuación)

3. La UTIC se encuentra aislada del Ayuntamiento, evitando multitudes de gente, saturación de servicios, e interrupción de actividades.	4. Falta de movilidad del personal a causa de activos situados en el suelo de la UTIC. 5. Falta de un sistema especializado para la gestión de activos dentro de la UTIC.
OPORTUNIDADES	**AMENAZAS**
1. Propuesta de bitácora de uso para el equipo de impresión multifuncional de la unidad. 2. Propuesta para un mejor uso y mejora de los servicios con los que cuenta la UTIC. 3. Propuesta de asignación de un espacio particular para los activos ubicados en el suelo. 4. Propuesta de un sistema para la gestión de activos con seguridad que sustituya el paquete de ofimática con el que se trabaja actualmente.	1. Uso compartido de equipo de oficina al contar con un multifuncional y prestar sus servicios a departamentos externos. 2. Mayor riesgo a desastres naturales por falta de espacio dentro de la UTIC. 3. Falta de equipo de vigilancia para el resguardo y protección del área y sus activos. 4. Falta de seguridad en la red de internet, provocando ataques e infiltrados en el servicio. 5. Fácil ingreso de usuarios desconocidos y personal del ayuntamiento a la UTIC.

3.2.1.2.2.2 FODA Seguridad Física

El análisis FODA de seguridad física presenta un panorama detallado de las condiciones que influyen en la protección física del sitio. Se identifican fortalezas, como la presencia de personal de recepción y vigilancia, así como medidas de control de acceso. Sin embargo, se destacan debilidades críticas, como la falta de un período de acceso definido y la ausencia de políticas formales para gestionar incidentes de seguridad física. Las oportunidades, como el establecimiento de un programa de gestión de riesgos y la provisión de capacitación, ofrecen vías para mejorar la seguridad física en la unidad.

Tabla 19. FODA de Seguridad Física. Fuente: Elaboración propia.

FORTALEZAS	**DEBILIDADES**
1. Presencia de personal de recepción y vigilancia en todo el ayuntamiento. 2. Sitio completamente cerrado con bardas de más de 2 metros de altura. 3. Accesos controlados por lector de huella y por chip. 4. Identificación de acceso autorizado a través de un listado exclusivo del personal de la UTIC. 5. Medidas de seguridad en el cableado, como la separación de cables de energía y comunicaciones. 6. Clasificación y etiquetado de cables y equipos. 7. Realización de inventario del equipo bimestralmente. 8. Implementación de un sistema de protección de intrusos.	1. No se cierran con seguros los accesos cuando el sitio no está siendo utilizado en horario de trabajo. 2. Uso compartido de equipo de oficina como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos. 3. No se ha establecido un programa de capacitación de gestión de riesgos para identificar y evaluar los riesgos asociados a la seguridad física. 4. No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física. 5. No se realizan pruebas de seguridad física de forma periódica en el sitio.

Tabla 19 (continuación)

9. Revisiones semestrales de controles de seguridad, como cámaras y cerraduras. 10. Evaluaciones trimestrales de la seguridad física en la Unidad	6. Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas. 7. El monitoreo de las cámaras de videovigilancia internas no está a cargo de los empleados de la UTIC, si no del departamento “”
OPORTUNIDADES	**AMENAZAS**
1. Propuesta de asignación de encargado para cerrar debidamente la oficina una vez desocupada por completa aun en los horarios de comida. 2. Implementar un formato para el uso y manejo del equipo de oficina multifuncional que asegure un control sobre este. 3. Establecer políticas y procedimientos formales para la gestión de incidentes de seguridad física y documentar los incidentes ocurridos. 4. Propuesta de formato para el registro de la realización de pruebas de seguridad física de forma periódica en el sitio.	1. Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC. 2. Falta de equipo de vigilancia para el resguardo y protección del área y sus activos. 3. Robo a mano armada por parte de usuarios externos. 4. Terremotos, sismos o desastres naturales. 5. Mala instalación y/o mantenimiento de los circuitos eléctricos por parte de los trabajadores de la Comisión Federal de Electricidad (CFE). 6. Falta de mantenimiento y revisiones periódicas en los controles de seguridad física con los que cuenta la UTIC. 7. Revueltas civiles, incendios o acciones mal intencionadas

Tabla 19 (continuación)

	8. provocadas por usuarios externos. 9. Manipulación del Hardware (cambio en las configuraciones, registro de teclas o uso de contraseñas) para comprometer la funcionalidad de los sistemas de seguridad por parte de usuarios externos. 10. Vandalismo por parte de usuarios externos. 11. Mala instalación de las cámaras de seguridad por parte de los proveedores. 12. Implementación y configuración errónea del sistema de acceso al site por parte de los proveedores.

3.2.1.2.2.2.1 Conclusión

Para fortalecer la seguridad física, es fundamental aprovechar la presencia del personal de seguridad y las medidas de control de acceso ya implementadas, al mismo tiempo que se abordan las debilidades, como la falta de políticas formales. La implementación de un programa de gestión de riesgos, la realización de pruebas periódicas y la documentación de incidentes son estrategias cruciales. Al adoptar un enfoque proactivo en estas áreas, se puede elevar la seguridad física del sitio, reducir las amenazas y mejorar la capacidad de respuesta ante posibles incidentes.

.

3.2.1.2.2.3 FODA Seguridad Lógica

El análisis FODA de seguridad lógica revela una combinación de fortalezas, oportunidades, debilidades y amenazas que impactan directamente en la gestión de la seguridad de la información en el sitio en cuestión. Se destacan fortalezas significativas, como la implementación de medidas de autenticación de dos factores y la revisión periódica de privilegios de acceso. Sin embargo, la falta de seguimiento detallado de acciones, la ausencia de registros de auditoría y la carencia de un plan de respuesta a incidentes representan debilidades críticas que podrían comprometer la integridad de la seguridad lógica.

Tabla 20. FODA de Seguridad Lógica. Fuente: Elaboración propia

FORTALEZAS	DEBILIDADES
1. Implementación de autenticación de dos factores. 2. Revisión regular de privilegios de acceso y eliminación de los innecesarios o inactivos. 3. Realización de copias de seguridad mensuales. 4. Utilización de un sistema de cifrado para proteger datos sensibles. 5. Implementación de medidas de protección de datos, como firewalls y sistemas de detección y prevención de intrusiones. 6. Requerimiento de contraseña para acceder a los equipos del departamento. 7. Existencia de políticas y restricciones para la instalación de software adicional en los equipos.	1. No se siguen procedimientos para cambiar periódicamente las contraseñas. 2. No se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas. 3. No se realizan actualizaciones de seguridad de forma regular en sistemas operativos y aplicaciones. 4. Falta de capacitación regular a los usuarios sobre las mejores prácticas de seguridad informática y protección de datos. 5. Ausencia de copias de seguridad de sistemas y datos en un lugar externo seguro. 6. Las versiones de Software no son compatibles con las nuevas actualizaciones.

Tabla 20 (continuación)

	7. Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere. 8. Falta de copias de seguridad periódicas de los datos almacenados en los equipos.
OPORTUNIDADES	**AMENAZAS**
1. Proponer la mejora de la seguridad lógica a través de la implementación de contraseñas seguras y cambios periódicos. 2. Implementar un lineamiento donde los empleados se comprometan a capacitar a los usuarios nuevos o pasantes en actividades o prácticas de seguridad informática y protección de datos. 3. Establecer un lineamiento y un cronograma donde se especifique los periodos de tiempo en el que los empleados corroboren si existen actualizaciones de seguridad de forma regular en sus sistemas operativos y aplicaciones. 4. Implementar un registro de consulta de incidentes previos para abordar posibles brechas que se manifiesten.	1. Brechas de seguridad debido a la falta de seguimiento y registros cuando se materializa. 2. Acceso no autorizado debido a la ausencia de un sistema de control de acceso. 3. Ataques cibernéticos por parte de usuarios externos. 4. Interrupciones por cuestiones de índole natural que interrumpan las actualizaciones (fallos eléctricos, de los proveedores de internet y desastres naturales). 5. Los servidores que brindan las actualizaciones disponibles presentan errores para la descarga e instalación de estas. 6. Desastres naturales eliminando la información y datos que contiene la UTIC sin opción de recuperación. 7. No se revisa continuamente si hay infiltrados por parte de descargas no seguras.

Tabla 20 (continuación)

5. Propuesta de un escrito donde especifique los tiempos de salvaguardado de la información y los datos importantes que manejen dentro de la UTIC.	

3.2.1.2.2.3.1 Conclusión

Con el objetivo de fortalecer la seguridad lógica, es imperativo capitalizar las áreas de fortaleza, como la revisión de privilegios y la implementación de autenticación de dos factores, al tiempo que se abordan las debilidades críticas. La oportunidad de mejorar la concienciación del personal sobre prácticas de seguridad y la realización de pruebas de penetración periódicas se destacan como estrategias clave. La conciencia y acción proactiva en estas áreas pueden mitigar amenazas potenciales y elevar el nivel de seguridad lógica del entorno.

3.2.1.2.2.4 FODA Servicios de la UTIC

El siguiente análisis se enfoca principalmente en el uso y la disposición de los servicios con los que cuenta la Unidad de Tecnologías de la Información y Comunicación (UTIC) analizando los puntos fuertes de dichos servicios e identificando las áreas en las que podrían mejorar o bien los puntos críticos de los mismos.

Tabla 21. FODA de Servicios Fuente: Elaboración propia.

FORTALEZAS	DEBILIDADES
1. La UTIC cuenta con servicios varios para la realización de sus actividades internas (internet, eléctrico, aire acondicionado, medico, contra incendios y redes). 2. La red de WIFI con la que cuenta es de alta velocidad al tener un paquete de 250 Mb y permite que el desempeño dentro de la UTIC sea eficiente.	1. Los enchufes eléctricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos.
3. Cuentan con un sistema de aire acondicionado que mantiene el site a una temperatura adecuada. 4. La iluminación con la que cuenta la UTIC es la adecuada para el desarrollo de las actividades. 5. Cuenta con un Rack que está instalado correctamente y en condiciones físicas excelentes y con una temperatura adecuada.	2. Material inflamable debajo de los interruptores principales de la UTIC, es decir, el centro de carga (caja de fusibles y pastillas) que comprometen a una mayor propagación de incendio en caso de corto circuito. 3. Sobrecargas por parte del uso de extensiones saturadas de equipos conectados.

Tabla 21 (continuación)

6. Los extintores tienen señalamientos sobre cómo actuar en un incendio interino de acuerdo con el tipo de sustancia del que este compuesto.	4. Equipo médico interno (botiquín medico) compartido con otras áreas además de no estar al alcance de los empleados de la UTIC si ocurre un accidente. 5. Bloqueo de entrada y salida con activos situados en el piso o bien por mobiliario cruzado en el paso. 6. El área de alojamiento del botiquín cubre otro accidente o bien no se encuentran para atender otra emergencia en la UTIC al mismo tiempo. 7. Falta de sistema de enfriamiento adecuado en el lugar del trabajo (aire acondicionado) ya que se cuenta solo dentro del site. 8. Uso de un sistema de enfriamiento deficiente o bien que no cubra el espacio de trabajo de la UTIC en su totalidad. 9. No cuentan con todos los señalamientos de emergencia, por lo que no están al alcance de la vista de cualquier usuario.

Tabla 21 (continuación)

OPORTUNIDADES	AMENAZAS
1. Solicitud para la Implementación de un mayor número de contactos eléctricos por parte del departamento de servicio, para satisfacer de manera eficaz todos los equipos sin la necesidad de extensiones. 2. Implementación de un lineamiento donde los trabajadores se comprometan a mantener actualizado el servicio del botiquín médico para evitar irregularidades en caso de ser ocupado.	1. Altas temperaturas climáticas provocarían un mal funcionamiento de los equipos y desempeño de los empleados al no contar con aire acondicionado. 2. Emergencias Médicas en la UTIC debido a herramientas mal posicionadas, o bien en mal estado de trabajadores externos que puedan presentar comportamiento extraño (explosión, arrojamiento de líquidos, piezas rotas, etc.). 3. Reparaciones en la institución con herramientas industriales o equipo grande y pesado, además de personal externo trabajando de manera ruda. 4. Condiciones climatológicas poco favorables (piso mojado por lluvia, insolación, desmayos por golpes de calor). 5. Fallas en los transformadores durante temporadas con viento y lluvia las cuales provocan una sobrecarga y/o apagones.

Tabla 21 (continuación)

	6. Incidentes en instalaciones cercanas o bien en los departamentos o en las áreas colindantes. 7. Acciones mal intencionadas por parte de usuarios externos. 8. Mala ejecución de acciones cómo fumar o manejar herramientas de fuego en áreas no permitidas por parte de usuarios internos o externos.

3.2.1.2.2.4.1 Conclusión

En el análisis anterior se concluye que algunos de los servicios no son suficientes para satisfacer las necesidades de la UTIC, o bien para maximizar el desempeño que realizan los empleados por lo que es indispensable buscar soluciones o estrategias que puedan ayudar a resolver estas deficiencias para tener un nivel más optimo en la UTIC.

3.2.1.2.2.5 FODA Infraestructura de la UTIC

El análisis FODA es una herramienta estratégica vital para evaluar la situación actual de la UTIC que ayuda a complementar la Auditoría además de que permite desarrollar una comprensión clara de sus fortalezas, debilidades, oportunidades y amenazas. Este análisis proporciona una visión integral de la situación interna y externa de la UTIC, lo que permite tomar decisiones estratégicas sólidas, aprovechar las fortalezas existentes, abordar las debilidades y maximizar las oportunidades.

Tabla 22. FODA de Infraestructura. Fuente: Elaboración propia.

FORTALEZAS	**DEBILIDADES**
1. La ventilación dentro de la UTIC es buena al mantenerse activa durante la realización de las actividades 2. Cuenta con un Rack que está instalado correctamente y en condiciones físicas excelentes y con una temperatura adecuada. 3. El cableado del Rack está debidamente instalado ya que cuenta con canaletas fijadas a las paredes y el pinado es correcto 4. La UTIC cuenta con dispositivos de telecomunicaciones en excelente estado, estos son los siguientes, 9 switches debidamente instalados y funcionales además de contar con 6 en reserva para reemplazo en caso de incidentes, un Router configurado y funcional y 5 servidores instalados.	1. El etiquetado de los activos y mobiliario no se basa en un ordenamiento de fácil lectura para los usuarios. 2. El etiquetado no es visible al estar ubicado la mayoría de las veces debajo, atrás o en los laterales de los activos o bien no portarlo. 3. El etiquetado no muestra los datos importantes de los activos ni un número de identificación (ID). 4. Los escritorios usados dentro de la UTIC son grandes y ocupan espacio con el que no cuentan, por lo que los hace inadecuados. 5. Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.

Tabla 22 (continuación)

5. La UTIC cuenta con 6 equipos de cómputo en excelentes condiciones físicas 6. Los racks tienen soportes de los cables siempre fijos, etiquetados y cada cable que llega al patch panel está debidamente peinado y ordenado. 7. Cuentan con un proceso documentado y aprobado por superiores para la entrega de reposiciones de equipo o materiales dentro del mismo departamento o externos. 8. Cuentan con material de reposición hablando sobre los periféricos y cableado como lo son cables ethernet, cables de corriente, etc.	6. Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas. 7. Equipos enchufados y apagados sin ser utilizados provocan que los cables se crucen y exista confusión en el multi contacto. 8. Daño a los equipos por falta de espacio de movilidad para los usuarios mientras trasladan equipos reparados entre ellos o bien a otras áreas. 9. La UTIC cuenta con un techo falso visiblemente dañado por la instalación del cableado en el cuarto del Site.

Tabla 22 (continuación)

	10. Ausencia de una barrera en la entrada/salida de la UTIC para prevenir filtraciones de agua por parte de las tuberías que pasan frente al área de la UTIC. 11. No cuentan con reglas específicas para el uso de los routers, switches y servidores 12. Los routers, switches y servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rinda debidamente. 13. Daño al cableado sin protección por parte de la caída del techo falso dañado. 14. Presencia de plagas dentro de la UTIC que pongan en riesgo la condición del cableado de los equipos de telecomunicaciones además del mobiliario y los activos. 15. El mobiliario referente a los asientos 16. no son la mejor opción hablando de comodidad para los usuarios de la UTIC.

Tabla 22 (continuación)

	17. Datos incorrectos o mal llenado del vale de salida y entrega por parte de la UTIC lo que ocasiona que el reemplazo no se pueda efectuar. 18. Presencia de un techo falso y el paso del drenaje frente al área de la UTIC. 19. Falta de políticas y reglas dentro de la UTIC. 20. Falta de explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general.
OPORTUNIDADES	**AMENAZAS**
1. Una mejor ubicación y clasificación del etiquetado para respetar las reglas establecidas por el estándar ISO 27002.	1. La UTIC está expuesta a inundaciones o filtraciones de agua gracias al techo falso y al paso de drenaje frente al área. 2. Etiquetado inadecuado de activos y mobiliario nuevo o proveniente de otros departamentos y externos. 3. Programas o servicios que brinden activos nuevos a la UTIC no considerados en su registro del etiquetado.

Tabla 22 (continuación)

	4. Posibles accidentes debido a emergencias o desastres naturales, al no poder evacuar el sitio de manera eficiente a raíz de la falta de espacio por los escritorios. 5. Ingreso de activos en grandes cantidades en la UTIC por parte de proveedores externos y programas de gobierno saturando el poco espacio de trabajo. 6. Insuficiencia de contactos eléctricos y uso de extensiones inadecuadas provocando que usuarios externos tengan disposición de enchufe de sus aparatos electrónicos lo que en ocasiones resulta en sobrecargas eléctricas. 7. Incendios provocados por usuarios externos con intención de comprometer y dañar los equipos y las instalaciones. 8. Mal comportamiento por parte de usuarios prestadores de servicio social o prácticas profesionales. 9. Terremotos o sismos causantes de daño a la estructura de las instalaciones.

Tabla 22 (continuación)

	10. El drenaje que se presenta frente al área de la UTIC muestra visibles reparaciones a medias y notables filtraciones de agua 11. Personal de limpieza no capacitado para el correcto aseo de los dispositivos de comunicaciones y redes 12. Falta de mantenimiento regular para routers, switches y servidores por parte de los proveedores. 13. Personal nuevo por parte de los proveedores en capacitación o a prueba que puedan realizar configuraciones incorrectas. 14. Equipos y/o activos defectuosos o con fallas de fabricación por parte de los proveedores. 15. Datos incorrectos o mal llenado de la solicitud de reparación o cambio por parte del solicitante lo que ocasiona que el reemplazo no pueda ser efectuado.

3.2.1.2.2.5.1 Conclusión

En el anterior análisis FODA permite identificar las fortalezas y acerca de la infraestructura de la UTIC. Al examinar las fortalezas, se pudieron identificar los puntos de la UTIC que destacan, como su ventilación, los equipos de telecomunicaciones que están en excelente estado además de contar con equipos de repuesto, el cableado de estos dispositivos esta adecuadamente instalados ya que cuenta con canaletas fijadas a las paredes y el peinado es correcto. Por otro lado, al examinar las debilidades, se pudieron identificar la falta de

espacio para todos los empleados, el techo visiblemente dañado, la falta de más contactos eléctricos para no sobre cargar los que se tienen evitando un accidente. Así como oportunidades clave en mejorade mobiliario, contar con mayor número de accesos que permitan la ventilación natural del área y amenazas potenciales en inundaciones o filtraciones de agua y la falta de Políticas y reglas dentro de la UTIC. Esta evaluación interna proporciono una visión clara de la situación actual de la entidad.

3.2.1.2.2.6 FODA del Sistema de Inventario de la UTIC

El siguiente análisis se enfoca principalmente en el uso, funcionalidad y la disposición del sistema de inventario con el que cuenta actualmente la Unidad de Tecnologías de la Información y Comunicación (UTIC) analizando los puntos fuertes de dicho sistema e identificando las áreas en las que podrían mejorar o bien los puntos críticos del mismo.

Tabla 23. FODA del Sistema de Inventario. Fuente: Elaboración propia.

FORTALEZAS	DEBILIDADES
1. La UTIC cuenta con un sistema adecuado a sus necesidades en el que registran todos los activos con los que cuentan internamente. 2. El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC. 3. El inventario se mantiene actualizado constantemente. 4. El inventario con el que se cuenta no necesita ciertos requerimientos por parte del equipo de cómputo.	1. El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC. 2. El inventario con el que cuentan no está desarrollado en un sistema gestor de bases de datos. 3. No se realizan respaldos o copias de seguridad del inventario. 4. Todos los usuarios internos de la UTIC pueden editar la información dentro del inventario ya que no cuentan con roles ni privilegios de acuerdo con su puesto. 5. El inventario actual desarrollado en hojas de cálculo al pasar el tiempo se satura de información y provoca perdidas de la información.

Tabla 23 (continuación)

	6. Para la consulta de las distintas categorías de activos disponibles, deben acceder a diferentes archivos individuales para realizar consultas. 7. El inventario empleado actualmente no cuenta con seguridad ni rol de usuarios y contraseñas para acceder al mismo. 8. El sistema de inventario no cuenta con ninguna medida de seguridad. 9. Ausencia de usuarios y contraseñas para restringir el acceso a usuarios externos. 10. Falta de copias de seguridad y respaldos. 11. Eliminación de los archivos (hojas de cálculo) permanentemente por parte de los empleados por error. 12. El inventario usado actualmente no registra los movimientos efectuados, con hora, fecha, ni cuenta de quien lo realizo. 13. La eliminación de alguno de los archivos individuales usados para el inventario provoca un daño catastrófico al no tener los datos en otra parte.

Tabla 23 (continuación)

	14. Confusión de los archivos manejados al momento de una carga o partida de datos.
OPORTUNIDADES	**AMENAZAS**
1. Desarrollo de un inventario a través de un sistema gestor de bases de datos oficial que cuente con relaciones entre diferentes tablas. 2. Aplicar roles y privilegios para la consulta de información del inventario proponiendo así restricciones entre los empleados internos. 3. Implementar seguridad al acceso del inventario, proponiendo que el manejo de este solo sea por parte de los usuarios internos a través de nombres de usuarios registrados y contraseñas individuales. 4. Implementar un sistema en el que toda las categorías y activos se encuentren disponibles en el mismo sin necesidad de abrir archivos distintos.	1. Acceso no autorizado al sistema de inventario por parte del personal de limpieza, prestadores de servicio social y residencias o personal externo. 2. Secuestro de la información por parte de un ataque cibernético al no contar con ninguna medida de seguridad en el sistema. 3. Manipulación externa del sistema de inventario a través de un ataque cibernético. 4. Microsoft está en constante actualización lo que al no contar con respaldos puede provocar perdida de los archivos. 5. Pérdida total de los datos en el inventario debido a desastres naturales. 6. Modificación no autorizada de datos por parte de usuarios externos. 7. Pérdida de información en su inventario desarrollado en hojas calculo debido a la saturación o mal funcionamiento de Microsoft Excel.

Tabla 23 (continuación)

	8. Corrupción de un archivo al tratarse de un documento de hojas de cálculo, al no tener la misma versión instalada o simplemente por la ineficiencia del programa ante tanta información. 9. Ineficiencia en la consulta y actualización de activos provenientes de otros departamentos debido a la ineficiencia por la saturación de información de Microsoft Excel.

3.2.1.2.2.6.1 Conclusión

En el anterior análisis FODA permite identificar las fortalezas y acerca del sistema de inventario de la UTIC. Al examinar las fortalezas, se pudieron identificar los puntos de la UTIC que destacan, el ser un sistema adecuado a sus necesidades, además de que es un sistema de fácil acceso por parte de los usuarios, lo que de igual manera permite que este constantemente actualizado, otra de sus características favorables es que no necesita requerimientos especiales por parte de los equipos de cómputo lo que trae consigo que sea capaz de abrirse en cualquier equipo de cómputo siempre y cuando cuente con el programa.

3.2.1.3 Actividad 2.3 Realizar el Análisis de Riesgos

El siguiente análisis se centra en identificar la prioridad de atención utilizando la matriz de riesgos para evaluar los posibles riesgos asociados con cada uno de los puntos inspeccionados. Esta evaluación se basa en las debilidades y amenazas previamente identificadas en los análisis FODA y considera la opinión de los empleados internos de la UTIC. Los riesgos se clasifican de acuerdo con la matriz diseñada anteriormente y se ordenan según el impacto que pueden provocar, lo que revela la prioridad con la que se recomienda abordar cada uno de ellos.

3.2.1.3.1 Análisis de riesgos de la Seguridad Física de la UTIC

A continuación, se presenta el catálogo de los posibles riesgos que puede enfrentar la Unidad de Tecnologías de la Información y Comunicación (UTIC) en el ámbito de Seguridad Física. Este catálogo relaciona dichos riesgos con las vulnerabilidades y amenazas correspondientes, que aumentan la probabilidad de que se materialicen dichas situaciones.

Tabla 24. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Seguridad Física. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo
1.- Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC. 2.- Falta de equipo de vigilancia para el resguardo y protección del área y sus activos. 3.- Robo a mano armada por parte de usuarios externos.	1.- No se cierran con seguros los accesos cuando el sitio no está siendo utilizado. 2.- Uso compartido de equipo de oficina como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.	1.- Robo de información, equipos o activos por parte de usuarios externos.

Tabla 24 (continuación)

	3.- El monitoreo de las cámaras de videovigilancia internas no está a cargo de los empleados de la UTIC sino del departamento	
Amenaza	Vulnerabilidad	Riesgo
4.- Terremotos, sismos o desastres naturales. 5.- Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC. 6.- Mala instalación y/o mantenimiento de los circuitos eléctricos por parte de los trabajadores de la Comisión Federal de Electricidad (CFE). 7.- Falta de mantenimiento y revisiones periódicas en los controles de seguridad física con los que cuenta la UTIC. 8.- Revueltas Civiles, incendios o acciones mal intencionadas provocadas por usuarios externos.	4.- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física. 5.- Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas. 6.- No se realizan pruebas de seguridad física de forma periódica en el sitio.	2.- Daño en los equipos de cómputo, el inmobiliario y corto circuito en los enchufes eléctricos.

Tabla 24 (continuación)

9.- Vandalismo por parte de usuarios externos. 10.- Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC. 11.- Manipulación del Hardware (cambio en las configuraciones, registro de teclas o uso de contraseñas) para comprometer la funcionalidad de los sistemas de seguridad, por parte de usuarios externos.	7.- No se ha establecido un programa de capacitación de gestión de riesgos para identificar y evaluar los riesgos asociados a la seguridad física. 8.- No se cierran con seguros los accesos cuando el sitio no está siendo utilizado. 9.- Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas. 10.- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física.	3.- Intervenciones en los equipos, información, inmobiliario o departamento por parte de usuarios externos no deseados.

Tabla 24 (continuación)

Amenaza	Vulnerabilidad	Riesgo
12.- Falta de mantenimiento y revisiones periódicas en los controles de seguridad física con los que cuenta la UTIC. 13.- Fácil acceso no autorizado de usuarios externo y personal del ayuntamiento a la UTIC. 14.- Robo a mano armada por parte de usuarios externos.	11.- Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas. 12.- No se cierran con seguros los accesos cuando el sitio no está siendo utilizado.	4.- Acceso no deseado a los activos de la UTIC, manipulación de la información y los datos.
15.- Mala instalación de las cámaras de seguridad por parte de los proveedores. 16.- Falta de mantenimiento y revisiones periódicas en los controles de seguridad física con los que cuenta la UTIC. 17.- Implementación y configuración errónea del sistema de acceso al site por parte de los proveedores.	13.- No se realizan pruebas de seguridad física de forma periódica en el sitio. 14.- Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas. 15.- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física.	5.- Los controles de seguridad física implementados no funcionan correctamente, lo que ocasiona, robos, intrusiones, accesos no deseados.

3.2.1.3.1.1 Recopilación de la situación actual de la SEGURIDAD FÍSICA por parte de los empleados de la UTIC.

Las siguientes tablas muestran la valoración realizada por los empleados internos de la Unidad de Tecnologías de la Información y Comunicación (UTIC), considerando el punto de vista de los seis integrantes del área. En estas evaluaciones, se abordan criterios relacionados con su seguridad física, basándose en las vulnerabilidades y amenazas mencionadas anteriormente en el análisis FODA de seguridad física.

Dado que se trata de evaluaciones cualitativas, estas permiten conocer la percepción de los empleados internos, influenciada por diversos aspectos, como el tiempo al que se refieren al responder las preguntas, su estado de ánimo y la relación que mantienen con la empresa. Por lo tanto, no se puede afirmar que estas evaluaciones garanticen resultados completamente precisos. En función de los resultados obtenidos, se llevarán a cabo pruebas relacionadas con los puntos de interés, que incluyen seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario.

3.2.1.3.1.1.1 Vulnerabilidades consideradas

	Vulnerabilidad: No se cierran con seguros los accesos cuando el sitio no esta siendo utilizado en horarios de trabajo.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			1		5

Figura 7. Análisis de Riesgos, Seguridad Física Vulnerabilidad 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 1, 2023)

Vulnerabilidad: No se ha establecido un programa de capacitacion de gestion de riesgos para identificar y evaluar los riesgos asociados a la seguridad física.					
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			2	4	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 8. Análisis de Riesgos, Seguridad Física Vulnerabilidad 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 2, 2023)

Vulnerabilidad: No se han establecido politicas y procedimientos formales para la gestion de incidentes de seguridad física					
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	5			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 9. Análisis de Riesgos, Seguridad Física Vulnerabilidad 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 3, 2023)

Vulnerabilidad: No se realizan pruebas de seguridad fisica de forma periodica en el sitio					
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 10. Análisis de Riesgos, Seguridad Física Vulnerabilidad 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 4, 2023)

	Vulnerabilidad: Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periodicas				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	6				
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4	2		

Figura 11. Análisis de Riesgos, Seguridad Física Vulnerabilidad 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 5, 2023)

	Vulnerabilidad: El monitoreo de las camaras de videovigilancia internas no esta acargo de los empleados de la UTIC sino del departamento x				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				5	1
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 12. Análisis de Riesgos, Seguridad Física Vulnerabilidad 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 6, 2023)

	Vulnerabilidad: Uso compartido de equipo de oficina como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			1		5

Figura 13. Análisis de Riesgos, Seguridad Física Vulnerabilidad 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Vulnerabilidad 7, 2023)

3.2.1.3.1.1.2 Amenazas consideradas

	Amenaza: Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			1		5

Figura 14. Análisis de Riesgos, Seguridad Física Amenaza 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 1, 2023)

	Amenaza: Robo a mano armada por parte de usuarios externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			2	4	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 15. Análisis de Riesgos, Seguridad Física Amenaza 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 2, 2023)

	Amenaza: Revueltas Civiles, incendios o acciones mal intencionadas provocadas por usuarios externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	5			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 16. Análisis de Riesgos, Seguridad Física Amenaza 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 3, 2023)

	Amenaza: Falta de mantenimiento y revisiones periodicas en los controles de seguridad fisica con los que cuenta la UTIC.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 17. Análisis de Riesgos, Seguridad Física Amenaza 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 4, 2023)

	Amenaza: Mala instalación y/o mantenimiento de los circuitos eléctricos por parte de los trabajadores de la Comision Federal de Electricidad (CFE).				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	6				
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4	2		

Figura 18. Análisis de Riesgos, Seguridad Física Amenaza 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 5, 2023)

Nivel de Impacto / Probabilidad	Amenaza: Terremotos, sismos o desastres naturales.				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				5	1
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			6		

Figura 19. Análisis de Riesgos, Seguridad Física Amenaza 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 6, 2023)

Nivel de Impacto / Probabilidad	Amenaza: Falta de equipo de vigilancia para el resguardo y proteccion del area y sus activos				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	3	2	1		

Figura 20. Análisis de Riesgos, Seguridad Física Amenaza 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 7, 2023)

Nivel de Impacto / Probabilidad	Amenaza: Bandalismo por parte de usuarios externos				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		3	2	1	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		6			

Figura 21. Análisis de Riesgos, Seguridad Física Amenaza 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 8, 2023)

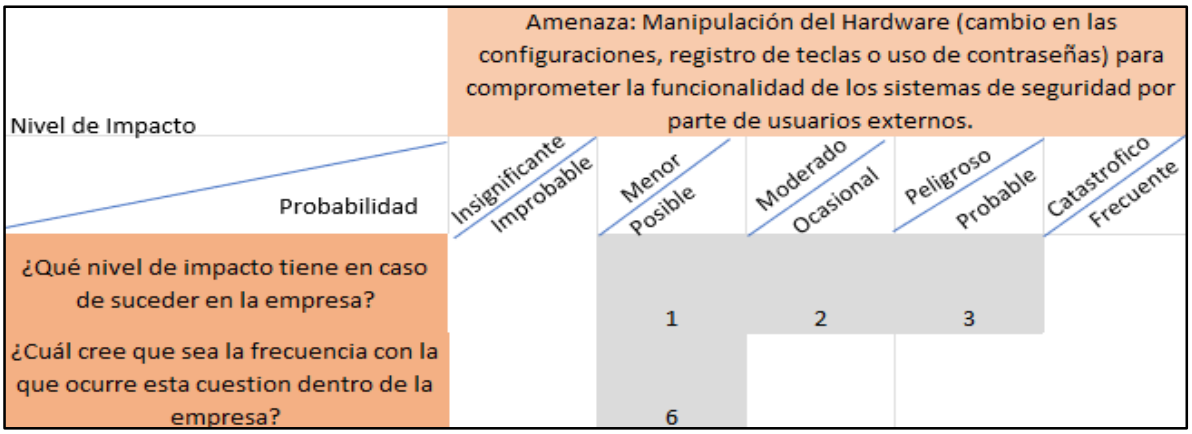


Figura 22. Análisis de Riesgos, Seguridad Física Amenaza 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 9, 2023)

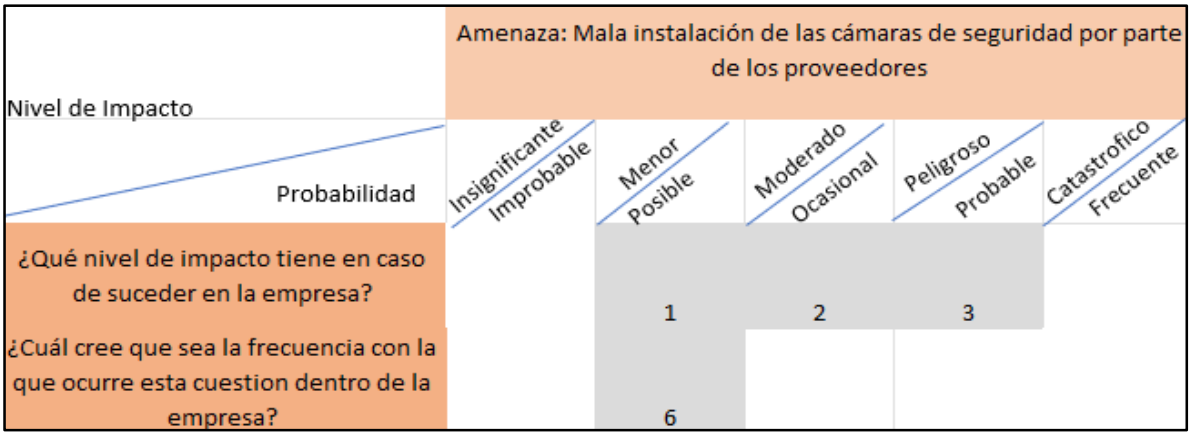


Figura 23. Análisis de Riesgos, Seguridad Física Amenaza 10. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 10, 2023)

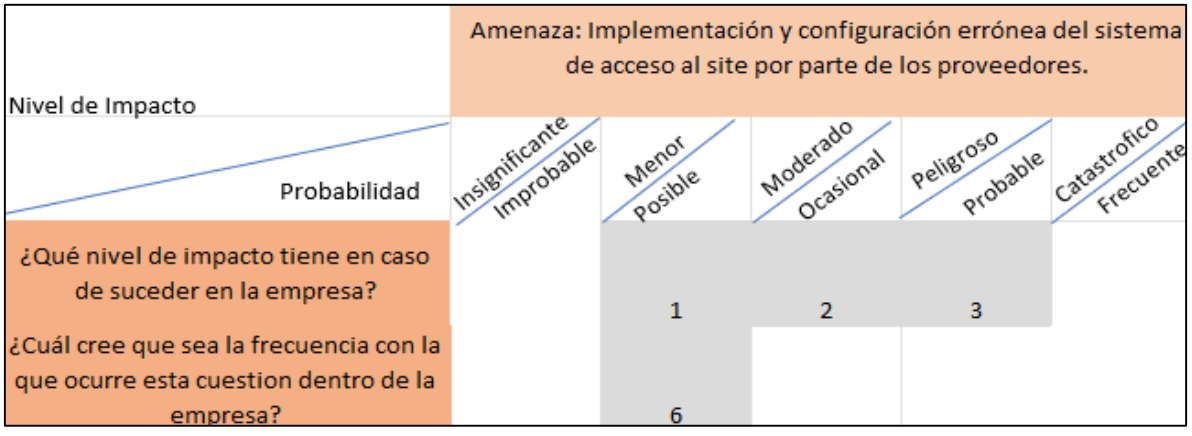


Figura 24. Análisis de Riesgos, Seguridad Física Amenaza 11. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Física Amenaza 11, 2023)

3.2.1.3.2 Análisis de riesgos de la Seguridad Lógica de la UTIC

A continuación, se presenta el catálogo de los posibles riesgos que puede enfrentar la Unidad de Tecnologías de la Información y Comunicación (UTIC) en el ámbito de Seguridad Lógica. Este catálogo relaciona los riesgos identificados con las vulnerabilidades y amenazas correspondientes, que aumentan la probabilidad de que se materialicen dichas situaciones.

Tabla 25. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Seguridad Lógica. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo
18.- Brechas de seguridad debido a la falta de seguimiento y registros cuando se materializa. 19.- Ataques cibernéticos por parte de usuarios externos. 20.- Los servidores que brindan las actualizaciones disponibles presentan errores para la descarga e instalación de estas. 21.- Acceso no autorizado debido a la ausencia de un sistema de control de acceso.	16.- No se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas. 17.- Falta de capacitación regular a los usuarios sobre las mejores prácticas de seguridad informática y protección de datos. 18.- Ausencia de copias de seguridad de sistemas y datos en un lugar externo seguro. 19.- No se siguen procedimientos para cambiar periódicamente las contraseñas.	6- Manipulación, alteración o secuestro de información y los datos por parte de usuarios externos o internos.

Tabla 25 (continuación)

Amenaza	Vulnerabilidad	Riesgo
22.- No se revisa continuamente si hay infiltrados por parte de descargas no seguras. 23.- Interrupciones por cuestiones de índole natural que interrumpan las actualizaciones (fallos eléctricos, de los proveedores de internet y desastres naturales). 24.- Los servidores que brindan las actualizaciones disponibles presentan errores para la descarga e instalación de las mismas.	20.- No se realizan actualizaciones de seguridad de forma regular en sistemas operativos y aplicaciones. 21.- Las versiones de software no son compatibles con las nuevas actualizaciones. 22.- Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere.	7.- Mal funcionamiento de los sistemas y aplicaciones al no contar con su versión más reciente.
25.- Ataques cibernéticos por parte de usuarios externos. 26.- Desastres naturales eliminando la información y datos que contiene la UTIC sin opción de recuperación. 27.- No se revisa continuamente si hay infiltrados por parte de descargas no seguras.	23.- No se siguen procedimientos para cambiar periódicamente las contraseñas. 24.- Ausencia de copias de seguridad de sistemas y datos en un lugar externo seguro. 25.- Falta de copias de seguridad periódicas de los datos almacenados en los equipos.	9.- Multas y sanciones formales gracias a irregularidades por parte de Auditores externos a la Unidad.

3.2.1.3.2.1 Recopilación de la situación actual sobre la SEGURIDAD LÓGICA por pare de los empleados de la UTIC

Las siguientes tablas muestran la valoración realizada por los empleados internos de la Unidad de Tecnologías de la Información y Comunicación (UTIC), considerando el punto de vista de los seis integrantes del área. En estas evaluaciones, se abordan criterios relacionados con la seguridad lógica, tomando como referencia las vulnerabilidades y amenazas señaladas previamente en el análisis FODA de seguridad lógica, ubicado en la página 90

3.2.1.3.2.1.1 Vulnerabilidades consideradas

	Vulnerabilidad: No se siguen procedimeintos para cambiar periodicamente las contraseñas				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			6		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 25. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 1, 2023)

	Vulnerabilidad: No se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	4	2			

Figura 26. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 2, 2023)

	Vulnerabilidad: No se realizan actualizaciones de seguridad de forma regular en sistemas operativos y aplicaciones				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	5	1			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	3	3			

Figura 27. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 3, 2023)

	Vulnerabilidad: Falta de capacitación regular a los usuarios sobre las mejores prácticas de seguridad informática y protección de				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	3		3		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 28. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 4, 2023)

	Vulnerabilidad: Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 29. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 5, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Las versiones de software no son compatibles con las nuevas actualizaciones .				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 30. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 6, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Ausencia de copias de seguridad de sistemas y datos en un lugar externo seguro.				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			6		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	6				

Figura 31. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 7, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Falta de copias de seguridad periodicas de los datos almacenados en los equipos.				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 32. Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 8, 2023)

3.2.1.3.2.1.2 Amenazas consideradas

	Amenaza: Brechas de seguridad debido a la falta de seguimiento y registros cuando se materializa				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			2	3	1
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 33. Análisis de Riesgos, Seguridad Lógica Amenaza 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 1, 2023)

	Amenaza: Ataques cibernéticos por parte de usuarios externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				4	2
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		1		5	

Figura 34. Análisis de Riesgos, Seguridad Lógica Amenaza 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 2, 2023).

	Amenaza: Acceso no autorizado debido a la ausencia de un sistema de control de acceso.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 35. Análisis de Riesgos, Seguridad Lógica Amenaza 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 3, 2023)

	Amenaza: Desastres naturales eliminando la información y datos que contiene la UTIC sin opción de recuperación.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				1	5
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	2	2	1	

Figura 36. Análisis de Riesgos, Seguridad Lógica Amenaza 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 4, 2023)

	Amenaza: Interrupciones por cuestiones de indole natural que interrumpan las actualizaciones (fallos electricos, de los proveedores de internet y desastres naturales)				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 37. Análisis de Riesgos, Seguridad Lógica Amenaza 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 5, 2023)

	Amenaza: No se revisa continuamente si hay infiltrados por parte de descargas no seguras.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	1	3		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	2	3		

Figura 38. Análisis de Riesgos, Seguridad Lógica Amenaza 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Seguridad Lógica Amenaza 6, 2023)

3.2.1.3.3 Análisis de riesgo de los Servicios de la UTIC

A continuación, se presenta el catálogo de los posibles riesgos que puede sufrir la UTIC relacionados al ámbito de sus Servicios, relacionando dichos riesgos con las vulnerabilidades y amenazas correspondientes que logran maximizar la probabilidad de que ocurra dicha situación.

Tabla 26. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Servicios. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo
28. Fallas en los transformadores durante temporadas con viento y lluvia las cuales provocan una sobre carga y/o apagones. 29.- Incidentes en instalaciones cercanas o bien en los departamentos o áreas colindantes. 30.- Acciones mal intencionadas por parte de usuarios externos. 31.- Mala ejecución de acciones como fumar, o manejar herramientas de fuego en áreas no permitidas por parte de usuarios internos y externos.	26. Los enchufes eléctricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos. 27.- Material inflamable debajo de los interruptores principales de la UTIC es decir el Centro de Carga (caja de fusibles y pastillas) que comprometen a una mayor propagación de incendio en caso de corto circuito. 28.- Sobrecargas por parte del uso de extensiones saturadas de equipos conectados.	10. Incendio

Tabla 26 (continuación)

32.- Emergencias Médicas en la UTIC debido a herramientas mal posicionadas, o bien en mal estado de trabajadores externos que puedan presentar comportamiento extraño (explosión, arrojamiento de líquidos, piezas rotas, Etc.). 33.- Reparaciones en la institución con herramientas industriales o equipo grande y pesado, además de personal externo trabajando de manera ruda. 34.- Condiciones climatológicas poco favorables (piso mojado por lluvia, insolación, desmayos por golpes de calor).	29.- Equipo médico interno (botiquín medico) es compartido con otras áreas además de no estar al alcance de los empleados de la UTIC si ocurre un accidente. 30.- Bloqueo de la entrada/salida con activos situados en el piso o bien por mobiliario cruzado en el paso. 31.- El área de alojamiento del botiquín, cubre otro accidente o bien no se encuentran para atender una emergencia en la UTIC al mismo tiempo.	11. Falta de acceso rápido y oportuno a los suministros y equipo médico en caso de accidentes o emergencias médicas en la UTIC.

Tabla 26 (continuación)

Amenaza	Vulnerabilidad	Riesgo
35. Altas temperaturas climáticas provocarían un mal funcionamiento de los equipos y desempeño de los empleados al no contar con aire acondicionado.	32. Falta de sistema de enfriamiento adecuado en el lugar del trabajo (aire acondicionado) ya que se cuenta solo dentro del site. 33.- Uso de un sistema de enfriamiento ineficiente o bien que no cubra el espacio de trabajo de la UTIC en su totalidad.	12. Cuando las temperaturas son extremadamente altas los empleados pueden experimentar dificultades para concentrarse, además el sobrecalentamiento de los equipos de cómputo puede provocar fallos y errores en el funcionamiento de estos, lo que podría resultar en una pérdida de datos, interrupción de los servicios o incluso daños permanentes a los dispositivos.
36. Accidentes por parte de usuarios externos por comportamiento erróneo al no contar con los señalamientos adecuados.	34. No cuentan con todos los señalamientos de emergencia, por lo que no están al alcance de la vista de cualquier usuario.	13. Incendios, terremotos, sismos, o emergencias que requieran el uso del botiquín médico.

3.2.1.3.3.1 Recopilación de la situación actual sobre los SERVICIOS por parte de los empleados de la UTIC.

Las siguientes tablas muestran la valoración por parte de los empleados internos de la UTIC, tomando como referencia el punto de vista de los 6 integrantes del área. en donde evalúan criterios relacionados con sus Servicios, (vulnerabilidades y amenazas mencionadas con anterioridad en el análisis FODA de Servicios ubicado en la página 93).

3.2.1.3.3.1.1 Vulnerabilidades consideradas

	Vulnerabilidad: Falta de sistema de enfriamiento adecuado en el lugar de trabajo (aire acondicionado) ya que se cuenta solo dentro del SAIT				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	3	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				4	2

Figura 39. Análisis de Riesgos, Servicios Vulnerabilidad 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 1, 2023)

	Vulnerabilidad: Los enchufes electricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 40. Análisis de Riesgos, Servicios Vulnerabilidad 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 2, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Equipo médico interno (botiquin medico) compartido con otras áreas además de no estar al alcance de los empleados de la UTIC si ocurre un accidente				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		4	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 41. Análisis de Riesgos, Servicios Vulnerabilidad 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 3, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Material flamable debajo de los interruptores principales de la UTIC, es decir, el centro de carga (caja de fusibles y pastillas) que comprometen a una mayor propagacion de incendio en caso de corto circuito				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 42. Análisis de Riesgos, Servicios Vulnerabilidad 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 4, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Sobrecargas por parte del uso de extensiones saturadas de equipos conectados				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	1	4	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		1	2	3	

Figura 43. Análisis de Riesgos, Servicios Vulnerabilidad 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 5, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Bloqueo de entrada y salida con activos situados en el piso o bien por moviliario cruzado en el paso				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	3	2	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			1	2	3

Figura 44. Análisis de Riesgos, Servicios Vulnerabilidad 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 6, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: El área de alojamineto del botiquin cubre otro accidente o bien no se encuentra para atender otra emergencia en la UTIC al mismo tiempo.				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			2	4	

Figura 45. Análisis de Riesgos, Servicios Vulnerabilidad 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 7, 2023)

	Vulnerabilidad: Uso de un sistema de enfriamiento deficiente o bien que no cubra el espacio de trabajo de la UTIC en su totalidad.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	3	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		1	2	3	

Figura 46. Análisis de Riesgos, Servicios Vulnerabilidad 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 8, 2023)

	Vulnerabilidad: No cuentan con todos los señalamientos de emergencia, por lo que no están al alcance de la vista de cualquier usuario.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	2	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 47. Análisis de Riesgos, Servicios Vulnerabilidad 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Vulnerabilidad 9, 2023)

3..2.1.3.3.1.2 Amenazas Consideradas

	Amenaza: Emergencias medicas en la UTIC debido a herramientas mal posicionadas, o bien en mal estado de trabajadores externos que puedan presentar comportamiento extraño (explosión, arrojamiento de liquidos, piezas rotas, etc.).				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			2	4	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4	2		

Figura 48. Análisis de Riesgos, Servicios Amenaza 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 1, 2023)

	Amenaza: Altas temperaturas climaticas provocarian un mal funcionamiento de los equipos y desempeño de los empleados al no contar con aire acondicionado.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 49. Análisis de Riesgos, Servicios Amenaza 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 2, 2023)

	Amenaza: Condiciones climatologicas poco favorables (piso mojado por lluevia, insolación, desmayos por golpes de calor)				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 50. Análisis de Riesgos, Servicios Amenaza 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 3, 2023)

	Amenaza: Reparaciones en la institución con herramientas industriales o equipo rande y pesado, además de personal externo trabjando de manera ruda.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 51. Análisis de Riesgos, Servicios Amenaza 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 4, 2023)

	Amenaza: Fallas en los transformadores durante temporadas con viento y lluvias las cuales provocan una sobre carga y/o apagones.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4		2	

Figura 52. Análisis de Riesgos, Servicios Amenaza 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 5, 2023)

	Amenaza: Incidentes en instalaciones cercanas o bien en los departamentos o en las áreas colindantes.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	2	2	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		1	2	3	

Figura 53. Análisis de Riesgos, Servicios Amenaza 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 6, 2023)

	Amenaza: Acciones mal intencionadas, por parte de usuarios externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 54. Análisis de Riesgos, Servicios Amenaza 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 7, 2023)

	Amenaza: Mala ejecución de acciones cómo fumar o manejar herramientas de fuego en áreas no permitidas por partde de usuarios internos o externos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 55. Análisis de Riesgos, Servicios Amenaza 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Servicios Amenaza 8, 2023)

3.2.1.3.4 Análisis de riesgo de los Infraestructura de la UTIC.

A continuación, se presenta el catálogo de los posibles riesgos que puede sufrir la UTIC relacionados al ámbito de su Infraestructura, relacionando dichos riesgos con las vulnerabilidades y amenazas correspondientes que logran maximizar la probabilidad de que ocurra dicha situación.

Tabla 27. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Infraestructura. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo
37.- Etiquetado inadecuado de activos y mobiliario nuevo o proveniente de otros departamentos y externos. 38.- Programas o servicios que brinden activos nuevos a la UTIC, no considerados en su registro del etiquetado.	35. El etiquetado de los activos y mobiliario no se basa en un ordenamiento de fácil lectura para los usuarios. 36.- El etiquetado no es visible al estar ubicado la mayoría de las veces debajo, atrás o en los laterales de los activos o bien no portarlo. 37.- El etiquetado no muestra los datos importantes de los activos ni un número de identificación (ID).	14.- Confusión en la identificación y ubicación de activos y dificultad en su gestión.

Tabla 27 (continuación)

39.- Posibles accidentes debido a emergencias o desastres naturales, al no poder evacuar el sitio de manera eficiente a raíz de la falta de espacio por los escritorios. 40.- Ingreso de activos en grandes cantidades a la UTIC por parte de proveedores externos y programas de gobierno, saturando el poco espacio de trabajo.	38.- Los escritorios usados dentro de la UTIC son grandes y ocupan espacio con el que no cuentan, por lo que los hace inadecuados. 39.- El mobiliario referente a los asientos no son la mejor opción hablando de comodidad y espacio para los usuarios de la UTIC. 40.- Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.	15. Limitación de espacio de trabajo y dificultad para llevar a cabo tareas adecuadamente.
Amenaza	Vulnerabilidad	Riesgo
41.- Insuficiencia de contactos eléctricos y uso de extensiones inadecuadas provocando que usuarios externos tengan disposición de enchufe de sus aparatos electrónicos lo que en ocasiones resulta en sobrecargas eléctricas.	41. Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas.	16. Sobrecarga eléctrica, cables cruzados, riesgo de incendio y daño a los equipos.

Tabla 27 (continuación)

42.- Incendios provocados por usuarios externos con intención de comprometer y dañar los equipos y las instalaciones. 43.- Mal comportamiento por parte de usuarios prestadores de servicio social o prácticas profesionales.	42.- Equipos enchufados y apagados sin ser utilizados provocan que los cables se crucen y exista confusión en el multi contacto. 43.- Daño a los equipos por la falta de espacio de movilidad para los usuarios mientras trasladan equipos reparados entre ellos o bien a otras áreas.	
44.- Terremotos o sismos causantes de daño en la estructura de las instalaciones. 45.- La UTIC está expuesto a inundaciones o filtraciones de agua gracias al techo falso y al paso del drenaje frente al área. 46.- El drenaje que se presenta frente al área de la UTIC muestra visibles reparaciones a medias y notables filtraciones de agua.	44.- La UTIC cuenta con un techo falso visiblemente dañado por la instalación del cableado en el cuarto del site. 45.- Presencia de un techo falso y el paso del drenaje frente al área de la UTIC. 46.- Ausencia de una barrera en la entrada/salida de la UTIC para prevenir filtraciones de agua por parte de las tuberías que pasan frente al área de la UTIC.	17.- Caída de objetos, filtraciones de agua y daño a los equipos.

Tabla 27 (continuación)

Amenaza	Vulnerabilidad	Riesgo
47.- Personal nuevo por parte de los proveedores en capacitación o a prueba que pueda realizar configuraciones incorrectas. 48.- Personal de limpieza no capacitado para el correcto aseo de los dispositivos de comunicaciones y redes.	47.- No cuentan con reglas específicas para el uso de los routers, switches y servidores. 48.- Los routers, switches y servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rinda debidamente.	18. Configuraciones incorrectas, vulnerabilidades de seguridad y mal funcionamiento de redes.
49.- Falta de mantenimiento regular para routers, switches y servidores por parte de los proveedores. 50.- Personal nuevo por parte de los proveedores en capacitación o a prueba que pueda realizar configuraciones incorrectas.	49.- Los routers, switches y servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rinda debidamente. 50.- Daño al cableado sin protección por parte de la caída del techo falso dañado. 51.- Presencia de plagas dentro de la UTIC que pongan en riesgo la condición del cableado y los equipos de telecomunicaciones además del mobiliario y los activos.	19. Riesgo de fallas, mal rendimiento, interrupción de servicios y vulnerabilidades de seguridad.

Tabla 27 (continuación)

Amenaza	Vulnerabilidad	Riesgo
51.- Equipos y/o activos defectuosos o con fallas de fabricación por parte de los proveedores. 52.- Datos incorrectos o mal llenado de la solicitud de reparación o cambio por parte del solicitante lo que ocasiona que el reemplazo no pueda ser efectuado.	52.- El material de reposición hablando de periféricos y cableado es bastante escaso, por lo que su cuidado debe ser mayor para asegura su periodo de vida. 53.- Datos incorrectos o mal llenado del vale de salida y entrega por parte de la UTIC lo que ocasiona que el reemplazo no se pueda efectuar.	20. Dificultad para reemplazar equipos defectuosos o dañados y posibles interrupciones del servicio.
53.- Personal de limpieza no capacitado para el correcto aseo de los dispositivos y mobiliario. 54.- Mal comportamiento por parte de usuarios prestadores de servicio social o prácticas profesionales.	54.- La falta de políticas y reglas dentro de la UTIC. 55.- Falta de explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general.	21. Utilización inadecuada de los recursos, daño o deterioro del mobiliario, y dificultad en el uso adecuado de las instalaciones.

3.2.1.3.4.1 Recopilación de la situación actual sobre los INFRAESTRUCTURA por parte de los empleados de la UTIC

Las siguientes tablas muestran la valoración por parte de los empleados internos de la UTIC, tomando como referencia el punto de vista de los 6 integrantes del área. en donde evalúan criterios relacionados con su Infraestructura, (vulnerabilidades y amenazas mencionadas con anterioridad en el análisis FODA de Infraestructura ubicado en la página 97).

3.2.1.3.4.1.1 Vulnerabilidades consideradas

	Vulnerabilidad: El etiquetado de los activos y mobiliario no se basa en un ordenamiento de fácil lectura para los usuarios.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				4	2
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 56. Análisis de Riesgos, Infraestructura Vulnerabilidad 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 1, 2023)

	Vulnerabilidad: Los escritorios usados dentro de la UTIC son grandes y ocupan espacio con el que no cuentan, por lo que los hace inadecuados				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?					6
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 57. Análisis de Riesgos, Infraestructura Vulnerabilidad 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 2, 2023)

	Vulnerabilidad: Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	1	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			2		4

Figura 58. Análisis de Riesgos, Infraestructura Vulnerabilidad 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 3, 2023)

	Vulnerabilidad: La UTIC cuenta con un techo falso visiblemente dañado por la instalación del cableado en el cuarto del SITE.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	1	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 59. Análisis de Riesgos, Infraestructura Vulnerabilidad 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 4, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: No cuentan con reglas específicas para el uso de los routers, switches y servidores.				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1		5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				2	4

Figura 60. Análisis de Riesgos, Infraestructura Vulnerabilidad 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 5, 2023)

Nivel de Impacto / Probabilidad	Vulnerabilidad: Los routers, switches y servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rindan debidamente				
	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1		5
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 61. Análisis de Riesgos, Infraestructura Vulnerabilidad 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 6, 2023)

	Vulnerabilidad: El mobiliario referante a los asientos no son la mejor opción hablando de comodidad para los usuarios de la UTIC.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		5	1		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 62. Análisis de Riesgos, Infraestructura Vulnerabilidad 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 7, 2023)

	Vulnerabilidad: Presencia de un techo falso y el paso del drenaje frente al área de la UTIC				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		6			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			2	4	

Figura 63. Análisis de Riesgos, Infraestructura Vulnerabilidad 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 8, 2023)

	Vulnerabilidad: Falta de políticas y reglas dentro de la UTIC				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	4			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 64. Análisis de Riesgos, Infraestructura Vulnerabilidad 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 9, 2023)

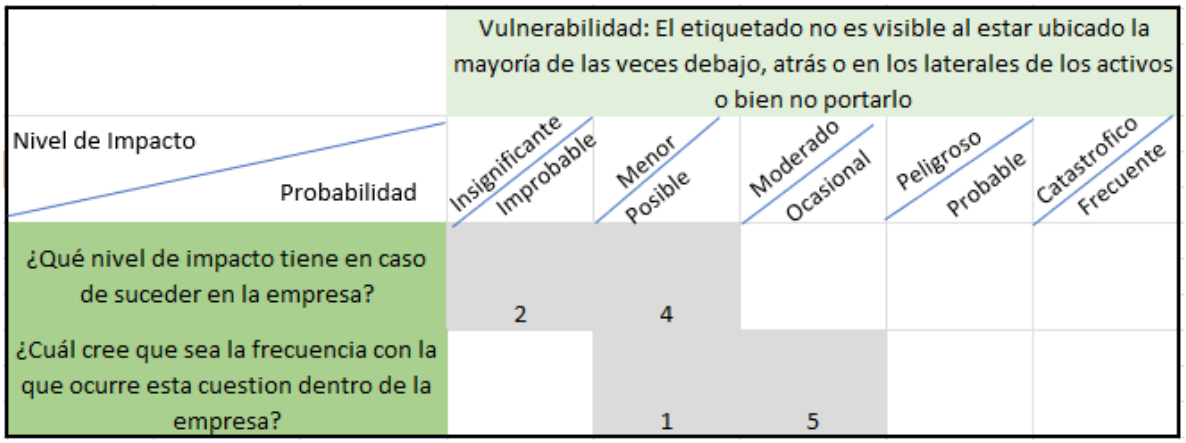


Figura 65. Análisis de Riesgos, Infraestructura Vulnerabilidad 10. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 10, 2023)

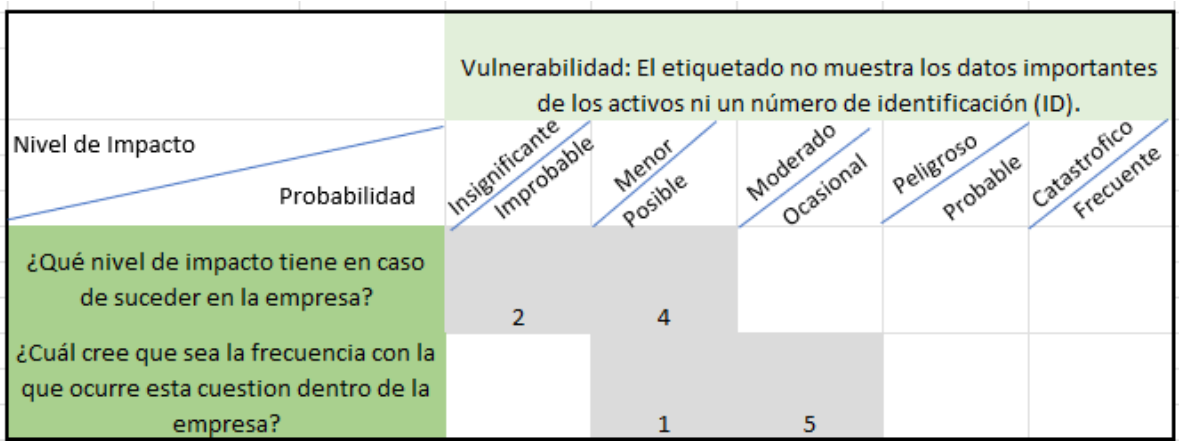


Figura 66. Análisis de Riesgos, Infraestructura Vulnerabilidad 11. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 11, 2023)

	Vulnerabilidad: Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	4			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				1	5

Figura 67. Análisis de Riesgos, Infraestructura Vulnerabilidad 12. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 12, 2023)

	Vulnerabilidad: Equipos enchufados y apagados sin ser utilizados, provocan que los cables se crucen y exista confusión en el multi contacto.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		4	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				1	5

Figura 68. Análisis de Riesgos, Infraestructura Vulnerabilidad 13. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 13, 2023)

	Vulnerabilidad: Daño a los equipos por falta de espacio de movilidad para los usuarios mientras rasladas equipos reparados entre ellos o bien a otras áreas.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			2	4	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			1	5	

Figura 69. Análisis de Riesgos, Infraestructura Vulnerabilidad 14. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 14, 2023)

	Vulnerabilidad: Ausencia de una barrera en la entrada/salida de la UTIC para prevenir filtraciones de agua por partde las tuberías que pasan frente al área de la UTIC				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	5		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	3	2		1	

Figura 70. Análisis de Riesgos, Infraestructura Vulnerabilidad 15. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 15, 2023)

	Vulnerabilidad: Daño al cableado sin protección por parte de la caída del techo falso dañado.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	4			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	5	1			

Figura 71. Análisis de Riesgos, Infraestructura Vulnerabilidad 16. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 16, 2023)

	Vulnerabilidad: Presencia de plagas dentro de la UTIC que pongan en riesgo la condición del cableado de los equipos de telecomunicaciones además del moiliario y los activos.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				5	1
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	5			

Figura 72. Análisis de Riesgos, Infraestructura Vulnerabilidad 17. Fuente: Elaboración propia. (propia, Análisis de Riesgos, Infraestructura Vulnerabilidad 17, 2023)

	Vulnerabilidad: Datos incorrectos o mal llenado del vale de salida y entrega por parte de la UTIC lo que ocasiona que el reemplazo no se pueda efectuar.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		4	2		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				2	4

Figura 73. Análisis de Riesgos, Infraestructura Vulnerabilidad 18. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Vulnerabilidad 18, 2023)

3.2.1.3.4.1.2 Amenazas Consideradas

	Amenaza: La UTIC está expuesta a inundaciones o filtraciones de agua gracias al techo falso y al paso del drenaje frente al área				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		6			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			2	4	

Figura 74. Análisis de Riesgos, Infraestructura Amenaza 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 1, 2023)

	Amenaza: Etiquetado inadecuado de activos y mobiliario nuevo o proviniente de otros departamentos y externos				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	4		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 75. Análisis de Riesgos, Infraestructura Amenaza 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 2, 2023)

	Amenaza: Posibles accidentes debido a emergencias o desastres naturales, al no poder evacuar el sitio de manera eficiente a raíz de la falta de espacio por los escritorios.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			6		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		5	1		

Figura 76. Análisis de Riesgos, Infraestructura Amenaza 3. Fuente: Elaboración propia. (propia, Análisis de Riesgos, Infraestructura Amenaza 3, 2023)

	Amenaza: Insuficiencia de contactos eléctricos y uso de extensiones inadecuadas provocando que usuarios externos tengan disposición de enchufe de sus aparatos electrónicos lo que en ocasiones resulta en sobrecargas eléctricas.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 77. Análisis de Riesgos, Infraestructura Amenaza 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 4, 2023)

	Amenaza: Terremotos o sismos causantes de daño a la estructura de las instalaciones.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				4	2
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		6			

Figura 78. Análisis de Riesgos, Infraestructura Amenaza 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 5, 2023)

	Amenaza: Falta de mantenimiento regular para routers, switches y servidores, por parte de los proveedores.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	4		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 79. Análisis de Riesgos, Infraestructura Amenaza 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 6, 2023)

	Amenaza: programas o servicios que brinden activos nuevos a la UTIC no considerados en su registro del etiquetdado.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		6			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				1	5

Figura 80. Análisis de Riesgos, Infraestructura Amenaza 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 7, 2023)

	Amenaza: Ingreso de activos en grandes cantidades en la UTIC por partde de proveedores externos y progamas de gobierno saturando el poco espacio de trabajo.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		6			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				1	5

Figura 81. Análisis de Riesgos, Infraestructura Amenaza 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 8, 2023)

	Amenaza: Equipos y/o activos defectuosos o con fallas de fabricación por parte de los proveedores.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	4	2			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4		2	

Figura 82. Análisis de Riesgos, Infraestructura Amenaza 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 9, 2023)

	Amenaza: Incendios provocados por usuarios externos con intención de comprometer y dañar los equipos y las instalaciones.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4		2	

Figura 83. Análisis de Riesgos, Infraestructura Amenaza 10. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 10, 2023)

	Amenaza: El drenaje que se presenta frente al área de la UTIC muestra visibles reparaciones a medias y notables filtraciones de agua				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		2	4		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2		4	

Figura 84. Análisis de Riesgos, Infraestructura Amenaza 11. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 11, 2023)

	Amenaza: Personal de limpieza no capacitado para el correcto aseo de los dispositivos de comunicaciones y redes.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2		4	

Figura 85. Análisis de Riesgos, Infraestructura Amenaza 12. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 12, 2023)

	Amenaza: Personal nuevo por parte de los poveedores en capacitacón o a prueba que puedan realizar configuraciones incorrectas.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	2	3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	3		2	

Figura 86. Análisis de Riesgos, Infraestructura Amenaza 13. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 13, 2023)

	Amenaza: Datos incorrectos o mal llenados en la solicitud de reparación o cambio por parte de otras áreas ocasiona que el reemplazo no pueda se efectuado.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	6				
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				5	1

Figura 87. Análisis de Riesgos, Infraestructura Amenaza 14. Fuente: Elaboración propia (propia., Análisis de Riesgos, Infraestructura Amenaza 14, 2023).

	Amenaza: Mal comportamiento por parte de usuarios prestadores de servicio social o prácticas profesionales.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	4	2			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		3	2	1	

Figura 88. Análisis de Riesgos, Infraestructura Amenaza 15. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Infraestructura Amenaza 15, 2023)

3.2.1.3.5 Análisis de riesgo del Sistema de Inventario de la UTIC

A continuación, se presenta el catálogo de los posibles riesgos que puede sufrir la UTIC relacionados al ámbito de su sistema de Inventario, relacionando dichos riesgos con las vulnerabilidades y amenazas correspondientes que logran maximizar la probabilidad de que ocurra dicha situación.

Tabla 28. Catálogo de Riesgos, Amenazas y Vulnerabilidades de Inventario. Fuente: Elaboración propia.

Amenaza	Vulnerabilidad	Riesgo
55.- Acceso no autorizado al sistema de inventario por parte del personal de limpieza, prestadores de servicio social y residencias o personal externo. 56.- Secuestro de la información por parte de algún ataque cibernético al no contar con ninguna medida de seguridad en el sistema.	56.- El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC. 57.- El sistema no cuenta con ninguna medida de seguridad. 58.- Ausencia de usuarios y contraseñas para restringir el acceso a usuarios externos	22. Pérdida o robo de información confidencial y manipulación no autorizada de datos.

Tabla 28 (continuación)

57.- Manipulación externa del sistema de inventario a través de un ataque cibernético. 58.- Microsoft está en constante actualización lo que al no contar con respaldos puede provocar perdida de los archivos.	59.- El inventario con el que cuentan no está desarrollado en un sistema gestor de bases de datos. 60.- El inventario actual desarrollado en hojas de cálculo al pasar el tiempo se satura de información y provoca perdidas de la información.	23. Pérdida de datos debido a errores, fallos o corrupción del sistema.
59.- Secuestro de la información por parte de algún ataque cibernético al no contar con ninguna medida de seguridad en el sistema. 60.- Perdida total de los datos en el inventario debido a desastres naturales.	61.- No se realizan respaldos o copias de seguridad del inventario. 62.- Eliminación de los archivos (hojas de cálculo) permanentemente por parte de los empleados por error.	24. Pérdida irreversible de datos en caso de fallos de hardware, errores humanos o desastres.

Tabla 28 (continuación)

Amenaza	Vulnerabilidad	Riesgo
61.- Modificación no autorizada de datos por parte de usuarios externos. 62.- Secuestro de la información por parte de algún ataque cibernético al no contar con ninguna medida de seguridad en el sistema.	63. Todos los usuarios internos de la UTIC pueden editar la información dentro del inventario ya que no cuentan con roles ni privilegios de acuerdo con su puesto. 64.- El inventario empleado actualmente no cuenta con seguridad alguna, rol de usuarios ni contraseñas para acceder al mismo. 65.-El inventario usado actualmente no registra los movimientos efectuados, con hora, fecha ni cuenta de quien los realizo.	25. Manipulación maliciosa o alteración no autorizada de datos críticos.

Tabla 28 (continuación)

63.- Pérdida de información en su inventario desarrollado en hojas calculo debido a la saturación o mal funcionamiento de Microsoft Excel. 64.- Corrupción del archivo al tratarse de un documento de hojas de cálculo, al no tener la misma versión instalada o simplemente por la ineficiencia del programa ante tanta información. 65.- Perdida total de los datos en el inventario debido a desastres naturales.	66.- El inventario actual desarrollado en hojas de cálculo al pasar el tiempo se satura de información y provoca perdidas de la información. 67.- No se realizan respaldos o copias de seguridad del inventario usado actualmente.	26. Pérdida de datos y dificultades en la gestión y recuperación de la información.

Tabla 28 (continuación)

66.- Ineficiencia en la consulta y actualización de activos provenientes de otros departamentos debido la ineficiencia por la saturación de información de Microsoft Excel. 67.- Corrupción del archivo al tratarse de un documento de hojas de cálculo, al no tener la misma versión instalada o simplemente por la ineficiencia del programa ante tanta información.	68. Para la consulta de las distintas categorías de activos disponibles, deben acceder a diferentes archivos individuales para realizar consultas. 69.- La eliminación de alguno de los archivos individuales usados para el inventario, provoca un daño catastrófico al no tener los datos en otra parte. 70.- Confusión de los archivos manejados al momento de una carga o partida de datos. 71. Falta de copias de seguridad y respaldos.	27. Dificultad y demora en la consulta de información, lo cual afecta la eficiencia y productividad.

3.2.1.3.5.1 Recopilación de la situación actual sobre el sistema de INVENTARIO por parte de los empleados de la UTIC.

Las siguientes tablas muestran la valoración por parte de los empleados internos de la UTIC, tomando como referencia el punto de vista de los 6 integrantes del área. en donde evalúan criterios relacionados con su sistema de Inventario, (vulnerabilidades y amenazas mencionadas con anterioridad en el análisis FODA del Sistema Inventario ubicado en la (pág. 103).

3.2.1.3.5.1.1 Vulnerabilidades consideradas

	Vulnerabilidad: El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?					6
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 89. Análisis de Riesgos, Inventario Vulnerabilidad 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 1, 2023)

	Vulnerabilidad: El inventario con el que cuentan no está desarrollado en un sistema gestor de base de datos				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			4	2	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 90. Análisis de Riesgos, Inventario Vulnerabilidad 2. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 2, 2023)

	Vulnerabilidad: No se realizan respaldos o copias de seguridad del inventario.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?			2	4	

Figura 91. Análisis de Riesgos, Inventario Vulnerabilidad 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 3, 2023)

	Vulnerabilidad: Todos los usuarios internos de la UTIC pueden editar la información dentro del inventario ya que no cuentan con roles ni privilegios de acuerdo con su puesto				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		5	1		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 92. Análisis de Riesgos, Inventario Vulnerabilidad 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 4, 2023)

	Vulnerabilidad: El inventario actual desarrollado en hojas de cálculo al pasar el tiempo se satura de información y provoca perdidas de la información				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	5			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?				6	

Figura 93. Análisis de Riesgos, Inventario Vulnerabilidad 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 5, 2023)

	Vulnerabilidad: Para la consulta de las distintas categorías de activos disponibles, deben acceder a diferentes archivos individuales para realizar consultas				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			6		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 94. Análisis de Riesgos, Inventario Vulnerabilidad 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 6, 2023)

	Vulnerabilidad: El inventario empleado actualmente no cuenta con seguridad ni rol de usuarios y contraseñas para acceder al mismo				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	3	1		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 95. Análisis de Riesgos, Inventario Vulnerabilidad 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 7, 2023)

	Vulnerabilidad: El sistema no cuenta con ninguna medida de seguridad				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	2	4			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 96. Análisis de Riesgos, Inventario Vulnerabilidad 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 8, 2023)

	Vulnerabilidad: Ausencia de usuarios y contraseñas para restringir el acceso a usuarios externos				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	5		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 97. Análisis de Riesgos, Inventario Vulnerabilidad 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 9, 2023)

	Vulnerabilidad: Falta de copias de seguridad y respaldos				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	5			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 98. Análisis de Riesgos, Inventario Vulnerabilidad 10. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 10, 2023)

	Vulnerabilidad: Eliminación de los archivos (hojas de cálculo) permanentemente por parte de los empleados por error.				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	2		3	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		4		2	

Figura 99. Análisis de Riesgos, Inventario Vulnerabilidad 11. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 11, 2023)

	Vulnerabilidad: El inventario usado actualmente no registra los movimientos efectuados, con hora, fecha, ni cuanta de quien lo realizo				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	2	3		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 100. Análisis de Riesgos, Inventario Vulnerabilidad 12. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 12, 2023)

	Vulnerabilidad: La eliminación de alguno de los archivos individuales usados para el inventario provoca un daño catastrófico al no tener los datos en otra parte				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	1			4
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2		4	

Figura 101. Análisis de Riesgos, Inventario Vulnerabilidad 13. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 13, 2023)

	Vulnerabilidad: Confusión de los archivos manejados al momento de una carga o partida de datos				
Nivel de Impacto / Probabilidad	Insignificante / Improbable	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	5			
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?					6

Figura 102. Análisis de Riesgos, Inventario Vulnerabilidad 14. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Vulnerabilidad 14, 2023)

3.2.1.3.5.1.2 Amenazas Consideradas

	Amenaza: Secuestro de la información por partde de un ataque cibernético al no contar con alguna medida de seguridad en el sistema.				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				2	4
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		6			

Figura 103. Análisis de Riesgos, Inventario Amenaza 1. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 1, 2023)

	Amenaza: Manipulación externa del sistema de inventario a través de un ataque cibernético				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?			1	5	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	5			

Figura 104. Análisis de Riesgos, Inventario Amenaza 2. Fuente: Elaboración* propia*. (propia., Análisis de Riesgos, Inventario Amenaza 2, 2023)

	Amenaza: Perdida total de los datos en el inventario debido a desastres naturales.				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 105. Análisis de Riesgos, Inventario Amenaza 3. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 3, 2023)

	Amenaza:Acceso no autorizado al sistema de inventario por parte del personal de limpieza, prestadores de servicio social y residencias o personal externos				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?		1	5		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	2	4			

Figura 106. Análisis de Riesgos, Inventario Amenaza 4. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 4, 2023)

	Amenaza: Modificación no autorizada de datos por parte de usuarios externos				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		6			

Figura 107. Análisis de Riesgos, Inventario Amenaza 5. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 5, 2023)

	Amenaza: Perdida de información en su inventario desarrollado en hojas de cálculo debido a la saturación o mal funcionamiento de Microsoft excel				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		6			

Figura 108. Análisis de Riesgos, Inventario Amenaza 6. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 6, 2023)

	Amenaza: Ineficiencia en la consulta y actualización de activos provenientes de otros departamentos debido a archivos individuales				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?	1	2	3		
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?		2	4		

Figura 109. Análisis de Riesgos, Inventario Amenaza 7. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 7, 2023)

	Amenaza: Microsoft está en constante actualización lo que al no contar con respaldos puede provocar perdida de los archivos				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	5			

Figura 110. Análisis de Riesgos, Inventario Amenaza 8. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 8, 2023)

	Amenaza: Corrupción de un archivo al tratarse de un documento de hojas de cálculo, al no tener la misma versión instalada o simplemente por la ineficiencia del programa ante tanta información.				
Nivel de Impacto / Probabilidad	Insignificante / Improbabl	Menor / Posible	Moderado / Ocasional	Peligroso / Probable	Catastrofico / Frecuente
¿Qué nivel de impacto tiene en caso de suceder en la empresa?				6	
¿Cuál cree que sea la frecuencia con la que ocurre esta cuestion dentro de la empresa?	1	5			

Figura 111. Análisis de Riesgos, Inventario Amenaza 9. Fuente: Elaboración propia. (propia., Análisis de Riesgos, Inventario Amenaza 9, 2023)

3.2.1.3.6 Clasificación de atención de acuerdo con las vulnerabilidades.

Con base en las evaluaciones cualitativas y en los catálogos de riesgos, amenazas y vulnerabilidades, se presenta la siguiente tabla. Esta tabla clasifica las vulnerabilidades identificadas según el nivel de prioridad recomendado para su atención, basado en los niveles: **MUY ALTA, ALTA, MEDIA y BAJA**. Cada nivel está organizado por los temas de interés correspondientes (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura e Inventario), y se respeta el sistema de colores de la matriz de riesgos mencionada previamente. Cabe destacar que la ponderación y clasificación utilizada en esta tabla provienen del formato establecido, ubicado en la página 50.

Tabla 29. Catálogo de Clasificación de atención de Seguridad Física. Fuente: Elaboración propia.

Seguridad Física	
Vulnerabilidad	**Conclusión**
|1.- No se cierran con seguros los accesos cuando el sitio no está siendo utilizado en horarios de trabajo.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 5 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 3 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 5 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 5 **Operación: 5*4= 20**
Vulnerabilidad	**Conclusión**
2.- El monitoreo de las cámaras de video vigilancia internas no está a cargo de los empleados de la UTIC sino del departamento x .	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 5 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 5 **Operación: 5*4= 20**
Vulnerabilidad	**Conclusión**
3.- Uso compartido de equipo de oficina como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados, es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 5 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 3 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 5 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 5 **Operación: 5*4= 20**
Vulnerabilidad	**Conclusión**
4.- No se realizan pruebas de seguridad física de forma periódica en el sitio.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Ocasional** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 6 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Ocasional (contiene el valor de 3 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 3 **Operación: 4*3= 12**
Vulnerabilidad	**Conclusión**
5.- Fallas en el funcionamiento de los controles de seguridad implementados debido a la falta de revisiones periódicas.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Insignificante** y 4 de los mismos respondieron en la probabilidad que resulta **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de Riesgos, ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 6 respuestas Insignificante (contiene el valor de 1 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 1 Valor de Probabilidad: 2 **Operación: 1*2= 2**
Vulnerabilidad	**Conclusión**
6.- No se ha establecido un programa de capacitación de gestión de riesgos para identificar y evaluar los riesgos asociados a la seguridad física.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 4 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Improbable (contiene el valor de 1 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 1 **Operación: 4*1= 4**
Vulnerabilidad	**Conclusión**
7.- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 6 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X.

Tabla 29 (continuación)

	6 empleados= 100% **Nivel de impacto:** 5 respuestas Menor (contiene el valor de 2 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Improbable (contiene el valor de 1 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 2 Valor de Probabilidad: 1 **Operación: 2*1= 2**

Tabla 30. Catálogo de Clasificación de atención de Seguridad Lógica. Fuente: Elaboración propia.

Seguridad Lógica	
Vulnerabilidad	**Conclusión**
1.- Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 3 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 2 **Operación: 4*2= 8**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
2.- Las versiones de software no son compatibles con las nuevas actualizaciones.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 3 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 2 **Operación: 4*2= 8**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
3.- Falta de copias de seguridad periódicas de los datos almacenados en los equipos.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 3 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 2 **Operación: 4*2= 8**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
4.- Falta de capacitación regular a los usuarios sobre las mejores prácticas de seguridad informática y protección de datos	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es Moderado y 4 de los mismos respondieron en la probabilidad que resulta Posible por lo que se concluye que la vulnerabilidad es catalogada como MEDIA en nivel de prioridad de atención en el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 4 respuestas Moderado (contiene el valor de 3 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 3 Valor de Probabilidad: 2 **Operación: 3*2= 6**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
5.- Ausencia de copias de seguridad de sistemas y datos en un lugar externo seguro.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 6 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 6 respuestas Moderado (contiene el valor de 3 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Improbable (contiene el valor de 1 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 3 Valor de Probabilidad: 1 **Operación: 3*1= 3**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
6.- No se realizan actualizaciones de seguridad de forma regular en sistemas operativos y aplicaciones.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Insignificante** y 3 de los mismos respondieron en la probabilidad que resulta **Improbable** y los otros 3 respondieron **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando ambas operaciones en el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 5 respuestas Insignificante (contiene el valor de 1 dentro de la matriz de riesgos)

Tabla 30 (continuación)

	Probabilidad: 3 respuestas Improbable (contiene el valor de 1 dentro de la matriz de riesgos) Y 3 respuestas Posible (contiene el valor de 2 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 1 Primer Valor de Probabilidad: 1 Segundo Valor de Probabilidad: 2 **Operación: 1*1= 1** **Segunda Operación: 1*2= 2**
Vulnerabilidad	**Conclusión**
8.- No se siguen procedimientos para cambiar periódicamente las contraseñas	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 6 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%**

Tabla 30 (continuación)

	Nivel de impacto: 6 respuestas Moderado (contiene el valor de 3 dentro de la matriz de riesgos). **Probabilidad:** 6 respuestas Improbable (contiene el valor de 1 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 3 Valor de Probabilidad: 1 **Operación: 3*1= 1**

Tabla 31. Catálogo de Clasificación de atención de Servicios. Fuente: Elaboración propia.

Servicios	
Vulnerabilidad	**Conclusión**
1.- Los enchufes eléctricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 6 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos). **Probabilidad:** 6 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 5 **Operación: 4*5= 20**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
2.- Material inflamable debajo de los interruptores principales de la UTIC, es decir, el centro de carga (caja de fusibles y pastillas) que comprometen a una mayor propagación de incendio en caso de corto circuito	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 6 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 5 **Operación: 4*5= 20**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
3.- Sobrecargas por parte del uso de extensiones saturadas de equipos conectados	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 3 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 4 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 3 respuestas Probable (contiene el valor de 4 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 4 **Operación: 4*4= 16**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
4.- El área de alojamiento del botiquín cubre otro accidente o bien no se encuentra para atender otra emergencia en la UTIC al mismo tiempo.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 5 respuestas Peligroso (contiene el valor de 4 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Probable (contiene el valor de 4 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 4 Valor de Probabilidad: 4 **Operación: 4*4= 16**

Tabla 30 (continuación)

Vulnerabilidad	Conclusión
5.- Bloqueo de entrada y salida con activos situados en el piso o bien por mobiliario cruzado en el paso	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 3 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 3 respuestas Moderado (contiene el valor de 3 dentro de la matriz de riesgos) **Probabilidad:** 3 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 3 Valor de Probabilidad: 5 **Operación: 3*5= 15**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
6.- No cuentan con señalamientos visuales al alcance de la vista de cualquier usuario sobre cómo actuar en caso de un incendio.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 3 respuestas Moderado (contiene el valor de 3 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 3 Valor de Probabilidad: 5 **Operación: 3*5= 15**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
7.- Equipo médico interno (botiquín medico) compartido con otras áreas además de no estar al alcance de los empleados de la UTIC si ocurre un accidente.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **6 empleados= 100%** **Nivel de impacto:** 4 respuestas Menor (contiene el valor de 2 dentro de la matriz de riesgos) **Probabilidad:** 6 respuestas Frecuente (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 2 Valor de Probabilidad: 5 **Operación: 2*5= 10**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
8.- Falta de sistema de enfriamiento adecuado en el lugar de trabajo (aire acondicionado) ya que se cuenta solo dentro del SAIT.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 4 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **Nivel de impacto:** 3 respuestas Menor (contiene el valor de 2 dentro de la matriz de riesgos) **Probabilidad:** 4 respuestas Probable (contiene el valor de 4 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 2 Valor de Probabilidad: 4 **Operación: 2*4= 8**

Tabla 31 (continuación)

Vulnerabilidad	Conclusión
9.- Uso de un sistema de enfriamiento deficiente o bien que no cubra el espacio de trabajo de la UTIC en su totalidad.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 3 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. **Nivel de impacto:** 3 respuestas Menor (contiene el valor de 2 dentro de la matriz de riesgos) **Probabilidad:** 3 respuestas Probable (contiene el valor de 4 dentro de la matriz de riesgos) **Valores Obtenidos** Valor de Impacto: 2 Valor de Probabilidad: 4 **Operación: 2*4= 8**

Tabla 32. Catálogo de Clasificación de atención de Infraestructura. Fuente: Elaboración propia.

Infraestructura	
Vulnerabilidad	**Conclusión**
1.- El etiquetado de los activos y mobiliario no se basa en un ordenamiento de fácil lectura para los usuarios.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 6 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 5 **Operación: 5*4=20**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
2.- Los escritorios usados dentro de la UTIC son grandes y ocupan espacio con el que no cuentan, por lo que los hace inadecuados.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Catastrófico** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 6 respuestas **Catastrófico** (contiene el valor de 5 dentro de la matriz de riesgos) Probabilidad: 6 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** **Valor de Impacto**: 5 **Valor de Probabilidad**: 5 **Operación: 5*5=25**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
3.- Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 3 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 4 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 5 **Operación: 4*5=20**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
4.- La UTIC cuenta con un techo falso visiblemente dañado por la instalación del cableado en el cuarto del SITE.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 3 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 6 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos) **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 5 **Operación: 4*5=20**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
5.- No cuentan con reglas específicas para el uso de los Routers, Switches y Servidores.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 4 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 4 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 5 **Operación: 4*5=20**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
6.- Los Routers, Switches y Servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rindan debidamente.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Catastrófico** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Peligroso** (contiene el valor de 5 dentro de la matriz de riesgos) Probabilidad: 6 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 5 **Valor de Probabilidad**: 5 **Operación: 5*5=25**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
7.- Daño a los equipos por falta de espacio de movilidad para los usuarios mientras trasladan equipos reparados entre ellos o bien a otras áreas.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 5 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MUY ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Probable** (contiene el valor de 4 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 4 **Operación: 4*4=16**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
8.- Falta de políticas y reglas dentro de la UTIC.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Probable** (contiene el valor de 4 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 4 **Operación: 4*4=16**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
9.- Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 5 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 5 **Operación: 2*5=10**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
10.- El mobiliario referente a los asientos no son la mejor opción hablando de comodidad para los usuarios de la UTIC.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 6 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 6 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 5 **Operación: 2*5=10**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
11.- Equipos enchufados y apagados sin ser utilizados, provocan que los cables se crucen y exista confusión en el multi contacto.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 5 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 5 **Operación: 2*5=10**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
12.- Datos incorrectos o mal llenado del vale de salida y entrega por parte de la UTIC lo que ocasiona que el reemplazo no se pueda efectuar.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 4 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 4 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 5 **Operación: 2*5=10**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
13.- Falta de explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 3 de los mismos respondieron en la probabilidad que resulta **Frecuente** por lo que se concluye que la vulnerabilidad es catalogada como **ALTA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 3 respuestas **Frecuente** (contiene el valor de 5 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 5 **Operación: 2*5=10**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
14.- Presencia de plagas dentro de la UTIC que pongan en riesgo la condición del cableado de los equipos de telecomunicaciones además del mobiliario y los activos.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Peligroso** y 5 de los mismos respondieron en la probabilidad que resulta **Posible** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIO** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Peligroso** (contiene el valor de 4 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Posible** (contiene el valor de 2 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 2 **Operación: 4*2=8**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
15.- El etiquetado no muestra los datos importantes de los activos ni un número de identificación (ID).	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 5 de los mismos respondieron en la probabilidad que resulta **Ocasional** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIO** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Ocasional** (contiene el valor de 3 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 3 **Operación: 2*3=6**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
16.- El etiquetado no es visible al estar ubicado la mayoría de las veces debajo, atrás o en los laterales de los activos o bien no portarlo.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 5 de los mismos respondieron en la probabilidad que resulta **Ocasional** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIO** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Ocasional** (contiene el valor de 3 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 3 **Operación: 2*3=6**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
17.- El material de reposición hablando de periféricos y cableado es bastante escaso por lo que su cuidado debe ser mayor para asegurar su periodo de vida.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 3 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 4 de los mismos respondieron en la probabilidad que resulta **Ocasional** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIO** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 3 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 4 respuestas **Ocasional** (contiene el valor de 3 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 3 **Operación: 2*3=6**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
18.- Presencia de un techo falso y el paso del drenaje frente al área de la UTIC.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 6 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 4 de los mismos respondieron en la probabilidad que resulta **Probable** por lo que se concluye que la vulnerabilidad es catalogada como **MEDIO** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 6 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 4 respuestas **Probable** (contiene el valor de 4 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 4 **Valor de Probabilidad**: 2 **Operación: 2*4=8**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
19.- Ausencia de una barrera en la entrada/salida de la UTIC para prevenir filtraciones de agua por parte de las tuberías que pasan frente al área de la UTIC.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 5 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Moderado** y 3 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 5 respuestas **Moderado** (contiene el valor de 3 dentro de la matriz de riesgos) Probabilidad: 3 respuestas **Improbable** (contiene el valor de 1 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 3 **Valor de Probabilidad**: 1 **Operación: 3*1=3**

Tabla 32 (continuación)

Vulnerabilidad	Conclusión
20.- Daño al cableado sin protección por parte de la caída del techo falso dañado.	Como resultado de la ponderación mediante la evaluación realizada a los empleados de la UTIC sobre el impacto y la probabilidad de dicha vulnerabilidad se obtuvo lo siguiente: 4 empleados de los 6 considerados es decir la mayoría respondieron en el nivel de impacto que es **Menor** y 5 de los mismos respondieron en la probabilidad que resulta **Improbable** por lo que se concluye que la vulnerabilidad es catalogada como **BAJA** en nivel de prioridad de atención considerando el formato de la matriz de riesgos ubicado en la página X. 6 empleados= 100% Nivel de impacto: 4 respuestas **Menor** (contiene el valor de 2 dentro de la matriz de riesgos) Probabilidad: 5 respuestas **Improbable** (contiene el valor de 1 dentro de la matriz de riesgos). **Valores Obtenidos** **Valor de Impacto**: 2 **Valor de Probabilidad**: 1 **Operación: 2*1=2**

En la siguiente actividad, se deben realizar visitas a las instalaciones de la UTIC, ya que esta observación directa facilita la identificación de posibles anomalías en la infraestructura de la unidad. Para determinar el tipo de pruebas a realizar, es esencial llevar a cabo una observación e inspección detallada de los aspectos previamente estudiados en la UTIC (seguridad física, seguridad lógica, servicios, infraestructura y sistema de inventario). A simple vista, se observa una notable falta de seguridad en los accesos, los cuales deberían ser uno de los elementos más protegidos al funcionar como la primera línea de control para resguardar la información y los activos de la unidad. Dado que estos accesos no cumplen adecuadamente con las medidas y requisitos de seguridad de acuerdo con el espacio disponible en la UTIC, se decide implementar pruebas específicas para cada uno de los aspectos.

En el caso de la seguridad física, las pruebas se orientan a verificar la funcionalidad y efectividad de los accesos y la protección que ofrecen. Esto incluye probar el cierre seguro de los accesos, el nivel de acceso permitido, así como las medidas de seguridad o protecciones disponibles. Además, se evaluarán aspectos como el cierre seguro del sitio, el nivel de vigilancia existente, la seguridad externa o el respaldo de otros recursos que contribuyan a elevar el nivel de protección de los activos y la información.

En cuanto a la seguridad lógica, las pruebas se enfocan en la protección de la información y en el estado de los equipos de cómputo internos. Se evaluarán aspectos como el uso actual de contraseñas en los equipos, los incidentes que hayan ocurrido y que puedan implicar posibles brechas o ataques a la información, los activos o los sistemas de la unidad. Además, se verificará la capacitación que reciben los empleados para operar los equipos internos, así como la actualización de las versiones de los sistemas, asegurando que estas permitan una operación eficiente y segura.

Para los servicios, las pruebas se centran en evaluar su funcionamiento e implementación, con el fin de determinar si requieren mejoras, si alguno de ellos resulta inapropiado para el área, o si están adecuadamente implementados. Estas pruebas considerarán los siguientes servicios: corriente eléctrica, sistemas contra incendios, aire acondicionado y servicios médicos.

Para las pruebas de infraestructura se inspeccionan distintos ámbitos, como el cableado de los equipos de cómputo y periféricos, además del cableado de los equipos de redes, el etiquetado y clasificación de los activos, además de la distribución de los equipos, mobiliario y activos que estén dentro de la unidad, las condiciones del techo y las paredes, están concentradas en aspectos que intervienen para el desarrollo de las actividades internas por parte de los empleados, y que sean notables ante la vista de los usuarios.

En las pruebas que se enfocan al sistema de inventario usado actualmente, se pondrán a prueba funciones como el acceso al mimo, manejo o intervención por parte de los empleados internos, disponibilidad de la información, además del sistema en donde este desarrollado, su función y el rol que tiene de acuerdo con las acciones que requieren los empleados internos, además de los productos que puede o no arrojar dependiendo de las necesidades de la unidad.

3.2.1.4 Actividad 2.4 Realizar Pruebas de Seguridad Física.

3.2.1.4.1 Descripción de la actividad

En esta actividad se requiere visitar las instalaciones de la UTIC ya que de esta manera es más fácil detectar aquellas anomalías que pueda presentar la infraestructura de la unidad, dicho esto se hace una mayor observación e inspección en los accesos a la UTIC, ya que a simple vista hay una notable falta de seguridad, ya que esta no es la adecuada de acuerdo a las medidas y espacios disponibles dentro de la UTIC, la seguridad considerada para las pruebas y que tiene un mayor impacto en la distribución son los accesos en donde están situados seguros y pasadores, los antes mencionados están situados en el perímetro interno de la unidad, sin mencionar que uno de ellos está ubicado al exterior del edificio de dicha unidad, además de que las ventanas contribuyen a la deficiencia de seguridad de los empleados, equipos y activos.

3.2.1.4.2 Resultado de la actividad

Tabla 33. Prueba 1 de Seguridad Física. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación del Cierre Seguro de Accesos dentro del Horario Laboral"	
OBJETIVO DE PRUEBA	El objetivo de esta prueba es evaluar, confirmar y verificar si los accesos del sitio se cierran de manera segura cuando no se está utilizando durante el horario laboral.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	La finalidad de esta prueba es verificar la efectividad y la consistencia en el cierre seguro de accesos en el sitio cuando no está siendo utilizado en horario laboral. Se busca evaluar si se implementan medidas adecuadas para prevenir accesos no autorizados durante períodos en los que la instalación (UTIC) no está en uso. Se espera que los accesos a la UTIC se cierren cuando no está en uso en horario laboral.
TÉCNICA	Evaluación, Observación, Inspección, Cuestionario, Revisión
ACTIVIDADES DE LA PRUEBA	1. Verificar visualmente el estado de cierre de puertas y otras vías de acceso principales dentro del horario laboral. 2. Revisar la presencia y funcionamiento de cerraduras, sistemas de seguridad electrónica u otros dispositivos de cierre. 3. Entrevistar al personal encargado del cierre de accesos para entender los procedimientos establecidos. 4. Verificar si existe un registro formal de las personas autorizadas para acceder dentro del horario laboral. 5. Evaluar la presencia y eficacia de medidas de seguridad adicionales, como sistemas de videovigilancia y sistemas de alarma.

Tabla 33 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Todos los criterios y objetivos se cumplen o superan de manera consistente. **Bueno**: La mayoría de los criterios y objetivos se cumplen de manera sólida. **Regular**: Algunos criterios u objetivos pueden no cumplirse completamente, y se necesitan ajustes para optimizar el proceso. **Suficiente**: Los criterios y objetivos esenciales se cumplen, pero puede haber limitaciones o áreas donde el rendimiento podría mejorar. **Deficiente**: Varios criterios u objetivos no se cumplen, y se requieren acciones correctivas inmediatas para mejorar el proceso.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Se tuvo que cuestionar al jefe de la UTIC sobre el cierre de accesos para entender los procedimientos establecidos.
INTERPRETACIÓN DE RESULTADOS	Se tomo la siguiente evidencia: Acceso principal a la UTIC sin vigilancia  *Figura 112. Acceso a la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Acceso a la UTIC, 2023)*

Tabla 33 (continuación)

	Vista por dentro:  *Figura 113. Vista trasera al Acceso a la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Vista trasera al Acceso a la UTIC, 2023)* Vista de las cerraduras:  *Figura 114. Vista de la Cerradura del Acceso Principal a la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Vista de la Cerradura del Acceso Principal a la UTIC, 2023)*

Tabla 33 (continuación)

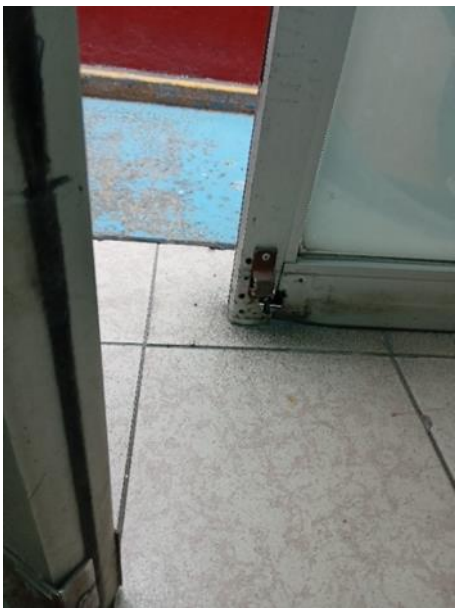


Figura 115. Segunda Vista de la Cerradura del Acceso Principal a la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Segunda Vista de la Cerradura del Acceso Principal a la UTIC, 2023)



Figura 116. Tercera Vista de la Cerradura del Acceso Principal a la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Tercera Vista de la Cerradura del Acceso Principal a la UTIC, 2023)

Tabla 33 (continuación)

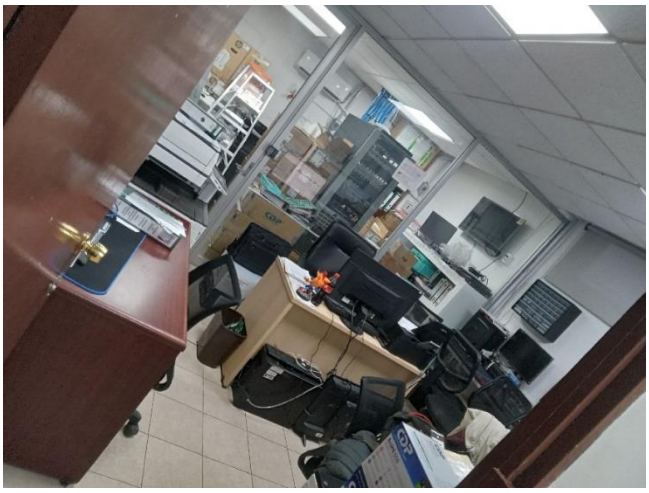
	Puerta de la UTIC abierta en horario laboral cuando no hay personal:  *Figura 117. Oficina de la UTIC. Fuente: H.* Ayuntamiento *de Tultitlán. (Tultitlán. H. A., Oficina de la UTIC, 2023)* Vista de las cerraduras con las que cuenta la UTIC:  *Figura 118. Cerraduras de la puerta de la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Cerraduras de la puerta de la UTIC, 2023)*

Tabla 33 (continuación)

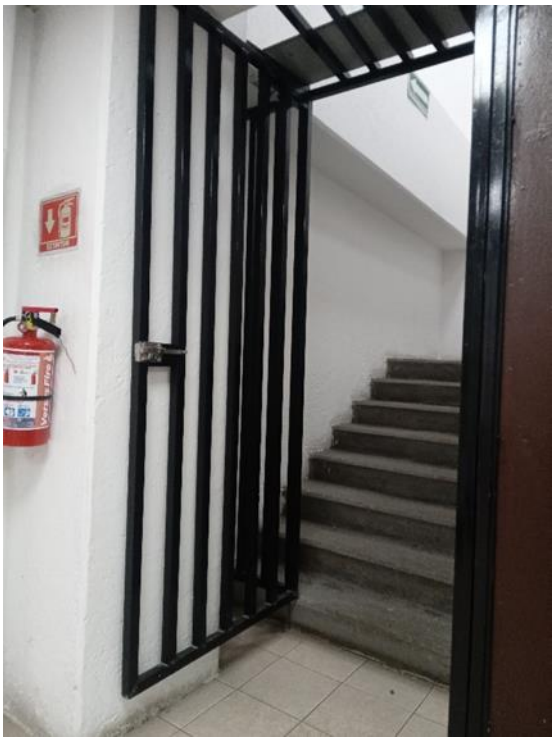
	Otro acceso proveniente de otros departamentos ubicados en segunda planta ubicado en la parte izquierda de la puerta a la UTIC:  *Figura 119. Segundo acceso hacia la UTIC. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Segundo acceso hacia la UTIC, 2023)*

Tabla 33 (continuación)

RECOMENDACIONES	Acuerdo a la norma ISO/IEC 27002 en su apartado 7 llamado "Controles Físicos" nos menciona que *"Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.* *Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia".* La recomendación en el apartado *7.1 Perímetro de Seguridad Física* en su sección *b) … Las puertas y ventanas deberían cerrarse con llave cuando estén desatendidas y se debería considerar la protección externa para las ventanas, particularmente a nivel del suelo;* y *c) se debiera contar con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado;* Además del apartado *7.2 Ingreso Físico* en su sección c*) establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, autenticación biométrica o de dos factores, como una tarjeta de acceso y un PIN secreto. Se deberían considerar las puertas de seguridad dobles para el acceso a áreas sensibles;*

Tabla 33 (continuación)

	y *d) establecer un área de recepción monitoreada por el personal u otros medios para controlar el acceso físico al sitio o edificio;* Para dar solución a esta vulnerabilidad acorde a lo anterior mencionado se recomienda a los empleados internos de la UTIC asignar debidamente a un encargado interno que se responsabilice de cerrar el acceso al área de manera correcta y segura aun en horario laboral siempre y cuando la oficina quede totalmente vacía sin importar el periodo de tiempo en el que se encuentre de esta manera evitando así todo acceso no autorizado ni deseado, esto para salvaguardar los activos y toda aquella información que se tenga dentro de esto.

Tabla 34. Prueba 2 de Seguridad Física. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación del Control de Uso Compartido de Equipos de Oficina"	
OBJETIVO DE PRUEBA	Esta prueba se centra en verificar si existe un control adecuado en el uso compartido de un equipo de impresión multifuncional, especialmente cuando se presta a departamentos externos.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito de esta prueba es evaluar la eficacia de los controles establecidos para el uso compartido de equipos de oficina, específicamente centrándose en la prestación de servicios de estos dispositivos a departamentos externos. El objetivo principal es asegurarse de que se implementen medidas adecuadas para garantizar un uso seguro y autorizado de los equipos de oficina compartidos. Se espera que el uso del activo de impresión multifuncional a otro personal del municipio haga un correcto uso de este.
TÉCNICA	Revisión, Evaluación, Observación, Verificación
ACTIVIDADES DE LA PRUEBA	1. Verificar si hay pautas claras sobre cómo prestar servicios de dispositivos a departamentos externos. 2. Analizar los registros de acceso y uso de los equipos de oficina compartidos. 3. Verificar la autorización y autenticación de los usuarios, especialmente aquellos de departamentos externos. 4. Asegurarse de que solo personal autorizado tenga acceso físico a los dispositivos.

Tabla 34 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Los registros de acceso y uso demuestran un control efectivo y autorización adecuada. **Bueno**: Los registros de acceso y uso son generalmente positivos, aunque puede haber pequeñas áreas de mejora. **Regular**: Algunos registros de acceso y uso pueden no cumplir completamente con los estándares. **Suficiente**: Los registros de acceso y uso cumplen con los estándares básicos, pero podrían mejorarse. **Deficiente**: Los registros de acceso y uso indican problemas sustanciales de seguridad.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Equipo de Impresión Multifuncional compartido  *Figura 120. Equipo de Impresión Multifuncional. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo de Impresión Multifuncional, 2023)*

Tabla 34 (continuación)

RECOMENDACIONES	Acuerdo a la norma ISO/IEC 27002 en su apartado 8 llamado "Administración de Activos" nos dice que *"identificar los activos organizacionales y definir las responsabilidades de protección adecuadas."* En su sección 8.1.2 Propiedad de los Activos nos dice que *"Los activos mantenidos en el inventario deberían ser propietarios."* En su lineamiento de implementación sección *c) definir y revisar periódicamente las restricciones de acceso y clasificaciones para los activos importantes, considerando las políticas de control de acceso pertinentes;* Cabe mencionar el apartado 9 Control de acceso dice *"limitar el acceso a la información y a las instalaciones de procesamiento de la información."* Además de tomar en cuenta la sección 9.1.1 Política de control de acceso dice *"Se debería establecer, documentar y revisar una política de control de acceso en base a los requisitos del negocio y de la seguridad de la información."* Para dar solución ante esta vulnerabilidad se recomiendan políticas donde se establezca el uso permitido de los recursos de TI, incluyendo la multifuncional, además de implementar una bitácora para la utilización de esta.

Tabla 35. Prueba 3 de Seguridad Física. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Revisión de Programa de Capacitación en Gestión de Riesgos de Seguridad Física"	
OBJETIVO DE PRUEBA	Esta prueba se enfoca en evaluar si la organización tiene un programa establecido de capacitación para la gestión de riesgos, específicamente aquellos asociados con la seguridad física.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es evaluar la efectividad y la adecuación del programa de capacitación en gestión de riesgos de seguridad física dentro de la organización. Se busca verificar si el personal está debidamente informado y capacitado para identificar, evaluar y responder adecuadamente a los riesgos relacionados con la seguridad física. Se espera identificar si el personal está adecuadamente informado, capacitado y preparado para abordar los riesgos específicos asociados con la seguridad física.
TÉCNICA	Revisión, Observación, Analizar
ACTIVIDADES DE LA PRUEBA	1. Revisar detalladamente el programa de capacitación en gestión de riesgos de seguridad física. 2. Entrevistar a empleados clave responsables de la seguridad física y gestión de riesgos. 3. Evaluar su conocimiento sobre los procedimientos de seguridad y su comprensión de los riesgos asociados. 4. Analizar la participación del personal en el programa de capacitación. 5. Evaluar si se realizan simulacros o ejercicios prácticos para poner a prueba la capacidad del personal para gestionar situaciones de riesgo de seguridad física.

Tabla 35 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: El programa de capacitación en gestión de riesgos de seguridad física es altamente efectivo y cumple con los estándares más altos. **Bueno**: El programa de capacitación es sólido y cubre de manera adecuada los aspectos clave de la gestión de riesgos de seguridad física. **Regular**: Existen áreas identificadas que necesitan mejoras en el programa de capacitación. **Suficiente**: Se cumplen los requisitos mínimos para el programa de capacitación. **Deficiente**: No existe un programa de capacitación.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	No existe un programa de capacitación por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 7 llamado Seguridad de recursos humanos en su sección *7.2.2 Concientización, educación y capacitación sobre la seguridad de la información.* Nos menciona que *"Todos los empleados de la organización y, donde sea pertinente, los contratistas deberían recibir educación y capacitación de concientización adecuada y actualizaciones regulares sobre las políticas y procedimientos organizacionales, según sea pertinente para su función laboral."*

Tabla 35 (continuación)

	Así mismo sobre su implementación tenemos lo siguiente: *Un programa de concientización sobre seguridad de la información debería apuntar a hacer que los empleados y, donde resulte pertinente, los contratistas conozcan sus responsabilidades en cuanto a la seguridad de la información y los medios a través de los que se descargan esas responsabilidades.* *Un programa de concientización de seguridad de la información se debería establecer de acuerdo con las políticas y procedimientos pertinentes de seguridad de la información de la organización, considerando la información de la organización que se va a proteger y los controles que se han implementado para protegerla información. El programa de concientización debería incluir varias actividades de concientización como campañas (por ejemplo, un "día de la seguridad de la información") y la entrega de panfletos o boletines informativos.* *El programa de concientización se debería planificar considerando los roles de los empleados en la organización y, donde corresponda, la expectativa que tiene la organización sobre la concientización de los contratistas. Las actividades del programa de concientización se deberían programar con el tiempo, de preferencia de manera regular, para que las actividades se repitan y abarquen a los nuevos empleados y contratistas. El programa de concientización también se debería actualizar de manera regular para que esté de acuerdo con las políticas y procedimientos de la organización y se debería basar en las lecciones aprendidas de los incidentes de seguridad de la información.*

Tabla 35 (continuación)

	Se debería realizar una capacitación de concientización según lo requiera el programa de concientización de seguridad de la información de la organización. La capacitación de concientización se puede realizar a través de distintos medios incluida la capacitación en el aula, a distancia, en línea, autónoma y otros. *La educación y la capacitación de seguridad de la información también debería abarcar aspectos generales como:* *a) indicar el compromiso de la dirección con la seguridad de la información en toda la organización;* *b) la necesidad de conocer y cumplir con las normas y obligaciones de seguridad de la información pertinentes, según se define en las políticas, normas, leyes, normativas, contratos y acuerdos;* *c) responsabilidad personal por las acciones e inoperancias propias y las responsabilidades generales hacia el aseguramiento y protección de la información que pertenece a la organización y a las partes externas.* *d) procedimientos básicos de seguridad de la información (como la denuncia de incidentes de seguridad de la información) y controles de la línea de base (como seguridad de contraseñas, controles de malware y despeje de escritorios);* *e) Puntos de contacto y recursos para la información adicional y asesoría sobre los asuntos de seguridad de la información, incluida una mayor información sobre la educación y los materiales de capacitación parala seguridad de la información.*

Tabla 35 (continuación)

	La educación y la capacitación sobre la seguridad de la información se debería realizar de manera periódica. *La educación y la capacitación inicial se aplica a quienes se les traslada a nuevos cargos o roles con requisitos de seguridad de la información sustancialmente diferentes, no solo para quienes comienzan sus labores y, se debería realizar antes de que el rol se active.* Lo anterior mencionado, aunque habla sobre la seguridad de la información se debiera aplicarse también a seguridad física, ya que como se mencionó antes no solo es seguridad lógica si no también física, y para dar solución a esta vulnerabilidad se recomienda implementar programas de capacitación en seguridad física y así la integración de las mejores prácticas de seguridad física en este programa.

Tabla 36. Prueba 4 de Seguridad Física. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Políticas y Procedimientos para la Gestión de Incidentes de Seguridad Física"	
OBJETIVO DE PRUEBA	Esta prueba se centra en verificar si la organización cuenta con políticas y procedimientos formales para manejar incidentes relacionados con la seguridad física.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es evaluar la efectividad y la adecuación de las políticas y procedimientos establecidos para gestionar incidentes relacionados con la seguridad física en la organización. Se busca verificar si existen procesos claros y eficientes para identificar, informar y mitigar incidentes de seguridad física. Se espera obtener una evaluación integral de la eficacia de las políticas y procedimientos para la gestión de incidentes de seguridad física.
TÉCNICA	Evaluación, Analizar, Verificación
ACTIVIDADES DE LA PRUEBA	1. Analizar detalladamente las políticas y procedimientos existentes para la gestión de incidentes de seguridad física. 2. Verificar si se realizan simulacros o ejercicios prácticos para probar la efectividad de las políticas y procedimientos en situaciones simuladas. 3. Analizar registros de incidentes anteriores relacionados con la seguridad física.

Tabla 36 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Las políticas y procedimientos para la gestión de incidentes de seguridad física son altamente efectivos, claros y bien definidos. **Bueno**: Las políticas y procedimientos son sólidos y abordan adecuadamente la gestión de incidentes de seguridad física. **Regular**: Existen áreas identificadas que necesitan mejoras en las políticas y procedimientos para la gestión de incidentes. **Suficiente**: Se cumplen los requisitos mínimos para las políticas y procedimientos, pero hay espacio para mejoras. **Deficiente**: No existen políticas ni procedimientos para la gestión de incidentes de seguridad física.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	SIN CONSIDERACIONES ESPECIALES
INTERPRETACIÓN DE RESULTADOS	No existen políticas ni procedimientos para la gestión de incidentes de seguridad física por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde al estándar ISO/IEC 27002 en su sección 16 llamado Administración de incidentes de seguridad de la información Nos dice su objetivo que *"garantizar un enfoque coherente y eficaz a la administración de incidentes de seguridad de la información, incluida la comunicación sobre los eventos y las debilidades de seguridad."*. En su apartado *16.1 Responsabilidades y procedimientos* menciona que *Se deberían establecer las responsabilidades y procedimientos de la dirección para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.*

Tabla 36 (continuación)

	Lo cual en sus lineamientos de implementación se va a enfocar en sus 3 incisos que lo componen: *Se deberían considerar las siguientes pautas para las responsabilidades de la dirección y los procedimientos respecto de la administración de incidentes de seguridad de la información.* *a) las responsabilidades de la dirección se deberían establecer para garantizar que se desarrollan y comunican los siguientes procedimientos adecuadamente dentro de la organización.* *1) procedimientos para la planificación y preparación de la respuesta ante incidentes;* *2) procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad;* *3) procedimientos para registrar actividades de administración de incidentes;* *4) procedimientos para administrar evidencia forense;* *5) procedimientos para la evaluación y la decisión sobre los eventos de seguridad de la información y la evaluación de las debilidades en la seguridad de la información;* *6) procedimientos para la respuesta incluidos aquellos para el escalamiento, la recuperación controlada desde un incidente y la comunicación a las personas internas y externas u organizaciones;*

Tabla 36 (continuación)

	b) los procedimientos establecidos deberían garantizar que: *a) el personal competente maneje los problemas relacionados a los incidentes de seguridad de la información dentro de la organización;* *b) que se implemente un punto de contacto para la detección e informe de los incidentes de seguridad.* *c) que se mantengan los contactos correspondientes con las autoridades, grupos de interés externos o foros que manejen los problemas relacionados con los incidentes de seguridad de la información;* *c) el informe de procedimientos debería incluir:* *1) la preparación de formularios de informes de eventos de seguridad de la información para apoyar la acción del informe y ayudar a la persona que lo hace a recordar todas las actividades necesarias en caso de un evento de seguridad de la información;* *2) el procedimiento que se debería realizar en caso de un evento de seguridad de la información, es decir, indicando todos los detalles inmediatamente, como el tipo de incumplimiento, si ocurre una falla, los mensajes en la pantalla e informar inmediatamente al punto de contacto y realizar solo acciones coordinadas;* *3) referencia a un proceso disciplinario formal establecido para lidiar con los empleados que caen en incumplimiento de seguridad;*

Tabla 36 (continuación)

	4) procesos de retroalimentación adecuados para asegurarse de que a aquellas personas que informan eventos de seguridad se les notifique sobre los resultados una vez que se ha abordado el problema y se haya cerrado. Cabe mencionar que, aunque lo anterior hable sobre incidentes de seguridad de la información, se debiera implementarse también para incidentes de seguridad física. Para dar solución a esta vulnerabilidad se recomienda lo siguiente: 1. Designar un equipo de respuesta a incidentes y asigna responsabilidades específicas. 2. Desarrollar planes de respuesta detallados para diversos escenarios de seguridad física. 3. Implementar sistemas de monitoreo físico y tecnológico para detectar incidentes. 4. Establecer procesos para analizar y clasificar incidentes según su gravedad. 5. Definir cómo se recopilará, preservará y analizará la evidencia física en caso de incidentes. 6. Proporcionar capacitación regular al personal designado para manejar incidentes. *7.* Realizar ejercicios de simulacro para mejorar las habilidades de respuesta.

Tabla 37. Prueba 5 de Seguridad Física. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Revisión del Control y Monitoreo de Cámaras de Videovigilancia Internas"	
OBJETIVO DE PRUEBA	La prueba se centraría en evaluar la eficacia y la adecuación del sistema de monitoreo de cámaras de videovigilancia internas, particularmente en relación con la responsabilidad asignada al departamento específico en lugar de los empleados de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	La finalidad de esta prueba es evaluar la eficacia y la seguridad en la implementación de los controles y el monitoreo de las cámaras de videovigilancia internas. Se busca verificar si se aplican políticas y procedimientos adecuados para el acceso, la gestión y la revisión de las imágenes capturadas por las cámaras de videovigilancia internas, en caso de que se presente un robo. Se espera obtener una evaluación integral de la eficacia y la seguridad en la implementación de controles y monitoreo de las cámaras de videovigilancia internas.
TÉCNICA	Revisión, Evaluación, Analizar, Cuestionario.
ACTIVIDADES DE LA PRUEBA	1. Analizar las políticas y procedimientos establecidos para el control y monitoreo de las cámaras de videovigilancia internas. 2. Entrevistar al personal encargado de la gestión y monitoreo de las cámaras de videovigilancia. 3. Realizar una inspección física de las cámaras de videovigilancia internas. 4. Analizar los registros de acceso a las imágenes de las cámaras de videovigilancia.

Tabla 37 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Las políticas y procedimientos para el control y monitoreo de cámaras son excelentes y cumplen con los estándares más altos. **Bueno**: Las políticas y procedimientos son sólidos y cumplen adecuadamente con los estándares establecidos. **Regular**: Existen áreas identificadas que necesitan mejoras en las políticas y procedimientos. **Suficiente**: Se cumplen los requisitos mínimos para las políticas y procedimientos, pero hay espacio para mejoras. **Deficiente**: No existen políticas ni procedimientos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente.**
CONSIDERACIONES ESPECIALES	Se tuvo que pedir al departamento de monitoreo, evidencia sobre el funcionamiento de la cámara interna de la UTIC.
INTERPRETACIÓN DE RESULTADOS	Ubicación de la cámara de videovigilancia de la UTIC:  *Figura 121. Cámara Interna de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cámara Interna de la UTIC, 2023)*

Tabla 37 (continuación)

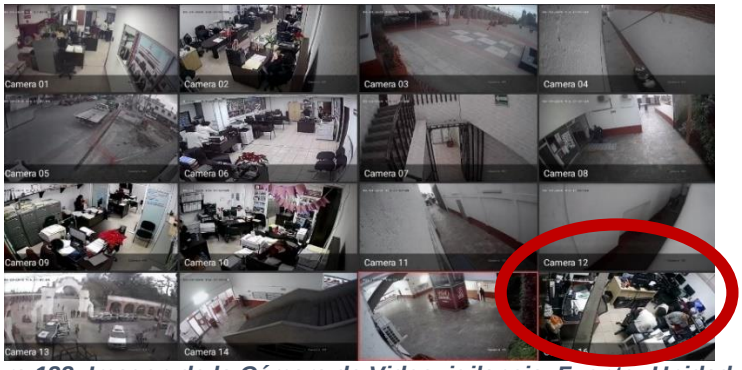
	Vista de la UTIC desde la cámara de videovigilancia (la UTIC se encuentra señalada en el círculo color rojo).  *Figura 122. Imagen de la Cámara de Videovigilancia. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Imagen de la Cámara de Videovigilancia, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27001 en su sección 7 llamado Soporte nos dice que *"La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información."* Cabe mencionar que también existen leyes en el Estado de México que respaldan el uso de cámaras de videovigilancia, como lo es "LEY QUE REGULA EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN PARA LA SEGURIDAD PÚBLICA DEL ESTADO DE MÉXICO" esta nos dice que *"La presente Ley es de orden e interés público y de observancia general en todo el territorio del Estado de México y tiene por objeto establecer las bases de coordinación entre las instituciones de seguridad pública del Gobierno del Estado de México y de los municipios de la entidad, en el uso y aprovechamiento de las tecnologías de la información y comunicación en el marco de los Sistemas Nacional y Estatal de Seguridad Pública, y sus fines son:* *I. Regular la ubicación, instalación y operación de equipos y sistemas tecnológicos a cargo de las instituciones de seguridad pública.*

Tabla 37 (continuación)

	II. Contribuir al mantenimiento del orden, la tranquilidad y la estabilidad en la convivencia, así como prevenir situaciones de emergencia o desastre e incrementar la seguridad pública. *III. Regular el uso y resguardo de la información obtenida, a través de equipos y sistemas tecnológicos en las materias de seguridad pública y procuración de justicia.* *IV. Regular las acciones de análisis de la información obtenida con equipos o sistemas tecnológicos en materia de seguridad pública, para generar inteligencia en la prevención de la delincuencia e infracciones administrativas.* *V. Establecer las bases para la estandarización u homologación de los equipos y sistemas tecnológicos en materia de seguridad pública."* Ya que las cámaras de seguridad no están monitoreadas por el jefe de la UTIC, y esto presenta una vulnerabilidad ya que si llegara a materializarse un robo debe de comunicarse al área de monitoreo para que revise la cámara de seguridad y el tiempo de respuesta es de 30 min a 1 hora aproximadamente. Es por ello por lo que la organización debe establecer un procedimiento documentado para la gestión de activos, incluyendo las cámaras de seguridad. Este procedimiento debería abordar la identificación, clasificación y control de los activos relacionados con la videovigilancia, garantizando su seguridad y disponibilidad. Además, la organización debe implementar medidas de seguridad física y lógica para proteger el acceso no autorizado a las cámaras y a la información capturada por ellas.

3.2.1.5 Actividad 2.5 Realizar Pruebas de Seguridad Lógica.

3.2.1.5.1 Descripción de la actividad

En esta actividad se requiere visitar las instalaciones de la UTIC ya que de esta manera es más fácil detectar aquellas vulnerabilidades que pueda presentar la seguridad lógica de la unidad, dicho esto se hace una mayor observación e inspección al uso de contraseñas y respaldo de la información de la UTIC, ya que a simple vista hay una notable falta de seguridad de la información y datos que manejan, ya que esta no es la adecuada de acuerdo a las medidas que proponen estándares y a las acciones realizadas dentro de la UTIC, la seguridad lógica considerada para las pruebas y que tiene un mayor impacto son las estrategias con las que cuentan que son capaces de proteger la información y los datos que manejan internamente, las antes mencionadas deben estar implementadas correctamente, sin mencionar que deben cumplir con funciones que sean capaces de prevenir, proteger datos sensibles o bien operaciones que impliquen información interna.

3.2.1.5.2 Resultado de la actividad

Tabla 38. Prueba 1 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Revisión de contraseñas seguras"	
OBJETIVO DE PRUEBA	Identificar si las contraseñas utilizadas actualmente son seguras y se cambian periódicamente evitando así intrusiones o mal uso de estas.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se revisa que el uso de las contraseñas seguras sea correcto ya que como buena práctica de seguridad es recomendable contar con una contraseña compuesta de ciertas características (caracteres especiales, mayúsculas, números, minúsculas, longitud mínima de 8 caracteres), además de ser actualizada constantemente en un periodo de al menos 3 meses. Se espera que las contraseñas utilizadas sean seguras y con los requerimientos establecidos garantizando los equipos y la información.
TÉCNICA	Revisión, Analizar, Observación, Inspección, Evaluación

Tabla 38 (continuación)

ACTIVIDADES DE LA PRUEBA	1. Revisar las contraseñas usadas actualmente en los inicios de sesión en los equipos de cómputo. 2. Inspeccionar el uso de contraseñas laborales en aplicaciones o programas. 3. Evaluar la seguridad actual de las contraseñas usadas en los equipos de la UTIC. 4. Consultar si los equipos de cómputo de la UTIC cuentan con inicio de sesión al encender los equipos. 5. Revisar si las contraseñas usadas son actualizadas al menos cada 3 meses y si existe un registro.
PROCESO DE MEDICIÓN	**Excelente:** Las contraseñas usadas actualmente son seguras, cuentan con todas las características requeridas y se actualizan trimestralmente. **Bueno:** Las contraseñas usadas actualmente son seguras, cuentan con la mayoría de las características requeridas y se actualizan al menos cada 6 meses. **Regular:** Las contraseñas usadas actualmente son parcialmente seguras, cuentan con algunas de las características requeridas y no se actualizan periódicamente. **Suficiente:** Las contraseñas usadas actualmente no son seguras, cuentan con al menos una característica requerida y no se actualizan periódicamente. **Deficiente:** No existen contraseñas seguras ni se actualizan periódicamente.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente.**

Tabla 38 (continuación)

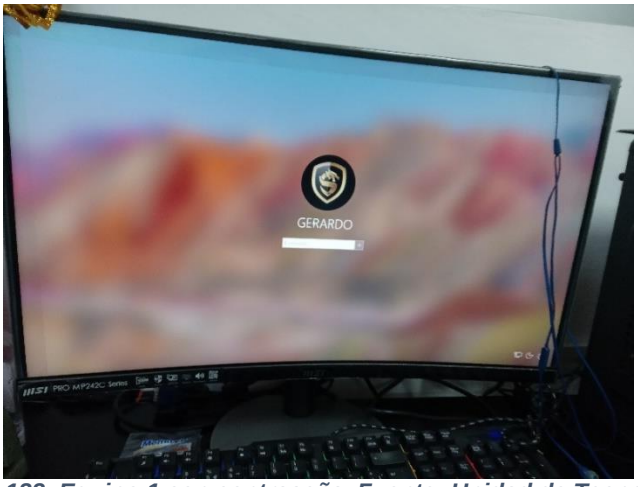
CONSIDERACIONES ESPECIALES	Se solicito a los empleados dar a conocer sus contraseñas al iniciar sesión en sus equipos para corroborar que este existiera y en caso de hacerlo fuera segura.
INTERPRETACIÓN DE RESULTADOS	Equipo 1/6 Al iniciar el equipo se puede apreciar que cuenta con usuario y contraseña para acceder a los archivos y todo lo que contiene en él, sin embargo, se pregunto acerca del estatus de la contraseña e indicaron que no se cambian periódicamente.  *Figura 123. Equipo 1 con contraseña. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo 1 con contraseña, 2023)*

Tabla 38 (continuación)

	Equipo 2/6 Al iniciar el equipo se puede aprecias que no cuenta con protección alguna que impida el acceso a otros usuarios, es decir, no tiene usuario ni contraseña:  *Figura 124. Equipo 2 sin contraseña. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo 2 sin contraseña, 2023)* Equipo 3/6 Al iniciar el equipo se puede aprecias que no cuenta con protección alguna que impida el acceso a otros usuarios, es decir, no tiene usuario ni contraseña:  *Figura 125. Equipo 3 sin contraseña. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo 3 sin contraseña, 2023)*

Tabla 38 (continuación)

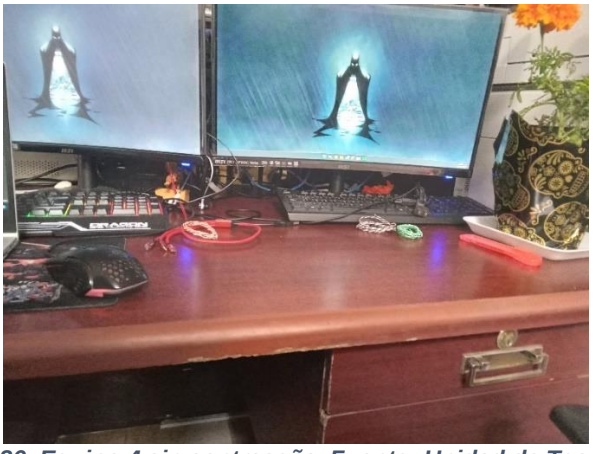
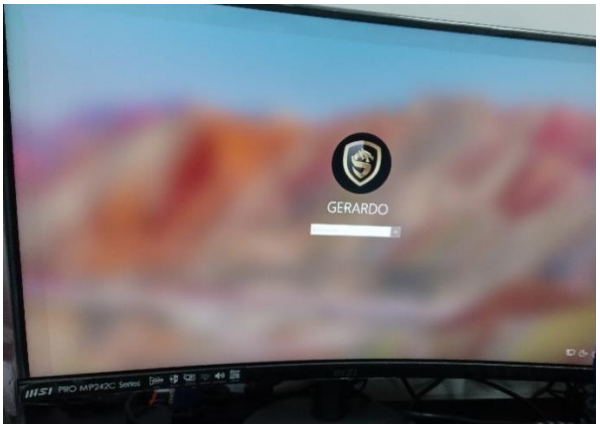
	Equipo 4/6 Al iniciar el equipo se puede apreciar que no cuenta con protección alguna que impida el acceso a otros usuarios, es decir, no tiene usuario ni contraseña:  ***Figura 126. Equipo 4 sin contraseña. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo 4 sin contraseña, 2023)*** Equipo 5/6 Al iniciar el equipo se puede apreciar que cuenta con usuario y contraseña para acceder a los archivos y todo lo que contiene en él, sin embargo, se pregunto acerca del estatus de la contraseña e indicaron que no se cambian periódicamente.  ***Figura 127. Equipo 5 con contraseña. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo 5 con contraseña, 2023)***

Tabla 38 (continuación)

RECOMENDACIONES	Acorde al estándar (ISO 27002:2022) en su apartado llamado "**Información para Autenticación**" nos menciona que "La asignación y gestión de la información de autenticación debería ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación". Con el propósito de "asegurar la autenticación adecuada de la entidad y evitar fallas en los procesos de autenticación." Sección C: cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas fuertes de acuerdo con las mejores prácticas recomendadas.

Tabla 38 (continuación)

	Sección C1: Las contraseñas no se basan en nada que otra persona pueda adivinar u obtener fácilmente utilizando información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento). Sección C3: use frases de contraseña fáciles de recordar e intente incluir caracteres alfanuméricos y especiales. Sección C4: las contraseñas tienen una longitud mínima. Sección D: las mismas contraseñas no se utilizan en distintos servicios y sistemas. Sin embargo, también menciona en su apartado llamado “Gestión de Contraseñas” en su sección b “hacer cumplir contraseñas fuertes de acuerdo con las recomendaciones de buenas prácticas [véase C) de "Responsabilidades del usuario”]”. En su sección D “hacer cumplir los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad, o al terminar o cambiar de empleo cuando un usuario tiene contraseñas conocidas para identidades que permanecen activas (por ejemplo, identidades compartidas). Sección G “no mostrar contraseñas en la pantalla cuando estas se ingresan”.

Tabla 38 (continuación)

	RECOMENDACIÓN Para dar solución a esta vulnerabilidad se recomienda a los empleados internos de la UTIC asesorar debidamente a los usuarios temporales, empleados nuevos o simplemente internos, sobre el uso de contraseñas evitando, de igual forma brindar correos empresariales y contraseñas iniciales momentáneas para tener un mejor control sobre el personal y los accesos que solicite. Por lo que en base a las practicas mencionadas en el estándar se recomienda que el uso de contraseñas internas sea seguro, creando una combinación de letras y números sin un orden especifico, alternando mayúsculas y minúsculas, o bien secuencias de números sin un contexto o significado e incluyendo caracteres especiales, además que sea de una longitud de mínimo 9 caracteres. Además, tener contraseñas diferentes para todas aquellas cuentas o situaciones laborales que las requieran, no compartir una misma contraseña para el desarrollo de sus actividades. Además de eso, asignar un responsable de confianza el cual debe asegurarse de que cumplan con las estrategias establecidas es una medida que garantiza la ejecución de estas y reduce el riesgo de quiebre en los accesos. Por otro lado, se recomienda ampliamente cambiar las contraseñas usadas cuando los empleados dejen de laborar internamente o cambien de área, esto para evitar mal uso de información o accesos no deseados.

Tabla 38 (continuación)

	Otra recomendación es mantener la opción de “mostrar contraseña” desactivada cada que se requiera ingresar las contraseñas creadas por cada usuario, de esta manera se evita conocer los datos que ingresa cada usuario y filtración de datos o mal uso de la información.

Tabla 39. Prueba 2 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Inspección de catalogo contra incidentes de seguridad lógica"	
OBJETIVO DE PRUEBA	Indagar sobre la existencia de un catálogo, carpeta o archivo que contenga el historial de incidentes donde se vio afectada la seguridad lógica de los equipos y que contenga las medidas que se realizaron para resolver dichos inconvenientes.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se revisará el historial con el que cuentan acerca de los incidentes que comprometieron la seguridad lógica de los equipos, ya que es importante su registro para la consulta de este en caso de circunstancias similares. Se espera que dicho historial contenga acciones o bien los métodos o estrategias que se usaron para resolver cada uno de los inconvenientes y sirva como futura consulta para usuarios internos nuevos o simplemente para la resolución de eventos parecidos.
TÉCNICA	Observación, Análisis, Revisión, Inspección, Consulta.
ACTIVIDADES DE LA PRUEBA	1.- Revisar los archivos, bitácoras o carpetas donde se encuentren registrados antecedentes relacionados con la seguridad lógica de los equipos. 2.- Consultar y Analizar el historial de incidentes de seguridad lógica corroborando que exista un orden y registro correcto. 3.- Observar si dentro de dicho historial se encuentran estrategias, herramientas o soluciones a los eventos que estén registrados. 4.- Inspeccionar la frecuencia con la que han ocurrido los incidentes y revisar si existen patrones repetitivos que comprometan la seguridad de los equipos.

Tabla 39 (continuación)

PROCESO DE MEDICIÓN	**Excelente:** La UTIC cuenta con un historial de incidentes relacionados a seguridad lógica, debidamente registrado, ordenado y con soluciones a dichos eventos atendidos. **Bueno:** La UTIC cuenta con un historial de incidentes relacionados a seguridad lógica, debidamente registrado, en desorden, pero con soluciones a dichos eventos atendidos **Regular:** La UTIC cuenta con un historial de incidentes relacionados a seguridad lógica, registrado, desordenado, pero con soluciones a los eventos atendidos. **Suficiente:** La UTIC cuenta con registros de algunos incidentes relacionados a seguridad lógica, sin orden ni soluciones a dichos eventos. **Deficiente:** La UTIC no cuenta con registros ni historial sobre incidentes relacionados a seguridad lógica.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente.**
CONSIDERACIONES ESPECIALES	Se solicitó al jefe de la UTIC acceso a los archivos, carpetas y documentación correspondientes a su seguridad lógica para corroborar la existencia de dicho historial y su condición actual.
INTERPRETACIÓN DE RESULTADOS	La UTIC no cuenta con ningún registro de algunos incidentes relacionados con su seguridad lógica, los empleados comentan que han sufrido inconvenientes, sin embargo, no registraron el acontecimiento, fecha, y solución de dicha problemática, por lo que no hay como evidenciar la falta de dicho catálogo con problemáticas y soluciones enfocadas a seguridad lógica.

Tabla 39 (continuación)

RECOMENDACIONES	Acorde al estándar (ISO 27035:2013) en su apartado llamado **"5. Fase de Planeamiento y Preparación"** nos menciona en su sección **"5.1 Revisión de actividades claves"** que "La gestión eficaz de incidentes de seguridad de la información requiere un planeamiento y preparación apropiados. Para poder hacer operativo un esquema de gestión, vulnerabilidades, incidentes y eventos de seguridad de la información de manera eficiente y eficaz, una organización debería completar un número de actividades preparatorias luego del planeamiento necesario". Dichas actividades las cuales se requieren para cumplir con ellos son las siguientes: En su sección A menciona que "El personal necesita reconocer un incidente, saber qué hacer y comprender los beneficios del enfoque para la organización. La gerencia necesita mostrar su apoyo del esquema de gestión para asegurar que la organización se comprometa a brindar recursos y a mantener una capacidad de respuesta a los incidentes." En su sección C menciona la siguiente: "Actividad para definir y documentar un esquema detallado de gestión de incidentes de seguridad de la información. En general, la documentación del esquema debería abarcar los formularios, procedimientos, elementos organizativos y herramientas de apoyo para la detección y para la información de evaluación y toma de decisiones relacionadas a proporcionar respuestas a y lecciones aprendidas de los incidentes de seguridad de la información".

Tabla 39 (continuación)

	Los temas que se deben incluir son los siguientes: 1) Se debe utilizar una escala de clasificación de eventos / incidentes de seguridad de la información para graduar los eventos / incidentes. En cualquier caso, la decisión debería basarse en los impactos adversos reales. 2) Los formularios de eventos / incidentes / vulnerabilidades de seguridad de la información son: - Llenados por la persona que proporciona información sobre el evento de seguridad (es decir, no un miembro del equipo de gestión de incidentes de seguridad de la información), con la información registrada en una base de datos de eventos / incidentes /vulnerabilidades de seguridad de la información. - Llenados por la persona que reporta una vulnerabilidad de seguridad de la información (que todavía no ha sido explotada para causar un evento de seguridad de la información y posiblemente un incidente de seguridad de la información) con la información registrada en la base de datos de eventos / incidentes /vulnerabilidades de seguridad de la información. **RECOMENDACIÓN** Para dar solución a esta deficiencia y basándose en las estrategias que el estándar contiene, se propone que la UTIC cuente con un formato en el que se registren dichos incidentes que pongan en riesgo la seguridad lógica de la información, para esto es necesario que dicho formato sea capaz de almacenar los dato críticos del acontecimiento, como lo son fecha, hora, tipo de incidente, clasificación de acuerdo al impacto que este llega o puede llegar a tener en la información almacenada en la UTIC.

Tabla 39 (continuación)

	Este formato solo podrá ser llenado por el jefe de la unidad ya que garantiza que los datos registrados sean reales y sin error alguno. Además al finalizar el registro del incidente debe quedar explícitamente detallado ya que en situaciones futuras será consultado y tomara el papel de guía para la resolución de acontecimientos similares, evitando así un grado mayor de impacto o bien una resolución previa y para logar esto es indispensable que en el catálogo se registren las herramientas o bien lo que se requiere para dicha solución, además de las especificaciones de su uso, pero claro está que esto puede componer parte del desarrollo de la solución. Es por ello por lo que se propone contar con dicho formato digitalmente para que el llenado de este sea más ágil, y a su vez destinar una carpeta en donde dicho formato una vez llenado correctamente se imprima y se anexe como historial, así la consulta puede ser fácil siempre y cuando la carpeta este en un lugar de fácil acceso.

Tabla 40. Prueba 3 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Inspección de últimas versiones"	
OBJETIVO DE PRUEBA	Verificar que las aplicaciones y programas que usen para el desarrollo de las actividades internas de la UTIC cuenten con su versión más actual a la fecha.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se inspeccionan los programas y aplicaciones usados para el desarrollo de las actividades internas de la UTIC, dichas aplicaciones y/o programas considerados para las pruebas son aquellos en donde se manejan documentos, archivos y demás correspondientes a los formatos expedidos por el Ayuntamiento, es decir solo aquellas que manejen información y documentación oficial ya que los equipos de cómputo internos se ocupan para actividades administrativas resultantes de operaciones de campo en muchas de las veces. Se espera que dichas aplicaciones/programas estén funcionando con las versiones más actuales y disponibles a la fecha, lo que garantiza un correcto funcionamiento y el riesgo de problemas o brechas de seguridad sea mínimo.
TÉCNICA	Observación, Inspección, Investigación.
ACTIVIDADES DE LA PRUEBA	1.- Inspeccionar los equipos de cómputo de la UTIC, enfocándose en los programas y aplicaciones mencionados con anterioridad. 2.-Observar los programas y aplicaciones usados para la realización de las actividades internas de la UTIC. 3.- Investigar si dichas aplicaciones cuentan con una versión más actual disponible.

Tabla 40 (continuación)

PROCESO DE MEDICIÓN	**Excelente:** Todos los equipos de cómputo cuentan con las versiones más actuales de dichas aplicaciones y/o programas usados. **Bueno:** La mayoría de los equipos de cómputo cuentan con las versiones más recientes de dichas aplicaciones y/o programas. **Regular:** La mitad de los equipos cuentan con las versiones más recientes de dichas aplicaciones. **Suficiente:** El equipo principal de la UTIC cuenta con las actualizaciones más recientes de las aplicaciones y/o programas usados. **Deficiente:** Ninguno de los equipos cuenta con las actualizaciones más recientes de las aplicaciones y/o programas usados.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Excelente.**
CONSIDERACIONES ESPECIALES	Se solicito acceso a todos los equipos de cómputo internos de la UTIC, incluyendo os que cuentan con inicios de sesión protegidos, para poder indagar el estado de las aplicaciones y/o programas usados.
INTERPRETACIÓN DE RESULTADOS	Se accedió al equipo de cómputo en el apartado de aplicaciones y programas, al consultar que tipo de herramienta usan para el desarrollo de sus actividades, respondieron que principalmente la paquetería de Office, por lo que se encontró instalada la última versión en uso de esta herramienta, dicha versión es Microsoft Office Profesional Plus 2021.

Tabla 40 (continuación)

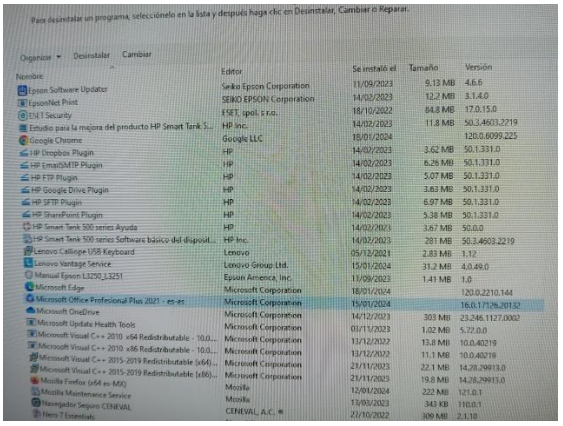
	Todos los equipos cuentan con la antes mencionada y los 6 empleados internos la usan para el desarrollo de sus actividades.  *Figura 128. Lista de aplicaciones que contiene el equipo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Lista de aplicaciones que contiene el equipo., 2023)*
RECOMENDACIONES	Acorde a la norma ISO 27002:2022 en su apartado llamado **"8. Controles Tecnológicos"** en su apartado **"8.1 Dispositivos de punto Final de Usuario"**, comenta que "La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debería protegerse", para esto la organización debería establecer una política de tema específico sobre la configuración segura y el manejo de los dispositivos de los terminales de los usuarios. La política de tópico específico debería comunicarse a todo el personal relevante. Para esto en su "e" menciona lo siguiente: e) requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para la aplicación de actualizaciones (por ejemplo, actualización automática activa);

Tabla 40 (continuación)

	RECOMENDACIÓN Para darle solución a esta vulnerabilidad y en base al apartado del estándar mencionado anteriormente, se recomienda que el jefe de la unidad sea el encargado de garantizar que los equipos sigan contando con la versión más actual posible, para esto puede activar la actualización automática o bien generar un recordatorio usual en u periodo de tiempo quincenal para evitar que una actualización pase desapercibida y en caso de esto sea poco el tiempo que pase al realizarla. Esto puede provocar una acción tediosa para los empleados, pero garantiza que las herramientas o bien la paquetería que usan para el desarrollo de sus aplicaciones se mantengan actualizada y funcionando perfectamente, evitando brechas o mal funcionamiento en el equipo directamente.

Tabla 41. Prueba 4 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Comprobación de Programa de Capacitación"	
OBJETIVO DE PRUEBA	Corroborar la existencia o falta de algún programa de capacitación sobre las mejores prácticas de seguridad informática y protección de datos.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es evaluar la efectividad y la adecuación del programa de capacitación a usuarios sobre las mejores prácticas de seguridad informática y protección de datos dentro de la organización. Se busca verificar si el personal está debidamente informado y capacitado para identificar, evaluar y responder adecuadamente a los riesgos relacionados con la seguridad lógica y protección de datos. Se espera identificar si el personal está adecuadamente informado, capacitado y preparado para abordar los riesgos específicos asociados con la seguridad lógica.
TÉCNICA	Revisión, Observación y Analizar
ACTIVIDADES DE LA PRUEBA	1. Revisar detalladamente el programa de capacitación en gestión de riesgos de seguridad lógica. 2. Entrevistar a empleados clave responsables de la seguridad lógica y protección de datos. 3. Evaluar su conocimiento sobre los procedimientos de seguridad y su comprensión de los riesgos asociados. 4. Analizar la participación del personal en el programa de capacitación. 5. Evaluar si se realizan simulacros o ejercicios prácticos para poner a prueba la capacidad del personal para gestionar situaciones de riesgo de seguridad lógica.

Tabla 41 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: El programa de capacitación en gestión de riesgos de seguridad informática y protección de datos es altamente efectivo y cumple con los estándares más altos. **Bueno**: El programa de capacitación es sólido y cubre de manera adecuada los aspectos clave de la gestión de riesgos de seguridad informática y protección de datos.
	Regular: Existen áreas identificadas que necesitan mejoras en el programa de capacitación. **Suficiente**: Se cumplen los requisitos mínimos para el programa de capacitación. **Deficiente**: No existe un programa de capacitación.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	No existe un programa de capacitación por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde al estándar (ISO 27002:2022) en su apartado llamado **"6.1 Conciencia, educación y entrenamiento sobre la seguridad de la información"** comenta que **"**El personal de la organización y las partes interesadas relevantes deberían recibir una adecuada concienciación, educación y capacitación en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral".

Tabla 41 (continuación)

	Dentro de sus generalidades comenta que “Se debería establecer un programa de concientización, educación y capacitación en seguridad de la información de acuerdo con la política de seguridad de la información de la organización, las políticas de tópico específico y los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la organización que debería protegerse y los controles de seguridad de la información que se han implementado. para proteger la información. La concientización, la educación y la capacitación en seguridad de la información deberían llevarse a cabo periódicamente. La concientización, la educación y la capacitación iniciales pueden aplicarse al personal nuevo y a aquellos que se transfieran a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes. La comprensión del personal debería evaluarse al final de una actividad de sensibilización, educación o formación. **RECOMENDACIÓN** Para dar solución a dicha vulnerabilidad y en base a lo antes mencionado de acuerdo con el estándar 27002:2022 se propone que la UTIC implemente diversas estrategias para maximizar la seguridad de la información y de los equipos de cómputo internos.

Tabla 41 (continuación)

	Para estas estrategias se propone una jerarquización de roles, principalmente asignar un líder dentro de la oficina quien será el encargado de supervisar y orientar a los demás trabajadores internos acerca de las responsabilidades que se les asignen, este mismo será encargado de la planificación y diseño de la arquitectura de red de la organización, asegurándose de que se implementen controles de seguridad adecuados en toda la infraestructura. También administrar quién tiene acceso a qué recursos dentro de la red, así como implementar políticas de contraseña Y para continuar dicha jerarquía se propone lo siguiente: Empleado 1: Administrador de Redes Responsabilidades: • Configuración y mantenimiento de switches, routers y otros dispositivos de red. • Monitoreo de la salud de la red y resolución de problemas de conectividad. • Mantenimiento de la integridad y disponibilidad de los servicios de red. Empleado 2: Administrador de Seguridad Responsabilidades: • Configuración y mantenimiento de firewalls, IDS/IPS y otros dispositivos de seguridad. • Análisis de logs y eventos de seguridad para detectar posibles amenazas. • Evaluación de vulnerabilidades y aplicación de medidas correctivas.

Tabla 41 (continuación)

	Empleado 3: Supervisor en Seguridad de Aplicaciones Responsabilidades: • Evaluación de la seguridad de aplicaciones y servicios en línea. • Desarrollo e implementación de políticas de seguridad para aplicaciones y bases de datos. • Pruebas de penetración y análisis de vulnerabilidades en aplicaciones. • Empleado 4: Encargado de mantenimiento en Infraestructura de Red. Responsabilidades: • Implementación y mantenimiento de infraestructura de red física y virtual. • Configuración y administración de servidores DNS, DHCP y otros servicios de red. • Optimización de la red para mejorar el rendimiento y la eficiencia. Empleado 5: Analista de Seguridad Responsabilidades: • Análisis de amenazas y tendencias de seguridad. • Investigación de incidentes de seguridad y elaboración de informes. • Sensibilización y formación del personal sobre prácticas de seguridad. De esta manera cada empleado tendrá responsabilidades relacionadas con la seguridad lógica del área, atendiendo diferentes aspectos vulnerables del área.

Tabla 42. Prueba 5 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Revisión de Copias de Seguridad"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es verificar si la organización realiza copias de seguridad de los sistemas y datos en algún lugar externo seguro.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es evaluar la regularidad y existencia de copias de seguridad de los sistemas, datos e información interna de la UTIC. Se busca verificar si se llevan a cabo dichas copias de seguridad dentro de la organización ya que es una medida principal en base a la seguridad lógica de los equipos, Se espera encontrar que los empleados internos de la UTIC realicen copias de seguridad de los sistemas y datos periódicamente y que estas sean almacenados o bien realizadas en un lugar externo seguro.
TÉCNICA	Observación, Análisis, Inspección
ACTIVIDADES DE LA PRUEBA	1.- Observar el proceso de realización de copias de seguridad por parte de los empleados de la UTIC. 2.- Analizar el proceso de realización de copias de seguridad por parte de los empleados, como inicia y como finaliza dicho proceso. 3.- Inspeccionar la realización de copias de seguridad para corroborar la existencia de su almacenado y protección desde un lugar externo seguro.
PROCESO DE MEDICIÓN	**Excelente**: Se realizan copias de seguridad periódicamente sobre todos los datos importantes internos de la UTIC y se protegen en un lugar externo seguro. **Bueno**: Se realizan copias de seguridad periódicamente sobre la mayoría de los datos importantes internos de la UTIC y se protegen en un lugar externo seguro. **Regular**: Se realizan copias de seguridad periódicamente en algunos datos importantes internos de la UTIC, pero no se protegen en un lugar externo seguro.

Tabla 42 (continuación)

	Suficiente: se realizan copias de seguridad rara la vez en algunos datos importantes de la UTIC, pero no se protegen en un lugar externo seguro. **Deficiente**: No se realizan copias de seguridad alguna, por lo que tampoco hay un lugar externo seguro donde almacenar.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	La UTIC no realiza copias de seguridad de los datos o información que contengan sus equipos por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde al estándar (ISO 27002:2022) en su apartado llamado **"8.13 Respaldo de la información"** donde menciona que "Las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse regularmente en de acuerdo con la política de tópico específico acordada sobre copias de seguridad" para permitir la recuperación de la pérdida de datos o sistemas. Menciona que "Se deberían desarrollar e implementar planes sobre cómo la organización respaldará la información, software y sistemas, para abordar la política de tópico específico sobre copias de seguridad".

Tabla 42 (continuación)

	Al diseñar un plan de respaldo, se deberían tener en cuenta los siguientes elementos: 1) Producir registros precisos y completos de las copias de seguridad y restauración documentada procedimientos; 2) Almacenar las copias de seguridad en un lugar remoto seguro y protegido, a una distancia suficiente para escapar de cualquier daño por un desastre en el sitio principal; **RECOMENDACIÓN** Para atender dicha vulnerabilidad con base a las al estándar ISO 27002:2022 mencionado anteriormente se recomienda que la UTIC realice copias de seguridad de los datos y la información relevante que contengan los equipos de cómputo internos, para ello se propone el desarrollo de un formato para registrar cuando se realicen dichos registros, además de crear un archivo o carpeta ya sea física o digital que contenga historial de las copias de seguridad realizadas. De igual manera se recomienda realizar las copias de seguridad y almacenarlas en un lugar seguro y remoto, se puede recomendar almacenarlas en la nube para tener acceso a la información en cualquier lugar y en cualquier momento. Se propone la contratación del servicio de almacenamiento en la nube “OneDrive” de Microsoft ya que es una muy buena opción para comenzar a almacenar las copias de seguridad que generen de los datos más relevantes para la UTIC,}

Tabla 42 (continuación)

	OneDrive cuenta con una versión gratuita disponible que permite acceder a documentos y archivos desde cualquier dispositivo y lugar, compartir archivos con otros usuarios, trabajar colaborativamente en archivos de office en tiempo real y respaldo de los archivos trabajados directamente en OneDrive.

Tabla 43. Prueba 6 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Actualizaciones Omitidas o No compartibles"	
OBJETIVO DE PRUEBA	Comprobar que las actualizaciones de las aplicaciones y sistemas en uso se realicen y no se posterguen por acciones de los empleados.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es asegurarse de que las actualizaciones de los sistemas y aplicaciones usados en los equipos de cómputo internos de la UTIC se realicen. Se espera que dichas actualizaciones no se encuentren paradas, postergadas o pausadas por causas externas o bien por motivos de los trabajadores.
TÉCNICA	Observación, Análisis, Inspección, Indagación
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar cada uno de los equipos de cómputo adentrándose en las aplicaciones y sistemas que usan para el desarrollo de sus actividades. 2. Observar la versión de los sistemas y aplicaciones con la que cuentan los equipos de cómputo. 3. Indagar cual es la versión de los sistemas y aplicaciones utilizados en los equipos y analizar si coincide con la usada o hay actualizaciones pendientes. 4. En caso de actualizaciones pendientes o bien versiones de disponibles recientes a la fecha, indagar el motivo de por qué no se han actualizado o instalado dichas versiones.
PROCESO DE MEDICIÓN	**Excelente**: Los empleados mantienen las aplicaciones y sistemas de los equipos de cómputo internos, debidamente actualizados o en su versión más reciente dentro del horario laboral.

Tabla 43 (continuación)

	Bueno: Los empleados realizan las actualizaciones de algunos de los sistemas y aplicaciones de los equipos de cómputo internos en horario laboral. **Regular**: Los empleados realizan algunas actualizaciones de los sistemas y aplicaciones de los equipos de cómputo internos en horario laboral. **Suficiente**: Los empleados realizan pocas actualizaciones de los sistemas y aplicaciones de los equipos de cómputo internos en horario laboral. **Deficiente**: Los empelados prefieren posponer las actualizaciones de los sistemas y aplicaciones de los equipos de cómputo internos durante el horario laboral.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.
CONSIDERACIONES ESPECIALES	Se solicito acceso a cada uno de los equipos de cómputo internos de la UTIC respectivamente a los empleados que los usan, para inspeccionar si hay actualizaciones pendientes, además de preguntar a cada uno de ellos por qué se posponen las mismas en caso de su existencia.
INTERPRETACIÓN DE RESULTADOS	Una vez inspeccionados los equipos se encontró que dos de los 6 equipos de cómputo internos de la UTIC cuentan con actualizaciones pendientes o bien en espera, los empleados respectivos a dichos equipos comentan que cuando el equipo de cómputo avisa que hay una nueva actualización o versión disponible, ´la posponen para continuar trabajando o realizando sus actividades.

Tabla 43 (continuación)

	Evidencia de actualización en espera y postergada por los empleados de la UTIC en uno de los equipos internos.  *Figura 129. Actualización Postergada. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Actualización Postergada, 2023)* Evidencia de actualización en espera y postergada por los empleados de la UTIC en uno de los equipos internos.  *Figura 130. Actualización Postergada en otro equipo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Actualización Postergada en otro equipo, 2023)*

Tabla 43 (continuación)

RECOMENDACIONES	Acorde al estándar (ISO 27002:2022) en su apartado llamado **"8.19 Instalación de software en sistema operacionales"** el cual menciona "Deberían implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos" para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas. Indicando en su apartado **"a"** lo siguiente: a) realizar actualizaciones del software operativo solo por parte de administradores capacitados según corresponda autorización de gestión. Así mismo en su apartado **"8.9 Gestión de la configuración"** menciona que "Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deberían establecerse, documentarse, implementarse, monitorearse y revisarse" con el propósito de garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida. Este a su vez menciona que "La organización debería definir e implementar procesos y herramientas para hacer cumplirlas configuraciones definidas (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para los sistemas recién instalados, así como para los sistemas operativos durante su vida útil". Y en su sección "g" comenta lo siguiente: g) invocar instalaciones que se encuentren de tiempo de espera que desconectan automáticamente los dispositivos informáticos después de un período predeterminado de inactividad;

Tabla 43 (continuación)

	RECOMENDACIÓN Para atender la vulnerabilidad anterior y de acuerdo con lo mencionado referente al estándar ISO 27002:2022 se recomienda que la UTIC asigne a un encargado de acuerdo con sus roles, en este caso se propone que el responsable sea el jefe de la unidad, para que monitoree y supervise que los empleados mantengan actualizados sus equipos de cómputo tratándose del sistema operativo que manejan en este caso Windows. De igual manera se recomienda implementar dentro de política del lugar un apartado donde comprometa a los empleados a mantener sus sistemas actualizados a la versión más reciente y no tener actualizaciones en espera. Esto acompañado de una sanción o un reporte que garantice que os empleados estarán pendientes de nuevas actualizaciones disponibles para sus equipos de cómputo. Llevar un registro de la realización de la actualización, indicando la fecha, la hora de inicio y la hora de termino o bien instalación, indicando quien la realizo, para tener un control más detallado sobre dichas actualizaciones y como respaldo en caso de una contrariedad por parte del fabricante (Microsoft Windows). Se propone que se dé una breve capacitación o introducción sobe este proceso referente a las actualizaciones o bien un manual del proceso a los usuarios nuevo o temporales para que mantengan de igual forma los equipos actualizados.

Tabla 44. Prueba 7 de Seguridad Lógica. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Copias de seguridad periódicas"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es verificar si la organización realiza copias de seguridad de los sistemas y datos almacenados en los equipos de manera periódica.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El propósito principal de esta prueba es evaluar la regularidad y existencia de copias de seguridad de los sistemas, datos e información almacenados en los equipos internos de la UTIC. Se busca verificar si se llevan a cabo dichas copias de seguridad dentro de la organización ya que es una medida principal en base a la seguridad lógica de los equipos, Se espera encontrar que los empleados internos de la UTIC realicen copias de seguridad de los sistemas y datos periódicamente.
TÉCNICA	Observación, Análisis, Inspección.
ACTIVIDADES DE LA PRUEBA	1.- Observar el proceso de realización de copias de seguridad por parte de los empleados de la UTIC. 2.- Analizar el proceso de realización de copias de seguridad por parte de los empleados, como inicia y como finaliza dicho proceso. 3.- Inspeccionar la realización de copias de seguridad para corroborar la existencia de su almacenado.
PROCESO DE MEDICIÓN	**Excelente**: Se realizan copias de seguridad periódicamente sobre todos los datos importantes internos de la UTIC. **Bueno**: Se realizan copias de seguridad periódicamente sobre la mayoría de los datos importantes internos de la UTIC. **Regular**: Se realizan copias de seguridad periódicamente en algunos datos importantes internos de la UTIC. **Suficiente**: se realizan copias de seguridad rara la vez en algunos datos importantes de la UTIC. **Deficiente**: No se realizan copias de seguridad alguna.

Tabla 44 (continuación)

CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	La UTIC no realiza copias de seguridad de los datos o información que contengan sus equipos por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde al estándar (ISO 27002:2022) en su apartado llamado **"8.13 Respaldo de la información"** donde menciona que "Las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse regularmente en de acuerdo con la política de tópico específico acordada sobre copias de seguridad" para permitir la recuperación de la pérdida de datos o sistemas. Menciona que "Se deberían desarrollar e implementar planes sobre cómo la organización respaldará la información, software y sistemas, para abordar la política de tópico específico sobre copias de seguridad". Al diseñar un plan de respaldo, se deberían tener en cuenta los siguientes elementos: 1) Producir registros precisos y completos de las copias de seguridad y restauración documentada procedimientos; 2) Almacenar las copias de seguridad en un lugar remoto seguro y protegido, a una distancia suficiente para escapar de cualquier daño por un desastre en el sitio principal;

Tabla 44 (continuación)

	3) Reflejar los requisitos de seguridad de la información involucrada y la criticidad de la información a la operación continua de la organización en la medida (por ejemplo, respaldo completo diferencial) y frecuencia de las copias de seguridad; **RECOMENDACIÓN** Para atender dicha vulnerabilidad con base a la norma ISO 27002:2022 mencionado anteriormente se recomienda que la UTIC realice copias de seguridad de los datos y la información relevante que contengan los equipos de cómputo internos, para ello se propone el desarrollo de un formato para registrar cuando se realicen dichos registros, además de crear un archivo o carpeta ya sea física o digital que contenga historial de las copias de seguridad realizadas. De igual manera se recomienda realizar las copias de seguridad y almacenarlas en un lugar seguro y remoto, se puede recomendar almacenarlas en la nube para tener acceso a la información en cualquier lugar y en cualquier momento. Se propone la contratación del servicio de almacenamiento en la nube “OneDrive” de Microsoft ya que es una muy buena opción para comenzar a almacenar las copias de seguridad que generen de los datos más relevantes para la UTIC.

Tabla 44 (continuación)

	OneDrive cuenta con una versión gratuita disponible que permite acceder a documentos y archivos desde cualquier dispositivo y lugar, compartir archivos con otros usuarios, trabajar colaborativamente en archivos de office en tiempo real y respaldo de los archivos trabajados directamente en OneDrive. Se propone que dichas copias de seguridad se realicen al menos una vez semanalmente ya que de acuerdo con el tipo de actividades administrativas que realizan internamente una semana es tiempo suficiente para que se almacene una gran cantidad de trabajo y realizar nuevamente el trabajo perdido en caso de no tener respaldos se sumaría a esa carga de trabajo y causaría una saturación en las labores de la UTIC.

3.2.1.6 Actividad 2.6 Realizar Pruebas de Servicios.

3.2.1.6.1 Descripción de la actividad

En esta actividad se requiere visitar las instalaciones de la UTIC ya que de esta manera es más fácil detectar aquellas anomalías que pueda presentar en los servicios con los que cuenta de la unidad, dicho esto se hace una mayor observación e inspección en los sistemas de atención contra emergencias en la UTIC, ya que a simple vista hay una notable falta de organización en esos sistemas, ya que esta no es la adecuada de acuerdo a las normas y estándares disponibles que aplican dentro de la UTIC, los sistemas de emergencia considerados para las pruebas y que tiene un mayor impacto en el área son los sistemas de protección contra incendios y el equipo médico interno (botiquín) en donde al parecer su implementación no es la correcta, los antes mencionados están situados en el suelo y en otra oficina respectivamente.

3.2.1.6.2 Resultado de la actividad

Tabla 45. Prueba 1 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Uso de enchufes eléctricos"	
OBJETIVO DE PRUEBA	El principal objetivo de esta prueba es verificar si los enchufes eléctricos instalados dentro de la UTIC son los suficientes para satisfacer todos los equipos utilizados internamente.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Como propósito de la prueba es comprobar la existencia de enchufes eléctricos dentro de la UTIC, así mismo saber si son los necesarios para satisfacer todos los equipos que usan internamente. Se espera que los enchufes eléctricos sean los necesarios para satisfacer todos los equipos que usan internamente, además de corroborar que estén instalados debidamente.
TÉCNICA	Observación, Verificación, Inspección.

Tabla 45 (continuación)

ACTIVIDADES DE LA PRUEBA	1. Inspeccionar la ubicación de los enchufes eléctricos instalados internamente en la UTIC. 2. Verificar si dichos enchufes eléctricos están debidamente instalados. 3. Observar si los enchufes eléctricos instalados son suficientes para satisfacer a todos los equipos internos de la UTIC. 4. Conocer qué tipo de medidas implementan en caso de que requieran un mayor número de contactos eléctricos al existente en los enchufes actuales.
PROCESO DE MEDICIÓN	**Excelente**: Los enchufes eléctricos internos en la UTIC son los suficientes para satisfacer a todos los equipos usados internamente, están debidamente instalados y no requieren implementar alguna solución contra una posible ausencia de estos. **Bueno**: Los enchufes eléctricos internos en la UTIC son los suficientes para satisfacer a todos los equipos usados internamente, la mayoría están debidamente instalados y no requieren implementar alguna solución contra una posible ausencia de estos. **Regular**: Los enchufes eléctricos internos en la UTIC son los suficientes para satisfacer a todos los equipos usados internamente, no están debidamente instalados y no requieren implementar alguna solución contra una posible ausencia de estos. **Suficiente**: Los enchufes eléctricos internos en la UTIC satisfacen a la mayoría de los equipos usados internamente, no están debidamente instalados y provocan una saturación y equipos enchufados. **Deficiente**: Los enchufes eléctricos internos en la UTIC no satisfacen todos los equipos usados internamente, no están debidamente instalados y provocan una saturación de equipos

Tabla 45 (continuación)

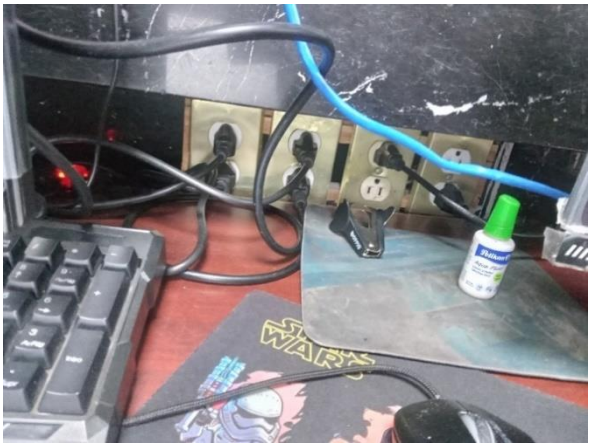
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Se revisó el interior de la UTIC buscando la ubicación de los enchufes eléctricos debidamente instalados, por lo que se encontró que cuentan solo con 7 contactos instalados correctamente.  *Figura 131. Vista 1 de los contactos eléctricos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 1 de los contactos eléctricos, 2023)*

Tabla 45 (continuación)

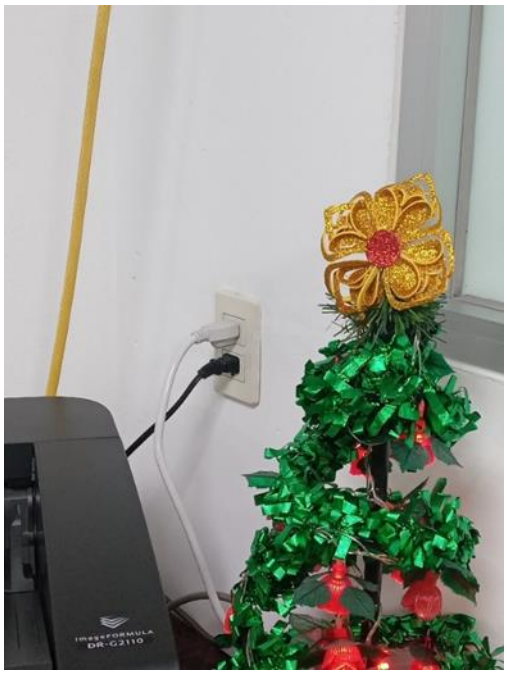


Figura 132. Vista 2 de los contactos eléctricos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 2 de los contactos eléctricos, 2023)

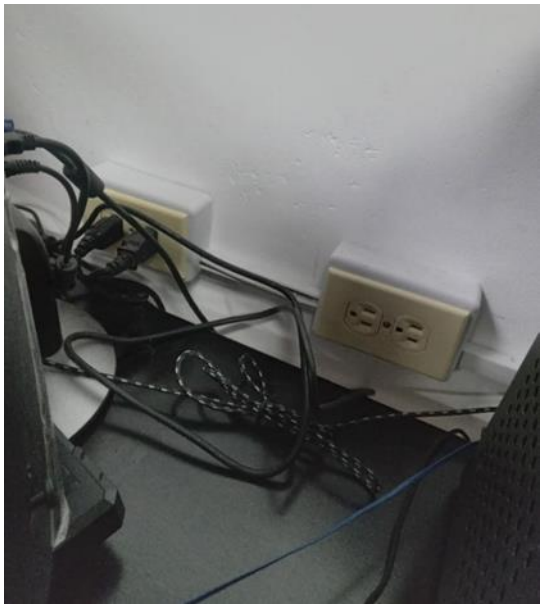


Figura 133. Vista 3 de los contactos eléctricos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 3 de los contactos eléctricos, 2023)

Tabla 45 (continuación)

	Además de ello, los equipos ubicados en el escritorio principal son alimentados por una bajada de corriente del techo falso, pasando por el marco de la puerta del cuarto del SITE y por una canaleta en el suelo, este brinda energía a un regulador que da oportunidad de enchufar diversos aparatos.

Tabla 45 (continuación)

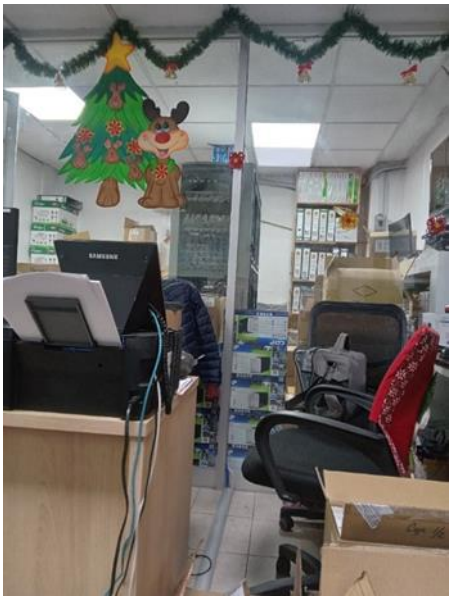


Figura 134. Bajada del contacto eléctrico. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Bajada del contacto eléctrico, 2023)



Figura 135. Bajada del contacto eléctrico. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Bajada del contacto eléctrico, 2023)

Tabla 45 (continuación)

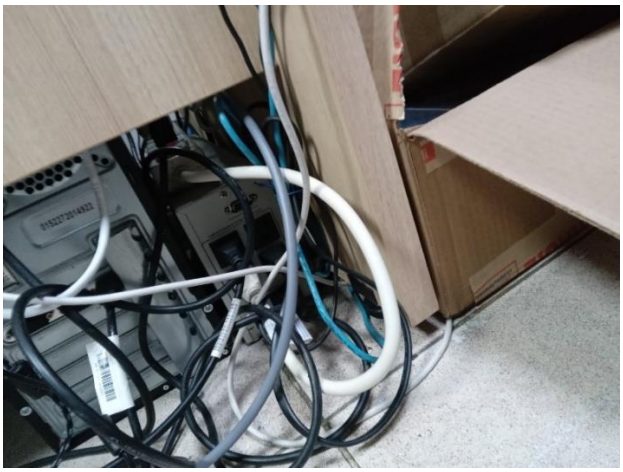


Figura 136. Extensiones eléctricas. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extensiones eléctricas, 2023)

La UTIC opto por implementar extensiones eléctricas, para ampliar el número de contactos eléctricos en donde puedan enchufar los dispositivos que usan cotidianamente.

En la siguiente imagen se muestra el tipo de extensiones que implementaron.

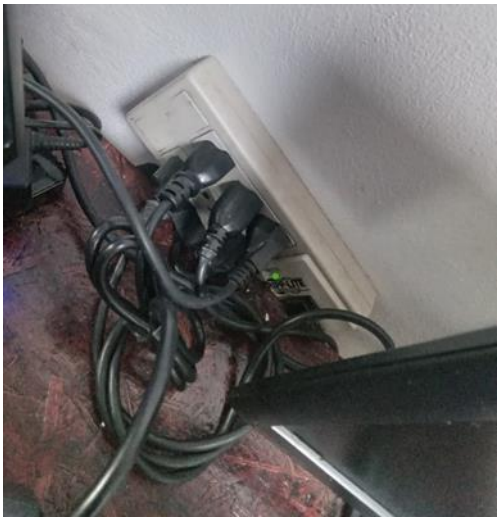


Figura 137. Extensiones eléctricas. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extensiones eléctricas, 2023)

Tabla 45 (continuación)

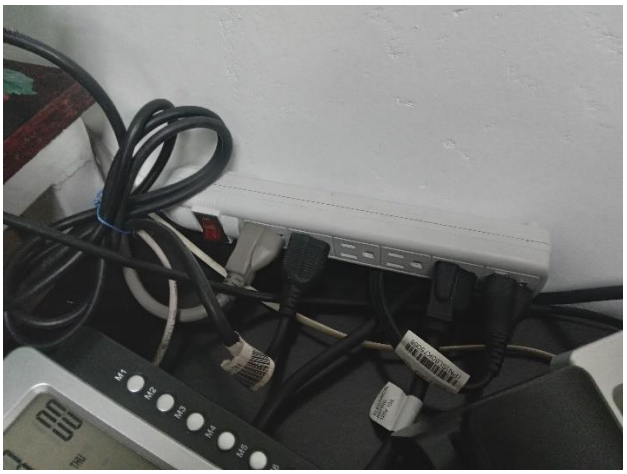
	 ***Figura 138. Extensiones eléctricas. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extensiones eléctrticas, 2023)*** Se llego a la conclusión de que los enchufes eléctricos internos de la UTIC no son los suficientes para satisfacer a todos los equipos con los que cuentan y requieren una alimentación de energía, por lo que se implementaron extensiones multicontactos para así tener mayor capacidad de enchufe y disponibilidad para todos los equipos, sin embargo, esto puede llegar a provocar una saturación de energía, calentamiento o corto circuito.

Tabla 45 (continuación)

RECOMENDACIONES	Acorde a la Norma Oficial Mexicana (NOM-001-SEDE-2012) en su artículo 240 llamado **"PROTECCION CONTRA SOBRECORRIENTE"** menciona que "La protección contra sobre corriente para conductores y equipos se instala para que abra el circuito, si la corriente alcanza un valor que cause una temperatura excesiva o peligrosa en los conductores o en su aislamiento" así mismo menciona que un "**Dispositivo de protección contra sobrecorriente tipo limitador de corriente"** es un dispositivo que, cuando interrumpe corrientes dentro de su rango de limitación de corriente, reduce la corriente que fluye en el circuito con falla a una magnitud significativamente menor que la que se tendría en el mismo circuito, si el dispositivo fuera reemplazado por un conductor sólido de impedancia comparable. En su apartado 240-4 llamado **"Protección de los conductores"** menciona que los conductores que no sean cordones flexibles, cables flexibles ni alambres de luminarias, se deben proteger contra sobrecorriente de acuerdo con su ampacidad. De igual manera en su Artículo 240-15 **"Conductores de fase"** especifica en su apartado **"a"** lo siguiente: Dispositivo de protección contra sobrecorriente requerido. a) Se debe conectar un fusible o una unidad de disparo por sobrecorriente de un interruptor automático, en serie con cada conductor de fase. Se considerará que una combinación de transformador de corriente y un relevador de sobrecorriente equivale a una unidad de disparo por sobrecorriente.

Tabla 45 (continuación)

	Por último, en su sección B llamada **"Ubicación"** y en su artículo 240-21 **"Ubicación en el circuito"** indica en qué lugar deben ir colocados estos dispositivos con lo siguiente: **240-21. Ubicación en el circuito:** Se debe proporcionar protección contra sobrecorriente en cada conductor de fase del circuito, y debe estar ubicada en el punto en el que los conductores reciben su alimentación.

Tabla 45 (continuación)

	RECOMENDACIÓN Para atender dicha vulnerabilidad y en base a lo estipulado de la norma mencionada con anterioridad, se recomienda como primera instancia que la UTIC no sobre cargue con el uso de dispositivos las extensiones o “multicontactos” usados, ya que esto evita una menor acumulación de energía la cual llega a causar sobrecalentamiento y corto circuito. Parte de la recomendación es el reemplazo y la implementación de Sistemas de Alimentación Ininterrumpida, pues estos a diferencia de los reguladores de voltaje y las extensiones brindan diferentes funciones que pueden favorecer el desempeño de la UTIC. Entre las funciones que desempeñan dichos sistemas o bien conocidos como UPS por sus siglas en ingles “Uninterruptible Power Supply” se encuentran las siguientes. • Proporciona energía de respaldo durante cortes de energía eléctrica. Utiliza baterías internas para mantener la energía durante un tiempo limitado. • Protege contra cortes de energía, fluctuaciones de voltaje, caídas de tensión y sobretensiones.

Tabla 45 (continuación)

	• Además de proporcionar energía de respaldo, algunos UPS pueden incluir características como regulación de voltaje y supresión de picos de voltaje. • Es comúnmente utilizado para proteger equipos sensibles como computadoras, servidores, sistemas de comunicaciones y dispositivos electrónicos críticos. Por lo que se recomienda su uso para prevenir algún apagón no deseado, interrupción de actividades, corto circuito y daño en los dispositivos por excesos de corriente eléctrica “sobre corriente”.

Tabla 46. Prueba 2 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "propagación de Incendio"	
OBJETIVO DE PRUEBA	Conocer la situación actual de la UTIC relacionada a estar preparados en caso de posibles incendios, saber si cuentan con el equipo indicado para evitar una propagación o bien una mayor magnitud de este.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	La prueba se concentra principalmente en identificar las medidas o el equipo con el que cuenta la UTIC en caso de sufrir un incendio, conocer si hay escenarios que puedan provocar una propagación. Se espera que la UTIC cuente con el equipo necesario para poder atender posibles incendios, ya que se trata de un área en donde se encuentran equipos de cómputo y redes enchufadas a contactos eléctricos, además de que no cuenten con escenarios que puedan causar un mayor impacto y propagación de este.
TÉCNICA	Inspección, Observación, Análisis,
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar el material con el que cuenta la UTIC para atender posibles incendios, ya que existen distintos tipos de herramientas y de compuestos para estos casos. 2. Análisis que dicho material sea el indicado para un área de trabajo como la UTIC la cual a su vez tienen dentro el espacio donde se ubica el site. 3. Observar con detenimiento los espacios y puntos críticos de la UTIC, es decir aquellos en donde es más probable ocurra un incendio y analizar los posibles escenarios que pueden llegar a ocurrir en caso de un incendio.

Tabla 46 (continuación)

	4. Buscar alguna solución o bien cambio que pueda evitar la propagación o un mayor impacto ante un posible incendio.
PROCESO DE MEDICIÓN	**Excelente**: La UTIC cuenta con más de 3 unidades del equipo indicado en caso de un posible incendio y no tiene ningún escenario que cause fácil propagación de este. **Bueno**: La UTIC cuenta con más de 2 unidades del equipo indicado en caso de un posible incendio y no tiene ningún escenario que cause fácil propagación de este. **Regular**: La UTIC cuanta con más de 1 unidad del equipo indicado en caso de un posible incendio y no tiene ningún escenario que cause fácil propagación de este. **Suficiente**: La UTIC cuanta con 1 unidad o más de 1, del equipo indicado en caso de un posible incendio y tiene 1 o más escenarios que causen fácil propagación de este. **Deficiente**: La UTIC no cuenta con el equipo indicado en caso de un posible incendio y tiene 1 o más escenarios que causen fácil propagación de este.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.

Tabla 46 (continuación)

CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	Analizando el equipo con el que cuenta la UTIC para combatir posibles incendios, se llegó a la conclusión de que es el indicado ya que es un extintor de clase C, este tipo de extintores están diseñados para combatir incendios en equipos eléctricos energizados, como dispositivos eléctricos, equipos electrónicos y sistemas de cableado. Estos extintores contienen agentes extintores que no son conductores de electricidad para garantizar la seguridad del usuario y minimizar el riesgo de descargas eléctricas, cuentan con dos unidades de este equipo que bien pueden ser suficientes para atender una emergencia. Extintor Situado en el Suelo detrás de la puerta de acceso en el área de actividades de la UTIC.  *Figura 139. Extintor 1. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extintor 1, 2023)*

Tabla 46 (continuación)

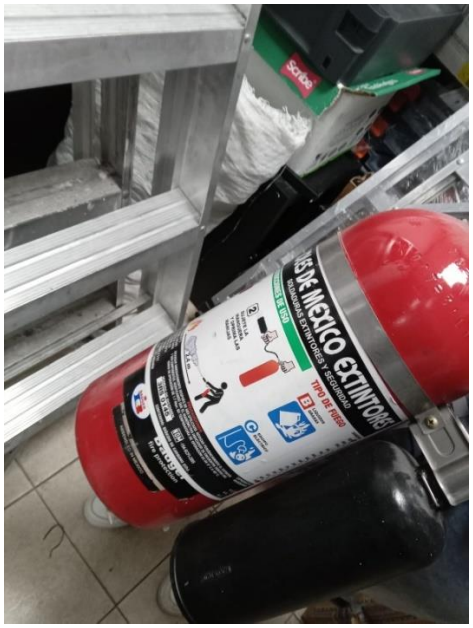
	Extintor situado en el suelo detrás de la puerta de acceso del site y rodeado de activos y objetos que impiden su fácil accesibilidad.  *Figura 140. Extintor 2. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extintor 2, 2023)* Por otro lado, se analizaron los posibles escenarios en donde un incendio es fácil de propagarse y se encontraron los siguientes. Debajo de la caja de corriente alterna se encuentran posicionados archivos varios, papeles, folders, cajas vacías y material inflamable que puede aportar a una propagación mayor de un incendio.

Tabla 46 (continuación)

	 ***Figura 141. Archivos Físicos bajo la corriente alterna de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Archivos Físicos bajo la corriente alterna de la UITC, 2023)*** Además, en el exterior de la UTIC, se encuentra colocado un extintor de polvo (ABC), pues es el más común en caso de un incendio, es por ello por lo que al no ser el interior de la UTIC se permiten colocar otro tipo de herramienta para atender otro tipo de incendios. Extintor correctamente ubicado al exterior de la UTIC

	 ***Figura 142. Extintor fuera de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extintor fuera de la UTIC, 2023)***

Tabla 46 (continuación)

RECOMENDACIONES	Acorde a la **"National Fire Protection Association"** o bien Asociación Nacional de Protección contra Incendios la "**NFPA 10"** es un estándar que especifica normas y requisitos para la instalación, inspección, mantenimiento y uso de extintores portátiles de incendio. Menciona como primer enfoque la ubicación de los extintores pues especifica que de acuerdo con su peso será la distancia que tendrá entre su posición y el suelo. Esto se refiere a "Si el extintor pesa 18,14 Kg, este debe ser colocado a 1.53 metros del suelo, en caso de que este pese menos debe ser colocado a 1.07 m de distancia del suelo acompañado siempre de un soporte que permitirá su fácil acceso". La ubicación de los Extintores debe ser despejada en su totalidad, evitando estar colocados detrás de columnas u objetos que impidan su visualización y localización. De igual manera menciona que "Los extintores deben ser ubicados y fijados al exterior de las puertas de acceso"

Tabla 46 (continuación)

	Otro punto es la clasificación pues en su apartado llamado **“Tipos y Clasificación de Extintores e Incendios”** comenta lo siguiente: **Extintores de Agua (Clase A):** - Son efectivos en incendios que involucran materiales combustibles sólidos como madera, papel, tela y plástico. - No son adecuados para incendios de líquidos inflamables o materiales energizados eléctricamente debido al riesgo de descarga eléctrica. **Extintores de Polvo Químico (Clase B y C):** - Clase B: Son efectivos en incendios que involucran líquidos inflamables como gasolina, aceites, pinturas y solventes. - Clase C: Son adecuados para incendios que involucran equipos energizados eléctricamente. - Son versátiles y ampliamente utilizados en entornos industriales y comerciales. **Extintores de Dióxido de Carbono (CO2) (Clase B y C):** - Clase B: Son efectivos en incendios que involucran líquidos inflamables. - Clase C: Son adecuados para incendios en equipos energizados eléctricamente. - No dejan residuos, por lo que son ideales para equipos electrónicos y salas de servidores.

Tabla 46 (continuación)

	Extintores de Espuma (Clase A y B): - Clase A: Son efectivos en incendios de materiales sólidos combustibles. - Clase B: Son adecuados para incendios de líquidos inflamables. - La espuma sofoca el fuego y evita su propagación. **Extintores de Polvo Específico (Clase D):** - Son diseñados para incendios que involucran metales combustibles como magnesio, titanio y sodio. - No son adecuados para otros tipos de incendios y deben ser utilizados por personal capacitado. **Clasificación de Incendios:** • **Clase A:** Incendios que involucran materiales sólidos combustibles como madera, papel, tela y plástico. • **Clase B:** Incendios que involucran líquidos inflamables como gasolina, aceites, pinturas y solventes. • **Clase C:** Incendios en equipos energizados eléctricamente. • **Clase D:** Incendios que involucran metales combustibles como magnesio, titanio y sodio. • **Clase K:** Incendios de aceites y grasas de cocina, comúnmente encontrados en cocinas comerciales.

Tabla 46 (continuación)

	RECOMENDACIÓN: Es por ello por lo que para atender la vulnerabilidad anterior y de acuerdo con la norma mencionada se recomienda que la UTIC coloque el extintor ubicado en el interior del cuarto del site fijado contra la pared a una altura de acuerdo a su peso, sin embargo, en caso de no poder realizar dicha colocación, se recomienda ubicarlo en un espacio visible al entrar al site y totalmente despejado para evitar tropiezos o accidentes. Realizar pruebas de control anuales y mantenimiento para poder asegurarse de que el equipo se mantenga en condiciones óptimas, esto claro con ayuda de especialistas locales en este caso se recomienda solicitarlas al equipo de Protección Civil del Municipio. Despejar completamente el escenario considerado como peligroso y mencionado en los resultados de esta prueba, pues es notablemente apto para una propagación en caso de un incendio generado por la caja de corriente que se encuentra encima, además de ordenar los activos situados en el suelo que permitan al menos el libre paso para poder atender el posible incendio. Mantener los activos, documentos o materiales con un mayor índice de ser inflamables, lejos de los contactos ubicados dentro del site, a falta de espacio está claro que habrá activos y objetos cercanos, sin embargo, mantenerlos ordenador para minimizar un poco el nivel de riesgo en caso de corto circuito.

Tabla 47 Prueba 3 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Presencia de Botiquín Médico"	
OBJETIVO DE PRUEBA	Corroborar la existencia de un servicio médico interno (botiquín) dentro de la UTIC, que garantice la atención a emergencias o accidentes de poca gravedad en los empleados dentro del área de trabajo.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El principal enfoque de la prueba es inspeccionar si la UTIC cuenta con el servicio médico interno mejor conocido como (Botiquín médico), el cual garantiza la atención a heridas o accidentes de poca gravedad en los empleados internos, además de analizar si cuanta con lo necesario y está debidamente actualizado. Se espera que la UTIC cuente con su propio botiquín médico para atender emergencia y/o accidentes que puedan ocurren en horario laboral y por parte de los trabajadore, que cuente con lo indispensable para situaciones de poca gravedad, que esté totalmente actualizado o bien su contenido este vigente y este ubicado en un lugar de fácil acceso para cuando se requiera.
TÉCNICA	Inspección, Observación, Análisis,
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar si la UTIC cuanta con su propio botiquín médico para atender emergencias internas que puedan llegar a presentarse. 2. Analizar si su contenido es el correcto, es decir cuente con lo necesario y que este esté debidamente vigente para su uso. 3. Observar el lugar en donde se encuentra dicho botiquín para analizar si se es un lugar de fácil acceso o hay restricciones para hacer uso de este.

Tabla 47 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: La UTIC cuenta con un botiquín medico interno, ubicado en un lugar de fácil acceso, con lo indispensable en su interior y claramente vigente para su uso e implementación. **Bueno**: La UTIC cuenta con un botiquín medico interno, ubicado en un lugar de fácil acceso, con lo indispensable en su interior y la mayoría de su contenido vigente para su uso e implementación. **Regular**: La UTIC cuenta con un botiquín medico interno, ubicado en un lugar de fácil acceso, con lo indispensable en su interior y la mitad de su contenido vigente para su uso e implementación. **Suficiente**: La UTIC cuenta con un botiquín medico interno, mal ubicado, cuenta con lo indispensable en su interior, pero la mayoría de su contenido no está vigente para su uso e implementación. **Deficiente**: La UTIC no cuenta con un botiquín medico interno.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Se solicito al jefe de la UTIC mostrara la ubicación del Botiquín Medico al que tienen acceso, además de permiso a la Lic. Mariana Celes Diaz enlace que es la encargada de este, para poder inspeccionar el contenido del botiquín y verificar que sea el adecuado.
INTERPRETACIÓN DE RESULTADOS	Revisada la situación se llegó a la conclusión de que el departamento de la UTIC no cuenta con un botiquín medico propio, sin embargo, tiene acceso a uno instalado dentro de la dependencia, además se revisó el contenido del botiquín y se obtuvieron los siguientes resultados.

Tabla 47 (continuación)

	El botiquín medico al que tienen acceso los empleados de la UTIC y que pueden usar en caso de emergencias internas está ubicado en la segunda planta con un único acceso y paso por dos escaleras como se muestra en las siguientes fotos.  ***Figura 143. Acceso al botiquín médico. Fuente: Ayuntamiento de Tultitlán. (Tultitlán. H. A., Acceso al botiquín médico, 2024)***

Tabla 47 (continuación)

	Acceso a la segunda planta y oficina la oficina de enlace de personal  *Figura 144. Acceso al botiquín médico. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Acceso al botiquín médico, 2023)* Inspeccionando su contenido se puede deducir que hay elementos básicos con los que no cuentan, a continuación, se muestra el contenido de dicho botiquín separado por las categorías de Material Seco, Material Liquido, Instrumental, Medicamentos y Material Complementario.

Tabla 47 (continuación)

	Material Seco: Vendas de rollo elásticas.  *Figura 145. Vendas del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Vendas del botiquín médico, 2023)* Gasas de 10 x 10 cm  *Figura 146. Gasas del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Gasas del botiquín médico, 2023)*

Tabla 47 (continuación)

	Tela Adhesiva  *Figura 147. Tela Adhesiva del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Tela Adhesiva del botiquín médico, 2023)* Abatelenguas  *Figura 148. Abatelenguas del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Abatelenguas del botiquín médico, 2023)*

Tabla 47 (continuación)

	Dentro del material liquido se encontró lo siguiente: **Material Liquido:** Agua Oxigenada de 112 ml.  *Figura 149. Agua Oxigenada del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Agua Oxigenada del botiquín médico, 2023)*

Tabla 47 (continuación)

	Jabón Germicida Liquido  *Figura 150 Jabón Germicida Líquido del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Jabón Germicida Líquido del botiquín médico, 2023)*

Tabla 47 (continuación)

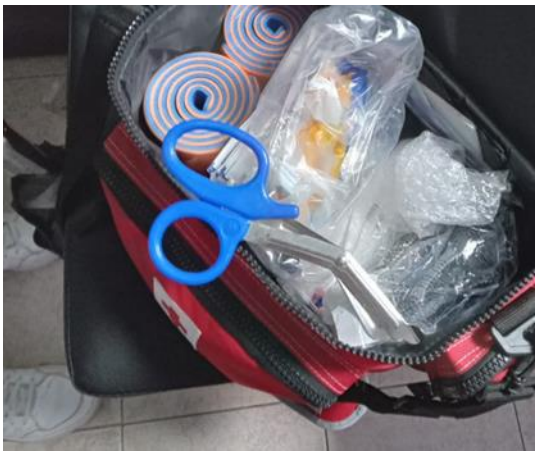
	Notablemente faltan otros complementos como tintura de yodo, alcohol y jabón neutro. Medicamentos: No se encontró ningún medicamento administrable ya que el botiquín no está bajo la supervisión de un médico. Instrumental: Tijeras de botón sin empaque  *Figura 151. Tijeras de botón sin empaque del botiquín médico. Fuente: Departamento de Enlace de Personal.*

Tabla 47 (continuación)

	Termómetro digital  *Figura 152 Termómetro digital del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Termómetro digital del botiquín médico, 2023)*
	Pinzas de Kelly rectas  *Figura 153. Pinzas de Kelly rectas del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Pinzas de Kelly rectas del botiquín médico, 2023)*

Tabla 47 (continuación)

	Material Complementario: Gafas de Protección Transparentes  *Figura 154 Gafas de Protección del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Gafas de Protección del botiquín médico, 2023)*
	Lampara de Diagnóstico  *Figura 155. Lampara de Diagnóstico. del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Lampara de Diagnóstico del botiquín médico, 2023)*

Tabla 47 (continuación)

	Glucómetro  *Figura 156. Glucómetro del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Glúcometro del botiquín médico, 2023)*
	Isopos de Algodón  *Figura 157. Isopos de algodón del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Isopos de algodón del botiquín médico, 2023)*

Tabla 47 (continuación)

	Oxímetro de Pulso  ***Figura 158. Oxímetro de Pulso del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Oxímetro de Pulso del botiquín médico, 2023)***
	Cubrebocas KNY-95  ***Figura 159. Cubrebocas KNY-95 del botiquín médico. Fuente: Departamento de Enlace de Personal. (Personal., Cubrebocas KNY-95 del botiquín médico, 2023)***

Tabla 47 (continuación)

RECOMENDACIONES	Acorde a la Norma Oficial Mexicana (NOM-005-STPS-1998) **"Condiciones de Seguridad e Higiene en los centros de trabajo"** menciona que la presente Norma rige en todo el territorio nacional y aplica en todos los centros de trabajo, comentando en su sección **5.7** que la dependencia debe **"**Proporcionar los medicamentos y materiales de curación necesarios para prestar los primeros auxilios dentro de las instalaciones". En su apartado llamado "Guía de Referencia Botiquín de Primeros Auxilios" dice lo siguiente "El contenido de esta guía es un complemento para la mejor comprensión de la Norma y no es de cumplimiento obligatorio". Está basado en el Manual de Primeros Auxilios de la Cruz Roja Mexicana quien nos menciona que un botiquín: Es el conjunto de materiales, equipo y medicamentos que se utilizan para aplicar los primeros auxilios a una persona que ha sufrido un accidente o una enfermedad repentina. Como características importantes para el botiquín se mencionarán: de fácil transporte, visible y de fácil acceso, que sea identificable con una cruz roja visible, de peso no excesivo, sin candados o dispositivos que dificulten el acceso a su contenido. Dicha guía recomienda los cuidados siguientes: a) que se encuentre en un lugar fresco y seco; b) que el instrumental se encuentre limpio; c) que los frascos estén cerrados y de preferencia que sean de plástico; d) que los medicamentos no hayan caducado, e) que el material se encuentre ordenado.

Tabla 47 (continuación)

	Si se cuenta con instrumental quirúrgico como: tijeras, pinzas o agujas, debe estar empacado éste, ya sea en pequeños paños de tela o en papel absorbente y etiquetado con el nombre del instrumental que contiene. El material que conforma el botiquín se puede clasificar de la siguiente manera: a) material seco; b) material líquido; c) instrumental; d) medicamentos, e) material complementario. Se debe tener en cuenta que la cantidad de material ha de ser la adecuada con respecto al uso al que se le vaya a destinar y a las posibilidades económicas con que se cuente. Todo el material que se menciona es básico y debe existir en cualquier botiquín. **MATERIAL SECO:** El material seco es aquél que por sus características debe permanecer en ese estado, éste comprende los siguientes elementos: • torundas de algodón; • gasas de 5 x 5 cm.; • compresas de gasa; • tela adhesiva; • vendas de rollo elásticas • abatelenguas; • apósitos de tela o vendas adhesivas, • venda triangular.

Tabla 47 (continuación)

	MATERIAL LIQUIDO: Comprende las siguientes soluciones: • tintura de yodo; • jabón neutro, de preferencia líquido; • vaselina; • alcohol, • agua hervida o estéril. • Agua oxigenada **INSTRUMENTAL:** El instrumental puede estar conformado de la siguiente manera: • tijeras rectas y tijeras de botón; • pinzas de Kelly rectas; • pinzas de disección sin dientes; • termómetro; • jeringas desechables de 3.5 y 10 ml. con sus respectivas agujas. **MEDICAMENTOS:** Este material queda a criterio del médico responsable del servicio de urgencias y se usará bajo estricto control del médico. **MATERIAL COMPLEMENTARIO:** Es aquél que puede o no formar parte del botiquín o que por su uso requiera de material específico. Algunos elementos que se pueden incluir son: • linterna de mano; • guantes de cirujano; • estetoscopio y esfignomanómetro; • tablillas para enferular, de madera o cartón; • isopos de algodón,

Tabla 47 (continuación)

	RECOMENDACIÓN Para atender la vulnerabilidad anterior en base los criterios que la NOM-005-STPS-1998 describe, se recomienda ampliamente que la UTIC adquiera su propio botiquín médico, esto garantiza que los empleados tengan una atención más rápida y con alta disponibilidad, además, de esta manera estarán preparados en caso de una emergencia ya que nunca se sabe cuándo pueda presentarse, esto en pocas palabras sería una acción preventiva. Además de tener fácil acceso tener su propio botiquín medico es útil ya que pueden personalizar los suministros con los que cuenta en su interior dependiendo de las necesidades que se vayan presentando con el paso del tiempo. Al tener un botiquín médico exclusivo, es más fácil mantener y controlar el inventario de suministros médicos. Se puede realizar un seguimiento más efectivo de los medicamentos, vendajes, equipos de primeros auxilios y otros suministros, asegurando que estén completos y en buen estado, sin mencionar que no se corre riesgo de contaminación de los suministros por parte de otros usuarios. Sin embargo, de igual manera se recomienda actualizar el contenido del botiquín al que tienen acceso, solicitando que contenga al menos todos los elementos mencionados por la NOM-005-STPS-1998 y de los que carecen actualmente.

Tabla 47 (continuación)

	Dichos suministros son los siguientes: a) Torundas de algodón b) Apósitos de tela o vendas adhesivas (curitas) c) Venda triangular d) Tintura de yodo e) Jabón neutro, liquido f) Alcohol g) Vaselina h) Agua estéril i) Pinzas de disección sin dientes j) Jeringas desechables de 3.5 y 10 ml k) Guantes de látex l) estetoscopio y esfignomanómetro; De esta forma contarán con una mayor gama de suministros y todos los involucrados que compartan dicho botiquín medico estarán mejor preparados en caso de una emergencia.

Tabla 48. Prueba 4 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Accesos Libres o Bloqueados"	
OBJETIVO DE PRUEBA	El principal objetivo de esta prueba es conocer el estado actual de los accesos a la UTIC, es decir que estén en condiciones para evacuar en caso de emergencia o bien sean aptos para el uso cotidiano.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El enfoque de esta prueba va más allá de saber si los accesos son libres o están siendo bloqueados por alguna cuestión, pues esto implica que sean aptos de usarse en caso de una emergencia, además el uso cotidiano implica diferentes actividades que se pueden ver afectadas en el caso de que haya alguna irregularidad. Se espera que los accesos de la UTIC estén en condiciones despejadas y funcionando debidamente pues garantiza la seguridad de los empleados y su eficacia en el desarrollo de diversas actividades en horario laboral.
TÉCNICA	Observación, Análisis, Inspección,
ACTIVIDADES DE LA PRUEBA	1. Observar con detenimiento el desempeño de los accesos a la UTIC. 2. Analizar cuál es la situación actual una vez conocido el desempeño de las entradas y salidas, imaginando posibles escenarios que pueden implicar su uso. 3. Inspeccionar que tipo de acciones o bienes, comprometen el correcto desempeño de los accesos a la UTIC

Tabla 48 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Los accesos a la UTIC funcionan correctamente, están despejados y se encuentran en excelentes condiciones. **Bueno**: Los accesos a la UTIC funcionan correctamente, están despejados y se encuentran en buenas condiciones. **Regular**: Los accesos a la UTIC funcionan correctamente, están parcialmente despejados y se encuentran en condiciones aceptables. **Suficiente**: Los accesos a la UTIC funcionan correctamente, están parcialmente bloqueados y se encuentran en condiciones aceptables. **Deficiente**: Los accesos a la UTIC funcionan correctamente, sin embargo, están siendo bloqueados y se encuentran en condiciones deplorables.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Una vez analizada la situación actual de la UTIC respecto a los accesos despejados, se consideró que a pesar de que no están bloqueados en su totalidad, hay activos en el suelo posicionados cerca del acceso principal que bien no permiten una salida exitosa en caso de una emergencia sin mencionar que la puerta de la UTIC no abre en su totalidad, además de activos en el suelo que evita que los empleados puedan desplazarse libremente en el interior de la UTIC. A continuación, se presentan evidencias de los accesos parcialmente bloqueados y los activos situados en el suelo que impiden el correcto paso de los empleados internos y usuarios.

Tabla 48 (continuación)

	Activos de la UTIC ubicados en el suelo e impidiendo el correcto paso de los empleados.  *Figura 160. Activos ubicados en el suelo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)*

Tabla 48 (continuación)

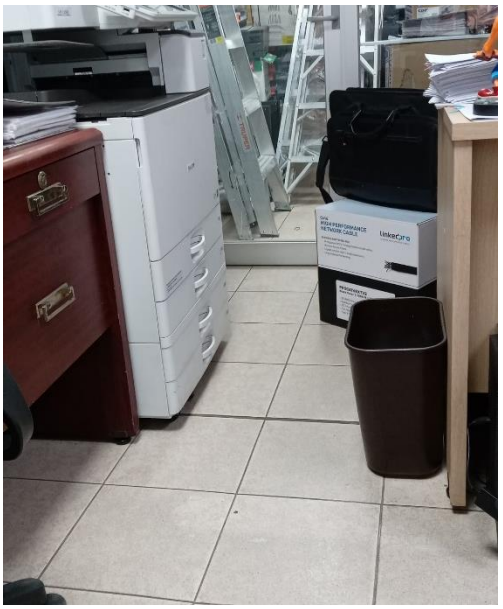
	Activos de la UTIC ubicados en el suelo e impidiendo el correcto paso de los empleados.  ***Figura 161. Activos ubicados en el suelo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)***

Tabla 48 (continuación)

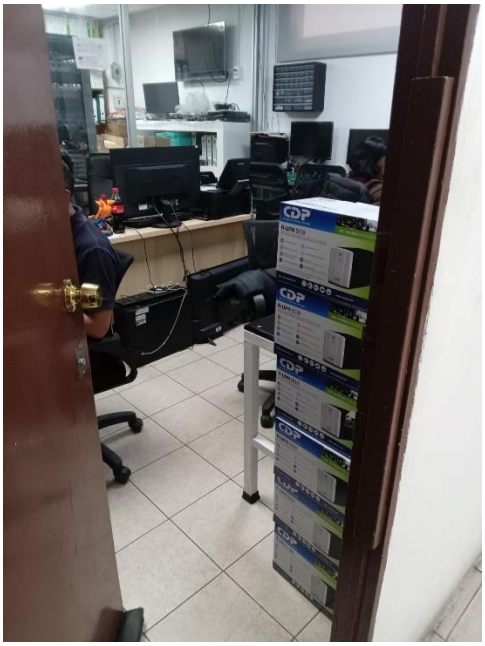
	Acceso principal de la UTIC parcialmente bloqueado, ya que la puerta no abre en su totalidad y hay activos situados del otro lado del acceso, dejando un espacio reducido para despejar la oficina en caso de una emergencia.  ***Figura 162. Materiales ubicados en el suelo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Materiales ubicados en el suelo, 2023)***

Tabla 48 (continuación)

RECOMENDACIONES	Acorde a la Norma Oficial Mexicana (NOM-001-STPS-2008) **"Edificios, locales, instalaciones y áreas en los centros de trabajo, Condiciones de seguridad"** comenta que su objetivo es: "Establecer las condiciones de seguridad de los edificios, locales, instalaciones y áreas en los centros de trabajo para su adecuado funcionamiento y conservación, con la finalidad de prevenir riesgos a los trabajadores" por lo que menciona en su apartado **"7. Requisitos de seguridad en el centro de trabajo"** en su sección 7.1.3 que: "cuando laboren trabajadores en los centros de trabajo, las puertas, vías de acceso y de circulación, escaleras, lugares de servicio y puestos de trabajo, deben facilitar sus actividades, desplazamientos y evacuaciones. Además, menciona en su apartado **"7.4 Pisos"** lo siguiente**:** Los pisos del centro de trabajo deben: • Mantenerse en condiciones tales que de acuerdo con el tipo de actividades que se desarrollen, no generen riesgos de trabajo. • Ser llanos en las zonas para el tránsito de las personas;

Tabla 48 (continuación)

	RECOMENDACIÓN: Para atender la vulnerabilidad anterior en base a la norma mencionada y sus estipulaciones, se recomienda que la UTIC designe un lugar específico para la ubicación de los activos que tienen situados en el suelo del área de trabajo, esto garantiza que los pocos espacios con los que cuentan para moverse libremente estén despejados y no sean causantes de accidentes. Se propone que todos estos activos sean correctamente ordenados dentro del cuarto del site al no contar con algún otro espacio disponible, cabe aclarar que, para no intervenir con la función de los dispositivos de redes ubicados dentro de ese espacio, estos activos deberán ser acomodades dejando espacios para moverse libremente, es decir en el contorno de dicho espacio. Quitando los activos ubicados a un costado del acceso principal notablemente habrá un poco más de espacio para entrar y salir de la oficina, sin embargo, se recomienda de igual forma se retire el “burlete” o “sello de puerta” colocado debajo de esta, ya que impide que la misma se abra en su totalidad y libremente.

Tabla 49. Prueba 5 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Condición del Sistema de Enfriamiento"	
OBJETIVO DE PRUEBA	Conocer la situación actual del sistema de enfriamiento, corroborar su existencia y el alcance con el que cuenta a la hora de ser usado en horario laboral dentro de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El enfoque de esta prueba se centra en corroborar la existencia de un sistema de enfriamiento (aire acondicionado) dentro de la UTIC, analizar su funcionamiento y el alcance que llega a tener durante su uso en el interior de las instalaciones. Se espera que el sistema de enfriamiento (aire acondicionado) usado en al interior de la UTIC ese en excelentes condiciones, además de que su alcance cubra toda el área de trabajo.
TÉCNICA	Observación, Inspección, Análisis, Pruebas de campo
ACTIVIDADES DE LA PRUEBA	1. Observar si existe un sistema de enfriamiento (aire acondicionado) instalado en el interior de la UTIC y el lugar en el que se encuentra. 2. Inspeccionar el artefacto verificando en qué condiciones físicas se encuentra actualmente y si está debidamente instalado. 3. Analizar su uso y el manejo que tiene actualmente además de su nivel de respuesta. 4. Realizar una prueba de campo de su funcionamiento para corroborar que este sea correcto y logre cubrir toda el área de trabajo.

Tabla 49 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: La UTIC cuenta con un sistema de enfriamiento en excelentes condiciones, correctamente instalado, con un uso controlado y cubre toda el área de trabajo con su beneficio. **Bueno**: La UTIC cuenta con un sistema de enfriamiento en excelentes condiciones, correctamente instalado, sin un uso controlado y cubre toda el área de trabajo con su beneficio. **Regular**: La UTIC cuenta con un sistema de enfriamiento en excelentes condiciones, correctamente instalado, sin un uso controlado y logra cubrir la mayoría del espacio de trabajo. **Suficiente**: La UTIC cuenta con un sistema de enfriamiento en excelentes condiciones, debidamente instalado, sin un uso controlado y logra cubrir la mitad del espacio de trabajo. **Deficiente**: La UTIC cuenta con un sistema de enfriamiento en excelentes condiciones, debidamente instalado, sin un uso controlado, pero solo logra cubrir un sitio en específico del espacio de trabajo.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Se solicito acceso al jefe de la unidad para ingresar al lugar donde está instalado el sistema de enfriamiento (aire acondicionado).
|INTERPRETACIÓN DE RESULTADOS	Al inspeccionar la situación actual de la UTIC referente a la posesión de un sistema de enfriamiento se logra percibir que efectivamente cuentan con un aire acondicionado, sin embargo este solo está situado dentro del espacio destinado por el site, el cual esta sellado para controlar el acceso, por lo que lo beneficios de dicho aparato de ventilación artificial no los gozan los empleados internos de la UTIC, solo funciona para mantener a los dispositivos de redes bajo condiciones climáticas favorables.

Tabla 49 (continuación)

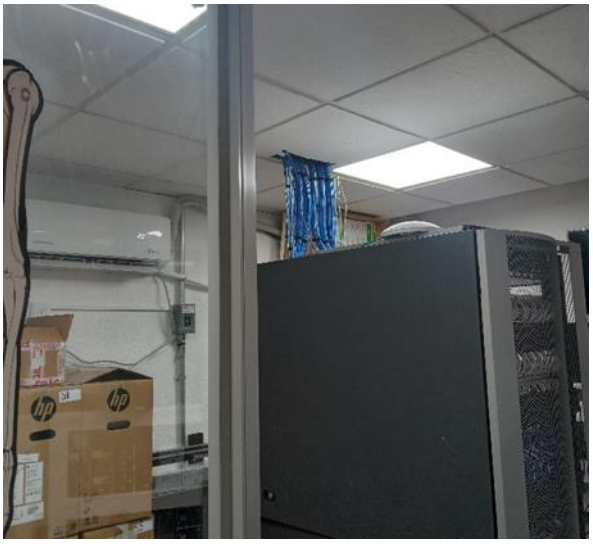
	A continuación, se presenta evidencia de la ubicación del aire acondicionado con el que cuenta la UTIC. Aire acondicionado dentro del site  *Figura 163. Vista 1 del Aire Acondicionado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 1 del Aire Acondicionado, 2023)* Presencia de un sistema de enfriamiento debidamente instalado dentro del site,  *Figura 164. Vista 2 del Aire Acondicionado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 2 del Aire Acondicionado, 2023)*

Tabla 49 (continuación)

	Presencia de un sistema de enfriamiento debidamente instalado dentro del site  *Figura 165. Vista 3 del Aire Acondicionado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 3 del Aire Acondicionado, 2023)*
RECOMENDACIONES	Acorde a la Norma Oficial Mexicana (NOM-023-ENER-2018) llamada **"Eficiencia energética en acondicionadores de aire tipo dividido, descarga libre y sin conductos de aire. Límites, métodos de prueba y etiquetado."** Menciona en su apartado "8.2.1" llamado **"Variación del aire**" que **"**La exactitud en las mediciones de temperatura debe permanecer dentro de ± 0,05 °C para las temperaturas del aire" por lo que si la temperatura es errónea fuera de ese margen el dispositivo usado no funciona correctamente.

Tabla 49 (continuación)

	Además, menciona en su apartado **"8.5.6 Instalación del equipo"** Estipulando en su sección "**87.5.6.1"** El equipo a ser probado debe ser instalado en el cuarto o cuartos de prueba, de acuerdo con las instrucciones de instalación del fabricante, usando accesorios y procedimientos recomendados de instalación. El equipo con la sección exterior remota debe tener la sección interior localizada en el cuarto de prueba interior y la sección exterior en el cuarto de prueba exterior; el equipo autocontenido con suministro de aire debe ser localizado adyacente o mediante una abertura en una pared o división separando el cuarto de prueba de acuerdo con las recomendaciones normales o primarias del fabricante. En todos los casos, las recomendaciones del fabricante con respecto a las distancias de las paredes adyacentes a los equipos, cantidad de extensiones a través de las paredes, etc. Por otro lado, en su apartado "**87.3.1.1"** llamado "Aplicación" menciona que "El equipo debe ser colocado en un sitio en el cual su beneficio sea aprovechado por todos los trabajadores implicados en el área o zona, para garantizar el desarrollo de actividades bajo condiciones favorables de ventilación en el entorno del área donde fue implementado"

Tabla 49 (continuación)

	RECOMENDACIÓN: Para atender la vulnerabilidad anterior y en base a la norma mencionada, se recomienda que la UTIC aplique otra medida que garantice una ventilación óptima para los empleados internos, pues al contar con un solo sistema de aire acondicionado, pero este a su vez ubicado dentro del site, no es suficiente, pues el mismo solo mantiene bajo condiciones óptimas los equipos y activos ubicados dentro de dicho lugar, por lo que los empleados no gozan del beneficio que este produce, sin embargo hay distintas soluciones que pueden emplear para su beneficio como lo son: - Implementar un artefacto electrónico movible que genere ventilación continua para mantener el lugar de trabajo fresco y en condiciones climáticas optimas: (Ventiladores portátiles, de piso, automáticos, recargables o desechables). - Colocar un ventilador de techo fijo para ventilar toda el área de trabajo de manera contante. - Mantener los accesos que provocan cierta ventilación abiertos para permitir el flujo de aire al interior del área de trabajo: (Ventanas y Puertas). De esta manera con cualquier de las opciones mencionadas, garantizan que el área de trabajo se mantenga ventilada y en condiciones óptimas para los empleados y más en temporada de altas temperaturas.

Tabla 50 Prueba 6 de Servicios. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Señalamientos de Emergencia"	
OBJETIVO DE PRUEBA	Corroborar la existencia de señalamientos de emergencia ubicados en las instalaciones de la UTIC y alrededores.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	El enfoque principal de esta prueba es identificar los tipos de señalamientos que existen en la UTIC y alrededores, aquellos que sirven para orientar a los usuarios sobre su comportamiento y guía para evacuación en caso de alguna emergencia. Se espera que la UTIC cuente con todos los señalamientos necesarios para saber cómo actuar en caso de emergencias o desastres naturales, además de que se encuentren al alcance de la vista de cualquier usuario y estén debidamente ubicados.
TÉCNICA	Observación, Análisis, Inspección.
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar la UTIC y las áreas que la rodean en busca de señalamientos de emergencia que cubran el trayecto entre el área de trabajo y un área segura para emergencias. 2. Observar que tipo de señalamientos son con los que se cuentan y si están ubicados en un lugar que permita ser visible para cualquier usuario. 3. Analizar la ruta de evacuación entre la UTIC y un área segura, para corroborar que los señalamientos estén debidamente instalados y sea correcta su ubicación.

Tabla 50 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: La UTIC y los espacios que la rodean cuentan con todos los señalamientos de emergencia, cubriendo los siguientes puntos: Ruta de Evacuación, Salida de Emergencia, Incendios, Sismos, Terremotos, con indicaciones claras e indicando el trayecto entre el espacio de trabajo y un área segura o punto de reunión. **Bueno**: La UTIC y los espacios que la rodean cuentan con la mayoría de los señalamientos de emergencia, cubriendo los siguientes puntos: Ruta de Evacuación, Salida de Emergencia, Incendios, Sismos, Terremotos, con indicaciones claras e indicando el trayecto entre el espacio de trabajo y un área segura o punto de reunión. **Regular**: La UTIC y los espacios que la rodean cuentan con la mitad de los señalamientos de emergencia, cubriendo los siguientes puntos: Ruta de Evacuación, Salida de Emergencia, Incendios, Sismos, Terremotos, con indicaciones claras e indicando el trayecto entre el espacio de trabajo y un área segura o punto de reunión. **Suficiente**: La UTIC y los espacios que la rodean cuentan con algunos de los señalamientos de emergencia, cubriendo los siguientes puntos: Ruta de Evacuación, Salida de Emergencia, Incendios, Sismos, Terremotos, con indicaciones claras e indicando el trayecto entre el espacio de trabajo y un área segura o punto de reunión. **Deficiente**: La UTIC y los espacios que la rodean cuentan con pocos de los señalamientos de emergencia y solo cubren algunos de los siguientes puntos: Ruta de Evacuación, Salida de Emergencia, Incendios, Sismos, Terremotos, con indicaciones claras e indicando el trayecto entre el espacio de trabajo y un área segura o punto de reunión.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.

Tabla 50 (continuación)

<table>
<tr><td>CONSIDERACIONES ESPECIALES</td><td>Sin consideraciones especiales</td></tr>
<tr><td>INTERPRETACIÓN DE RESULTADOS</td><td>Al inspeccionar la UTIC y los espacios que la rodean se encontró que solo cuentan con algunos señalamientos de emergencia, a continuación, se muestran evidencias de los señalamientos con los que cuentan,

Señalamiento indicador de “Salida de emergencia” ubicado sobre la salida del edificio en donde se encuentra la UTIC


Figura 166. Señalamiento de Salida de Emergencia. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Salida de Emergencia, 2023)

Señalamiento indicador de “Ruta de Evacuación” frente al acceso del edificio donde se ubica la UTIC.

Figura 167. Señalamiento de Ruta de Evacuación. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Ruta de Evacuación, 2023)</td></tr>
</table>

Tabla 50 (continuación)

	Señalamiento indicador de “Ruta de Evacuación” situado a un costado de la entrada al edificio donde se ubica la UTIC.  *Figura 168. Señalamiento de Ruta de Evacuación. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Ruta de Evacuación, 2023)*

Tabla 50 (continuación)

	Señalamiento indicador de “Extintor” situado enfrente del acceso a la UTIC.  *Figura 169. Señalamiento del Extintor. Fuente: H. Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Exintor, 2023)*

Tabla 50 (continuación)

RECOMENDACIONES	Acorde a la **"National Fire Protection Association"** o bien Asociación Nacional de Protección contra Incendios la "**NFPA 101"** aborda los requisitos para la señalización de salida, que incluye señales de salida iluminadas, rutas de evacuación claras y otros elementos de orientación para ayudar a las personas a evacuar de manera segura en caso de emergencia. En su Capítulo 7 llamado **"Medios de Egreso"** en su sección 7.10.1.4 **"Acceso a las Salidas**". El acceso a las salidas deberá estar marcado por signos aprobados, fácilmente visibles en todos los casos cuando la salida o el camino para alcanzarla no sea fácilmente evidente para los ocupantes. El emplazamiento de la señal deberá ser tal que ningún punto en el corredor del acceso a la salida esté a más de 100 pies (30 m) del signo más cercano y no esté más alejado de la capacidad indicada. Además, en su sección 7.10.1.7 **"Tipos de Señalamientos de Emergencia"** menciona las categorías de los señalamientos con los que deben contar. **Señales de Salida:** - Indican las rutas de evacuación y las salidas de emergencia. - Deben ser claramente visibles y estar ubicadas en lugares estratégicos dentro del edificio. **Señales de Primeros Auxilios:** - Indican la ubicación de equipos y suministros de primeros auxilios, como botiquines y estaciones de lavado de ojos.

Tabla 50 (continuación)

	Señales de Extintores: - Indican la ubicación de extintores de incendio y proporcionan instrucciones sobre cómo usarlos. **Señales de Alarma de Incendio:** - Indican la ubicación de alarmas de incendio y proporcionan instrucciones sobre cómo activarlas en caso de emergencia. **Señales de Peligro:** - Alertan sobre peligros específicos, como sustancias químicas peligrosas, equipos peligrosos o áreas restringidas. **Señales de Evacuación:** - Indican la forma en la que debe realizarse una evacuación, acompañado de instrucciones claras, a veces ilustradas **RECOMENDACIÓN:** Para atender la vulnerabilidad y en base a la norma mencionada se recomienda la colocación de los señalamientos de emergencia con los que no cuentan, o al menos los más comunes y que pueden ayudar a los usuarios en su comportamiento durante una emergencia o evacuación. Se propone que la UTIC haga una solicitud o bien un comunicado donde reporte la falta de dichos señalamientos para que las autoridades correspondientes actúen ante la notable ausencia de estos.

Tabla 50 (continuación)

	Señalamientos Faltantes **Señalamientos de Primeros Auxilios:** - Ausencia de algún señalamiento que indique donde se encuentra ubicado el botiquín de primeros auxilios por ejemplo (señalamiento de botiquín médico o primeros auxilios). **Señales de Peligro:** - Ausencia de algún señalamiento que indique las áreas que puedan resultar peligrosas para los usuarios por ejemplo (señalamiento de escaleras). **Señales de Evacuación:** - Ausencia de algún señalamiento que indique el comportamiento que deben tener los usuarios al evacuar en caso de una emergencia por ejemplo (señalamientos de evacuación para sismos, incendios, terremotos). De esta manera la UTIC y su entorno estará mejor equipado con los señalamientos para que usuarios externos e internos tengan conocimientos de la ubicación de salidas, accesos o bien rutas, así como comportamiento en caso de una emergencia.

3.2.1.7 Actividad 2.7 Realizar Pruebas de Infraestructura

3.2.1.7.1 Descripción de la actividad

En esta actividad se requiere visitar las instalaciones de la UTIC ya que de esta manera es más fácil detectar aquellas anomalías que pueda presentar la infraestructura de la unidad, dicho esto se hace una mayor observación e inspección en el inmobiliario, ya que a simple vista hay una notable falta de espacio ya que este no es el adecuado de acuerdo a las medidas y espacios disponibles dentro de la UTIC, el inmobiliario considerado para las pruebas y que tiene un mayor impacto en la distribución son los escritorios en donde están situados los equipos de cómputo, los antes mencionados están situados en el perímetro interno de la unidad, sin mencionar que uno de ellos están en el centro de dicha unidad, además de que las sillas de escritorio contribuyen a la reducción de espacio disponible para la movilidad de los empleados y usuarios, por otro se nota que el cableado no está organizado favorablemente ya que si se encuentran separados los eléctricos de los de red, sin embargo los cables de los dispositivos y periféricos se encuentran totalmente en desorden detrás de los equipos de cómputo, además de que los de red, no se encuentran protegidos por canaletas fijadas a los muros y deja este tipo de cables suspendidos en el aire.

3.2.1.7.2 Resultado de la actividad

Tabla 51 Prueba 1 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA “Evaluar la Eficiencia en el Etiquetado de Activos y Mobiliario”	
OBJETIVO DE PRUEBA	El objetivo de esta prueba es evaluar si el etiquetado de los activos y mobiliario sigue un ordenamiento que facilita la lectura para los usuarios.

Tabla 51 (continuación)

DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	La finalidad de esta prueba es evaluar la efectividad del sistema de etiquetado de activos y mobiliario, con un enfoque en la organización y la facilidad de lectura para los usuarios, además se analizará la visibilidad y ubicación de los etiquetados en relación con los activos, incluyendo la presencia o ausencia de etiquetas y su posición detrás, debajo o en los laterales de los activos. Se busca determinar si el etiquetado actual proporciona información clara y accesible para la identificación de activos y mobiliario en la UTIC. Se espera obtener una evaluación completa de la efectividad del sistema de etiquetado en términos de organización y legibilidad para los usuarios.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Analizar el diseño y contenido de las etiquetas actuales en activos y mobiliario. 2. Analizar la ubicación actual de las etiquetas en los activos dentro de la UTIC. 3. Verificar si las etiquetas están situadas en la parte frontal, superior o lugares fácilmente visibles. 4. Evaluar si las etiquetas contienen información relevante para la identificación. 5. Realizar una inspección visual para evaluar la organización física de los activos y mobiliario etiquetados. 6. Realizar simulaciones en las que los usuarios intenten identificar activos basándose en las etiquetas. 7. Realizar simulaciones donde los usuarios intenten identificar activos y mobiliario basándose en las etiquetas. 8. Registrar cualquier error o confusión en la identificación de activos y mobiliario durante la simulación.

Tabla 51 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Las etiquetas están organizadas de manera lógica y son fácilmente legibles. **Bueno**: Las etiquetas son efectivas en la mayoría de los casos, pero puede haber áreas de mejora en la organización o legibilidad. **Regular**: Existen áreas identificadas que necesitan mejoras en la organización o legibilidad de las etiquetas. **Suficiente**: Se cumplen los requisitos mínimos para la organización y legibilidad de las etiquetas. **Deficiente**: La organización y legibilidad de las etiquetas son insatisfactorias y no cumplen con los estándares.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Etiquetado de un Disco Duro Externo:  *Figura 170. Etiquetado 1. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Etiquetado 1, 2023)*

Tabla 51 (continuación)

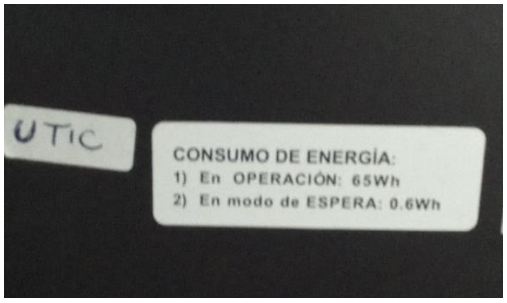
	Etiquetado del gabinete 1:  ***Figura 171. Etiquetado 2. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Etiquetado 2, 2023)*** Etiquetado del gabinete 2:  ***Figura 172. Etiquetado 3. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Etiquetado 3, 2023)*** Etiquetado del gabinete 3:  ***Figura 173. Etiquetado 4. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Etiquetado 4, 2023)***

Tabla 51 (continuación)

	Etiquetado del monitor:  *Figura 174. Etiquetado 5. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Etiquetado 5, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado Administración de activos en su sección 8.2.2 nos dice que *"Se debería desarrollar e implementar un conjunto de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización."* *Los procedimientos para el etiquetado de la información deberían cubrir la información y sus activos relacionados en formatos físicos o electrónicos. El etiquetado debería reflejar el esquema de clasificación establecido en 8.2.1 Clasificación de la información (La clasificación se debería incluir en los procesos de la organización y debería ser coherente y consistente en toda la organización.* *Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, es decir, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación se deberían actualizar de acuerdo con los cambios en su valor, sensibilidad y criticidad a través de su ciclo de vida.).* *Las etiquetas se deberían poder reconocer fácilmente. Los procedimientos deberían brindar orientación sobre dónde y cómo se adhieren las etiquetas considerando cómo se accede a la información o cómo se manejan los activos en función de los tipos de medios.*

Tabla 51 (continuación)

	Los procedimientos pueden definir los casos donde se omite el etiquetado, es decir, etiquetando la información no confidencial para reducir las cargas de trabajo. Los empleados y contratistas deberían estar al tanto de los procedimientos de etiquetado. *El etiquetado de información clasificada es un requisito clave para los acuerdos para compartir información.* *Las etiquetas físicas y los metadatos son una forma común de etiquetado. El etiquetado de información y sus activos relacionados pueden tener efectos negativos a veces. Los activos clasificados son más fáciles de identificar y, en consecuencia, de sufrir robos de personas internas o de atacantes externos* Aunque en su versión 17799:2005 menciona lo siguiente: *Las etiquetas deberían ser fácilmente reconocibles. Los procedimientos deberían brindar orientación sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a la información o cómo se manejan los activos según los tipos de medios de almacenamiento. Los procedimientos pueden definir:* *a) casos en los que se omite el etiquetado (por ejemplo, etiquetado de información no confidencial para reducir la carga de trabajo);* *b) cómo etiquetar la información enviada o almacenada en medios electrónicos o físicos, o cualquier otro formato;* *c) cómo manejar los casos en los que el etiquetado no es posible (por ejemplo, debido a restricciones técnicas).*

Tabla 51 (continuación)

	Los ejemplos de técnicas de etiquetado incluyen: *a) etiquetas físicas;* *b) encabezados y pies de página;* *c) metadatos;* *d) marca de agua;* *e) sellos de goma.* *La información digital debería utilizar metadatos para identificar, gestionar y controlar la información, especialmente en lo que respecta a la confidencialidad. Los metadatos también deberían permitir una búsqueda eficiente y correcta de información. Los metadatos deberían facilitar que los sistemas interactúen y tomen decisiones en función de las etiquetas de clasificación asociadas.* Para dar solución a esta vulnerabilidad se recomienda que el etiquetado sea físico para los activos acorde a un Numero de Identificación (ID), Nombre del Activo, Marca del Activo, Área al que pertenece el activo, Propietario del Activo. Así mismo la ubicación de la etiqueta sea visible aun cuando el activo se encuentre obstruido por algún material u otro activo. Esto para facilitar su inventariado que se realiza en la UTIC.

Tabla 52. Prueba 2 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar la Idoneidad del Mobiliario en la UTIC"	
OBJETIVO DE PRUEBA	El objetivo de la prueba es evaluar si los escritorios utilizados en la UTIC son adecuados en términos de tamaño y ocupación de espacio, identificando cualquier inadecuación que pueda afectar la eficiencia y el espacio disponible.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Esta prueba tiene como propósito evaluar la idoneidad y adecuación del mobiliario utilizado en la Unidad de Tecnologías de la Información y Comunicación (UTIC). Se busca determinar si el mobiliario actual satisface las necesidades funcionales de los usuarios y contribuye al entorno de trabajo de manera eficiente. Se espera obtener una evaluación completa de la idoneidad del mobiliario en la UTIC, considerando la opinión de los usuarios, la ergonomía y la eficacia en la realización de tareas.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Analizar el diseño y tipo de mobiliario utilizado en la UTIC. 2. Evaluar la adecuación del mobiliario para las tareas y actividades realizadas en el entorno. 3. Realizar una inspección ergonómica del mobiliario, evaluando la altura de las mesas, sillas y otros elementos en relación con las necesidades de los usuarios. 4. Evaluar la eficacia del mobiliario en el apoyo a las actividades laborales.

Tabla 52 (continuación)

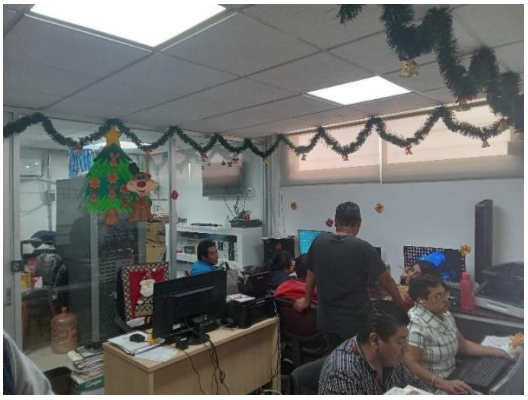
PROCESO DE MEDICIÓN	**Excelente**: El mobiliario es altamente adecuado y eficiente para las tareas realizadas en la UTIC. **Bueno**: El mobiliario es en su mayoría adecuado y funcional, aunque puede haber áreas de mejora. **Regular**: Algunos usuarios pueden experimentar dificultades ocasionales o incomodidades con el mobiliario actual. **Suficiente**: En general, los usuarios pueden realizar sus tareas, aunque con algunas dificultades. **Deficiente**: Los usuarios encuentran dificultades significativas y experimentan incomodidades al utilizar el mobiliario, lo que requiere acciones correctivas inmediatas.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista general de la oficina de la UTIC:  *Figura 175. Vista General de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista General de la UTIC, 2023)*

Tabla 52 (continuación)

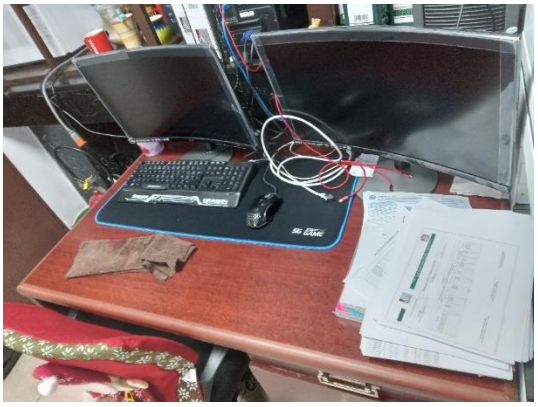
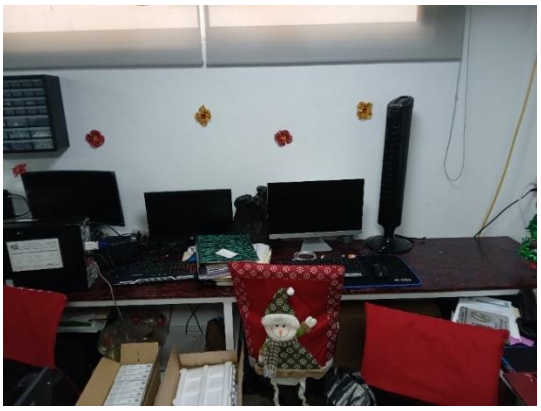
	Vista del escritorio situado a la derecha de la puerta:  *Figura 176. Vista del escritorio 1. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del escritorio 1, 2023)* Vista del segundo escritorio situado en la parte izquierda de la oficina:  *Figura 177. Vista del escritorio 2. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del escritorio 2, 2023)*

Tabla 52 (continuación)

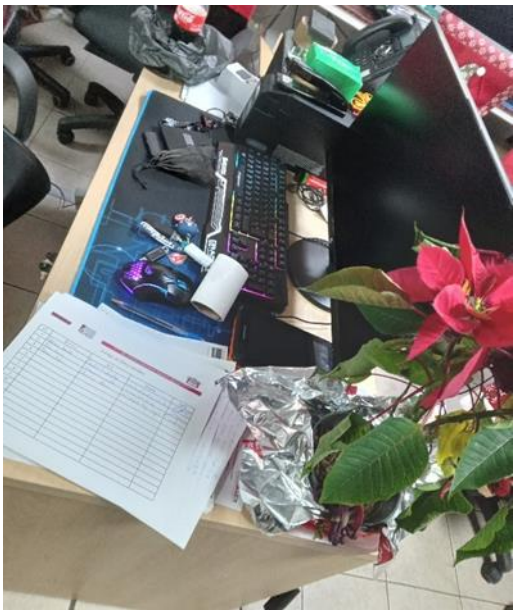
	Vista del escritorio del jefe de la UTIC situado al centro de la oficina:  *Figura 178. Vista del escritorio principal. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del escitorio principal, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su sección 11 llamada Seguridad Física y Ambiental en su apartado 11.1.5 *"Trabajo en áreas seguras"* menciona que *"Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras."* En su orientación sobre su implantación esta "*Se deberían considerar las siguientes pautas:* *a) el personal debería estar al tanto de la existencia de, o de las actividades dentro de un área segura según se considere necesario.* *b) se debería evitar el trabajo no supervisado en áreas seguras, tanto por motivos de seguridad como para evitar las oportunidades de actividades maliciosas;* c) *las áreas seguras vacantes se deberían cerrar físicamente con candado y se deberían revisar de manera periódica;*

Tabla 52 (continuación)

	d) *no se deberían permitir los equipos fotográficos, de video o audio, como las cámaras de dispositivos móviles, a menos que se autoricen.* *Las disposiciones para trabajar en áreas seguras incluyen controles para los empleados y usuarios de terceros trabajando en el área segura y cubren todas las actividades que se realizan en el área segura.* Considerando la importancia de mantener la seguridad en áreas seguras según el ISO/IEC 27002, es fundamental extender estas pautas específicamente al mobiliario, como los escritorios, que forman parte integral de los entornos de trabajo. Aquí hay algunas recomendaciones específicas para garantizar la seguridad del mobiliario en áreas seguras: El diseño de los espacios de trabajo, incluidos los escritorios, debe tener en cuenta la seguridad física. Se recomienda colocar los escritorios de manera que minimicen la posibilidad de observación no autorizada o acceso no supervisado, o en su defecto hacer cambio de estos para maximizar el espacio de trabajo.

Tabla 53. Prueba 3 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar la Movilidad y Ubicación de Activos en la UTIC"	
OBJETIVO DE PRUEBA	Esta prueba tiene como propósito evaluar la disposición de activos en el suelo y la configuración de escritorios en la UTIC, específicamente en cómo afecta la libre movilidad de los empleados.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si la ubicación de activos y la distribución de escritorios obstaculizan o facilitan la movilidad dentro del espacio de trabajo. Se espera obtener una evaluación integral de cómo la ubicación de activos en el suelo y la disposición de escritorios afectan la libre movilidad de los empleados en la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Evaluar la presencia de activos situados en el suelo y su impacto en la circulación de los empleados. 2. Verificar si la disposición de estos activos afecta negativamente la movilidad y el acceso a las áreas de trabajo. 3. Realizar simulaciones del flujo de trabajo, considerando la distribución de escritorios y la ubicación de activos.
PROCESO DE MEDICIÓN	**Excelente**: La disposición de activos y escritorios permite una movilidad óptima y sin obstáculos para los empleados. **Bueno**: La disposición de activos y escritorios es en su mayoría eficiente, aunque puede haber áreas de mejora. **Regular**: Existen áreas identificadas que necesitan mejoras en la disposición de activos y escritorios para mejorar la movilidad.

Tabla 53 (continuación)

	Suficiente: Se cumplen los requisitos mínimos para la movilidad, pero hay áreas que necesitan mejoras. **Deficiente**: La disposición de activos y escritorios es insatisfactoria y afecta negativamente la movilidad de los empleados.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Activos situados en el suelo y pasillo de la UTIC.  ***Figura 179. Activos situados en el suelo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)***

Tabla 53 (continuación)

	Activos, Materiales, Archivos situados en el suelo dentro del site:  *Figura 180. Activos, Materiales, Archivos de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos, Materiales, Archivos de la UTIC, 2023)* Activos, Materiales, Archivos situados en el suelo dentro del site:  *Figura 181. Activos, Materiales, Archivos de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos, Materiales, Archivos de la UTIC, 2023)*

Tabla 53 (continuación)

	Activos, Materiales, Archivos situados en el suelo dentro del site:  *Figura 182. Activos, Materiales, Archivos de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos, Materiales, Archivos de la UTIC, 2023)* Activos, Materiales, Archivos, Equipo de impresión situados en el suelo dentro del site:  *Figura 183. Activos, Materiales, Archivos,* Equipos *de Impresión. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos, Materiales, Archivos, Equipos de Impresión, 2023)*

Tabla 53 (continuación)

	Activos sobre el pasillo para ingresar al rack:  *Figura 184. Activos sobre el pasillo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos sobre el pasillo, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su Sección 11 llamado Seguridad Física y Ambiental en su apartado 11.1.1 Perímetro de seguridad física nos menciona que *"evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información."* En su inciso *a) se deberían definir perímetros de seguridad y el emplazamiento y la ubicación de cada uno de los perímetros debería depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos;* Acorde a lo anterior y como resultado de la prueba, los activos situados en el piso es una mala práctica por parte de la UTIC, ya que obstruyen el paso y se puede ocasionar un accidente debido a la obstrucción de los pasillos disponibles, por lo cual se recomienda que todo activo que se ingrese a la UTIC sea en una extensión de esta, es decir, en un almacén o bodega cerca del departamento donde solo los empleados de la UTIC tengan acceso.

Tabla 54. Prueba 4 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar la Organización y Manejo de Cables en la UTIC"	
OBJETIVO DE PRUEBA	Esta prueba tiene como propósito evaluar la organización y manejo de cables en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si la presencia de equipos enchufados y apagados sin utilizarse contribuye al cruce de cables y genera confusión en los multicontactos, afectando la eficiencia y seguridad del entorno. Se espera obtener una evaluación integral de la organización y manejo de cables en la UTIC, centrándose en la presencia de equipos enchufados y apagados sin ser utilizados.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Evaluar la configuración actual de equipos y cables en la UTIC. 2. Verificar la presencia de equipos enchufados y apagados que no están en uso. 3. Identificar equipos que permanecen enchufados y apagados sin estar en uso activo. 4. Inspeccionar la disposición de cables para determinar si hay cruces o enredos que podrían causar confusión. 5. Identificar cualquier situación que genere confusión en el manejo de multicontactos.
PROCESO DE MEDICIÓN	**Excelente**: La organización y manejo de cables son óptimos, sin presencia de equipos enchufados y apagados sin ser utilizados. **Bueno**: La organización y manejo de cables son en su mayoría adecuados, aunque puede haber áreas de mejora.

Tabla 54 (continuación)

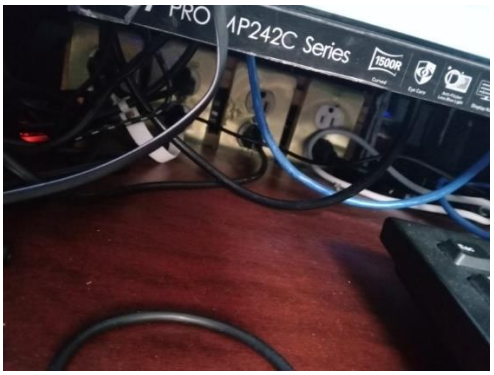
	Regular: Algunos usuarios pueden experimentar dificultades ocasionales en el manejo de multicontactos. **Suficiente**: En general, los usuarios pueden manejar los multicontactos, aunque con ciertas dificultades. **Deficiente**: La organización de cables es insatisfactoria y afecta significativamente la eficiencia y seguridad en el manejo de multicontactos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Cableado eléctrico del escritorio 1:  *Figura 185. Cableado 1. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 1, 2023)*

Tabla 54 (continuación)

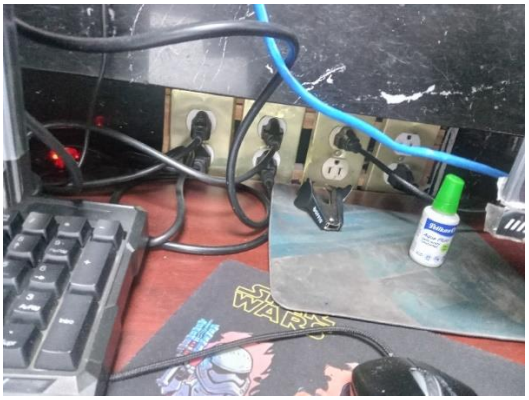
	Cableado eléctrico del escritorio 2:  *Figura 186. Cableado 2. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 2, 2023)* Cableado eléctrico sin organización:  *Figura 187. Cableado 3. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 3, 2023)*

Tabla 54 (continuación)

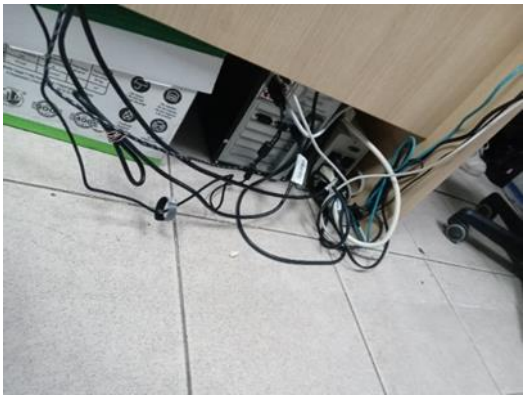
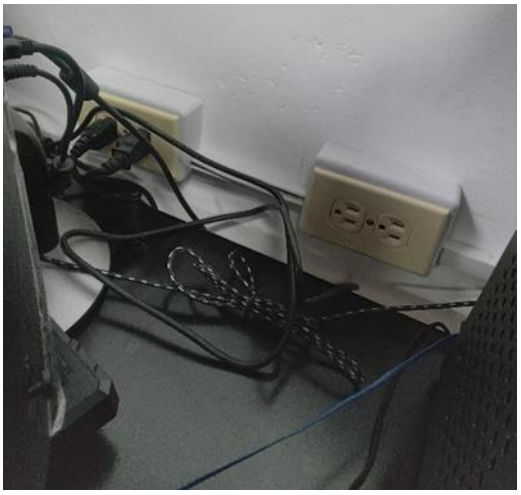
	Cableado eléctrico el escritorio principal:  *Figura 188. Cableado 4. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 4, 2023)* Cableado de los periféricos sin Identificarse:  *Figura 189. Cableado 5. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado5, 2023)*

Tabla 54 (continuación)

	Puertos del cableado sin identificarse:  *Figura 190. Cableado 6. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 6, 2023)* Cableado sin organización:  *Figura 191. Cableado 7. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 7, 2023)*

Tabla 54 (continuación)

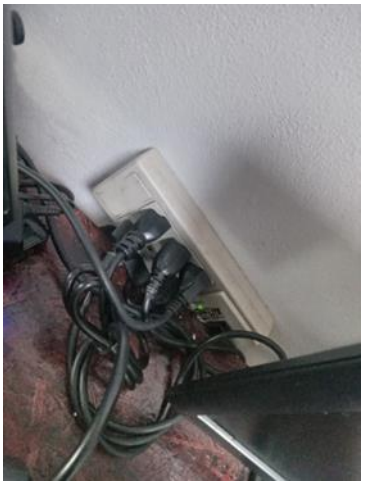
	Uso de extensiones multicontactos:  *Figura 192. Cableado 8. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 8, 2023)* Cableado eléctrico sin identificar:  *Figura 193. Cableado 9. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 9, 2023)*

Tabla 54 (continuación)

	Cableado eléctrico sin identificar:  *Figura 194. Cableado 10. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 10, 2023)* Cableado del escritorio principal sin identificar:  *Figura 195. Cableado 11. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 11, 2023)*

Tabla 54 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado *"Seguridad Física y Ambiental"* en su apartado 11.2.3 nombrado *"Seguridad del Cableado"* menciona que *"Los cables de electricidad y telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger de la intercepción, interferencia o daños".* Aunque en la UTIC si cuente con la separación de estos cables de electricidad y telecomunicaciones, el uso de más cableado como lo puede ser de los cables de alimentación de las computadoras, todo el cableado de los periféricos como lo son USB y Teclados, no están correctamente separados y existe una mala gestión ya que en algún momento puede haber confusión del cableado y desenchufar el incorrecto dando así paso a otro incidente. El ISO/IEC 27002 nos da pautas que son las siguientes *a) las líneas de energía y telecomunicaciones hacia las instalaciones de procesamiento de información que sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como un protector de cable de piso y un poste de servicios públicos; si los cables están bajo tierra, protegiéndolos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);* *b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;* *c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:* *1) instalación de conductos blindados y habitaciones o cajas cerradas y alarmasen los puntos de inspección y terminación;*

Tabla 54 (continuación)

	2) *uso de blindaje electromagnético para proteger los cables;* 3) *barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;* 4) *acceso controlado a paneles de conexiones y salas de cables (por ejemplo, con llaves mecánicas o PIN);* 5) *uso de cables de fibra óptica;* d) *etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.* Para dar solución a esta vulnerabilidad se recomienda que todo el cableado sea identificado con etiquetas físicas de extremo a extremo, además de agruparlos con cinchos sujeta-cables (material velcro) acorde al tipo de periférico (Mouse, teclado, bocinas, cable de corriente, cable ethernet, etc.).

Tabla 55. Prueba 5 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar el Espacio de Movilidad para Traslado de Equipos en la UTIC"	
OBJETIVO DE PRUEBA	Esta prueba tiene como propósito evaluar el espacio de movilidad en la UTIC durante el traslado de equipos reparados entre usuarios o hacia otras áreas.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si la falta de espacio contribuye al daño de equipos durante estos procesos. Se espera obtener una evaluación completa del espacio de movilidad durante el traslado de equipos en la UTIC, centrándose en la posible contribución de la falta de espacio al daño de los equipos.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Evaluar el espacio físico disponible para el traslado de equipos reparados en la UTIC. 2. Registrar los procesos habituales de traslado de equipos entre usuarios o a otras áreas. 3. Recopilar percepciones sobre posibles problemas o inconvenientes experimentados. 4. Observar posibles situaciones en las que la falta de espacio pueda resultar en daño a los equipos.
PROCESO DE MEDICIÓN	**Excelente**: El espacio de movilidad para el traslado de equipos es óptimo y no contribuye al daño de los equipos. **Bueno**: El espacio de movilidad es en su mayoría adecuado, aunque puede haber áreas de mejora. **Regular**: Algunos usuarios pueden experimentar dificultades ocasionales en el manejo de equipos durante los traslados. **Suficiente**: En general, los usuarios pueden realizar traslados, aunque con ciertas dificultades.

Tabla 55 (continuación)

	Deficiente: El espacio de movilidad es insatisfactorio y contribuye significativamente al daño de los equipos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Equipos situados fuera del área de la UTIC mientras se arreglan:  *Figura 196. Reparación de equipos fuera de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reparación de equipos fuera de la UTIC, 2023)*

Tabla 55 (continuación)

	Piezas mal ubicadas:  *Figura 197. Reparación de equipos fuera de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reparación de equipos fuera de la UTIC, 2023)* Equipo en proceso de reparación fuera de la UTIC:  *Figura 198. Equipo en proceso de reparación. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo en proceso de reparación, 2023)*

Tabla 55 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 menciona en varios de sus apartados sobre el traslado de los activos, se encontró lo siguiente: En su apartado 6 llamado *"Organización de la seguridad de la información"* en su sección 6.1.2 Segregación de deberes nos menciona que *"Se deberían segregar los deberes y áreas de responsabilidad en conflicto para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización."* Esto se menciona ya que se debiera asegurar que existan responsabilidades claras para la seguridad de la información durante el traslado de equipos. Además, en su apartado 8 llamado *"Gestión de activos"* En su sección 8.1 Responsabilidad por los activos nos menciona que *"identificar los activos organizacionales y definir las responsabilidades de protección adecuadas."* Esto se menciona ya que se asignan responsabilidades para asegurar que los activos sean debidamente protegidos. Al trasladar equipos, se debe asignar la responsabilidad de garantizar la seguridad de los activos durante el proceso de traslado. Y por último el apartado 11 llamado *Seguridad física y del entorno* Esto se menciona ya que, al trasladar equipos, es importante asegurarse de que los controles de seguridad física estén en su lugar tanto en las instalaciones de origen como en las de destino. Esto podría incluir medidas como la escolta de activos, la supervisión durante el transporte, etc.

Tabla 55 (continuación)

	Para dar solución a esta vulnerabilidad se recomienda que se asigne a un responsable para el traslado de los equipos que requieran mantenimiento en la UTIC, y un escolta de seguridad, esto puede ser un policía municipal que se encuentre en servicio en el municipio. Además de que el responsable de los traslados este consciente del riesgo que puede llevar esta responsabilidad.

Tabla 56. Prueba 6 de infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar el Estado del Techo Falso en el Cuarto del Site"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es evaluar el estado del techo falso en el cuarto del site de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si el techo falso está visiblemente dañado debido a la instalación del cableado en esta área específica. Se espera obtener una evaluación completa del estado del techo falso en el cuarto del site de la UTIC, identificando cualquier daño visible y comprendiendo las posibles causas y consecuencias.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar visualmente el techo falso en el cuarto del site de la UTIC. 2. Identificar cualquier daño visible, como grietas, desprendimientos o deformidades. 3. Revisar el historial de instalación de cableado en el cuarto del site. 4. Identificar eventos o procesos que puedan haber contribuido al daño del techo falso. 5. Simular condiciones actuales que puedan afectar el estado del techo falso, como movimientos o cambios de temperatura.
PROCESO DE MEDICIÓN	**Excelente**: El techo falso está en perfecto estado, sin daños visibles ni riesgos asociados. **Bueno**: El techo falso está en su mayoría en buen estado, aunque puede haber áreas de mejora.

Tabla 56 (continuación)

	Regular: Existen áreas identificadas que necesitan reparaciones o mejoras en el techo falso. **Suficiente**: Se cumplen los requisitos mínimos para la integridad del techo falso, pero hay áreas que necesitan reparación. **Deficiente**: El techo falso está en un estado crítico y presenta riesgos significativos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Regular**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista del techo falso dañado por el cableado del Rack.  ***Figura 199. Vista 1 del techo falso de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 1 del techo falso de la UTIC, 2023)***

Tabla 56 (continuación)

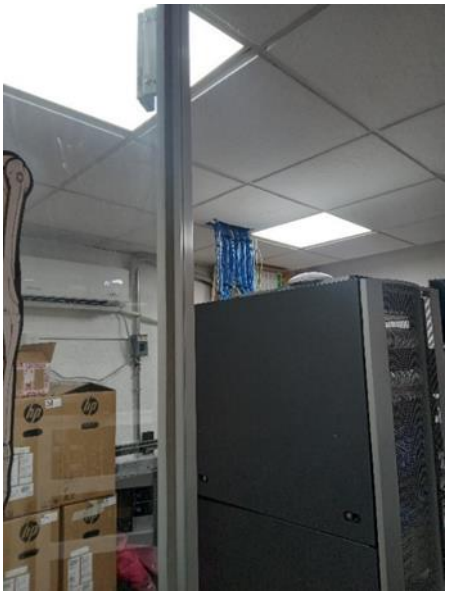
	Vista del techo falso dañado por el cableado del Rack.  *Figura 200. Vista 2 del techo falso de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 2 del techo falso de la UTIC, 2023)* Vista del techo falso dañado por el cableado del Rack.  *Figura 201. Vista 3 del techo falso de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 3 del techo falso de la UTIC, 2023)*

Tabla 56 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.1.4 Protección contra las amenazas externas y ambientales menciona que *"Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes"* En su orientación acerca de su implementación está a considerar lo siguiente: *"Se debería obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre."* Para dar solución a esta vulnerabilidad que se presenta, se recomienda cambiar el plafón de esa sección del techo falso ya que al hacer la instalación del cableado del site este error causado por el hombre, puede llegar a ser catastrófico si hay paso de tuberías que pudieran llegar a tener fugas de agua que ocasionen un corto circuito si llegara a los dispositivos de telecomunicaciones que están situados en el Rack.

Tabla 57. Prueba 7 de infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar la Protección contra Filtraciones de Agua en la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es evaluar la presencia de barreras en la entrada/salida de la UTIC para prevenir filtraciones de agua provenientes de las tuberías que pasan frente al área de esta.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se espera obtener una evaluación completa de la protección contra filtraciones de agua en la entrada/salida de la UTIC, identificando la presencia de barreras y evaluando su eficacia.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Inspeccionar visualmente la entrada/salida de la UTIC, especialmente en áreas cercanas a las tuberías. 2. Identificar la presencia o ausencia de barreras para prevenir filtraciones de agua. 3. Registrar cualquier historial previo de filtraciones de agua en la UTIC. 4. Simular condiciones adversas, como lluvias intensas, para evaluar la eficacia de las barreras existentes o la ausencia de ellas.
PROCESO DE MEDICIÓN	**Excelente**: La entrada/salida de la UTIC cuenta con barreras altamente efectivas que previenen cualquier filtración de agua. **Bueno**: La entrada/salida tiene barreras efectivas, aunque puede haber áreas de mejora. **Regular**: Existen áreas identificadas que necesitan mejoras en la protección contra filtraciones de agua. **Suficiente**: Se cumplen los requisitos mínimos para la protección contra filtraciones, pero hay áreas que necesitan mejoras.

Tabla 57 (continuación)

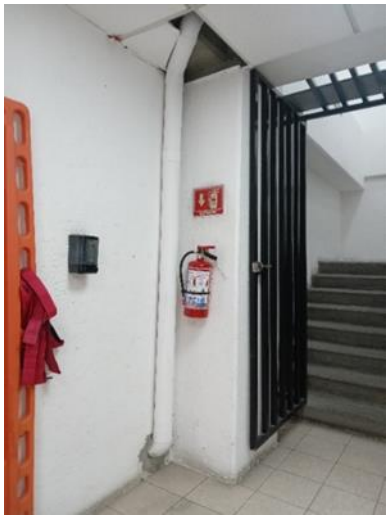
	Deficiente: La entrada/salida carece de barreras efectivas, lo
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista general de la ubicación del tubo de drenaje:  *Figura 202. Vista del Drenaje. Fuente: Ayuntamiento de Tultitlán. (Comunicación. U. d., Vista del Drenaje, 2023)*

Tabla 57 (continuación)

	Vista del “remachado” del tubo de drenaje:  *Figura 203. "Remachado" del tubo de drenaje. Fuente: Ayuntamiento de Tultitlán. (Comunicación. U. d., "Remachado" del tubo de drenaje, 2023)*
	Protección de la puerta principal de la UTIC:  *Figura 204. Protección de la puerta principal de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Protección de la puerta principal de la UTIC, 2023)*

Tabla 57 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.1.4 Protección contra las amenazas externas y ambientales menciona que *"Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes"* En su orientación acerca de su implementación está a considerar lo siguiente: *"Se debería obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre."* Para dar solución a esta vulnerabilidad se recomienda que la tubería sobresaliente que se encuentra en el pasillo donde se encuentra la UTIC sea aislada totalmente con las protecciones debidas como lo puede ser un muro de concreto, o bien que el tubo del drenaje sea oculto dentro del muro de construcción al que esta remachado.

Tabla 58. Prueba 8 de infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar Políticas y Reglas para el Uso de Equipos de Red en la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de están prueba es evaluar la existencia de reglas y políticas específicas para el uso de Routers, Switches y Servidores en la UTIC Se busca determinar si hay pautas claras y documentadas que regulen el manejo y funcionamiento de estos equipos.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se espera obtener una evaluación completa de la existencia y eficacia de reglas específicas para el uso de Routers, switches y servidores en la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar la documentación existente, manuales o políticas de la UTIC en relación con el uso de Routers, switches y servidores. 2. Identificar la presencia o ausencia de reglas específicas y pautas de uso. 3. Realizar encuestas a usuarios para evaluar su conocimiento sobre las reglas existentes y su percepción sobre la necesidad de reglas adicionales. 4. Comparar las reglas existentes (si las hay) con las mejores prácticas de seguridad y administración de redes.
PROCESO DE MEDICIÓN	**Excelente**: La UTIC cuenta con reglas bien definidas y documentadas para el uso de Routers, switches y servidores. **Bueno**: Existen reglas efectivas para el uso de equipos de red, aunque puede haber áreas de mejora. **Regular**: Existen algunas reglas, pero necesitan mejoras para abordar completamente las necesidades de seguridad y administración.

Tabla 58 (continuación)

	Suficiente: Se cumplen los requisitos mínimos para el uso de equipos de red, pero hay áreas que necesitan mejoras. **Deficiente**: No hay reglas o políticas establecidas para el uso de Routers, switches y servidores, o las existentes son insuficientes.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Cableado mal organizado por la falta de políticas sobre su uso y cuidado:  ***Figura 205. Dispositivos de telecomunicaciones. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Dispositivos de telecomunicciones, 2023)***

Tabla 58 (continuación)

	Cableado mal organizado por la falta de políticas sobre su uso y cuidado:  *Figura 206. Dispositivos de telecomunicaciones. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Dispositivos de telecomunicciones, 2023)*

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."* Acorde a su implementación esta lo siguiente: *Las políticas de seguridad de la información deberían abordar los requisitos creados por:* *a) estrategia comercial;* *b) normativas, legislación y contratos;* *c) el entorno de amenazas a la seguridad actual y proyectada.*

Tabla 58 (continuación)

	La política de seguridad de la información debería tener enunciados respecto a lo siguiente: *a) definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;* *b) asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;* *c) procesos para manejar desviaciones y excepciones.* *A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.* *Algunos ejemplos de dichos temas de políticas incluyen:* *a) control de accesos;* *b) clasificación de la información;* *c) seguridad física y ambiental;* *d) temas orientados al usuario final como:* *1) uso aceptable de activos;* *2) escritorio despejado y pantalla despejada* *3) transferencia de información;* *4) dispositivos móviles y teletrabajo;* *5) restricciones sobre las instalaciones y el uso de software;*

Tabla 58 (continuación)

	e) *respaldo;* f) *transferencia de información;* g) *protección contra malware;* h) *administración de vulnerabilidades técnicas;* i) *controles criptográficos;* j) *seguridad en las comunicaciones;* k) *privacidad y protección de información personal identificable;* l) *relaciones con los proveedores.* *Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de concientización, educación y capacitación sobre la seguridad de la información.* Para dar solución a esta vulnerabilidad se recomienda que en las Políticas de Seguridad y/o reglamento se tenga establecido el uso de los dispositivos de telecomunicaciones, así como responsabilidades y sanciones hacia aquel empleado o proveedor que realce mantenimiento preventivo y correctivo.

Tabla 59. Prueba 9 de infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Verificar el mantenimiento de los Routers, Switches y Servidores"	
OBJETIVO DE PRUEBA	La finalidad de están prueba es evaluar el estado del mantenimiento de los Routers, Switches y Servidores en la UTIC Se busca determinar si se lleva a cabo un mantenimiento frecuente para garantizar el funcionamiento adecuado y el rendimiento óptimo de estos equipos.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se espera obtener una evaluación completa del estado del mantenimiento de Routers, Switches y Servidores en la UTIC, identificando la frecuencia de las actividades de mantenimiento y cualquier área que requiera mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar el historial de mantenimiento de Routers, Switches y Servidores en la UTIC. 2. Identificar la frecuencia y la consistencia de las actividades de mantenimiento realizadas. 3. Realizar una inspección visual de los Routers, Switches y Servidores para identificar posibles signos de desgaste o falta de mantenimiento. 4. Evaluar la limpieza, conexión física y condiciones generales de los equipos. 5. Realizar simulaciones de cargas y evaluar el rendimiento de los equipos.
PROCESO DE MEDICIÓN	**Excelente**: Los Routers, Switches y Servidores reciben un mantenimiento regular y consistente, garantizando un rendimiento óptimo. **Bueno**: Existen prácticas efectivas de mantenimiento, aunque puede haber áreas de mejora.

Tabla 59 (continuación)

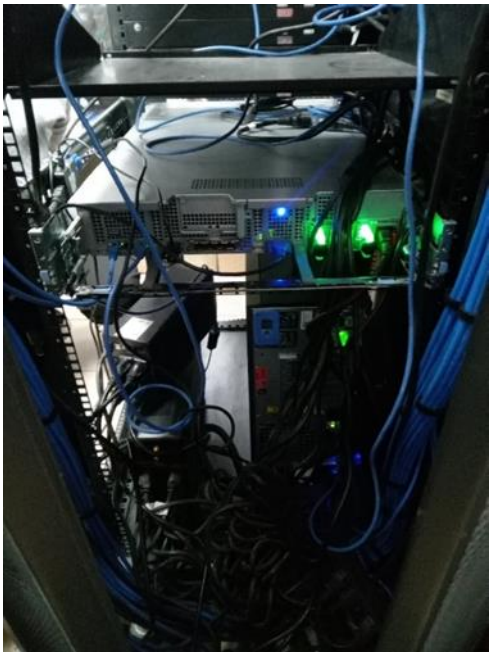
	Regular: Se lleva a cabo algún mantenimiento, pero necesita mejoras para abordar completamente las necesidades de los equipos. **Suficiente**: Los equipos pueden experimentar problemas periódicos relacionados con la falta de actividades de mantenimiento. **Deficiente**: No se lleva a cabo un mantenimiento frecuente de los Routers, Switches y Servidores, lo que puede causar un mal funcionamiento y rendimiento inadecuado.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista interior del rack demuestra que no hay un mantenimiento:  *Figura 207. Vista interior 1 del rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vsita interior 1 del rack, 2023)*

Tabla 59 (continuación)

	Vista del cableado sin una correcta organización:  *Figura 208. Vista del cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del cableado, 2023)* Presencia de polvo en la ubicación del servidor:  *Figura 209. Vista del Servidor. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del Servidor, 2023)*

Tabla 59 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.2.4 Mantenimiento de equipos menciona que *"Los equipos se deberían mantener correctamente para garantizar su disponibilidad e integridad continuas."* En su orientación de su implementación esta lo siguiente: *a) los equipos se deberían mantener de acuerdo a los intervalos y especificaciones de servicio recomendados por el proveedor;* *b) solo el personal de mantenimiento autorizado debería realizar reparaciones y labores de mantenimiento y servicio a los equipos;* *c) se deberían mantener registros de todas las fallas sospechosas o reales y de todo el mantenimiento preventivo y correctivo;* *d) se deberían implementar controles adecuados cuando se programa el mantenimiento de equipos considerando si este mantenimiento lo realizará el personal en terreno o externo a la organización; donde sea necesario se debería eliminar la información confidencial del equipo o bien lo debería realizar el personal de mantenimiento;* *e) se debería cumplir con todos los requisitos de mantenimiento impuestos por las políticas de seguros;* *f) f) luego de volver a poner al equipo en funcionamiento después de su mantenimiento, se debería inspeccionar para garantizar que no ha sido adulterado y que funciona adecuadamente.*

Tabla 59 (continuación)

	Para dar solución a esta vulnerabilidad se debiera establecer en las políticas lineamientos acerca del mantenimiento que se debería de implementar, además del personal que este capacitado para realizarlo y/o los proveedores autorizados, cabe mencionar que el momento y la frecuencia en que se debe dar mantenimiento a Routers, Switches y Servidores dependen de varios factores, como la carga de trabajo, la criticidad de los sistemas, el entorno operativo y las mejores prácticas recomendadas por el fabricante. Aunque se debiera considerar: Limpieza física: • Routers y Switches: Limpiar regularmente el polvo y asegurar de que la ventilación sea adecuada para prevenir el sobrecalentamiento. • Servidores: Limpiar el polvo y asegurar de que los sistemas de enfriamiento estén funcionando correctamente.

Tabla 60. Prueba 10 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar la Protección del Cableado del Rack"	
OBJETIVO DE PRUEBA	La finalidad de están prueba es evaluar la protección del cableado que se extiende desde el rack hacia los departamentos vecinos en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si el cableado está adecuadamente protegido contra daños, especialmente aquellos causados por la caída del techo falso dañado.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Realizar una inspección visual del cableado que se extiende desde el rack hacia los departamentos vecinos. 2. Identificar posibles áreas de daño o falta de protección. 3. Registrar cualquier daño actual en el cableado que pueda estar relacionado con la caída del techo falso dañado. 4. Revisar las medidas de protección existentes para el cableado, como canalizaciones, cubiertas o sistemas de gestión de cables. 5. Simular condiciones adversas, como la caída de objetos, para evaluar la resistencia del cableado y la efectividad de las medidas de protección.
PROCESO DE MEDICIÓN	**Excelente**: El cableado está completamente protegido con medidas efectivas que resisten condiciones adversas. **Bueno**: Existen medidas de protección efectivas, aunque puede haber áreas de mejora.

Tabla 60 (continuación)

	Regular: Existen algunas medidas de protección, pero necesitan mejoras para abordar completamente las necesidades del cableado. **Suficiente**: Se cumplen los requisitos mínimos para la protección del cableado, pero hay áreas que necesitan mejoras. **Deficiente**: El cableado no está adecuadamente protegido.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista de las canaletas con los que cuenta el Rack:  ***Figura 210. Cableado 1 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 1 del Rack, 2023)***

.

Tabla 60 (continuación)

	Cableado sin protección:  ***Figura 211. Cableado 2 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 2 del Rack, 2023)***

	Cableado sin identificación:  ***Figura 212. Cableado 3 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 3 del Rack, 2023)***

Tabla 60 (continuación)

Cableado mezclado:

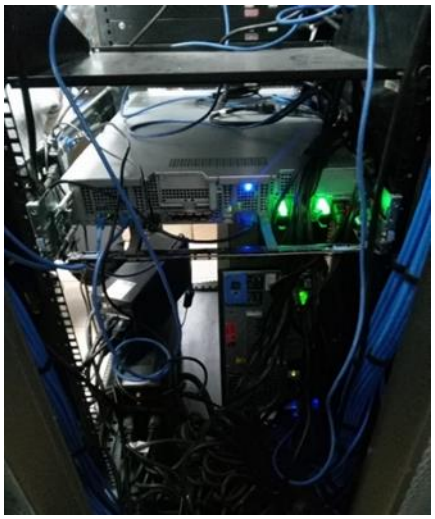


Figura 213. Cableado 4 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 4 del Rack, 2023)

Identificación de los enlaces:



Figura 214. Cableado 5 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 5 del Rack, 2023)

Tabla 60 (continuación)

	Cableado mal organizado:  *Figura 215. Cableado 6 del Rack. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado 6 del Rack, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado *"Seguridad Física y Ambiental"* en su apartado 11.2.3 nombrado *"Seguridad del Cableado"* menciona que *"Los cables de electricidad y telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger de la intercepción, interferencia o daños".* El ISO/IEC 27002 nos da pautas que son las siguientes a) *las líneas de energía y telecomunicaciones hacia las instalaciones de procesamiento de información que sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como un protector de cable de piso y un poste de servicios públicos; si los cables están bajo tierra, protegiéndolos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);* b) *separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;*

Tabla 60 (continuación)

	c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen: *1) instalación de conductos blindados y habitaciones o cajas cerradas y alarmasen los puntos de inspección y terminación;* *2) uso de blindaje electromagnético para proteger los cables;* *3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;* *4) acceso controlado a paneles de conexiones y salas de cables (por ejemplo, con llaves mecánicas o PIN);* *5) uso de cables de fibra óptica;* *d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.* Para dar solución a esta vulnerabilidad se recomienda que el peinado de los cables de ethernet esté debidamente ordenados acorde a los enlaces que se distribuyen a las áreas del Ayuntamiento. Para que su clasificación y ubicación sea de más fácil lectura si a futuro se presenta un problema con el enlace, se recomienda que con ayuda de cincho sujeta cables (material velcro) de colores para su identificación, además de que el cableado este etiquetado de extremo a extremo y no solo en el Switch como se muestra en las fotografías anteriores.

Tabla 61. Prueba 11 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluar las Medidas de Control de Plagas en la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de están prueba es evaluar las medidas de control de plagas en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si existen medidas adecuadas para prevenir y controlar la presencia de plagas que puedan poner en riesgo la condición del cableado, equipos de telecomunicaciones, mobiliario y activos en la UTIC. Se espera obtener una evaluación completa de las medidas de control de plagas en la UTIC, identificando cualquier área que requiera mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Realizar una inspección detallada de las áreas sensibles, como salas de equipos, áreas de cableado y almacenamiento de activos, en busca de signos de presencia de plagas. 2. Identificar cualquier daño existente o potencial causado por plagas. 3. Registrar las observaciones actuales relacionadas con la presencia de plagas en la UTIC. 4. Revisar las medidas de control de plagas implementadas en la UTIC, como procedimientos de limpieza, trampas, o contratos con servicios de exterminación. 5. Entrevistar al personal de limpieza y mantenimiento para obtener información sobre las acciones tomadas para prevenir y controlar plagas. 6. Simular condiciones que podrían atraer plagas para evaluar la resistencia de las medidas de control existentes.

Tabla 61 (continuación)

PROCESO DE MEDICIÓN	**Excelente**: Las medidas de control de plagas son altamente efectivas, y no se identifican problemas que requieran acciones inmediatas. **Bueno**: Existen medidas de control efectivas, aunque puede haber áreas de mejora. **Regular**: Existen algunas medidas de control, pero necesitan mejoras para abordar completamente las necesidades de prevención y control de plagas. **Suficiente**: Se cumplen los requisitos mínimos para el control de plagas, pero hay áreas que necesitan mejoras. **Deficiente**: No existe control de plagas.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Debido que no existe un control de plagas dentro de la UTIC por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	En México, la Secretaría de Salud y la Secretaría de Agricultura y Desarrollo Rural son algunas de las entidades que podrían tener regulaciones relacionadas con el control de plagas. Además, las normas de la Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS) podrían abordar aspectos relacionados con el control de plagas en instalaciones que manejan alimentos o productos de consumo.

Tabla 61 (continuación)

	Cabe mencionar que en la UTIC no hay manejo ni producción de alimentos, sin embargo, las plagas pueden presentarse por diversos motivos. Una de las razones por las que suelen proliferar plagas en oficinas o restaurantes es la generación de una gran cantidad de desechos orgánicos diariamente y una limpieza inadecuada tanto del entorno como del abastecimiento. Claro está que se deben de llevar a cabo protocolos de higiene y limpieza, pero es indudable que los complejos de oficina son ideales para los pequeños invasores. De hecho, si una oficina o empresa cuenta con la prestación de comedor para los trabajadores, hay que tener particular cuidado y conciencia en cómo y dónde almacenamos los víveres y la comida, junto con realizar procesos de limpieza de forma constante. La presencia de roedores es molesta ya que por su naturaleza buscan roer, masticar, desgastar y cortar todo tipo de materiales, incluyendo los cables de ethernet y eléctricos, lo que resultaría en un grave problema en la UTIC y hacia todo el palacio municipal en general. La NOM-232-SSA1-2009, que establece los requisitos sanitarios que deben cumplir los plaguicidas de uso agrícola, doméstico, urbano, forestal, industrial y de jardín. La NOM-232-SSA1-2009 incluye disposiciones relacionadas con la fabricación, etiquetado, registro, importación, exportación, almacenamiento, transporte, comercialización, publicidad, uso, manejo y disposición final de plaguicidas.

Tabla 61 (continuación)

	Para dar solución a esta vulnerabilidad se recomienda que el H. Ayuntamiento de Tultitlán haga contrato con alguna empresa dedicada al control de plagas para que acorde a esto se haga una desinfección y se sanitase todas las oficinas incluyendo la UTIC, e implemente estaciones de cebo como lo dicta la NOM-256-SSA1-2012.

Tabla 62. Prueba 12 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Comodidad en Mobiliario de Asientos en la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de están prueba es analizar la comodidad proporcionada por el mobiliario de asientos en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si el mobiliario actualmente utilizado ofrece niveles adecuados de comodidad para los usuarios de la UTIC, identificando posibles áreas de mejora. Se espera obtener una evaluación completa de la comodidad proporcionada por el mobiliario de asientos en la UTIC, identificando áreas que requieran mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Realizar encuestas entre los usuarios de la UTIC para evaluar su nivel de satisfacción con el mobiliario de asientos actual. 2. Realizar una revisión ergonómica del mobiliario de asientos, evaluando la alineación corporal, el soporte lumbar y otros aspectos relacionados con la comodidad. 3. Identificar cualquier característica que pueda mejorar la ergonomía. 4. Observar el uso cotidiano del mobiliario de asientos en la UTIC. 5. Identificar situaciones en las que los usuarios puedan experimentar incomodidad.
PROCESO DE MEDICIÓN	**Excelente**: El mobiliario de asientos es altamente cómodo y cumple con las expectativas de los usuarios. **Bueno**: La mayoría de los usuarios se sienten satisfechos, pero algunos pueden tener sugerencias para mejorar la comodidad.

Tabla 62 (continuación)

	Regular: Algunos usuarios expresan incomodidades y sugieren áreas específicas de mejora. **Suficiente**: Varios usuarios expresan insatisfacción con la comodidad del mobiliario de asientos. **Deficiente**: El mobiliario de asientos es incómodo, y los usuarios están insatisfechos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	Tipos de asientos de oficina con los que cuenta la UTIC:  *Figura 216. Asientos de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Asientos de la UTIC, 2023)*
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su sección 11 llamada Seguridad Física y Ambiental en su apartado 11.1.5 “Trabajo en áreas seguras” menciona que *“Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras.”*

Tabla 62 (continuación)

	En su orientación sobre su implantación esta “Se deberían considerar las siguientes pautas: *a) el personal debería estar al tanto de la existencia de, o de las actividades dentro de un área segura según se considere necesario.* *b) se debería evitar el trabajo no supervisado en áreas seguras, tanto por motivos de seguridad como para evitar las oportunidades de actividades maliciosas;* *c) las áreas seguras vacantes se deberían cerrar físicamente con candado y se deberían revisar de manera periódica;* *d) no se deberían permitir los equipos fotográficos, de video o audio, como las cámaras de dispositivos móviles, a menos que se autoricen.* *Las disposiciones para trabajar en áreas seguras incluyen controles para los empleados y usuarios de terceros trabajando en el área segura y cubren todas las actividades que se realizan en el área segura.* Considerando la importancia de mantener la seguridad en áreas seguras según el ISO/IEC 27002, es fundamental extender estas pautas específicamente al mobiliario, como los son los asientos, que forman parte integral de los entornos de trabajo. Aquí hay algunas sugerencias para conciliar las necesidades de comodidad con las disposiciones de seguridad física, basadas en las pautas proporcionadas en la sección 11.1.5 del ISO/IEC 27002: Se debiera asegurar de que los asientos en las áreas seguras estén diseñados ergonómicamente para proporcionar comodidad a los empleados sin comprometer la seguridad. Esto puede incluir sillas ajustables y soporte lumbar.

Tabla 62 (continuación)

	Ya que el permanecer sentados de una manera incorrecta traerá problemas de salud hacia sus empleados, lo cual debería de considerarse para el trabajo en áreas seguras.

Tabla 63. Prueba 13 de Infraestructura. Fuente: Elaboración propia.

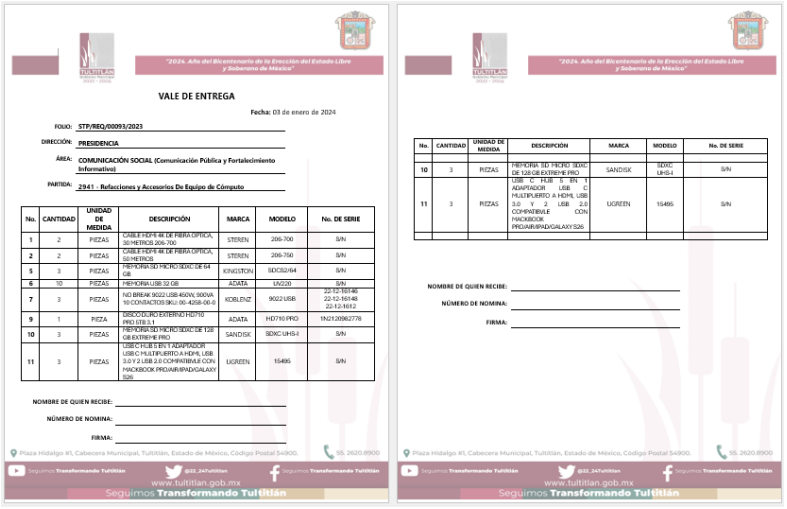
DESARROLLO DE PRUEBA "Evaluación en el Proceso de Vale de Salida y Entrega en la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es analizar la precisión y exactitud en el proceso de llenado del vale de salida y entrega por parte de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si los datos proporcionados en los vales son correctos y están completos, evitando obstáculos que impidan el reemplazo efectivo de equipos. Se espera obtener una evaluación completa de la precisión en el proceso de vale de salida y entrega en la UTIC, identificando áreas que requieran mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar vales de salida y entrega anteriores completados por la UTIC. 2. Identificar posibles errores, omisiones o datos incorrectos en los registros anteriores. 3. Verificar la exactitud de los datos en los vales con los usuarios finales involucrados en el proceso de entrega y reemplazo. 4. Entrevistar al personal de la UTIC responsable del llenado de vales de salida y entrega.
PROCESO DE MEDICIÓN	**Excelente**: El proceso de llenado de vales es altamente preciso, con datos correctos y completos en todos los registros. **Bueno**: El proceso de llenado de vales es preciso, aunque puede haber áreas de mejora. **Regular**: El proceso de llenado de vales cumple con los requisitos mínimos, pero necesita mejoras para abordar las necesidades de exactitud.

Tabla 63 (continuación)

	Suficiente: Se cumplen los requisitos mínimos para la exactitud, pero hay áreas que necesitan mejoras significativas. **Deficiente**: El proceso de llenado de vales es insuficientemente preciso, y muchos usuarios finales están insatisfechos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.
CONSIDERACIONES ESPECIALES	Se tuvo que cuestionar al personal de la UTIC si han sufrido este tipo de errores.
INTERPRETACIÓN DE RESULTADOS	Formato del Vale de Salida:  TULTITLAN Gobierno Municipal 2022 - 2024 "2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México". VALE DE SALIDA Fecha: Miercoles, 09 de agosto de 2023 **Folio de Requisición:** 14 **Descripción del Bien:** DISCO DURO EXTERNO DE 2TB **Marca:** ADATA **Modelo:** HD710 PRO **Serie:** 1L4220385961 **No. De Nomina:** **Nombre:** FABIOLA OCAÑA MOJICA **Dirección:** SINDICATURA DE INGRESOS Nombre y Firma Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900 Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán www.tultitlan.gob.mx Seguimos Transformando Tultitlán *Figura 217. Formato 1 de Vale de Salida. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Formato 1 de Vale de Salida, 2023)*

Tabla 63 (continuación)

Formato lleno del vale de entrega:



VALE DE ENTREGA

Fecha: 03 de enero de 2024

FOLIO: STP/REQ/00093/2023

DIRECCIÓN: PRESIDENCIA

ÁREA: COMUNICACIÓN SOCIAL (Comunicación Pública y Fortalecimiento Informativo)

PARTIDA: 2941 - Refacciones y Accesorios De Equipo de Cómputo

No.	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN	MARCA	MODELO	No. DE SERIE
1	2	PIEZAS	CABLE HDMI 4K DE FIBRA ÓPTICA, 30 METROS 205-700	STEREN	205-700	S/N
2	2	PIEZAS	CABLE HDMI 4K DE FIBRA ÓPTICA, 50 METROS	STEREN	205-750	S/N
5	3	PIEZAS	MEMORIA SD MICRO SDXC DE 64 GB	KINGSTON	SDCS2/64	S/N
6	10	PIEZAS	MEMORIA USB 32 GB	ADATA	UV220	S/N
7	3	PIEZAS	NO BREAK 9022 USB 450W, 900VA 10 CONTACTOS SKU: 00-4258-06-0	KOBLENZ	9022 USB	22-12-16146 22-12-16148 22-12-1612
9	1	PIEZA	DISCO DURO EXTERNO HD710 PRO 1TB 3.1	ADATA	HD710 PRO	1N2120962778
10	3	PIEZAS	MEMORIA SD MICRO SDXC DE 128 GB EXTREME PRO	SANDISK	SDXC UHS-I	S/N
11	3	PIEZAS	USB C HUB 5 EN 1 ADAPTADOR USB C MULTIPUERTO A HDMI, USB 3.0 Y 2 USB 2.0 COMPATIBLE CON MACBOOK PRO/AIR/IPAD/GALAXY S26	UGREEN	15496	S/N

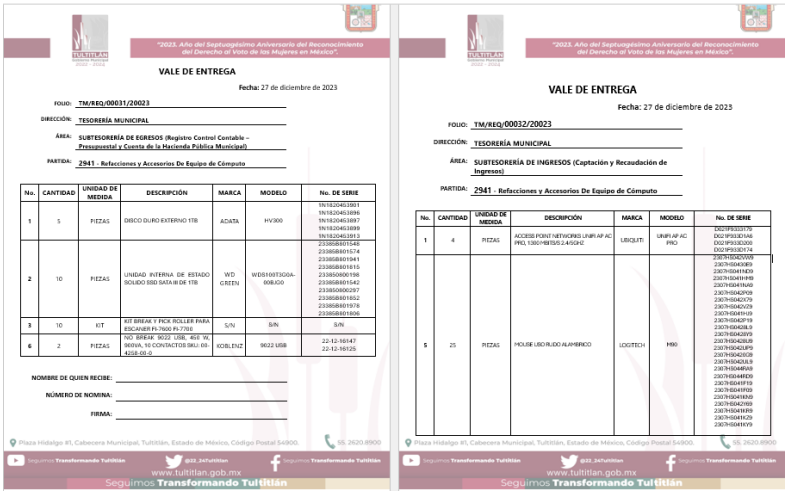
NOMBRE DE QUIEN RECIBE: _____

NÚMERO DE NOMINA: _____

FIRMA: _____

Figura 218. Formato 1 de Vale de Entrega. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Formato 1 de Vale de Entrega, 2023)

Mismo vale de entrega con diferente requisición:



VALE DE ENTREGA

Fecha: 27 de diciembre de 2023

FOLIO: TM/REQ/00031/20023

DIRECCIÓN: TESORERÍA MUNICIPAL

ÁREA: SUBTESORERÍA DE EGRESOS (Registro Control Contable – Presupuestal y Cuenta de la Hacienda Pública Municipal)

PARTIDA: 2941 - Refacciones y Accesorios De Equipo de Cómputo

No.	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN	MARCA	MODELO	No. DE SERIE
1	5	PIEZAS	DISCO DURO EXTERNO 1TB	ADATA	HV300	1N1820463881 1N1820463896 1N1820463897 1N1820463899 1N1820463913
2	10	PIEZAS	UNIDAD INTERNA DE ESTADO SOLIDO SSD SATA III DE 1TB	WD GREEN	WDS100T3G0A-00B JG0	233958601548 233958601574 233958601941 233958601815 233958600196 233958601542 233950600297 233958601852 233958601978 233958601606
3	10	KIT	KIT BREAK Y PICK ROLLER PARA ESCANER FI-7600 FI-7700	S/N	S/N	S/N
6	2	PIEZAS	NO BREAK 9022, USB, 450 W, 900VA, 10 CONTACTOS SKU: 00-4258-06-0	KOBLENZ	9022 USB	22-12-16147 22-12-16125

NOMBRE DE QUIEN RECIBE: _____

NÚMERO DE NOMINA: _____

FIRMA: _____

VALE DE ENTREGA

Fecha: 27 de diciembre de 2023

FOLIO: TM/REQ/00032/20023

DIRECCIÓN: TESORERÍA MUNICIPAL

ÁREA: SUBTESORERÍA DE INGRESOS (Captación y Recaudación de Ingresos)

PARTIDA: 2941 - Refacciones y Accesorios De Equipo de Cómputo

No.	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN	MARCA	MODELO	No. DE SERIE
1	4	PIEZAS	ACCESS POINT NETWORKS UNIFI AP AC PRO, 1300+450 MBPS 2.4/5GHZ	UBIQUITI	UNIFI AP AC PRO	D021P93D176 D021P93D1A6 D021P93D205 D021P93D174
5	25	PIEZAS	MOUSE USB RUDO ALAMBRICO	LOGITECH	M90	2307HG042W8 2307HG043B9 2307HG041KD9 2307HG041HB 2307HG041M6 2307HG042P09 2307HG042C79 2307HG042V29 2307HG041H9 2307HG042F19 2307HG042L9 2307HG042B9 2307HG042UB9 2307HG042X29 2307HG042L9 2307HG044R93 2307HG044HD9 2307HG041F19 2307HG041R29 2307HG041K89 2307HG042Y89 2307HG041R9 2307HG041K29 2307HG041K79

Figura 219. Formato 2 de Vale de Entrega. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Formato 2 de Vale de Entrega, 2023)

Tabla 63 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 Políticas para la seguridad de la información* *Las políticas internas son especialmente útiles en organizaciones de mayor tamaño y complejidad, donde aquellos que definen y aprueban los niveles ampliados de control se segregan de los que implementan los controles o en situaciones donde una política se aplica a varias personas o funciones distintas de la organización. Las políticas para la seguridad de la información se pueden emitir en un documento de política de seguridad de la información* *único o como un conjunto de documentos individual espero relacionados.* *Algunas organizaciones utilizan otros términos para estos documentos de políticas como "Normas", "Directivas" o "Reglas".* Para dar solución a esta vulnerabilidad se recomienda que haya o se implemente una sección nueva en la política para el correcto llenado del vale de salida, e implementar sanciones en caso de que un empleado de la UTIC haga un mal llenado de este.

Tabla 64. Prueba 14 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Políticas y Reglas en la UTIC"	
OBJETIVO DE PRUEBA	El propósito de esta prueba es analizar si existen políticas y reglas dentro de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar la existencia y eficacia de políticas y reglas que guíen el funcionamiento interno, seguridad y cumplimiento normativo de la UTIC. Se espera obtener una evaluación integral de la falta de políticas y reglas dentro de la UTIC, identificando áreas específicas que requieran mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar la documentación existente, incluyendo manuales, protocolos y políticas actuales en la UTIC. 2. Identificar la presencia o ausencia de políticas y reglas. 3. Comparar las prácticas actuales en la UTIC con las mejores prácticas de la industria y normativas relevantes. 4. Identificar brechas y áreas de mejora en la implementación de políticas.
PROCESO DE MEDICIÓN	**Excelente**: La UTIC cuenta con políticas y reglas exhaustivas y efectivas que cumplen con las mejores prácticas y normativas relevantes. **Bueno**: Existen políticas y reglas en la UTIC, pero puede haber áreas de mejora. **Regular**: Existen algunas políticas y reglas, pero son limitadas en alcance o efectividad. **Suficiente**: La falta de políticas y reglas es significativa y afecta el funcionamiento y la seguridad de la UTIC.

Tabla 64 (continuación)

	Deficiente: La falta de políticas y reglas es crítica y representa un riesgo grave para la UTIC.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	No existen políticas ni reglas dentro de la UTIC por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."* Acorde a su implementación esta lo siguiente: *Las políticas de seguridad de la información deberían abordar los requisitos creados por:* *a) estrategia comercial;* *b) normativas, legislación y contratos;* *c) el entorno de amenazas a la seguridad actual y proyectada.* *La política de seguridad de la información debería tener enunciados respecto a lo siguiente:* a) *definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;*

Tabla 64 (continuación)

	b) *asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;* c) *procesos para manejar desviaciones y excepciones.* *A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.* *Algunos ejemplos de dichos temas de políticas incluyen:* a) *control de accesos;* b) *clasificación de la información;* c) *seguridad física y ambiental;* d) *temas orientados al usuario final como:* 1) *uso aceptable de activos;* 2) *escritorio despejado y pantalla despejada* 3) *transferencia de información;* 4) *dispositivos móviles y teletrabajo;* 5) *restricciones sobre las instalaciones y el uso de software;* e) *respaldo;* f) *transferencia de información;* g) *protección contra malware;* h) *administración de vulnerabilidades técnicas;* i) *controles criptográficos;* j) *seguridad en las comunicaciones;* k) *privacidad y protección de información personal identificable;* l) *relaciones con los proveedores.*

Tabla 64 (continuación)

	Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de concientización, educación y capacitación sobre la seguridad de la información. Para dar solución a esta vulnerabilidad se recomienda la inmediata implementación de políticas, acorde a lo anterior mencionado y hacer uso de sanciones a todo aquel que las incumpla ya que la ausencia de políticas y reglas en la UTIC puede tener varias consecuencias negativas que afectan tanto a los empleados como a la organización en su conjunto. Algunas posibles consecuencias podrías ser: 1) La falta de políticas deja a los empleados sin una guía clara sobre cómo deben realizar sus tareas y comportarse en el entorno laboral. 2) La falta de políticas puede contribuir a la aparición de prácticas no profesionales. *3)* Sin políticas éticas claras, pueden surgir problemas de comportamiento no ético que afectan la reputación de la empresa.

Tabla 65. Prueba 15 de Infraestructura. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Orientación sobre el Uso Adecuado de Equipos en la UTIC"	
OBJETIVO DE PRUEBA	El propósito de esta prueba es analizar la explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar la existencia y eficacia de procesos de orientación para garantizar un uso adecuado de los recursos. Se espera obtener una evaluación integral sobre la falta de explicación hacia los usuarios nuevos o externos en la UTIC, identificando áreas específicas que requieran mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Entrevistar a usuarios nuevos o externos que hayan ingresado recientemente a la UTIC. 2. Obtener retroalimentación sobre la información recibida en relación con el uso adecuado de equipos. 3. Revisar cualquier material de orientación existente proporcionado a usuarios nuevos o externos. 4. Identificar los procedimientos y prácticas actuales en cuanto a la orientación sobre el uso de equipos. 5. Comparar las prácticas actuales de orientación en la UTIC con las mejores prácticas de la industria.
PROCESO DE MEDICIÓN	**Excelente**: Los usuarios están completamente informados sobre el uso adecuado de equipos y recursos. **Bueno**: La mayoría de los usuarios nuevos o externos tiene información suficiente, aunque algunas áreas pueden necesitar clarificación o expansión. **Regular**: Puede haber áreas significativas donde la información proporcionada no sea suficiente.

Tabla 65 (continuación)

	Suficiente: Se requieren acciones inmediatas para mejorar los procesos de orientación. **Deficiente**: La falta de explicación es crítica y representa un riesgo significativo.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	No hay una explicación previa por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."* Acorde a su implementación esta lo siguiente: *Las políticas de seguridad de la información deberían abordar los requisitos creados por:* *a) estrategia comercial;* *b) normativas, legislación y contratos;* *c) el entorno de amenazas a la seguridad actual y proyectada.* a)

Tabla 65 (continuación)

	La política de seguridad de la información debería tener enunciados respecto a lo siguiente: b) *definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;* *c) asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;* *d) procesos para manejar desviaciones y excepciones.* *A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.* *Algunos ejemplos de dichos temas de políticas incluyen:* *a) control de accesos;* *b) clasificación de la información;* *c) seguridad física y ambiental;* *d) temas orientados al usuario final como:* *1) uso aceptable de activos;* *2) escritorio despejado y pantalla despejada* *3) transferencia de información;* *4) dispositivos móviles y teletrabajo;* *5) restricciones sobre las instalaciones y el uso de software;* *e) respaldo;* *f) transferencia de información;* *g) protección contra malware;* h) *administración de vulnerabilidades técnicas;*

Tabla 65 (continuación)

	i) controles criptográficos; *j) seguridad en las comunicaciones;* *k) privacidad y protección de información personal identificable;* *l) relaciones con los proveedores.* *Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de concientización, educación y capacitación sobre la seguridad de la información.* Para dar solución a esta vulnerabilidad, se debiera establecer en las políticas que un empleado encargado debiera dar una breve explicación acerca de cómo se trabaja dentro de la UTIC y cual serian sus reglas y comportamientos que también debieran seguir y que se debiera de comunicar a los empleados y a las partes externas como se menciona anteriormente.

3.2.1.8 Actividad 2.8 Realizar Pruebas del Sistema de Inventario.

3.2.1.8.1 Descripción de la actividad

En esta actividad se requiere visitar las instalaciones de la UTIC ya que de esta manera es más fácil detectar aquellas anomalías que pueda presentar el sistema de inventario usado actualmente en la unidad, dicho esto se hace una mayor observación e inspección en los roles, privilegios y respaldos de los datos en la UTIC, ya que a simple vista hay una notable falta de seguridad y restricciones del sistema, ya que esta no es la adecuada de acuerdo a las responsabilidades y datos disponibles en el inventario, los criterios considerados para las pruebas y que tiene un mayor impacto en la distribución son los roles, privilegios, uso de contraseñas, respaldos y copias de seguridad en donde se pone en práctica la jerarquía de los trabajadores, los antes mencionados están acostumbrados al acceso total e intervención de la información, además de no tener seguridad alguna en el sistema de inventario usado actualmente.

3.2.1.8.2 Resultado de la actividad

Tabla 66. Prueba 1 del Sistema de Inventario. Fuente: Elaboración propia

DESARROLLO DE PRUEBA "Evaluación de Accesibilidad y Utilidad del Sistema de Inventario en la UTIC"	
OBJETIVO DE PRUEBA	El propósito de esta prueba es analizar la accesibilidad y utilidad del sistema de inventario en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar la facilidad de acceso y consulta del sistema por parte de usuarios internos y externos. Se espera obtener una evaluación completa de la accesibilidad y utilidad del sistema de inventario en la UTIC, identificando áreas específicas que requieran mejoras.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Realizar pruebas de acceso al sistema de inventario por parte de usuarios internos y externos.

Tabla 66 (continuación)

	2. Evaluar la facilidad y rapidez con la que pueden acceder a la plataforma. 3. Realizar encuestas entre usuarios internos y externos para evaluar su experiencia con el sistema de inventario. 4. Analizar datos de utilización del sistema de inventario, incluyendo la frecuencia de consultas y el tipo de información buscada.
PROCESO DE MEDICIÓN	**Excelente**: El sistema de inventario no es de fácil acceso. **Bueno**: Aunque hay facilidad de acceso, el sistema tiene medidas de seguridad aceptables. **Regular**: La facilidad de acceso presenta riesgos significativos para la seguridad del sistema de inventario. **Suficiente**: La facilidad de acceso representa un riesgo crítico para la seguridad, y se identifican vulnerabilidades importantes. **Deficiente**: El sistema de inventario es altamente accesible.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Suficiente**.
CONSIDERACIONES ESPECIALES	Se tuvo que cuestionar al Jefe de la UTIC como es que sus empleados ingresan para visualizar el inventario.

Tabla 66 (continuación)

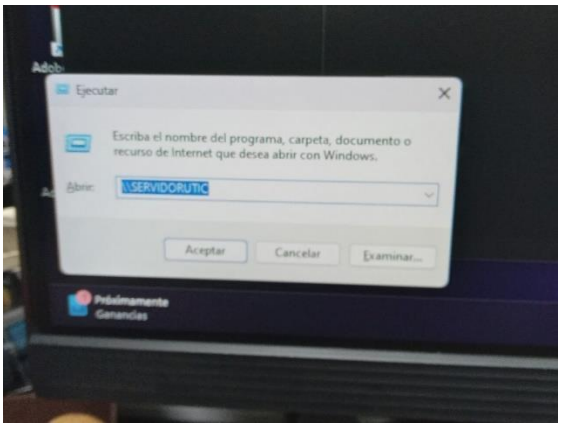
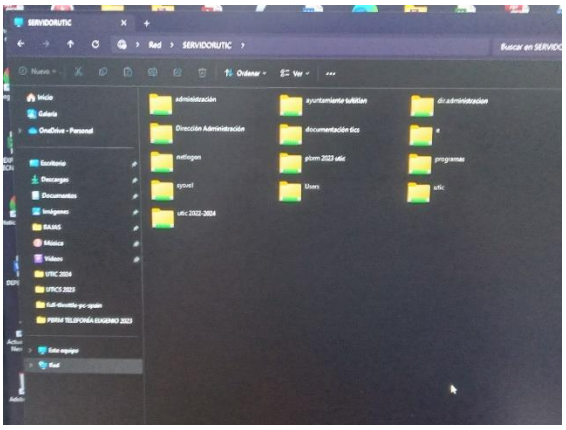
INTERPRETACIÓN DE RESULTADOS	Para ingresar al inventario se debe de ingresar a la URL de la carpeta en red donde se tiene almacenado, en este caso "SERVIDORUTIC"  *Figura 220. Función Ejecutar de Windows. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Función Ejecutar de Windows, 2023)* Ingresa directamente a las carpetas sin ninguna medida de seguridad:  *Figura 221. Carpetas en Red. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Carpetas en Red, 2023)*

Tabla 66 (continuación)

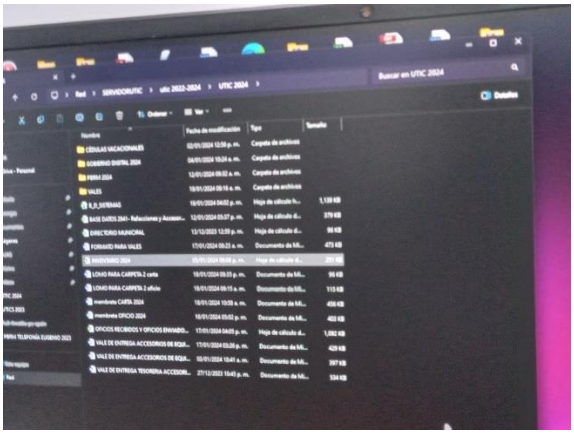
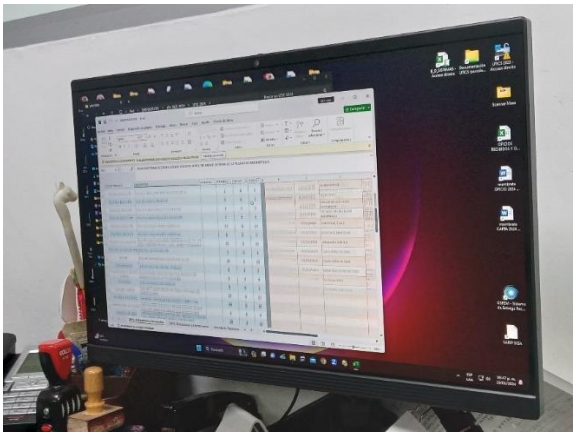
	Se ingresa a la carpeta de UTIC 2022-2024 donde se almacena el archivo de Excel de su inventario:  *Figura 222. Archivos de la Carpeta UTIC 2022-2024. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Achivos de la Carpeta UTIC 2022-2024, 2023)* Se puede visualizar el inventario sin requerir ninguna medida de seguridad:  *Figura 223. Vista del Sistema de Inventario de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del Sistema de Inventario de la UTIC, 2023)*

Tabla 66 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.* *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Para dar solución a esta vulnerabilidad se recomienda que el inventario sea migrado a un Software especializado, o en su defecto que se realice un programa que ayude a las necesidades de la UTIC, ya que todos los empleados tienen acceso a este inventario que se encuentra en Red dentro de esta unidad y cualquiera puede manipular o borrar permanentemente información sensible.

Tabla 66 (continuación)

	Se recomienda también que el programa tenga un control de acceso acuerdo a los diferentes roles que tengan los empleados.

Tabla 67. Prueba 2 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación del Desarrollo del Sistema de Inventario"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es analizar la gestión del inventario en la UTIC en relación con la utilización de sistemas gestores de bases de datos.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar la eficacia del actual sistema de inventario y evaluar las ventajas y desventajas de no contar con un sistema basado en bases de datos. Se espera obtener una evaluación integral de la gestión del inventario en la UTIC, enfocándose en la ausencia de un sistema gestor de bases de datos
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Evaluar el sistema de inventario actual utilizado en la UTIC. 2. Identificar sus características, limitaciones y métodos de gestión. 3. Comparar el sistema actual con sistemas gestores de bases de datos utilizados en la industria. 4. Analizar las ventajas potenciales de migrar a un sistema basado en bases de datos. 5. Evaluar la eficiencia y fiabilidad del sistema actual en términos de actualización, búsqueda y mantenimiento de registros.
PROCESO DE MEDICIÓN	**Excelente**: El sistema actual de inventario demuestra ser altamente eficiente y confiable, incluso sin un sistema gestor de bases de datos. **Bueno**: Aunque hay limitaciones, el sistema actual cumple con las necesidades básicas de la UTIC.

Tabla 67 (continuación)

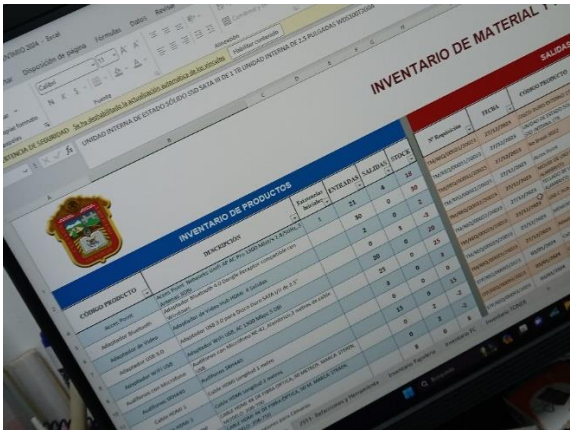
	Regular: Las limitaciones del sistema actual son significativas, afectando la eficiencia y confiabilidad del inventario. **Suficiente**: Las limitaciones del sistema actual son críticas, impactando negativamente la gestión del inventario. **Deficiente**: La ausencia de un sistema gestor de bases de datos es crítica y representa un riesgo significativo para la gestión del inventario.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Vista del inventario total de la partida X  ***Figura 224. Vista del Sistema de Inventario. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del Sistema de Inventario de la UTIC, 2023)***

Tabla 67 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.* *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Realizar un inventario en Excel puede ser una solución práctica y accesible, pero también conlleva algunos riesgos que es importante tener en cuenta. Algunos de los riesgos asociados con la gestión de inventarios en Excel incluyen: 1) La introducción manual de datos aumenta el riesgo de errores, como equivocaciones al ingresar cantidades, descripciones o ubicaciones.

Tabla 67 (continuación)

	2) Actualizar el inventario de manera oportuna y precisa puede volverse complicado a medida que el volumen de datos aumenta, lo que podría resultar en información desactualizada. 3) Los archivos de Excel pueden carecer de características avanzadas de seguridad, lo que aumenta el riesgo de acceso no autorizado o de pérdida de información crítica. 4) La gestión del inventario en Excel puede depender en gran medida de las habilidades individuales de quienes trabajan con la hoja de cálculo, lo que puede ser un riesgo si hay rotación de personal. 5) Fallos técnicos, errores humanos o mal manejo de archivos pueden resultar en la pérdida de datos, especialmente si no se realizan copias de seguridad de manera regular. Para dar solución a esta vulnerabilidad se recomienda que se migre la información del inventario a un programa o software especializado o realizado a sus medidas y necesidades de la Unidad, además de tener en cuenta que sea implementado junto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

Tabla 68. Prueba 3 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de la Estrategia de Respaldo y Copias de Seguridad del Inventario en la UTIC"	
OBJETIVO DE PRUEBA	El propósito de esta prueba es analizar la estrategia actual (o la falta de ella) de respaldo y copias de seguridad del inventario en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar la efectividad y la seguridad de las prácticas de respaldo implementadas o identificar áreas críticas que requieran atención. Se espera obtener una evaluación completa de la estrategia de respaldo y copias de seguridad del inventario en la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar las políticas actuales (si existen) relacionadas con el respaldo y copias de seguridad del inventario en la UTIC. 2. Identificar cualquier política establecida y su alcance. 3. Entrevistar al personal de la UTIC responsable del inventario y su respaldo. 4. Evaluar la existencia y efectividad de procedimientos de respaldo implementados para el inventario. 5. Realizar una simulación controlada para evaluar la eficacia del proceso de recuperación de datos a partir de respaldos existentes.
PROCESO DE MEDICIÓN	**Excelente**: Existen políticas claras y efectivas de respaldo, y se realizan respaldos de manera regular y consistente. **Bueno**: Existen algunas políticas de respaldo, y se realizan respaldos con cierta regularidad. **Regular**: La falta de políticas claras y la inconsistencia en los respaldos son evidentes.

Tabla 68 (continuación)

	Suficiente: La ausencia de políticas y prácticas de respaldo representa un riesgo significativo. **Deficiente**: La ausencia total de políticas y prácticas de respaldo es crítica y representa un riesgo extremo.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente.**
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	No se realizan copias de seguridad, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.*

Tabla 68 (continuación)

	Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos). Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información* *"Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."* *Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios. Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:* *a) se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;* b) *el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización;*

Tabla 68 (continuación)

	c) *los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;* d) *la información de respaldo debería tener un nivel de protección física y ambiental adecuada () de acuerdo con las normas que se aplican en la ubicación principal;* e) *los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;* f) *en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.* *Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos. Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio.*

Tabla 68 (continuación)

	En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre. Para solucionar esta vulnerabilidad se recomienda lo siguiente: Establecer una Política de Respaldo: 1) Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas. Esto debe incluir los requisitos de retención y protección. Además de asignar en la política al miembro que realizara los respaldos con un día especifico y en hora dedicada a realizarlo. 2) Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo. Documentar los procedimientos de restauración de manera detallada y mantenlos actualizados. 3) Establecer un plan para almacenar los respaldos en una ubicación remota, lo suficientemente distante como para evitar daños ante desastres en la ubicación principal. *4)* Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental, de acuerdo con las normas aplicables en la ubicación principal.

Tabla 68 (continuación)

	5) Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración. Verificar la confiabilidad de los datos de respaldo y su capacidad para restaurar los sistemas en caso de emergencia. *6)* Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados. Esto garantiza la integridad de los respaldos de acuerdo con la política establecida.

Tabla 69. Prueba 4 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Seguridad y Gestión de Permisos en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es analizar la seguridad y la gestión de permisos en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de control sobre la edición de información por parte de los usuarios internos y evaluar la implementación de roles y privilegios de acuerdo con los puestos. Se espera obtener una evaluación completa de la seguridad y la gestión de permisos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar la configuración actual de permisos en el sistema de inventario de la UTIC. 2. Identificar si existen roles y privilegios establecidos de acuerdo con los puestos de los usuarios. 3. Entrevistar a usuarios internos de la UTIC para obtener información sobre sus capacidades de edición en el sistema de inventario. 4. Analizar los registros de edición en el sistema de inventario para identificar patrones de cambios realizados por los usuarios. 5. Comparar la gestión de permisos actual con las mejores prácticas de seguridad en sistemas de inventario.
PROCESO DE MEDICIÓN	**Excelente**: Existen roles y privilegios claramente definidos en el sistema de inventario, y los usuarios solo pueden editar la información relevante para sus responsabilidades. **Bueno**: Existen algunos roles y privilegios, pero puede haber áreas de mejora en términos de restricciones de edición.

Tabla 69 (continuación)

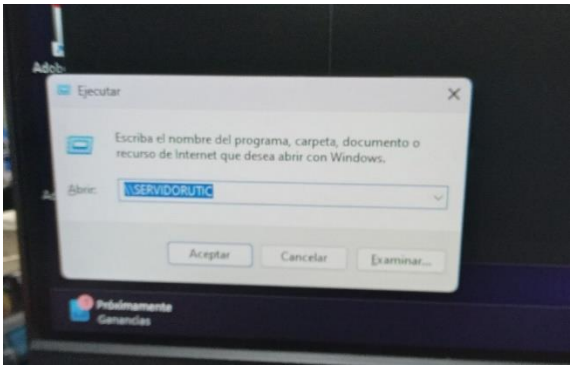
	Regular: La falta de roles y privilegios es evidente, y los usuarios pueden editar información más allá de sus responsabilidades. **Suficiente**: La ausencia total de roles y privilegios representa un riesgo significativo para la seguridad del sistema de inventario. **Deficiente**: La ausencia total de roles y privilegios es crítica y representa un riesgo extremo para la integridad de los datos del inventario.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	No cuentan con ningún permiso, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo solo se anexa la siguiente evidencia:  *Figura 225. Función de Ejecutar de Windows. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Función Ejecutar de Windows, 2023)*

Tabla 69 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.* *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Para solucionar esta vulnerabilidad se recomienda: 1) Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información. O se puede considerar software específico de gestión de activos o adaptar herramientas existentes según las necesidades de la UTIC.

Tabla 69 (continuación)

	2) Establecer roles de usuario en el sistema de gestión de activos que reflejen los roles y responsabilidades de las personas dentro de la UTIC. Se deben de definir niveles de privilegio según las tareas que cada rol deba realizar en relación con los activos de información. 3) Facilitar la identificación de activos en el ciclo de vida de la información a través del software. Asegurarse de que los usuarios puedan fácilmente asociar activos a las diferentes etapas del ciclo de vida de la información, como creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. 4) Implementar funcionalidades en el software que permitan la asignación de propiedad y clasificación para cada activo identificado. Esto asegura una adecuada gestión y control de los activos de información. 5) Proporcionar capacitación a los usuarios sobre el uso adecuado del software y los roles de privilegio asignados. Asegurarse de que comprendan cómo utilizar la herramienta para gestionar activos de manera segura y eficiente.

Tabla 70. Prueba 5 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de la Eficiencia y Sostenibilidad del Inventario en Hojas de Cálculo en la UTIC"	
OBJETIVO DE PRUEBA	El propósito de la prueba es analizar la eficiencia y sostenibilidad del sistema de inventario actual desarrollado en hojas de cálculo en la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si el sistema actual es capaz de gestionar eficientemente la creciente cantidad de información y prevenir pérdidas de datos.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar el diseño actual de las hojas de cálculo utilizadas para el inventario en la UTIC. 2. Identificar la estructura de datos, la capacidad de almacenamiento y cualquier limitación existente. 3. Analizar las hojas de cálculo para identificar áreas donde la información se ha saturado y puede provocar pérdidas de datos. 4. Evaluar la eficiencia del sistema para manejar grandes cantidades de información. 5. Comparar el sistema actual con sistemas de inventario alternativos, como bases de datos, en términos de capacidad y sostenibilidad.
PROCESO DE MEDICIÓN	**Excelente**: El sistema de inventario en hojas de cálculo es altamente eficiente y sostenible, gestionando eficazmente grandes cantidades de información. **Bueno**: Aunque eficiente, el sistema de inventario en hojas de cálculo puede mostrar algunas limitaciones en la capacidad de almacenamiento.

Tabla 70 (continuación)

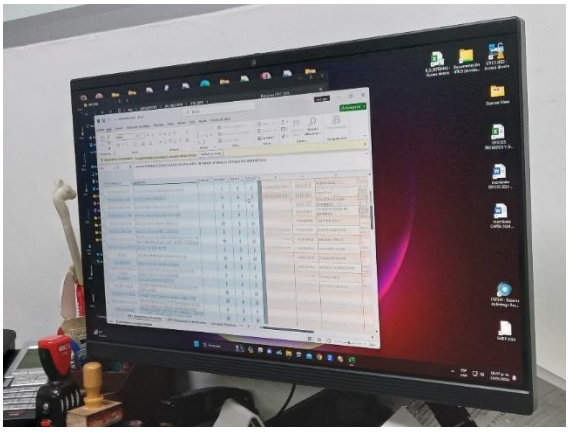
	Regular: El sistema de inventario en hojas de cálculo muestra signos de saturación de datos, y existe riesgo de pérdida de información. **Suficiente**: La saturación de datos en el sistema de inventario es crítica, afectando la eficiencia y sostenibilidad. **Deficiente**: La saturación de datos es crítica y representa un riesgo extremo para la integridad del inventario.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente.**
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	Vista del Inventario, se observa que, aunque cumple la función la información en algún momento puede comprometerse si varios usuarios manipulan la información.  *Figura 226. Vista 1 del Sistema de Inventario. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del Sistema de Inventario de la UTIC, 2023)*

Tabla 70 (continuación)

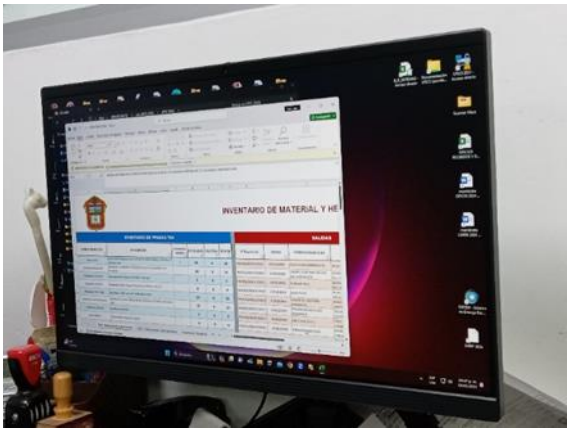
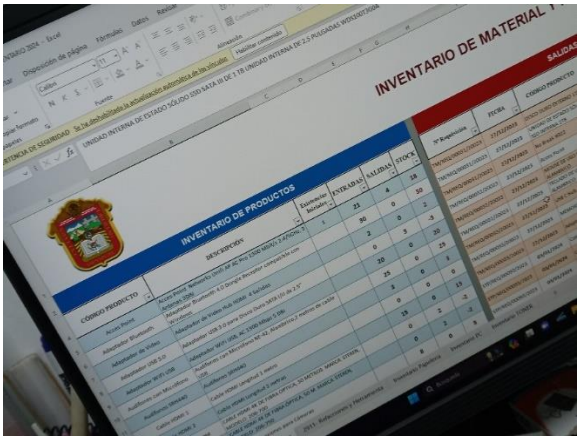
	En un mismo archivo tienen todas las partidas correspondientes que se manejan:  *Figura 227. Vista 2 del Sistema de Inventario. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 2 del Sistema de Inventario, 2023)* Se puede visualizar los campos los cuales ellos manejan:  *Figura 228. Vista 3 del Sistema de Inventario. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista 3 del Sistema de Inventario, 2023)*

Tabla 70 (continuación)

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.* *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Realizar un inventario en Excel puede ser una solución práctica y accesible, pero también conlleva algunos riesgos que es importante tener en cuenta. Algunos de los riesgos asociados con la gestión de inventarios en Excel incluyen:

Tabla 70 (continuación)

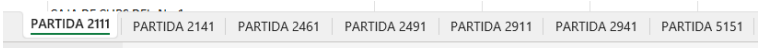
	1) La introducción manual de datos aumenta el riesgo de errores, como equivocaciones al ingresar cantidades, descripciones o ubicaciones. 2) Actualizar el inventario de manera oportuna y precisa puede volverse complicado a medida que el volumen de datos aumenta, lo que podría resultar en información desactualizada. 3) Los archivos de Excel pueden carecer de características avanzadas de seguridad, lo que aumenta el riesgo de acceso no autorizado o de pérdida de información crítica. 4) La gestión del inventario en Excel puede depender en gran medida de las habilidades individuales de quienes trabajan con la hoja de cálculo, lo que puede ser un riesgo si hay rotación de personal. 5) Fallos técnicos, errores humanos o mal manejo de archivos pueden resultar en la pérdida de datos, especialmente si no se realizan copias de seguridad de manera regular. Para dar solución a esta vulnerabilidad se recomienda que: 1) Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información. O se puede considerar software específico de gestión de activos o adaptar herramientas existentes según las necesidades de la UTIC. Además de tener en cuenta que sea implementado junto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

Tabla 71. Prueba 6 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de la Accesibilidad y Eficiencia en la Consulta de Categorías de Activos en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	La finalidad de esta prueba es analizar la accesibilidad y eficiencia en la consulta de las distintas categorías de activos en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar si el proceso actual de consulta, que requiere acceder a diferentes archivos individuales, es óptimo y eficiente. Se espera obtener una evaluación detallada de la accesibilidad y eficiencia en la consulta de categorías de activos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar la estructura actual de consulta de activos en el sistema de inventario de la UTIC. 2. Identificar la necesidad de acceder a diferentes archivos individuales para consultar distintas categorías de activos. 3. Analizar el tiempo y los recursos requeridos para realizar consultas en el sistema actual. 4. Evaluar la eficiencia del proceso y la carga de trabajo asociada. 5. Identificar cualquier desafío relacionado con la necesidad de acceder a archivos individuales.

PROCESO DE MEDICIÓN	**Excelente**: El proceso de consulta de categorías de activos es altamente accesible y eficiente. **Bueno**: Aunque eficiente, el proceso de consulta podría beneficiarse de pequeñas mejoras. **Regular**: El proceso de consulta presenta ciertas dificultades y requiere acceso a diferentes archivos individuales.

Tabla 71 (continuación)

	Suficiente: La necesidad de acceder a diferentes archivos individuales afecta significativamente la eficiencia. **Deficiente**: La consulta de categorías de activos es críticamente ineficiente y poco accesible.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Como se observa en el mismo archivo se tienen todas las partidas correspondientes:  *Figura 229. Partidas de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación.*

RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.*

Tabla 71 (continuación)

	El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación. *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Para dar solución a esta vulnerabilidad se recomienda que: 1) Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información. O se puede considerar software específico de gestión de activos o adaptar herramientas existentes según las necesidades de la UTIC, ya que al manejar partidas ayuda a clasificar a los activos según el tipo de bien que sea. Además de tener en cuenta que sea implementado junto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

Tabla 72. Prueba 7 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Medidas de Seguridad en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	Esta evaluación tiene la finalidad de analizar la ausencia de medidas de seguridad en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de riesgo asociado a la falta de seguridad y proponer acciones correctivas para proteger la integridad y confidencialidad de los datos del inventario. Se espera obtener una evaluación detallada de la ausencia de medidas de seguridad en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar las configuraciones actuales del sistema de inventario en la UTIC. 2. Identificar la falta de medidas de seguridad, como contraseñas, cifrado u otras medidas de protección. 3. Analizar los posibles riesgos asociados a la falta de seguridad en el sistema de inventario. 4. Evaluar las posibles consecuencias de accesos no autorizados o manipulación de datos. 5. Evaluar las brechas y sugerir medidas correctivas.
PROCESO DE MEDICIÓN	**Excelente**: Los datos del inventario están protegidos contra accesos no autorizados y manipulación indebida. **Bueno**: La mayoría de los usuarios considera que el sistema es seguro, pero se identifican oportunidades de fortalecimiento. **Regular**: Se reconocen deficiencias y se requieren acciones inmediatas para implementar medidas de seguridad básicas. **Suficiente**: Se requieren acciones correctivas urgentes para implementar medidas de seguridad efectivas.

Tabla 72 (continuación)

	Deficiente: Ni existe medida de seguridad alguna,
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	No cuenta con ninguna medida de seguridad, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación.*

Tabla 72 (continuación)

	Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos Para solucionar esta vulnerabilidad se recomienda lo siguiente: 1) Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información. O se puede considerar software específico de gestión de activos o adaptar herramientas existentes según las necesidades de la UTIC, sin olvidar mencionar que debe de contar con un Inicio de sesión que restrinja el acceso a las diferentes funciones de pudiera llegar a tener este acorde a el rol, ocupación y tareas de cada empleado.

Tabla 73. Prueba 8 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Estrategias de Respaldo y Recuperación en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	Esta evaluación tiene la finalidad de analizar la falta de copias de seguridad y respaldos en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de riesgo asociado a la ausencia de estrategias de respaldo y proponer acciones correctivas para garantizar la integridad y disponibilidad de los datos del inventario. Se espera obtener una evaluación detallada de la falta de copias de seguridad y respaldos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar las estrategias actuales de respaldo y recuperación en el sistema de inventario de la UTIC. 2. Identificar la falta de copias de seguridad y respaldos. 3. Analizar los riesgos potenciales asociados a la falta de copias de seguridad y respaldos en el sistema de inventario. 4. Evaluar las posibles consecuencias de la pérdida de datos y la incapacidad de recuperar información crítica. 5. Comparar la falta de copias de seguridad y respaldos con las mejores prácticas de seguridad en sistemas de inventario.
PROCESO DE MEDICIÓN	**Excelente**: El sistema de inventario cuenta con estrategias de respaldo y recuperación altamente efectivas. **Bueno**: Aunque existen algunas estrategias de respaldo, puede haber áreas de mejora.

Tabla 73 (continuación)

	Regular: Se reconocen deficiencias y se requieren acciones inmediatas para implementar estrategias básicas de respaldo. **Suficiente**: La ausencia de copias de seguridad y respaldos es crítica y representa un riesgo significativo. **Deficiente**: Ausencia total de copias de seguridad y respaldos.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Ausencia total de copias de seguridad y respaldos, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.*

Tabla 73 (continuación)

	El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación. *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información* *"Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."* *Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios. Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:* g) *se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;*

Tabla 73 (continuación)

	h) el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización; *i) los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;* *j) la información de respaldo debería tener un nivel de protección física y ambiental adecuada () de acuerdo con las normas que se aplican en la ubicación principal;* *k) los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;* *l) en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.*

Tabla 73 (continuación)

	Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos. Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre. Para solucionar esta vulnerabilidad se recomienda lo siguiente: Establecer una Política de Respaldo: 1) Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas. Esto debe incluir los requisitos de retención y protección. Además de asignar en la política al miembro que realizara los respaldos con un día especifico y en hora dedicada a realizarlo. 2) Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo. Documentar los procedimientos de restauración de manera detallada y mantenlos actualizados. *3)* Establecer un plan para almacenar los respaldos en una ubicación remota, lo suficientemente distante como para evitar daños ante desastres en la ubicación principal.

Tabla 73 (continuación)

	4) Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental, de acuerdo con las normas aplicables en la ubicación principal. 5) Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración. Verificar la confiabilidad de los datos de respaldo y su capacidad para restaurar los sistemas en caso de emergencia. *6)* Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados. Esto garantiza la integridad de los respaldos de acuerdo con la política establecida.

Tabla 74. Prueba 9 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Controles de Eliminación de Archivos en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	Esta evaluación tiene como propósito analizar la eliminación accidental y permanente de archivos (hojas de cálculo) por parte de los empleados en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de riesgo asociado a esta práctica y proponer acciones correctivas para prevenir la pérdida involuntaria de datos críticos. Se espera obtener una evaluación detallada de la eliminación accidental y permanente de archivos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar las políticas y procedimientos actuales relacionados con la eliminación de archivos en el sistema de inventario de la UTIC. 2. Identificar la ausencia de controles para prevenir la eliminación accidental y permanente. 3. Analizar incidentes anteriores de eliminación accidental de archivos para comprender la frecuencia. 4. Entrevistar a usuarios y responsables de la UTIC para obtener información sobre las causas subyacentes de la eliminación accidental 5. Proponer e implementar controles preventivos, como confirmaciones de eliminación, versiones de archivos o medidas que eviten la eliminación permanente por error.
PROCESO DE MEDICIÓN	**Excelente**: El sistema de inventario cuenta con controles altamente efectivos para prevenir la eliminación accidental y permanente de archivos.

Tabla 74 (continuación)

	Bueno: La mayoría de los usuarios es consciente de las prácticas seguras, pero se identifican oportunidades de fortalecimiento. **Regular**: La falta de controles para prevenir la eliminación accidental representa un riesgo moderado. **Suficiente**: La ausencia de controles preventivos es crítica. **Deficiente**: Ausencia total de controles preventivos es crítica y representa un riesgo extremo.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	La ausencia total de controles preventivos es crítica, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.*

Tabla 74 (continuación)

	Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación. *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información* *"Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."* *Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios. Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:* m) *se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;*

Tabla 74 (continuación)

	n) el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización; *o) los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;* *p) la información de respaldo debería tener un nivel de protección física y ambiental adecuada () de acuerdo con las normas que se aplican en la ubicación principal;* *q) los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;* *r) en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.*

Tabla 74 (continuación)

	Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos. Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre. Para solucionar esta vulnerabilidad se recomienda lo siguiente: 1) Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas. Esto debe incluir los requisitos de retención y protección. Además de asignar en la política al miembro que realizara los respaldos con un día especifico y en hora dedicada a realizarlo. 2) Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo. Documentar los procedimientos de restauración de manera detallada y mantenlos actualizados. 3) Establecer un plan para almacenar los respaldos en una ubicación remota, lo suficientemente distante como para evitar daños ante desastres en la ubicación principal.

Tabla 74 (continuación)

	4) Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental, de acuerdo con las normas aplicables en la ubicación principal. 5) Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración. Verificar la confiabilidad de los datos de respaldo y su capacidad para restaurar los sistemas en caso de emergencia. 6) Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados. Esto garantiza la integridad de los respaldos de acuerdo con la política establecida.

Tabla 75. Prueba 10 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Registros de Movimientos en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	Esta evaluación tiene la finalidad analizar la falta de registros de movimientos en el sistema de inventario actual de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de riesgo asociado a la ausencia de información detallada sobre los movimientos de activos y proponer acciones correctivas para mejorar el seguimiento y la transparencia en el inventario. Se espera obtener una evaluación detallada de la falta de registros de movimientos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar las funcionalidades actuales del sistema de inventario de la UTIC en términos de registro de movimientos. 2. Identificar la falta de información detallada, incluyendo hora, fecha y responsable, en los registros de movimientos. 3. Evaluar la importancia de la hora, fecha y cuenta del responsable en los registros. 4. Proponer e implementar mejoras en el sistema de inventario para incluir registros detallados de movimientos, con información de hora, fecha y responsable.
PROCESO DE MEDICIÓN	**Excelente**: El sistema de inventario registra de manera detallada y efectiva todos los movimientos, incluyendo hora, fecha y responsable. **Bueno**: Aunque existen algunos registros de movimientos, puede haber áreas de mejora.

Tabla 75 (continuación)

	Regular: La falta de registros detallados representa un riesgo moderado para el seguimiento y la transparencia en el inventario. **Suficiente**: La ausencia de registros detallados es crítica y representa un riesgo significativo. **Deficiente**: Ausencia total de registros detallados es crítica y representa un riesgo extremo.
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales
INTERPRETACIÓN DE RESULTADOS	No hay registro de quien hace el movimiento ni hora ni fecha, por lo que no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.*

Tabla 75 (continuación)

	El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación. *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información* *"Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."* *Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios. Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:* s) *se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;*

Tabla 75 (continuación)

	t) *el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización;* u) *los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;* v) *la información de respaldo debería tener un nivel de protección física y ambiental adecuada () de acuerdo con las normas que se aplican en la ubicación principal;* w) *los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;* x) *en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.*

Tabla 75 (continuación)

	Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos. Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre. Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."* Acorde a su implementación esta lo siguiente: *Las políticas de seguridad de la información deberían abordar los requisitos creados por:* *d) estrategia comercial;* *e) normativas, legislación y contratos;* *f) el entorno de amenazas a la seguridad actual y proyectada.* *La política de seguridad de la información debería tener enunciados respecto a lo siguiente:* *e) definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades*

Tabla 75 (continuación)

	f) asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos; *g) procesos para manejar desviaciones y excepciones.* *A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.* *Algunos ejemplos de dichos temas de políticas incluyen:* *e) control de accesos;* *f) clasificación de la información;* *g) seguridad física y ambiental;* *h) temas orientados al usuario final como:* *6) uso aceptable de activos;* *7) escritorio despejado y pantalla despejada* *8) transferencia de información;* *9) dispositivos móviles y teletrabajo;* *10) restricciones sobre las instalaciones y el uso de software;* *m) respaldo;* *n) transferencia de información;* *o) protección contra malware;* *p) administración de vulnerabilidades técnicas;* *q) controles criptográficos;* *r) seguridad en las comunicaciones;* *s) privacidad y protección de información personal identificable;* *t) relaciones con los proveedores.*

Tabla 75 (continuación)

	Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de concientización, educación y capacitación sobre la seguridad de la información. Para solucionar esta vulnerabilidad se recomienda lo siguiente: 1) En su inventario actual deberían implementar una celda específicamente para ingresar al personal que hace el movimiento en el inventario, esto como medida de seguridad ya que, si no cuentan con esto, en dado caso que se materialice un error saber quién ocasiono el cruce de información o que esta sea errónea aplicarle debidas sanciones establecidas en las políticas. *2)* Implementar sanciones en caso de un error humano en las políticas.

Tabla 76. Prueba 11 del Sistema de Inventario. Fuente: Elaboración propia.

DESARROLLO DE PRUEBA "Evaluación de Procedimientos y Controles durante Cargas y Partidas de Datos en el Sistema de Inventario de la UTIC"	
OBJETIVO DE PRUEBA	Esta evaluación tiene la finalidad de analizar la confusión de archivos manejados durante cargas o partidas de datos en el sistema de inventario de la UTIC.
DESCRIPCIÓN DE LA PRUEBA Y VALOR ESPERADO	Se busca determinar el nivel de riesgo asociado a esta confusión y proponer acciones correctivas para mejorar los procedimientos y controles durante estas operaciones. Se espera obtener una evaluación detallada de la confusión de archivos durante cargas o partidas de datos en el sistema de inventario de la UTIC.
TÉCNICA	Evaluación, Observación, Verificar
ACTIVIDADES DE LA PRUEBA	1. Revisar los procedimientos actuales relacionados con cargas y partidas de datos en el sistema de inventario de la UTIC. 2. Identificar posibles puntos de confusión y áreas donde se pueden mejorar los controles. 3. Analizar incidentes anteriores de confusión durante cargas o partidas de datos para comprender la frecuencia y las circunstancias. 4. Proponer e implementar mejoras en los procedimientos y controles durante cargas y partidas de datos para reducir la confusión. 5. Incluir medidas como verificaciones adicionales, etiquetado claro de archivos y validaciones de datos.
PROCESO DE MEDICIÓN	**Excelente**: Los procedimientos y controles durante cargas y partidas de datos son altamente efectivos y reducen al mínimo la confusión.

Tabla 76 (continuación)

	Bueno: Aunque existen algunos procedimientos, puede haber áreas de mejora. **Regular**: Se reconocen deficiencias y se requieren acciones. **Suficiente**: Se requieren acciones correctivas urgentes para implementar mejoras en los procedimientos y controles. **Deficiente**: La ausencia total de procedimientos y controles efectivos es crítica
CRITERIOS DE TERMINACIÓN / VALOR OBTENIDO	Tras hacer las pruebas antes mencionadas, se rectificó que varios criterios u objetivos no se cumplen. Por lo que el valor obtenido es **Deficiente**.
CONSIDERACIONES ESPECIALES	Sin consideraciones especiales.
INTERPRETACIÓN DE RESULTADOS	Aunque existen algunos procedimientos, no hay manera de medir ni de interpretar la condición actual o bien dicha prueba, así mismo no se puede anexar evidencia alguna.
RECOMENDACIONES	Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."* Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.*

Tabla 76 (continuación)

	El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad y clasificación. *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).* Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."* Acorde a su implementación esta lo siguiente: *Las políticas de seguridad de la información deberían abordar los requisitos creados por:* *a) estrategia comercial;* *b) normativas, legislación y contratos;* c) *el entorno de amenazas a la seguridad actual y proyectada.*

Tabla 76 (continuación)

	La política de seguridad de la información debería tener enunciados respecto a lo siguiente: *a) definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;* *b) asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;* *c) procesos para manejar desviaciones y excepciones.* *A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.* *Algunos ejemplos de dichos temas de políticas incluyen:* *a) control de accesos;* *b) clasificación de la información;* *c) seguridad física y ambiental;* *d) temas orientados al usuario final como:* *e) uso aceptable de activos;* *f) escritorio despejado y pantalla despejada* *g) transferencia de información;* *h) dispositivos móviles y teletrabajo;* *i) restricciones sobre las instalaciones y el uso de software;*

Tabla 76 (continuación)

	j) seguridad física y ambiental; *k) temas orientados al usuario final como:* *1) uso aceptable de activos;* *2) escritorio despejado y pantalla despejada* *3) transferencia de información;* *4) dispositivos móviles y teletrabajo;* *5) restricciones sobre las instalaciones y el uso de software;* *e) respaldo;* *f) transferencia de información;* *g) protección contra malware;* *h) administración de vulnerabilidades técnicas;* *i) controles criptográficos;* *j) seguridad en las comunicaciones;* *k) privacidad y protección de información personal identificable;* *l) relaciones con los proveedores.* *Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de concientización, educación y capacitación sobre la seguridad de la información.* Para dar solución a esta vulnerabilidad se recomienda: 1) Que las partidas que se encuentras clasificadas por hojas en Microsoft Excel sean identificadas por colores para evitar confusión alguna. *2)* Implementar sanciones en las políticas a quien no tenga cuidado al llenado de una partida.

CAPÍTULO IV

RESULTADOS

4.1 Tercer Objetivo: Entregar Resultados

4.1.1 Actividades

4.1.1.1 Actividad 3.1 Analizar y sintetizar los hallazgos de la Auditoría en un informe final.

4.1.1.2 Actividad 3.2 Generar recomendaciones de acuerdo con los estándares y normas utilizados

4.1.1.2.1 Descripción de las actividades

Después de realizar todas las pruebas de acuerdo con cada uno de los puntos de interés (Seguridad Física, Seguridad Lógica, Servicios, Infraestructura y Sistema de Inventario), se realizó un informe ejecutivo donde se extrae de manera clara las deficiencias que se analizaron, los posibles escenarios donde pueden ocurrir, el nivel de atención que requiere además de las recomendaciones de acuerdo con los estándares mencionados dentro de cada una de las pruebas realizadas.

4.1.1.2.2 Resultado de las actividades

Informe Ejecutivo

Informe Final de la Auditoría

Honorable Ayuntamiento de Tultitlán Año 2023-2024

Entrega: 02 de Febrero de 2024

Jefe de la Unidad de Tecnologías de la Información y Comunicación (UTIC) Jonathan Rodrigo Pérez Del Río

Atte. Oscar Y. Moran y Ana L. Santos

Apreciado Jefe de la UTIC

Tenemos el agrado de dirigirnos a Ud. a efectos de elevar ante su consideración el alcance del trabajo de Auditoría con Normas ISO de la Familia 2700 y otros Estándares para los procesos internos del H. Ayuntamiento de Tultitlán practicada en el periodo del 2 de octubre de 2023 a 2 de Febrero del presente año, sobre la base del análisis y procedimientos detallados de todas las informaciones recopiladas y emitidos en el presente informe, que a nuestro criterio es razonable.

Síntesis de la revisión realizada, clasificado en las siguientes secciones:

a) Seguridad Física
b) Seguridad Lógica
c) Servicios
d) Infraestructura
e) Sistema de Inventario

El contenido del informe ha sido dividido de la siguiente forma a efectos de facilitar su análisis.

a. Situación. Describe brevemente las debilidades resultantes de nuestro análisis.

b. Efectos y/o implicancias probables. Enuncian los posibles riesgos a que se encuentran expuestos las operaciones realizadas por la Cooperativa.

c. Índice de importancia establecida. Indica con una calificación del 0 al 3 el grado crítico del problema y la oportunidad en que se deben tomar las acciones correctivas del caso.

0 = Muy Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

2 = Medio (acciones diferidas correctivas)

3 = Bajo (acciones diferidas preventivas)

d. Sugerencias. Indicamos a la Gerencia la adopción de las medidas correctivas tendientes a subsanar las debilidades comentadas.

Según el análisis realizado hemos encontrado carencias en que no existen medidas de seguridad física suficientes en los accesos que protejan debidamente a los equipos; no se manejan respaldos de la información; falta de sistemas de atención contra emergencias, accesos de los usuarios; falta de espacio en su área de trabajo; y falta de un sistema de inventario.

El detalle de las deficiencias encontradas, como así también las sugerencias de solución se encuentran especificadas en el siguiente informe. La aprobación y puesta en práctica de estas sugerencias ayudarán a la UTIC a brindar un servicio más eficiente a todos empelados y usuarios.

Agradecemos la colaboración prestada durante nuestra visita por todo el personal de la UTIC y quedamos a su disposición para cualquier aclaración y/o ampliación de la presente que estime necesaria.

Atte. Oscar Y. Moran y Ana L. Santos.

A. Seguridad Física

A.1. Evaluación del Cierre Seguro de Accesos dentro del Horario Laboral

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de los equipos y activos internos del área como, por ejemplo:

- No se cierran con seguro los accesos cuando el sitio no está siendo utilizado en horario de trabajo.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad física enfocada al cierre seguro del lugar en horario laboral cuando el sitio no está siendo utilizado, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Fácil acceso no autorizado de usuarios externos y personal del ayuntamiento a la UTIC.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acuerdo al ISO/IEC 27002 en su apartado 7 llamado “Controles Físicos” nos menciona que se debe *“Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización”.*

Para dar solución a esta vulnerabilidad acorde a lo anterior mencionado se recomienda:

- Establecer a un encargado que se responsabilice de cerrar el acceso al área de manera correcta y segura aun en horario laboral siempre y cuando la oficina quede totalmente vacía sin importar el periodo de tiempo en el que se encuentre de esta manera evitando todo acceso no autorizado ni deseado.

A.2 Evaluación del Control de uso compartido de Equipos de Oficina.

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el correcto uso de los equipos de oficina internos del área como, por ejemplo:

- Uso Compartido de equipo de oficina, como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad física enfocada al uso compartido de equipos de oficina, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Robo de información, equipos o activos por parte de usuarios externos.
- Uso comprometido del equipo de oficina y daños sin responsables definidos por parte de usuario externos.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acuerdo al ISO/IEC 27002 en su apartado 8 llamado “Administración de Activos” nos dice que se debe *“identificar los activos organizacionales y definir las responsabilidades de protección adecuadas”.*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer en las políticas el uso permitido de los recursos de TI como lo es el equipo de impresión multifuncional con sus respectivas sanciones.
- Implementar una bitácora para la utilización del equipo de oficina, el cual debe registrar, la hora, fecha, usuario externo, propósito para el cual hizo uso de este.

A.3 Revisión de Programa de Capacitación en Gestión de Riesgos de Seguridad Física.

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad mencionando los programas de capacitación en gestión de riesgos de seguridad física, como, por ejemplo:

- No se ha establecido un programa de capacitación de gestión de riesgos para identificar y atender los riesgos asociados a la seguridad física.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad física enfocada al programa de capacitación en gestión de riesgos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Puede dejar a la organización vulnerable a diversas amenazas, como robos, intrusiones, vandalismo o desastres naturales. Sin una comprensión adecuada de los posibles riesgos y medidas preventivas, el personal podría no estar preparado para identificar situaciones de riesgo o para implementar medidas de seguridad eficaces. Esto podría aumentar la probabilidad de incidentes que podrían tener consecuencias negativas para la seguridad y el funcionamiento normal de la organización.

c. Índice de Importancia Establecido.

- 3 (tres) = Bajo

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 7 llamado Seguridad de recursos humanos en su sección *7.2.2 Concientización, educación y capacitación sobre la seguridad de la información*

Nos menciona que *"Todos los empleados de la organización y, donde sea pertinente, los contratistas deberían recibir educación y capacitación de concientización adecuada y*

actualizaciones regulares sobre las políticas y procedimientos organizacionales, según sea pertinente para su función laboral."

Para dar solución a esta vulnerabilidad acorde a lo anterior mencionado se recomienda:

- Implementar programas de capacitación semestrales en seguridad física y así la integración de las mejores prácticas de seguridad física en este programa.

A.4 Evaluación de Políticas y Procedimientos para la Gestión de Incidentes de Seguridad Física.

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad mencionando la falta de políticas y procedimientos para la gestión de incidentes de seguridad física como, por ejemplo:

- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad física enfocada a las políticas y a los procedimientos para la gestión de incidentes, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- La ausencia de políticas y procedimientos formales para la gestión de incidentes de seguridad física puede llevar a una respuesta ineficaz ante eventos no deseados, como intrusiones, robos, vandalismo o desastres naturales. Sin un marco establecido, el personal podría carecer de una guía clara sobre cómo abordar y mitigar los incidentes de seguridad física de manera efectiva.

c. Índice de Importancia Establecido.

- 3 (tres) = Bajo

d. Sugerencias

Acorde al estándar ISO/IEC 27002 en su sección 16 llamado Administración de incidentes de seguridad de la información

Nos dice su objetivo que se debiera *"garantizar un enfoque coherente y eficaz a la administración de incidentes de seguridad de la información, incluida la comunicación sobre los eventos y las debilidades de seguridad."*

Para dar solución a esta vulnerabilidad acorde a lo anterior mencionado se recomienda:

- Designar un equipo de respuesta a incidentes y asignar responsabilidades específicas.
- Desarrollar planes de respuesta detallados para diversos escenarios de seguridad física.
- Implementar sistemas de monitoreo físico y tecnológico para detectar incidentes.
- Establecer procesos para analizar, clasificar y atender incidentes según su gravedad.
- Definir cómo se recopilará, preservará y analizará la evidencia física en caso de incidentes.
- Proporcionar capacitación regular al personal designado para manejar incidentes.
- Realizar ejercicios de simulacro para mejorar las habilidades de respuesta.

A.5 Revisión del Control y Monitoreo de Cámaras de Videovigilancia Internas

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la revisión del control y monitoreo de cámaras de videovigilancia internas como, por ejemplo:

- El monitoreo de las cámaras de videovigilancia internas no está a cargo de los empleados de la UTIC, si no del departamento “X”.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad física enfocada a la revisión del control y monitoreo de cámaras de videovigilancia internas, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- La separación de las responsabilidades de monitoreo de videovigilancia entre diferentes departamentos podría resultar en una falta de coordinación y comunicación efectiva entre la seguridad de la información y la seguridad física. Esto podría llevar a brechas en la detección y respuesta a incidentes, ya que los equipos pueden no estar al tanto de manera oportuna de los eventos que afectan tanto a la seguridad física como a la de la información. La falta de una gestión unificada de la seguridad podría debilitar la capacidad de la organización para abordar de manera integral los riesgos y amenazas potenciales que podrían surgir en el entorno de seguridad.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alta

d. Sugerencias

Acorde a la norma ISO/IEC 27001 en su sección 7 llamado Soporte nos dice que *“La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.”*

Cabe mencionar que también existen leyes en el Estado de México que respaldan el uso de cámaras de videovigilancia, como lo es “LEY QUE REGULA EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN PARA LA SEGURIDAD PÚBLICA DEL ESTADO DE MÉXICO” esta nos dice que *“La presente Ley es de orden e interés público y de observancia general en todo el territorio del Estado de México y tiene por objeto establecer las bases de coordinación entre las instituciones de seguridad pública del Gobierno del Estado de México y de los municipios de la entidad, en el uso y aprovechamiento de las tecnologías de la información y comunicación en el marco de los Sistemas Nacional y Estatal de Seguridad Pública…”*

Para dar solución a esta vulnerabilidad acorde a lo anterior mencionado se recomienda:

- La organización debe establecer un procedimiento documentado para la gestión de activos, incluyendo las cámaras de seguridad. Este procedimiento debería abordar la identificación, clasificación y control de los activos relacionados con la videovigilancia, garantizando su seguridad y disponibilidad.
- La organización debe implementar medidas de seguridad física y lógica para proteger el acceso no autorizado a las cámaras y a la información capturada por ellas.

B. Seguridad Lógica

B.1. Revisión de contraseñas seguras

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- No se siguen procedimientos para cambiar periódicamente las contraseñas.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a los procedimientos para cambiar periódicamente las contraseñas, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación, alteración o secuestro de información y los datos por parte de usuarios externos o internos.

c. Índice de Importancia Establecido.

- 3 (Tres) = Bajo

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado "**Información para Autenticación**" menciona que "La asignación y gestión de la información de autenticación debería ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación".

Para dar solución ante esta vulnerabilidad se recomiendan:

- Uso de contraseñas internas que sean seguras, creando una combinación de letras y números sin un orden especifico, alternando mayúsculas y minúsculas, o bien secuencias de números sin un contexto o significado e incluyendo caracteres especiales, además que sea de una longitud de mínimo 9 caracteres.
- Contraseñas diferentes para todas aquellas cuentas o situaciones laborales que las requieran.

- Cambiar las contraseñas usadas cuando los empleados dejen de laborar internamente o cambien de área.
- Mantener la opción de “mostrar contraseña” desactivada cada que se requiera ingresar las contraseñas creadas por cada usuario.

B.2. Inspección de catálogo contra incidentes de seguridad lógica

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- No se lleva un registro de los incidentes de seguridad ocurridos y las acciones tomadas.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a la existencia de un catálogo contra incidentes de seguridad lógica, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación, alteración o secuestro de información y los datos por parte de usuarios externos o internos.

c. Índice de Importancia Establecido.

- 3 (Tres) = Bajo

d. Sugerencias

Acorde al estándar (ISO 27035:2013) en su apartado llamado **“5. Fase de Planeamiento y Preparación”** nos menciona en su sección **“5.1 Revisión de actividades claves”** que “La gestión eficaz de incidentes de seguridad de la información requiere un planeamiento y preparación apropiados.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Un formato en el que se registren dichos incidentes que pongan en riesgo la seguridad lógica de la información, capaz de almacenar los datos críticos del acontecimiento, como lo son fecha, hora, tipo de incidente, clasificación de acuerdo con el impacto que este llega o puede llegar a tener en la información almacenada en la UTIC.

B.3. Inspección de últimas versiones

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- No se realizan actualizaciones de seguridad de forma regular en sistemas operativos y aplicaciones.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a la realización de actualizaciones de seguridad en sistemas y aplicaciones, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Mal funcionamiento de los sistemas y aplicaciones al no contar con su versión más reciente.

c. Índice de Importancia Establecido.

- 3 (Tres) = Bajo

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado **"8. Controles Tecnológicos"** en su apartado **"8.1 Dispositivos de punto Final de Usuario"**, comenta que "La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debería protegerse", y cuenta con algunos requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para la aplicación de actualizaciones (por ejemplo, actualización automática activa).

Para dar solución ante esta vulnerabilidad se recomiendan:

- Asignar a un encargado que garantice que los equipos sigan contando con la versión más actual posible.
- Activar la actualización automática o bien generar un recordatorio usual en u periodo de tiempo quincenal.

B.4. Comprobación de Programa de Capacitación

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- Falta de capacitación regular a los usuarios sobre las mejores prácticas de seguridad informática y protección de datos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a la existencia de un programa de capacitación sobre seguridad lógica, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación, alteración, perdida o secuestro de información y los datos por parte de usuarios externos o internos.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado **"6.1 Conciencia, educación y entrenamiento sobre la seguridad de la información"** comenta que **"**El personal de la organización y las partes interesadas relevantes deberían recibir una adecuada concienciación, educación y capacitación en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral".

Para dar solución ante esta vulnerabilidad se recomiendan:

- Una jerarquización de roles, principalmente asignar un líder dentro de la oficina quien será el encargado de supervisar y orientar a los demás trabajadores internos acerca de las responsabilidades que se le asignen respecto a seguridad lógica.

B.5. Revisión de Copias de Seguridad

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- Ausencia de Copias de seguridad de sistemas y datos en un lugar externo seguro.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a la existencia de copias de seguridad de la información y los sistemas en un lugar externo seguro, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación, alteración, perdida o secuestro de información y los datos por parte de usuarios externos o internos.

c. Índice de Importancia Establecido.

- 3 (Tres) = Bajo

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado **“8.13 Respaldo de la información”** donde menciona que “Las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse regularmente en de acuerdo con la política de tópico específico acordada sobre copias de seguridad” para permitir la recuperación de la pérdida de datos o sistemas.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Realizar copias de seguridad de los datos y la información relevante que contengan los equipos de cómputo internos.
- Un formato para registrar cuando se realicen dichos respaldos, además de crear un archivo o carpeta ya sea física o digital que contenga historial de las copias de seguridad realizadas.

- Almacenar las copias de seguridad en un lugar seguro y remoto, se puede recomendar almacenarlas en la nube para tener acceso a la información en cualquier lugar y en cualquier momento.
- Se propone la contratación del servicio de almacenamiento en la nube “OneDrive” de Microsoft.

B.6. Actualizaciones Omitidas o No compatibles

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- Las versiones de software no son compatibles con las nuevas actualizaciones.
- Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a las actualizaciones no compatibles u omitidas de las aplicaciones y sistemas, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Mal funcionamiento de los sistemas y aplicaciones al no contar con su versión más reciente.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado **“8.19 Instalación de software en sistema operacionales”** el cual menciona “Deberían implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos” para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas, como lo son realizar actualizaciones del software operativo solo por parte de administradores capacitados según corresponda autorización de gestión.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Asignar a un encargado de acuerdo con los roles internos de la UTIC.
- Monitorear y supervisar que los empleados mantengan actualizados sus equipos de cómputo.
- Implementar dentro de política del lugar, un apartado donde comprometa a los empleados a mantener sus sistemas actualizados a la versión más reciente y no tener actualizaciones en espera.
- Llevar un registro de la realización de la actualización, indicando la fecha, la hora de inicio y la hora de termino o bien instalación, indicando quien la realizo.

B.7. Copias de seguridad periódicas

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan la seguridad de la información y los datos internos del área como, por ejemplo:

- Falta de copias de seguridad periódicas de los datos almacenados en los equipos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada con la seguridad lógica enfocada a las copias de seguridad realizadas periódicamente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Multas y sanciones formales gracias a irregularidades por parte de Auditores externos a la Unidad.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde al estándar (ISO 27002:2022) en su apartado llamado **“8.13 Respaldo de la información”** donde menciona que “Las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse regularmente en de acuerdo con la política de tópico específico acordada sobre copias de seguridad”

Para dar solución ante esta vulnerabilidad se recomiendan:

- Realizar copias de seguridad de los datos y la información relevante que contengan los equipos de cómputo internos.

- Almacenarlas en un lugar seguro y remoto, se puede recomendar almacenarlas en la nube para tener acceso a la información en cualquier lugar y en cualquier momento.
- Contratación del servicio de almacenamiento en la nube “OneDrive” de Microsoft.
- Realizar al menos una vez semanalmente las copias de seguridad de la información y datos relevantes de la UTIC.

C. Servicios

C.1. Uso de Contactos Eléctricos

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- Los enchufes eléctricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos.
- Sobrecargas por parte del uso de extensiones saturadas de equipos conectados.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada a la escasez de los enchufes eléctricos internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Incendio.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la Norma Oficial Mexicana (NOM-001-SEDE-2012) en su artículo 240 llamado **"PROTECCION CONTRA SOBRECORRIENTE"** menciona que "La protección contra sobre corriente para conductores y equipos se instala para que abra el circuito, si la corriente alcanza un valor que cause una temperatura excesiva o peligrosa en los conductores o en su aislamiento"

Para dar solución ante esta vulnerabilidad se recomiendan:

- No sobrecargar con el uso de dispositivos las extensiones o "multicontactos" usados.
- Reemplazo y la implementación de Sistemas de Alimentación Ininterrumpida.

C.2. Propagación de Incendio

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- Material inflamable debajo de los interruptores principales de la UTIC, es decir, el centro de carga (caja de fusibles y pastillas) que comprometen a una mayor propagación de incendio en caso de corto circuito.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada a los extintores que se encuentran en el área y los posibles escenarios que causarían una fácil propagación de incendio, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Incendio.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la **"National Fire Protection Association"** o bien Asociación Nacional de Protección contra Incendios la "**NFPA 10"** es un estándar que especifica normas y requisitos para la instalación, inspección, mantenimiento y uso de extintores portátiles de incendio.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Colocar el extintor para circuitería ubicado en el interior del cuarto del site fijado contra la pared.
- Someter a mantenimiento los extintores de acuerdo a la duración del material.
- En caso de no ser posible ubicar el extintor en un espacio visible al entrar al site y totalmente despejado para evitar tropiezos o accidentes.
- Realizar pruebas de control anuales y mantenimiento para poder asegurarse de que el equipo se mantenga en condiciones óptimas.
- Despejar completamente el escenario considerado como peligroso y mencionado en los resultados de esta prueba.
- Mantener los activos, documentos o materiales con un mayor índice de ser inflamables, lejos de los contactos ubicados dentro del site.

C.3. Presencia de Botiquín Médico

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- Equipo médico interno (botiquín medico) compartido con otras áreas además de no estar al alcance de los empleados de la UTIC si ocurre un accidente.
- El área de alojamiento del botiquín cubre otro accidente o bien no se encuentran para atender otra emergencia en la UTIC al mismo tiempo.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada al contenido y el uso compartido del botiquín medico además de su ubicación, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Falta de acceso rápido y oportuno a los suministros y equipo médico en caso de accidentes o emergencias médicas en la UTIC.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde a la Norma Oficial Mexicana (NOM-005-STPS-1998) **"Condiciones de Seguridad e Higiene en los centros de trabajo"** se establece que la dependencia debe **"**Proporcionar los medicamentos y materiales de curación necesarios para prestar los primeros auxilios dentro de las instalaciones".

Para dar solución ante esta vulnerabilidad se recomiendan:

- Adquirir su propio botiquín médico.
- Actualizar el contenido del botiquín al que tienen acceso.
- Solicitar que el botiquín médico que comparten contenga al menos todos los elementos mencionados por la NOM-005-STPS-1998 y de los que carecen actualmente.

C.4. Accesos Libres Bloqueados

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- Bloqueo de entrada y salida con activos situados en el piso o bien por mobiliario cruzado en el paso.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada al bloqueo de accesos por parte de activos en el suelo o mobiliario se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Falta de acceso rápido y oportuno a los suministros y equipo médico en caso de accidentes o emergencias médicas en la UTIC.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la Norma Oficial Mexicana (NOM-001-STPS-2008) **"Edificios, locales, instalaciones y áreas en los centros de trabajo, Condiciones de seguridad"** comenta que su objetivo es "Establecer las condiciones de seguridad de los edificios, locales, instalaciones y áreas en los centros de trabajo para su adecuado funcionamiento y conservación, con la finalidad de prevenir riesgos a los trabajadores"

Para dar solución ante esta vulnerabilidad se recomiendan:

- Designar un lugar específico para la ubicación de los activos que tienen situados en el suelo del área de trabajo.
- Ordenar los activos correctamente dentro del cuarto del site al no contar con algún otro espacio disponible.
- Quitar los activos situados a un costado del acceso principal para aumentar el espacio de entrada/salida.
- Retirar el "burlete" o "sello de puerta" colocado debajo de esta, ya que impide que la misma se abra en su totalidad y libremente.

C.5. Condición del Sistema de Enfriamiento

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- Falta de sistema de enfriamiento adecuado en el lugar del trabajo (aire acondicionado) ya que se cuenta solo dentro del site.
- Uso de un sistema de enfriamiento eficiente o bien que no cubra el espacio de trabajo de la UTIC en su totalidad.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada a la existencia y el uso de un sistema de enfriamiento al interior de la UTIC, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Cuando las temperaturas son extremadamente altas los empleados pueden experimentar dificultades para concentrarse, además el sobrecalentamiento de los equipos de cómputo puede provocar fallos y errores en el funcionamiento de estos, lo que podría resultar en una pérdida de datos, interrupción de los servicios o incluso daños permanentes a los dispositivos.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde a la Norma Oficial Mexicana (NOM-023-ENER-2018) llamada **"Eficiencia energética en acondicionadores de aire tipo dividido, descarga libre y sin conductos de aire. Límites, métodos de prueba y etiquetado."** Menciona en su apartado "8.2.1" llamado **"Variación del aire**" que **"**La exactitud en las mediciones de temperatura debe permanecer dentro de ± 0,05 °C para las temperaturas del aire" por lo que si la temperatura es errónea fuera de ese margen el dispositivo usado no funciona correctamente, además estipula que "El equipo debe ser colocado en un sitio en el cual su beneficio sea aprovechado por todos los trabajadores implicados en el área o zona, para garantizar el desarrollo de actividades bajo condiciones favorables de ventilación en el entorno del área donde fue implementado"

Para dar solución ante esta vulnerabilidad se recomiendan:

- Aplicar otra medida que garantice una ventilación óptima para los empleados internos (Implementar un artefacto electrónico movible que genere ventilación continua para mantener el lugar de trabajo fresco y en condiciones climáticas optimas: Ventiladores portátiles, de piso, automáticos, recargables o desechables, Colocar un ventilador de techo fijo para ventilar toda el área de trabajo de manera contante, Mantener los accesos que provocan cierta ventilación abiertos para permitir el flujo de aire al interior del área de trabajo: Ventanas y Puertas).

C.6. Señalamientos de Emergencia

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan el buen funcionamiento y desempeño de los servicios disponibles en el área como, por ejemplo:

- No cuentan con todos los señalamientos de emergencia, por lo que no están al alcance de la vista de cualquier usuario.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada a los servicios con los que cuenta la UTIC enfocada a la existencia de distintos señalamientos de emergencia a la vista de cualquier usuario, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Accidentes por parte de usuarios externos por comportamiento erróneo al no contar con los señalamientos adecuados.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la **"National Fire Protection Association"** o bien Asociación Nacional de Protección contra Incendios la "**NFPA 101"** aborda los requisitos para la señalización de salida, que incluye señales de salida iluminadas, rutas de evacuación claras y otros elementos de orientación para ayudar a las personas a evacuar de manera segura en caso de emergencia.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Colocar los señalamientos de emergencia con los que no cuentan, o al menos los más comunes y que pueden ayudar a los usuarios en su comportamiento durante una emergencia o evacuación.
- Solicitud o bien un comunicado donde reporte la falta de dichos señalamientos para que las autoridades correspondientes actúen ante la notable ausencia de estos.

D. Infraestructura

D.1. Evaluar la Eficiencia en el Etiquetado de Activos y Mobiliario

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- El etiquetado de los activos y mobiliario no se basa en un ordenamiento de fácil lectura para los usuarios.
- El etiquetado no es visible al estar ubicado la mayoría de las veces debajo, atrás o en los laterales de los activos o bien no portarlo.
- El etiquetado no muestra los datos importantes de los activos ni un número de identificación (ID).

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a existencia y eficiencia del etiquetado en los activos y mobiliario, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Confusión en la identificación y ubicación de activos y dificultad en su gestión.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto
- 2 (Dos) = Medio

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado Administración de activos en su sección 8.2.2 nos dice que *"Se debería desarrollar e implementar un conjunto de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Corroborar que el etiquetado sea físico para los activos acorde a un Numero de Identificación (ID), Nombre del Activo, Marca del Activo, Área al que pertenece el activo, Propietario del Activo.
- Cambiar la ubicación de la etiqueta de tal manera que esta sea visible aun cuando el activo se encuentre obstruido por algún material u otro activo.

D.2. Evaluar la Idoneidad del Mobiliario en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Los escritorios usados dentro de la UTIC son grandes y ocupan espacio con el que no cuentan, por lo que los hace inadecuados.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la idoneidad del mobiliario (escritorios) de la UTIC, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Limitación de espacio de trabajo y dificultad para llevar a cabo tareas adecuadamente.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su sección 11 llamada Seguridad Física y Ambiental en su apartado 11.1.5 *"Trabajo en áreas seguras"* menciona que *"Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Colocar los escritorios de manera que minimicen la posibilidad de observación no autorizada o acceso no supervisado, o en su defecto hacer cambio de estos para maximizar el espacio de trabajo.

D.3. Evaluar la Movilidad y Ubicación de Activos en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la idoneidad del mobiliario (escritorios) de la UTIC, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Limitación de espacio de trabajo y dificultad para llevar a cabo tareas adecuadamente.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su Sección 11 llamado Seguridad Física y Ambiental en su apartado 11.1.1 Perímetro de seguridad física nos menciona que *"evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información."* En su inciso *a) se deberían definir perímetros de seguridad y el emplazamiento y la ubicación de cada uno de los perímetros debería depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos;*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Asignar un espacio con el rol de un almacén o bodega cerca del departamento donde solo los empleados de la UTIC tengan acceso, para ingresar todo activo que llegue o tengan que comprometa la libre movilidad en el área de trabajo.

D.4. Evaluar la Organización y Manejo de Cables en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas.
- Equipos enchufados y apagados sin ser utilizados provocan que los cables se crucen y exista confusión en el multi contacto.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada al uso de extensiones mal posicionadas dentro de la UTIC, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Sobrecarga eléctrica, cables cruzados, riesgo de incendio y daño a los equipos.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado *"Seguridad Física y Ambiental"* en su apartado 11.2.3 nombrado *"Seguridad del Cableado"* menciona que *"Los*

cables de electricidad y telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger de la intercepción, interferencia o daños".

Para dar solución ante esta vulnerabilidad se recomiendan:

- Identificar con etiquetas físicas de extremo a extremo el cableado de la UTIC.
- Agruparlos con cinchos sujeta-cables o velcro acorde al tipo de periférico (Mouse, teclado, bocinas, cable de corriente, cable ethernet, etc.).

D.5. Evaluar el Espacio de Movilidad para Traslado de Equipos en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Daño a los equipos por la falta de espacio de movilidad para los usuarios mientras trasladan equipos reparados entre ellos o bien a otras áreas.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la falta de espacio de movilidad en el traslado de equipos dentro de la UTIC o bien hacia otras áreas, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Sobrecarga eléctrica, cables cruzados, riesgo de incendio y daño a los equipos.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 menciona en varios de sus apartados sobre el traslado de los activos, se encontró lo siguiente: En su apartado 6 llamado *"Organización de la seguridad de la información"* en su sección 6.1.2 Segregación de deberes nos menciona que *"Se deberían segregar los deberes y áreas de responsabilidad en conflicto para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Asignar a un responsable para el traslado de los equipos que requieran mantenimiento en la UTIC, y un escolta de seguridad.

D.6. Evaluar el Estado del Techo Falso en el Cuarto del Site

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- La UTIC cuenta con un techo falso visiblemente dañado por la instalación del cableado en el cuarto del site.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada al daño del techo falso en el cuarto del site por la instalación del cableado, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Caída de objetos, filtraciones de agua y daño a los equipos.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.1.4 Protección contra las amenazas externas y ambientales menciona que *"Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes"* En su orientación acerca de su implementación está a considerar lo siguiente:

"Se debería obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre."

Para dar solución ante esta vulnerabilidad se recomiendan:

- Cambiar el plafón de esa sección del techo falso ya que al hacer la instalación del cableado del site este error causado por el hombre, puede llegar a ser catastrófico si hay paso de tuberías que pudieran llegar a tener fugas de agua que ocasionen un corto circuito si llegara a los dispositivos de telecomunicaciones que están situados en el Rack.

D.7. Evaluar la Protección contra Filtraciones de Agua en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Presencia de un techo falso y el paso del drenaje frente al área de la UTIC.
- Ausencia de una barrera en la entrada/salida de la UTIC para prevenir filtraciones de agua por parte de las tuberías que pasan frente al área de la UTIC.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la ausencia de barreras que impidan filtraciones de agua por el paso de drenaje frente al área de trabajo, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Caída de objetos, filtraciones de agua y daño a los equipos.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio
- 3 (Tres) = Bajo

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.1.4 Protección contra las amenazas externas y ambientales menciona que *"Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes"* En su orientación acerca de su implementación está a considerar lo siguiente:

"Se debería obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre."

Para dar solución ante esta vulnerabilidad se recomiendan:

- Aislar la tubería sobresaliente que se encuentra en el pasillo donde se encuentra la UTIC, con las protecciones debidas como lo puede ser un muro de concreto, o bien que el tubo del drenaje sea oculto dentro del muro de construcción al que esta remachado.

D.8. Evaluar Políticas y Reglas para el Uso de Equipos de Red en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- No cuentan con reglas específicas para el uso de los routers, switches y servidores.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada al uso con el que cuentan actualmente los dispositivos de redes internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Configuraciones incorrectas, vulnerabilidades de seguridad y mal funcionamiento de redes.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer el uso de los dispositivos de telecomunicaciones, así como responsabilidades y sanciones hacia aquel empleado o proveedor que realice mantenimiento preventivo y correctivo dentro de una política interna.

D.9. Verificar el mantenimiento de los Routers, Switches y Servidores

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Los routers, switches y servidores no cuentan con un mantenimiento frecuente, lo que puede ocasionar un mal funcionamiento y no rinda debidamente.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada al mantenimiento con el que cuentan actualmente los dispositivos de redes internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Configuraciones incorrectas, vulnerabilidades de seguridad y mal funcionamiento de redes.

c. Índice de Importancia Establecido.

- 0 (cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado Seguridad Física y Ambiental en su sección 11.2.4 Mantenimiento de equipos menciona que *"Los equipos se deberían mantener correctamente para garantizar su disponibilidad e integridad continuas."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer en las políticas lineamientos acerca del mantenimiento que se debería de implementar, además del personal que este capacitado para realizarlo y/o los proveedores autorizados.

D.10. Evaluar la Protección del Cableado del Rack

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Daño al cableado sin protección por parte de la caída del techo falso dañado.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la protección con la que cuenta el cableado del rack, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Riesgo de fallas, mal rendimiento, interrupción de servicios y vulnerabilidades de seguridad.

c. Índice de Importancia Establecido.

- 3 (Tres) = Bajo

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 11 llamado *"Seguridad Física y Ambiental"* en su apartado 11.2.3 nombrado *"Seguridad del Cableado"* menciona que *"Los cables de electricidad y telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger de la intercepción, interferencia o daños".*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Peinar de los cables de ethernet debidamente ordenados acorde a los enlaces que se distribuyen a las áreas del Ayuntamiento.
- Ordenar con ayuda de cincho sujeta cables o velcro de colores para su identificación, además de que el cableado este etiquetado de extremo a extremo y no solo en el Switch como se muestra en las fotografías de la prueba.

D.11. Evaluar las Medidas de Control de Plagas en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Presencia de plagas dentro de la UTIC que pongan en riesgo la condición del cableado y los equipos de telecomunicaciones además del mobiliario y los activos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la posible presencia de plagas en el cuarto del site, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Riesgo de fallas, mal rendimiento, interrupción de servicios y vulnerabilidades de seguridad.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

En México, la Secretaría de Salud y la Secretaría de Agricultura y Desarrollo Rural son algunas de las entidades que podrían tener regulaciones relacionadas con el control de plagas. Además, las normas de la Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS) podrían abordar aspectos relacionados con el control de plagas en instalaciones que manejan alimentos o productos de consumo.

Cabe mencionar que en la UTIC no hay manejo ni producción de alimentos, sin embargo, las plagas pueden presentarse por diversos motivos. Una de las razones por las que suelen proliferar plagas en oficinas o restaurantes es la generación de una gran cantidad de desechos orgánicos diariamente y una limpieza inadecuada tanto del entorno como del abastecimiento.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Hacer contrato con alguna empresa dedicada al control de plagas para que acorde a esto se haga una desinfección y se sanitase todas las oficinas incluyendo la UTIC, e implemente estaciones de cebo como lo dicta la NOM-256-SSA1-2012.

D.12. Evaluación de Comodidad en Mobiliario de Asientos en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- El mobiliario referente a los asientos no son la mejor opción hablando de comodidad y espacio para los usuarios de la UTIC.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la comodidad del mobiliario (asientos) de los empleados internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Limitación de espacio de trabajo y dificultad para llevar a cabo tareas adecuadamente.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su sección 11 llamada Seguridad Física y Ambiental en su apartado 11.1.5 “Trabajo en áreas seguras” menciona que *“Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras.”*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Asegurarse de que los asientos en las áreas seguras estén diseñados ergonómicamente para proporcionar comodidad a los empleados sin compr6ometer la seguridad. Esto puede incluir sillas ajustables y soporte lumbar.

D.13. Evaluación en el Proceso de Vale de Salida y Entrega en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Datos incorrectos o mal llenado del vale de salida y entrega por parte de la UTIC lo que ocasiona que el reemplazo no se pueda efectuar.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada al proceso de vales de salida y entrega internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Dificultad para reemplazar equipos defectuosos o dañados y posibles interrupciones del servicio.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 Políticas para la seguridad de la información*

Las políticas internas son especialmente útiles en organizaciones de mayor tamaño y complejidad, donde aquellos que definen y aprueban los niveles ampliados de control se segregan de los que implementan los controles o en situaciones donde una política se aplica a varias personas o funciones distintas de la organización. Las políticas para la seguridad

de la información se pueden emitir en un documento de política de seguridad de la información único o como un conjunto de documentos individual espero relacionados.

Algunas organizaciones utilizan otros términos para estos documentos de políticas como "Normas", "Directivas" o "Reglas".

Para dar solución ante esta vulnerabilidad se recomiendan:

- Implementar una sección nueva dentro de la política interna, para el correcto llenado del vale de salida, e implementar sanciones en caso de que un empleado de la UTIC haga un mal llenado de este. (MANUAL DE PROCEDIMIENTOS).

D.14. Evaluación de Políticas y Reglas en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- La falta de políticas y reglas dentro de la UTIC.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la ausencia de políticas y reglas que regulen el comportamiento y uso de activos internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Utilización inadecuada de los recursos, daño o deterioro del mobiliario, y dificultad en el uso adecuado de las instalaciones.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Implementar políticas, acorde a la falta de reglas que regulen el lugar y hacer uso de sanciones a todo aquel que las incumpla.

D.15. Evaluación de Orientación sobre el Uso Adecuado de Equipos en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena distribución y uso de la infraestructura en el área como, por ejemplo:

- Falta de explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte a la infraestructura de la UTIC enfocada a la ausencia de políticas y reglas que regulen el comportamiento y uso de activos internos, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Utilización inadecuada de los recursos, daño o deterioro del mobiliario, y dificultad en el uso adecuado de las instalaciones.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer en las políticas que un empleado encargado debiera dar una breve explicación acerca de cómo se trabaja dentro de la UTIC y cual serian sus reglas y comportamientos que también debieran seguir y que se debiera de comunicar a los empleados y a las partes externas.

E. Sistema de Inventario

E.1. Evaluación de Accesibilidad y Utilidad del Sistema de Inventario en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la ausencia de seguridad en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida o robo de información confidencial y manipulación no autorizada de datos.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección *8.1.1 Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Sobre su orientación esta lo siguiente: *Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Migrar a un Software especializado, o en su defecto que se realice un programa que ayude a las necesidades de la UTIC.
- Implementar un control de acceso en el sistema de inventario de acuerdo con los diferentes roles que tengan los empleados.

E.2. Evaluación del Desarrollo del Sistema de Inventario

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- El inventario con el que cuentan no está desarrollado en un sistema gestor de bases de datos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a su desarrollo en hojas de cálculo usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida de datos debido a errores, fallos o corrupción del sistema.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección *8.1.1 Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Sobre su orientación esta lo siguiente: *Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Migrar la información del inventario a un programa o software especializado o realizado a sus medidas y necesidades de la Unidad.
- Implementar sistema de inventario en conjunto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

E.3. Evaluación de la Estrategia de Respaldo y Copias de Seguridad del Inventario en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- No se realizan respaldos o copias de seguridad del inventario.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la ausencia de seguridad en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida irreversible de datos en caso de fallos de hardware, errores humanos o desastres.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección *8.1.1 Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información "Se deberían realizar copias*

de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer una Política de Respaldo.
- Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas.
- Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo.
- Establecer un plan para almacenar los respaldos en una ubicación remota.
- Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental.
- Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración.
- Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados.

E.4. Evaluación de Seguridad y Gestión de Permisos en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- Todos los usuarios internos de la UTIC pueden editar la información dentro del inventario ya que no cuentan con roles ni privilegios de acuerdo con su puesto.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la ausencia de seguridad en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación maliciosa o alteración no autorizada de datos críticos.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección *8.1.1 Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).

Para dar solución ante esta vulnerabilidad se recomiendan:

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Establecer roles de usuario en el sistema de gestión de activos que reflejen los roles y responsabilidades de las personas dentro de la UTIC.
- Facilitar la identificación de activos en el ciclo de vida de la información a través del software.
- Implementar funcionalidades en el software que permitan la asignación de propiedad y clasificación para cada activo identificado.
- Proporcionar capacitación a los usuarios sobre el uso adecuado del software y los roles de privilegio asignados.

E.5. Evaluación de la Eficiencia y Sostenibilidad del Inventario en Hojas de Cálculo en la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- El inventario actual desarrollado en hojas de cálculo al pasar el tiempo se satura de información y provoca perdidas de la información.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada al uso de hojas de cálculo con rol de inventario el cual es usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida de datos y dificultades en la gestión y recuperación de la información.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Realizar un inventario en Excel puede ser una solución práctica y accesible, pero también conlleva algunos riesgos que es importante tener en cuenta.

1) La introducción manual de datos aumenta el riesgo de errores, como equivocaciones al ingresar cantidades, descripciones o ubicaciones.
2) Actualizar el inventario de manera oportuna y precisa puede volverse complicado a medida que el volumen de datos aumenta, lo que podría resultar en información desactualizada.
3) Los archivos de Excel pueden carecer de características avanzadas de seguridad, lo que aumenta el riesgo de acceso no autorizado o de pérdida de información crítica.
4) La gestión del inventario en Excel puede depender en gran medida de las habilidades individuales de quienes trabajan con la hoja de cálculo, lo que puede ser un riesgo si hay rotación de personal.

5) Fallos técnicos, errores humanos o mal manejo de archivos pueden resultar en la pérdida de datos, especialmente si no se realizan copias de seguridad de manera regular.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Implementar sistema de inventario en conjunto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

E.6. Evaluación de la Accesibilidad y Eficiencia en la Consulta de Categorías de Activos en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- Para la consulta de las distintas categorías de activos disponibles, deben acceder a diferentes archivos individuales para realizar consultas.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la consulta y dificultad de esta en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Dificultad y demora en la consulta de información, lo cual afecta la eficiencia y productividad.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Implementar sistema de inventario en conjunto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

E.7. Evaluación de Medidas de Seguridad en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- El inventario empleado actualmente no cuenta con seguridad alguna, rol de usuarios ni contraseñas para acceder al mismo.
- El sistema no cuenta con ninguna medida de seguridad.

- Ausencia de usuarios y contraseñas para restringir el acceso a usuarios externos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a las medidas de seguridad con las que cuenta el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida de datos y dificultades en la gestión y recuperación de la información.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda. El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.

- Implementar un Inicio de sesión que restrinja el acceso a las diferentes funciones de pudiera llegar a tener este acorde a el rol, ocupación y tareas de cada empleado.

E.8. Evaluación de Estrategias de Respaldo y Recuperación en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- Falta de copias de seguridad y respaldos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la recuperación de la información y los respaldos de esta en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida o robo de información confidencial y manipulación no autorizada de datos.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado *Administración de Activos* en su sección 8.1.1 *Inventario de Activos* nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección *12.3 Respaldo* menciona que *"brindar protección contra la pérdida de datos."* Además de mencionar en su subsección *12.3.1 Respaldo de información "Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas.
- Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo.
- Establecer un plan para almacenar los respaldos en una ubicación remota, lo suficientemente distante como para evitar daños ante desastres en la ubicación principal.
- Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental, de acuerdo con las normas aplicables en la ubicación principal.
- Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración.
- Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados.

E.9. Evaluación de Controles de Eliminación de Archivos en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- Eliminación de los archivos (hojas de cálculo) permanentemente por parte de los empleados por error.
- La eliminación de alguno de los archivos individuales usados para el inventario provoca un daño catastrófico al no tener los datos en otra parte.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a la recuperación de la información y los respaldos de esta en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Pérdida irreversible de datos en caso de fallos de hardware, errores humanos o desastres.
- Dificultad y demora en la consulta de información, lo cual afecta la eficiencia y productividad.

c. Índice de Importancia Establecido.

- 2 (Dos) = Medio

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado Administración de Activos en su sección 8.1.1 Inventario de Activos nos menciona que *“Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos.”*

Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección 12.3 Respaldo menciona que “brindar protección contra la pérdida de datos.” Además de mencionar en su subsección 12.3.1 Respaldo de información *“Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada.”* Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Establecer un apartado de sanciones que regule a los empleados en caso de la eliminación de archivos o información sensible sin opción de recuperación.
- Desarrollar y documentar una política de respaldo que defina claramente los requisitos de la organización en términos de respaldo de información, software y sistemas.
- Asegurarse de que se produzcan registros precisos y completos de las copias de respaldo.
- Establecer un plan para almacenar los respaldos en una ubicación remota, lo suficientemente distante como para evitar daños ante desastres en la ubicación principal.
- Asegurarse de que la información de respaldo tenga un nivel adecuado de protección física y ambiental, de acuerdo con las normas aplicables en la ubicación principal.
- Implementar un programa regular de pruebas de respaldo que incluya la prueba de los medios de respaldo y los procedimientos de restauración.
- Establecer procedimientos operativos para monitorear la ejecución de respaldos y abordar cualquier falla de los respaldos programados.

E.10. Evaluación de Registros de Movimientos en el Sistema de Inventario de la UTIC

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- El inventario usado actualmente no registra los movimientos efectuados, con hora, fecha ni cuenta de quien los realizo.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada a las acciones mal intencionadas sin registro que puedan suceder en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Manipulación maliciosa o alteración no autorizada de datos críticos.

c. Índice de Importancia Establecido.

- 0 (Cero) = Muy Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 8 llamado Administración de Activos en su sección 8.1.1 Inventario de Activos nos menciona que *"Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos."*

Cabe mencionar que en el apartado 12 llamado Seguridad de las operaciones en su sección12.3 Respaldo menciona que "brindar protección contra la pérdida de datos." Además de mencionar en su subsección 12.3.1 Respaldo de información *"Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían*

probar de manera regular de acuerdo con una política de respaldo acordada." Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas. La política de respaldo debería definir los requisitos de retención y protección. Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios.

Para dar solución ante esta vulnerabilidad se recomiendan:

- Implementar una celda específicamente para ingresar al personal que hace el movimiento en el inventario.
- Implementar sanciones en caso de un error humano en las políticas.

E.11. Evaluación de Procedimientos y Controles durante Cargas y Partidas de Datos en el Sistema de Inventario de la UTIC.

a. Situación

Con respecto al relevamiento efectuado, se ha notado que la UTIC tiene una notable falta de estrategias que garantizan una buena función y seguridad de la información en el sistema de inventario usado dentro del área como, por ejemplo:

- Confusión de los archivos manejados al momento de una carga o partida de datos.

b. Efectos y/o implicaciones probables

Una vez identificada la situación actual relacionada en parte al sistema de inventario de la UTIC enfocada al proceso de consultas en los diferentes archivos manejados en el sistema de inventario usado actualmente, se puede definir el riesgo que esto implica al no atender dicha vulnerabilidad.

- Dificultad y demora en la consulta de información, lo cual afecta la eficiencia y productividad.

c. Índice de Importancia Establecido.

- 1 (Uno) = Alto

d. Sugerencias

Acorde a la norma ISO/IEC 27002 en su apartado 5 llamado Políticas de seguridad de la información en su sección *5.1.1 "Políticas para la seguridad de la información"* menciona que *"Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes."*

Para dar solución ante esta vulnerabilidad se recomiendan:

- Clasificar las hojas de cálculo de Microsoft Excel donde se encuentran las partidas, por colores para evitar confusión alguna.
- Implementar sanciones en las políticas a quien no tenga cuidado al llenado de una partida.

CAPÍTULO V
IMPLEMENTACIONES

5.1.1.3 Actividad 3.3 Implementar las Recomendaciones

5.1.1.3.1 Descripción de la actividad

A continuación, se muestran las estrategias implementadas de acuerdo con las recomendaciones que se diseñaron en base a los estándares, con el objetivo de reemplazar y mejorar las vulnerabilidades que se encontraron, por lo que se muestra un antes y un después de dichas deficiencias funcionando en la UTIC.

5.1.1.3.2 Resultado de la actividad

Vulnerabilidad Atendida enfocada a Seguridad Física

- No se cierran con seguro los accesos cuando el sitio no está siendo utilizado en horario de trabajo.

Recomendación:

- Establecer a un encargado que se responsabilice de cerrar el acceso al área de manera correcta y segura aun en horario laboral siempre y cuando la oficina quede totalmente vacía sin importar el periodo de tiempo en el que se encuentre de esta manera evitando todo acceso no autorizado ni deseado.

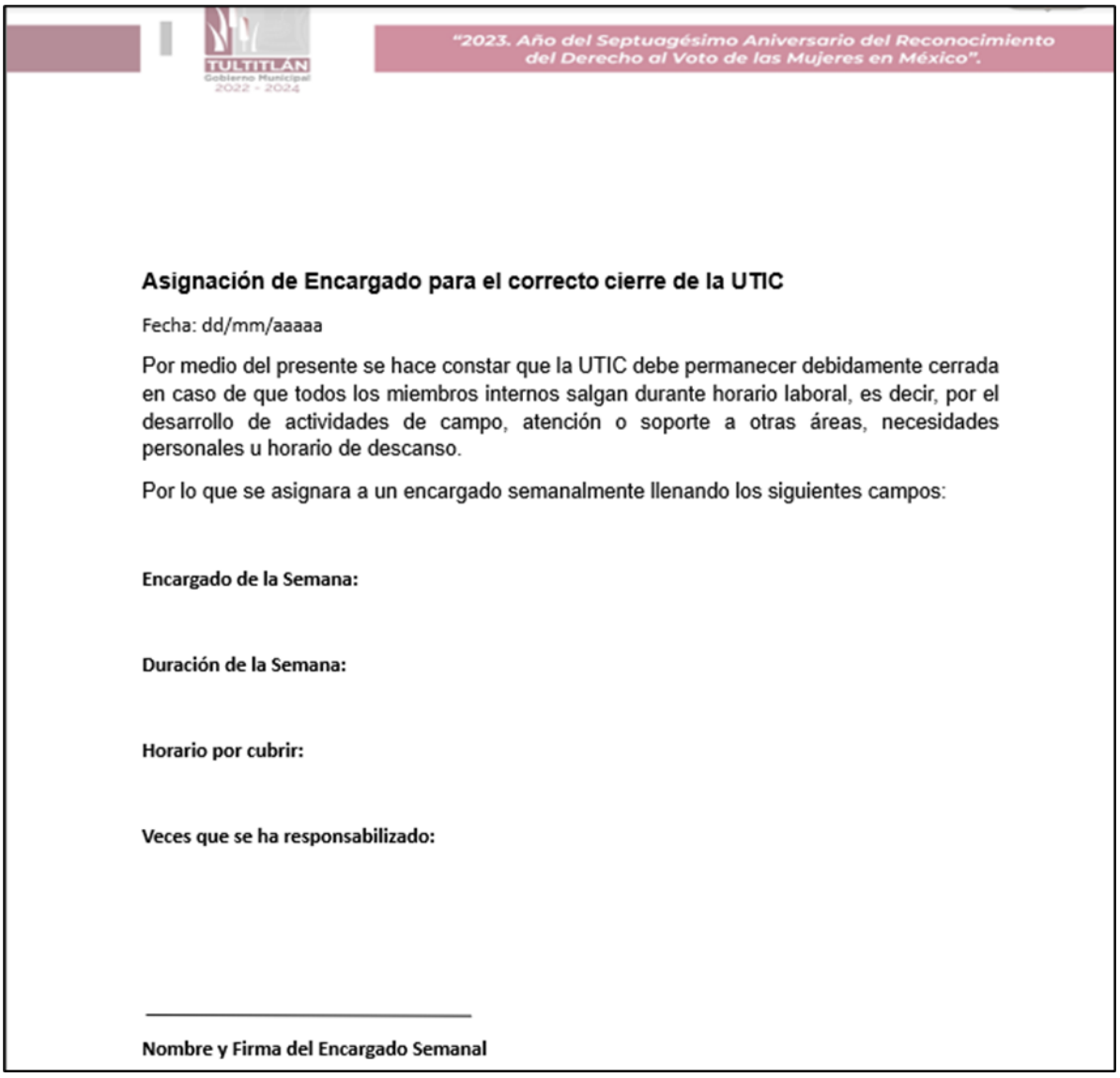
Estrategia Implementada.

Antes: Durante el horario laboral de la UTIC, se identificaron distintos momentos en los que el espacio de trabajo se queda totalmente solo y abierto ya que hay actividades en campo y personales que bien requieren salidas imprevistas, sin embargo, dejar el área de trabajo con tantos activos y equipos en su interior sin supervisión alguna o bien cerrado debidamente puede ocasionar robos y manipulación por parte de usuarios externos a la UTIC, a continuación se anexa Figura de cierta ocasión en la que se llegó al área de trabajo y se encontraba vacía y abierta totalmente.



Figura 230. Oficina de la UTIC sin vigilancia. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Oficina de la UTIC sin vigilancia, 2023)

Después: Como medida preventiva se implementó un escrito donde se asigne como encargado a alguno de los empleados internos de la UTIC, el cual se encargará por un periodo de tiempo de una semana, de cerrar el espacio de trabajo en caso de que todos salgan o este se quede vacío, sin importar si el periodo de tiempo es poco, ya que esto subirá el nivel de seguridad en caso de que usuarios externos quieran manipular o bien robar activos o información interna, se le brinda el archivo en digital al jefe de la unidad para poder generarlo cada que se cambie el rol del encargado, así será más fácil editarlo y tener acceso a él.



TULTITLÁN
Gobierno Municipal
2022 - 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Asignación de Encargado para el correcto cierre de la UTIC

Fecha: dd/mm/aaaaa

Por medio del presente se hace constar que la UTIC debe permanecer debidamente cerrada en caso de que todos los miembros internos salgan durante horario laboral, es decir, por el desarrollo de actividades de campo, atención o soporte a otras áreas, necesidades personales u horario de descanso.

Por lo que se asignara a un encargado semanalmente llenando los siguientes campos:

Encargado de la Semana:

Duración de la Semana:

Horario por cubrir:

Veces que se ha responsabilizado:

Nombre y Firma del Encargado Semanal

Figura 231. Formato de Asignación de Cierre. Fuente: Elaboración propia. (propia., Formato de Asignacion de Cierre, 2023)

Instrucciones: Para el correcto llenado de los campos siga las siguientes recomendaciones.

Encargado de la Semana:	Anotar nombre completo y puesto del encargado que se eligió para cubrir el periodo semanal.
Duración de la semana:	Anotar la duración de la semana colocando el día de inicio y el día de termino contemplando la cantidad de días con los que cumple el periodo semanal, ejemplo: Del 12 de enero al 19 de enero.
Horario por Cubrir:	Anotar el horario en el que deberá cubrir el área, es decir durante que horas será responsable de cerrar el espacio de trabajo en caso de que se quede vacío dentro de la jornada laboral. Nota: este puede ser el mismo de la jornada laboral de la UTIC.
Veces que se ha responsabilizado:	Anotar el numero de veces que se ha responsabilizado, ya que habrá ocasiones en las que se repita el encargado. Nota: La semana completa cuenta como 1 rol, ejemplo: el encargado ha cubierto 4 semanas, se ha responsabilizado 4 veces.

Figura 232. Formato de llenado de la Asignación de Cierre. Fuente: Elaboración propia. (propia., Formato de llenado de la Asignacion de Cierre, 2023)



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

TULTITLÁN Gobierno Municipal 2022 - 2024

Asignación de Encargado para el correcto cierre de la UTIC

Fecha: 15/02/2024

Por medio del presente se hace constar que la UTIC debe permanecer debidamente cerrada en caso de que todos los miembros internos salgan durante horario laboral, es decir, por el desarrollo de actividades de campo, atención o soporte a otras áreas, necesidades personales u horario de descanso.

Por lo que se asignara a un encargado semanalmente llenando los siguientes campos:

Encargado de la Semana: Jonathan Rodrigo Pérez Del Río

Duración de la Semana: 19 Febrero al 23 de Febrero

Horario por cubrir: 9.00 hrs a 18:00 hrs

Veces que se ha responsabilizado: 1

Jonathan Rodrigo Pérez Del Río

Nombre y Firma del Encargado Semanal

Jonathan Rodrigo Pérez Del Río

Nombre y Firma del Jefe de la UTIC

TULTITLÁN Gobierno Municipal 2022 - 2024 Unidad de Tecnologías de la Información y Comun

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900.

55. 2620.8900

Seguimos Transformando Tultitlán

@22_24Tultitlan

Seguimos Transformando Tultitlán

Figura 233. Escrito firmado de la asignación del encargado de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (propia., Escrito firmado de la asignación del encargado de la UTIC, 2023)

Vulnerabilidad Atendida enfocada a Seguridad Física

- Uso Compartido de equipo de oficina, como lo es un equipo de impresión multifuncional y prestar los servicios de este dispositivo a departamentos externos.

Recomendación

- Implementar una bitácora para la utilización del equipo de oficina, el cual debe registrar, la hora, fecha, usuario externo, propósito para el cual hizo uso de este.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios externos a la UTIC usan el equipo de impresión multifuncional interno por lo que no hay como evidenciar un antes de la estrategia.

Después: Se diseño el siguiente formato y se le brindo el archivo a la UTIC para que lleve un control sobre el control del equipo de impresión multifuncional.



Fecha	Hora	Nombre	Dpto./Área	Asunto	Estado del Equipo	Firma

Nombre y Firma del jefe de la Unidad

Figura 234. Formato de Bitácora. Fuente: Elaboración propia. (propia., Formato de Bitácora, 2023)



Llenado de los Campos de la Bitácora

Fecha	Anotar la fecha en la que se esta haciendo uso del equipo en el formato dd/mm/aaaaa.
Hora	Anotar la hora exacta en la que se usa el equipo usando el formato de 24H.
Nombre	Anotar el Nombre (s) y el primer apellido.
Dpto./Área	Anotar el departamento o el área en el que labora el usuario.
Asunto	Anotar el número del asunto por el cual se requiere el equipo, de acuerdo con las siguientes opciones: Impresiones ---------- 1 Copias ---------- 2 Escaneo ---------- 3 Envío por cuenta de empelado --------- 4 Otro ----- 5
Estado del Equipo	Anotar en base al número, el estado en el que se encontró el equipo de acuerdo a las siguientes opciones (pueden colocarse más de uno): 1 = Funcionando Correctamente 2 = En espera por otra función 3 = No está funcionando correctamente 4 = Apagado 5 = Desconectado
Firma	Colocar la firma del empleado que hizo uso del equipo una vez que lleno los campos anteriores.

Figura 235. Formato de llenado de la Bitácora. Fuente: Elaboración propia. (propia., Formato de llenado de la Bitácora, 2023)



Figura 236. Bitácora del uso de la impresora en uso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Bitácora del uso de la impresora en uso, 2024)

Vulnerabilidad Atendida enfocada a Seguridad Física

- No se han establecido políticas y procedimientos formales para la gestión de incidentes de seguridad física.

Recomendación

- Diseñar una política de comportamiento interno para todos los usuarios que accedan a la UTIC.
- Establecer sanciones para el incumplimiento de las reglas establecidas dentro de la política de comportamiento.

Estrategia Implementada.

Antes: Durante la inspección que se realizó a la UTIC, es notable la ausencia de una política que regule el comportamiento y buen uso de los equipos y activos internos de la UTIC al contar con usuarios temporales nuevos constantemente (servicio social y prácticas profesionales). Por lo que no se pude evidenciar la ausencia de dicha política.

Después: Se diseño la siguiente política enfocándose al correcto uso de los activos y al comportamiento de los usuarios dentro de la UTIC, por lo que abarca temas generales que puedan ser aplicados para todo tipo de usuario que quiera ingresar a la UTIC.

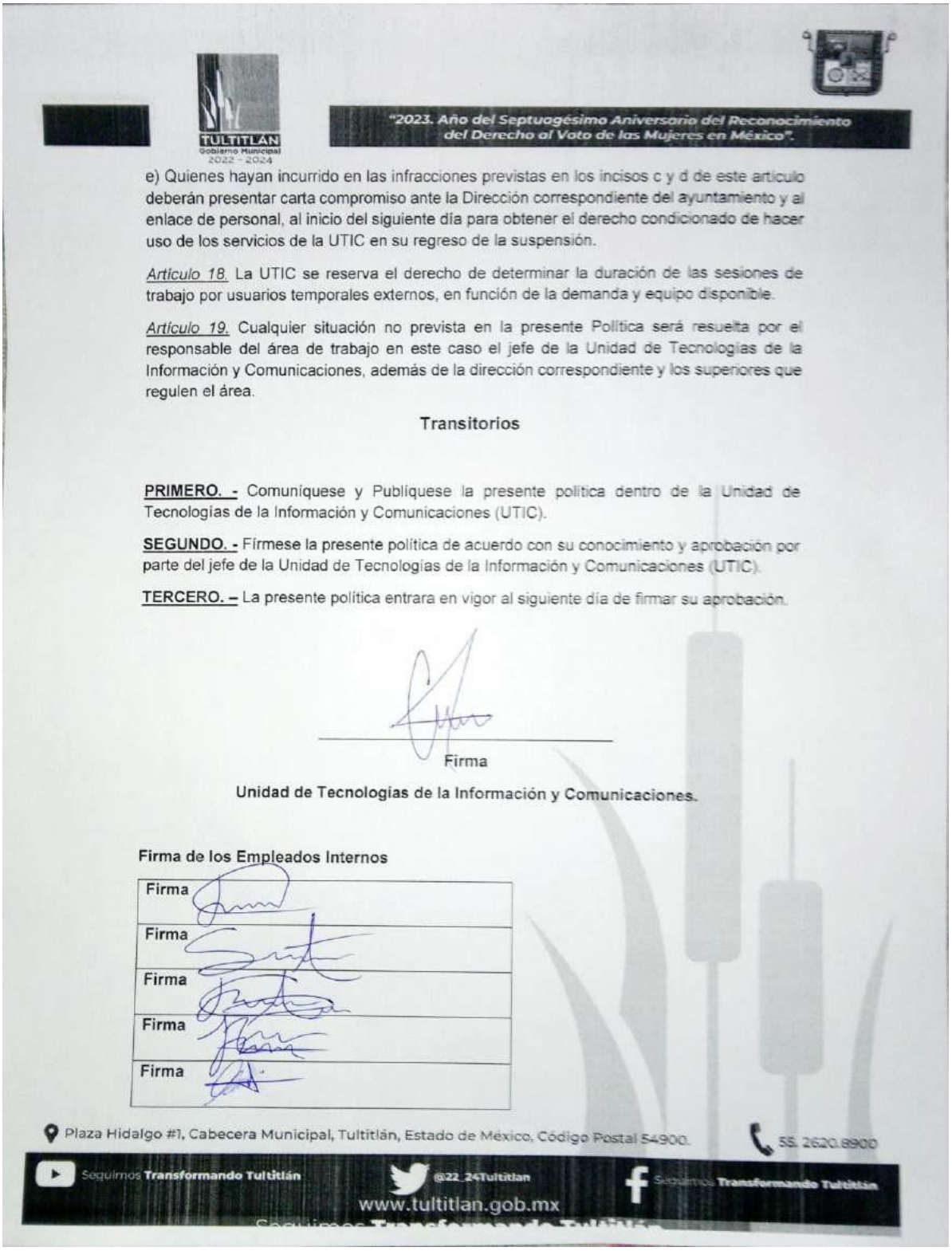


Política de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

Contenido:

- Capítulo I
- Disposiciones Generales
- Capítulo II
- De la autoridad
- De los usuarios
- Son derechos de los usuarios
- Capítulo III
- Normas del personal interno
- Capítulo IV
- Prohibiciones de los usuarios
- Capítulo V
- De las sanciones
- Transitorios.

Figura 237. Caratula de la política. Fuente: Elaboración propia. (propia., Caratula de la política, 2024)



TULTITLÁN Gobierno Municipal 2022 – 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

e) Quienes hayan incurrido en las infracciones previstas en los incisos c y d de este artículo deberán presentar carta compromiso ante la Dirección correspondiente del ayuntamiento y al enlace de personal, al inicio del siguiente día para obtener el derecho condicionado de hacer uso de los servicios de la UTIC en su regreso de la suspensión.

Artículo 18. La UTIC se reserva el derecho de determinar la duración de las sesiones de trabajo por usuarios temporales externos, en función de la demanda y equipo disponible.

Artículo 19. Cualquier situación no prevista en la presente Política será resuelta por el responsable del área de trabajo en este caso el jefe de la Unidad de Tecnologías de la Información y Comunicaciones, además de la dirección correspondiente y los superiores que regulen el área.

Transitorios

PRIMERO. - Comuníquese y Publíquese la presente política dentro de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

SEGUNDO. - Fírmese la presente política de acuerdo con su conocimiento y aprobación por parte del jefe de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

TERCERO. – La presente política entrara en vigor al siguiente día de firmar su aprobación.

Firma

Unidad de Tecnologías de la Información y Comunicaciones.

Firma de los Empleados Internos

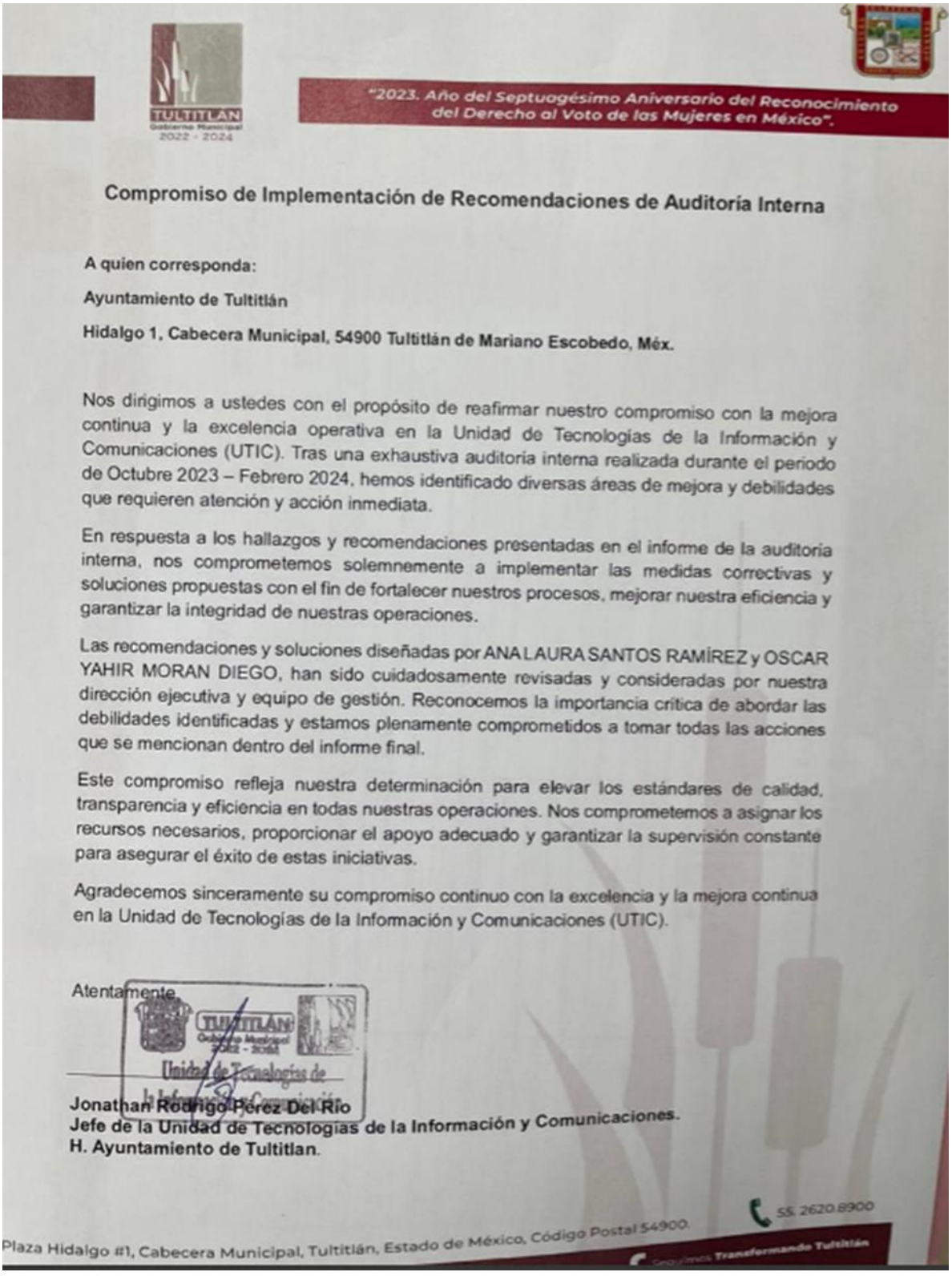
Firma
Firma
Firma
Firma
Firma

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 238. Política aprobada. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Política aprobada, 2024)



TULTITLÁN
Gobierno Municipal
2022 - 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Compromiso de Implementación de Recomendaciones de Auditoría Interna

A quien corresponda:

Ayuntamiento de Tultitlán

Hidalgo 1, Cabecera Municipal, 54900 Tultitlán de Mariano Escobedo, Méx.

Nos dirigimos a ustedes con el propósito de reafirmar nuestro compromiso con la mejora continua y la excelencia operativa en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC). Tras una exhaustiva auditoria interna realizada durante el periodo de Octubre 2023 – Febrero 2024, hemos identificado diversas áreas de mejora y debilidades que requieren atención y acción inmediata.

En respuesta a los hallazgos y recomendaciones presentadas en el informe de la auditoria interna, nos comprometemos solemnemente a implementar las medidas correctivas y soluciones propuestas con el fin de fortalecer nuestros procesos, mejorar nuestra eficiencia y garantizar la integridad de nuestras operaciones.

Las recomendaciones y soluciones diseñadas por ANA LAURA SANTOS RAMÍREZ y OSCAR YAHIR MORAN DIEGO, han sido cuidadosamente revisadas y consideradas por nuestra dirección ejecutiva y equipo de gestión. Reconocemos la importancia crítica de abordar las debilidades identificadas y estamos plenamente comprometidos a tomar todas las acciones que se mencionan dentro del informe final.

Este compromiso refleja nuestra determinación para elevar los estándares de calidad, transparencia y eficiencia en todas nuestras operaciones. Nos comprometemos a asignar los recursos necesarios, proporcionar el apoyo adecuado y garantizar la supervisión constante para asegurar el éxito de estas iniciativas.

Agradecemos sinceramente su compromiso continuo con la excelencia y la mejora continua en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

Atentamente

TULTITLÁN Gobierno Municipal 2022 - 2024
Unidad de Tecnologías de la Información y Comunicación

Jonathan Rodrigo Pérez Del Río
Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.
H. Ayuntamiento de Tultitlan.

55. 2620.8900

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900.

Seguimos Transformando Tultitlán

Figura 239. Compromiso Firmado de Implementación de Recomendaciones de Auditoría Interna.

Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Compromiso Firmado de Implementacion de Recomendaciones de Auditoría Interna, 2024)

Vulnerabilidad Atendida enfocada a Seguridad Lógica

- No se siguen procedimientos para cambiar periódicamente las contraseñas.

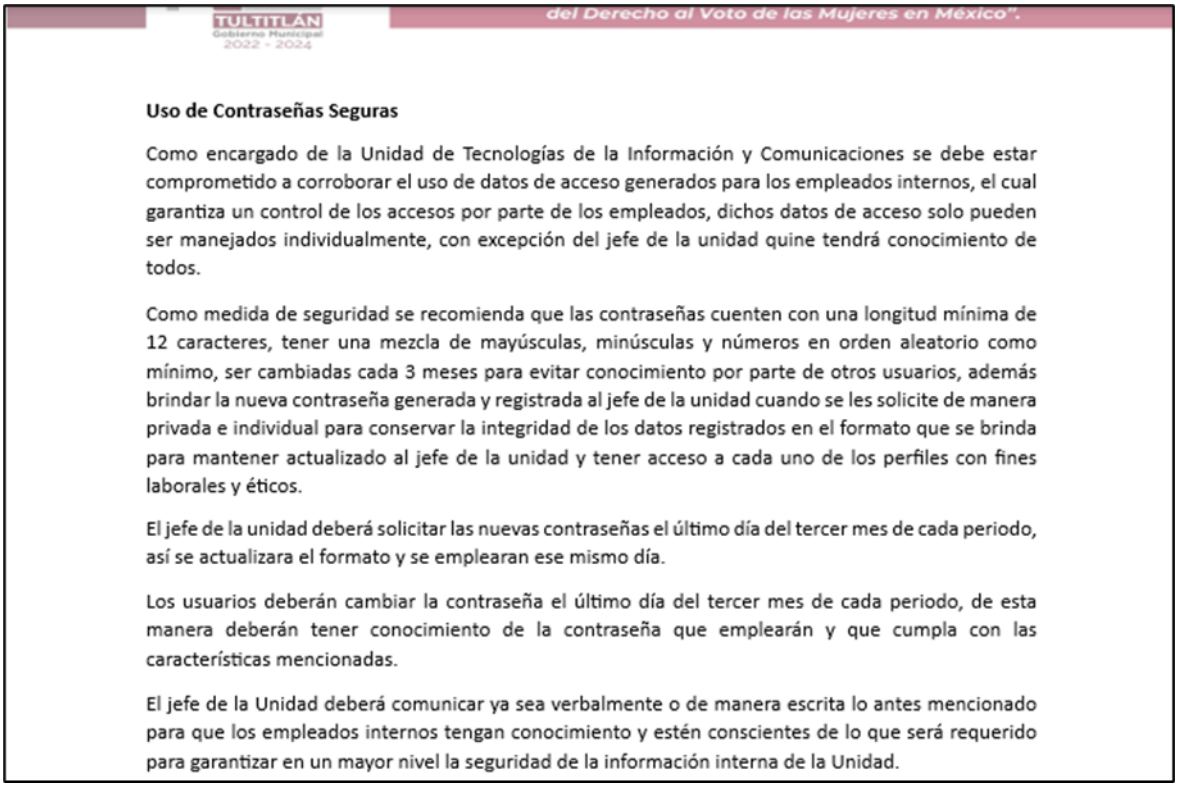
Recomendación

- Uso de contraseñas internas que sean seguras, creando una combinación de letras y números sin un orden especifico, alternando mayúsculas y minúsculas, o bien secuencias de números sin un contexto o significado e incluyendo caracteres especiales, además que sea de una longitud de mínimo 9 caracteres.
- Contraseñas diferentes para todas aquellas cuentas o situaciones laborales que las requieran.
- Cambiar las contraseñas usadas cuando los empleados dejen de laborar internamente o cambien de área.
- Mantener la opción de “mostrar contraseña” desactivada cada que se requiera ingresar las contraseñas creadas por cada usuario.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC usan contraseñas personales que no cumplen con las características mínimas para hacerlas seguras, sin embargo, no se permitió anexar evidencia de las contraseñas usadas actualmente, pues los empleados aseguran que son privadas, lo que hace que se cuestione si ocupan las mismas contraseñas para sus actividades intrapersonales fuera de lo laboral.

Después: Se desarrollan nombres de usuario y contraseñas seguras para los empleados internos los cuales sirven para tener un mejor control y seguridad al momento de acceder, así mismo en caso de que los empleados dejen de laborar o bien sean trasladados, será fácil para el encargado de la UTIC cambiar los datos de acceso para la llegada de un usuario nuevo. además, se especifica cada cuando se deben cambiar las contraseñas para garantizar que se conozcan y que se haga mal uso de los perfiles laborales de cada uno de los empleados, y estas se brindan al jefe de la UTIC registrándolas en acuerdo que registra dichos cambios y los datos que usan para acceder durante cierto periodo de tiempo.



TULTITLÁN Gobierno Municipal 2022 - 2024

del Derecho al Voto de las Mujeres en México".

Uso de Contraseñas Seguras

Como encargado de la Unidad de Tecnologías de la Información y Comunicaciones se debe estar comprometido a corroborar el uso de datos de acceso generados para los empleados internos, el cual garantiza un control de los accesos por parte de los empleados, dichos datos de acceso solo pueden ser manejados individualmente, con excepción del jefe de la unidad quine tendrá conocimiento de todos.

Como medida de seguridad se recomienda que las contraseñas cuenten con una longitud mínima de 12 caracteres, tener una mezcla de mayúsculas, minúsculas y números en orden aleatorio como mínimo, ser cambiadas cada 3 meses para evitar conocimiento por parte de otros usuarios, además brindar la nueva contraseña generada y registrada al jefe de la unidad cuando se les solicite de manera privada e individual para conservar la integridad de los datos registrados en el formato que se brinda para mantener actualizado al jefe de la unidad y tener acceso a cada uno de los perfiles con fines laborales y éticos.

El jefe de la unidad deberá solicitar las nuevas contraseñas el último día del tercer mes de cada periodo, así se actualizara el formato y se emplearan ese mismo día.

Los usuarios deberán cambiar la contraseña el último día del tercer mes de cada periodo, de esta manera deberán tener conocimiento de la contraseña que emplearán y que cumpla con las características mencionadas.

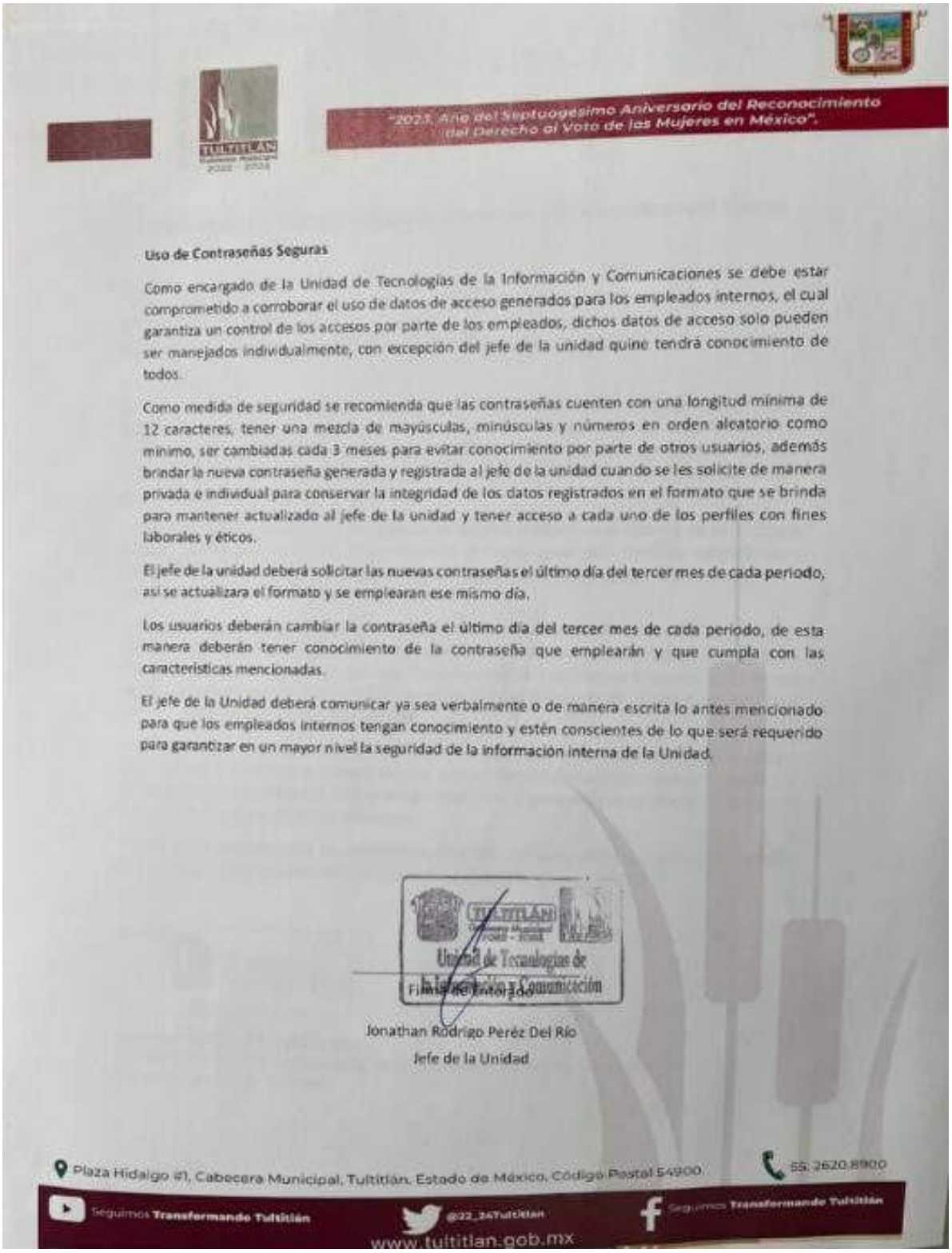
El jefe de la Unidad deberá comunicar ya sea verbalmente o de manera escrita lo antes mencionado para que los empleados internos tengan conocimiento y estén conscientes de lo que será requerido para garantizar en un mayor nivel la seguridad de la información interna de la Unidad.

Figura 240. Compromiso de uso de contraseñas seguras. Fuente: Elaboración propia. (propia., Compromiso de uso de contraseñas seguras, 2024)



REGISTRO DE DATOS PARA EL INICIO DE SESION DE LOS EMPLEADOS INTERNOS DE LA UTIC						El llenado de los formatos solo uede ser ejectado por el Jefe de la Unidad a cargo actualmente.
Empleado 1		Empleado 2		Empleado 3		
Nombre:	Jonathan Rodrigo Peréz Del Rio	Nombre:	María Olga Mota de la Cruz	Nombre:	José Luis Maldonado Jiménez	
Cargo:	Jefe de la Unidad	Cargo:	Secretaria	Cargo:	Capturista	
ID:	Jonathan_P20240201	ID:	Olga_M20240201	ID:	Jose.Luis_M20240201	
Contraseña:	aJ27wkl8gD21	Cntraseña:	Bk38YLm9He32	Cntraseña:	cL49zmN0iF43	Los empleados registrados deben ser los que laboran en tiempo real dentro de la UTIC, se pueden registran usuarios o empleados temporales como: Servicio Social y Prácticas Profesionales.
Periodo:	25 de Febrero - 25 de Mayo	Periodo:		Periodo:		
Empleado 4		Empleado 5		Empleado 6		
Nombre:	José Ángel Hernández Tovar	Nombre:	Marlene Méndez Estrada	Nombre:	Gerardo Hernández Cañas	
Cargo:	Capturista	Cargo:	Auxiliar	Cargo:	Auxiliar	
ID:	Jose.Angel_H20240201	ID:	Marlene_M20240201	ID:	Gerardo_H20240201	
Contraseña:	Dm50ANo1Jg54	Cntraseña:	eN61boP2kH65	Cntraseña:	Fo72CPq3Li76	
Periodo:		Periodo:		Periodo:		El llenado de los formatos debe ser acorde al tiempo de actualizacion especificado
Empleado 7		Empleado 8		Empleado 9		
Nombre:		Nombre:		Nombre:		
Cargo:		Cargo:		Cargo:		

Figura 241. Datos de Inicio de sesión con contraseñas seguras. Fuente: Elaboración propia. (propia., Datos de Inicio de sesión con contraseñas seguras, 2024)



"2023, Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Uso de Contraseñas Seguras

Como encargado de la Unidad de Tecnologías de la Información y Comunicaciones se debe estar comprometido a corroborar el uso de datos de acceso generados para los empleados internos, el cual garantiza un control de los accesos por parte de los empleados, dichos datos de acceso solo pueden ser manejados individualmente, con excepción del jefe de la unidad quine tendrá conocimiento de todos.

Como medida de seguridad se recomienda que las contraseñas cuenten con una longitud mínima de 12 caracteres, tener una mezcla de mayúsculas, minúsculas y números en orden aleatorio como mínimo, ser cambiadas cada 3 meses para evitar conocimiento por parte de otros usuarios, además brindar la nueva contraseña generada y registrada al jefe de la unidad cuando se les solicite de manera privada e individual para conservar la integridad de los datos registrados en el formato que se brinda para mantener actualizado al jefe de la unidad y tener acceso a cada uno de los perfiles con fines laborales y éticos.

El jefe de la unidad deberá solicitar las nuevas contraseñas el último día del tercer mes de cada periodo, así se actualizara el formato y se emplearan ese mismo día.

Los usuarios deberán cambiar la contraseña el último día del tercer mes de cada periodo, de esta manera deberán tener conocimiento de la contraseña que emplearán y que cumpla con las características mencionadas.

El jefe de la Unidad deberá comunicar ya sea verbalmente o de manera escrita lo antes mencionado para que los empleados internos tengan conocimiento y estén conscientes de lo que será requerido para garantizar en un mayor nivel la seguridad de la información interna de la Unidad.

Unidad de Tecnologías de la Información y Comunicación

Firma de Enterado

Jonathan Rodrigo Peréz Del Río
Jefe de la Unidad

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55 2620 8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 242. Compromiso firmado de uso de contraseñas seguras. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Compromiso firmado de uso de contraseñas seguras, 2024)

Vulnerabilidad Atendida enfocada a Seguridad Lógica

- Las versiones de software no son compatibles con las nuevas actualizaciones.
- Los empleados omiten realizar las actualizaciones al estar usando los sistemas y aplicaciones cuando el equipo lo sugiere.

Recomendación

- Asignar a un encargado de acuerdo con los roles internos de la UTIC.
- Monitorear y supervisar que los empleados mantengan actualizados sus equipos de cómputo.
- Implementar dentro de política del lugar, un apartado donde comprometa a los empleados a mantener sus sistemas actualizados a la versión más reciente y no tener actualizaciones en espera.
- Llevar un registro de la realización de la actualización, indicando la fecha, la hora de inicio y la hora de termino o bien instalación, indicando quien la realizo.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC no realizan o bien omiten las actualizaciones de los sistemas de los equipos de cómputo, mencionando que a veces es por la carga de trabajo ya que temen que sen tardadas dichas actualizaciones y los atrasen en sus actividades.

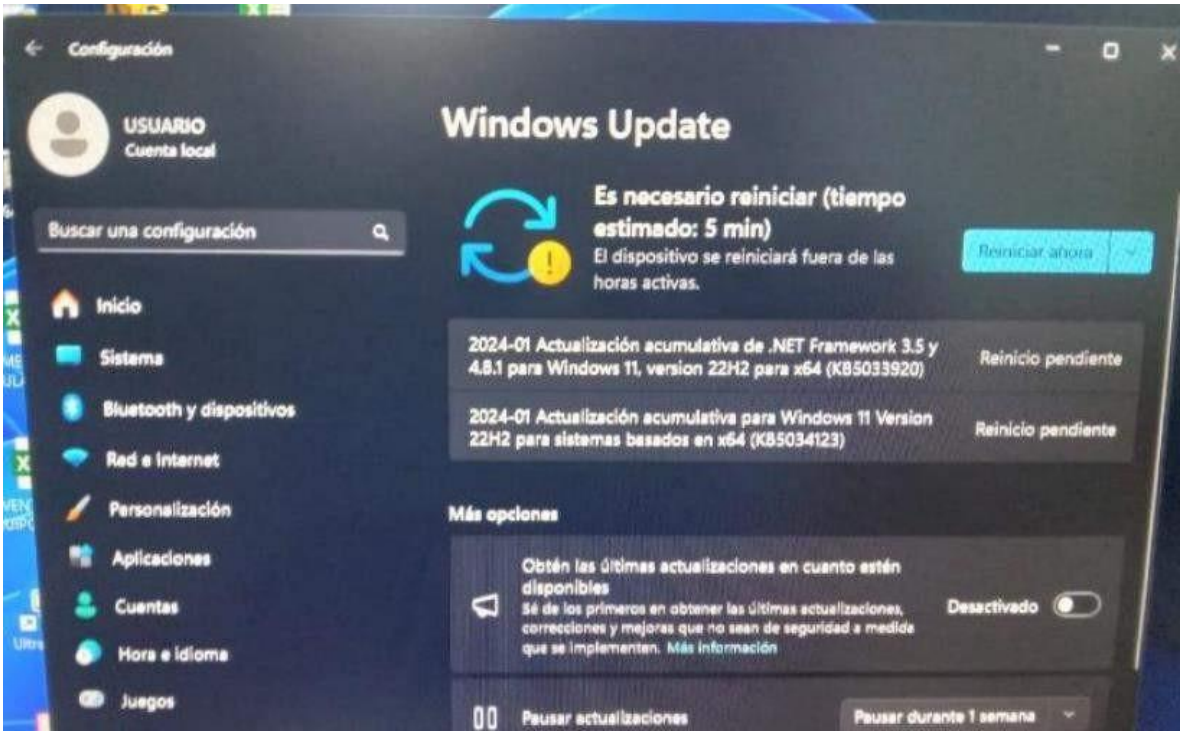


Figura 243. Equipo mostrando mensaje de actualización. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo mostrando mensaje de actualización, 2024)



Figura 244. Equipo aleatorio mostrando mensaje de actualización. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Equipo aleatorio mostrando mensaje de actulización., 2024)

Después: Primero se asigna a un encargado que tenga monitoreados los equipos internos, revisando que no tengan actualizaciones de la versión de sistema pendientes u omitidas, además dentro de la política interna que se desarrolló hay un apartado que comenta en uno de sus puntos la omisión de actualizaciones, por último, se brinda el formato para llevar el registro de las actualizaciones que se hagan y se logren correctamente.

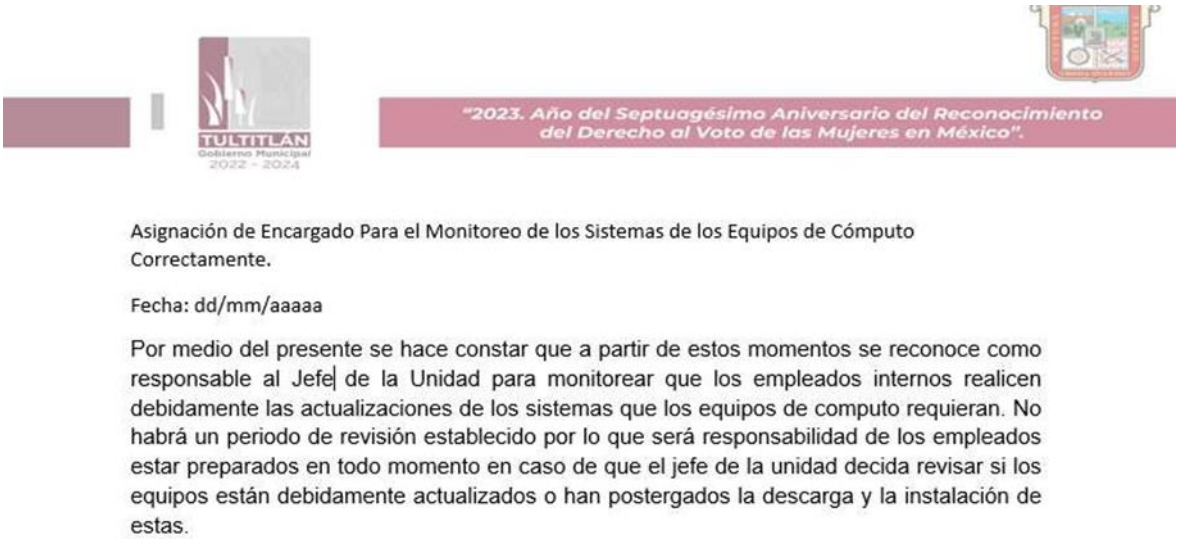


Figura 245. Compromiso de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC. Fuente: Elaboración propia. (propia., Compromiso de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC, 2024)



TULTITLÁN
Gobierno Municipal
2022 - 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Asignación de Encargado Para el Monitoreo de los Sistemas de los Equipos de Cómputo Correctamente.

Fecha: 15/02/2024

Por medio del presente se hace constar que a partir de estos momentos se reconoce como responsable a Marlene Méndez Estrada para monitorear que los empleados internos realicen debidamente las actualizaciones de los sistemas que los equipos de computo requieran. No habrá un periodo de revisión establecido por lo que será responsabilidad de los empleados estar preparados en todo momento en caso de que el jefe de la unidad decida revisar si los equipos están debidamente actualizados o han postergados la descarga y la instalación de estas.

Encargado

Firma de Enterado:

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900.

55. 2620.8900

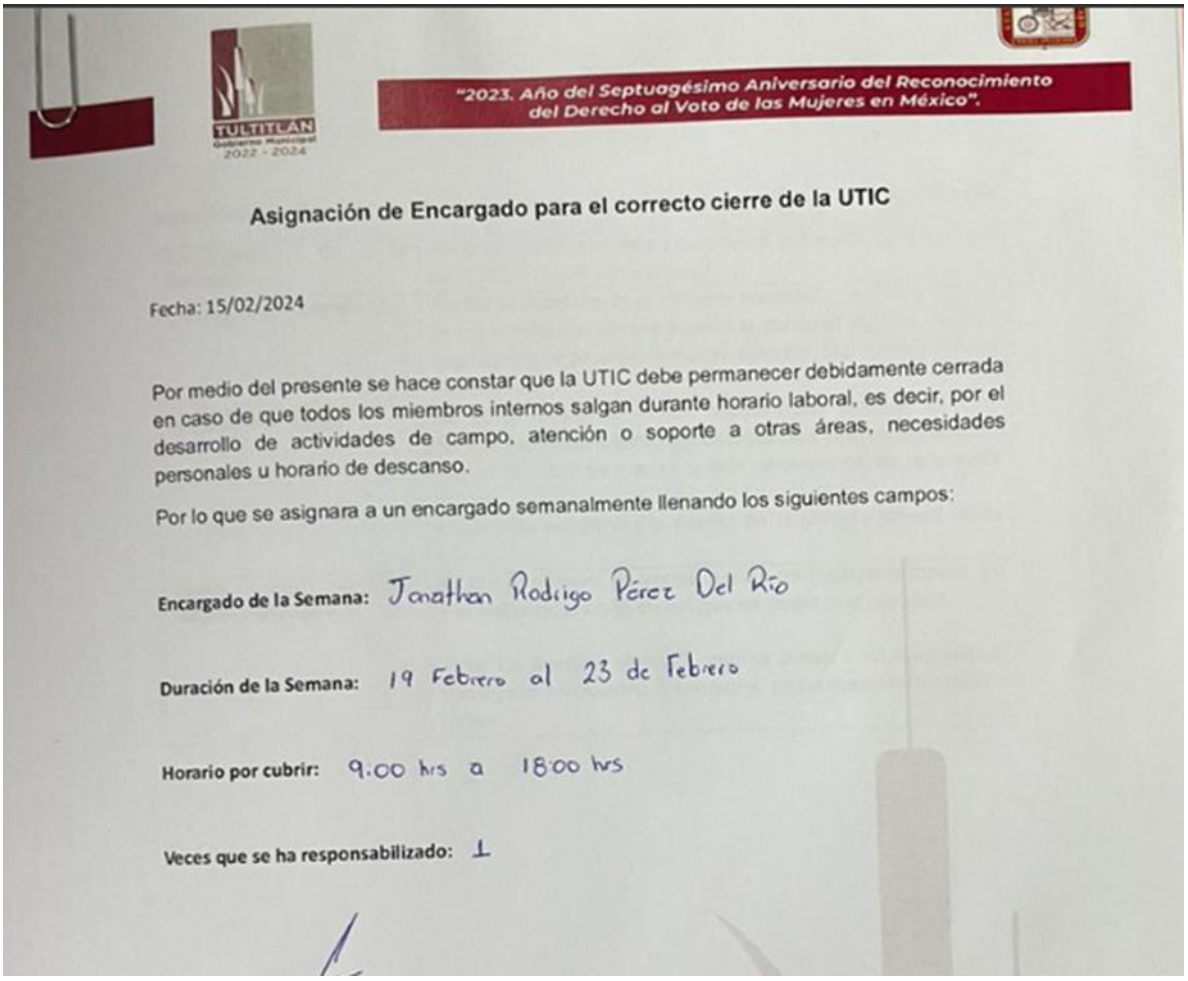
Seguimos Transformando Tultitlán

@22_24Tultitlan

Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 246. Compromiso firmado de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., 2024)



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Asignación de Encargado para el correcto cierre de la UTIC

Fecha: 15/02/2024

Por medio del presente se hace constar que la UTIC debe permanecer debidamente cerrada en caso de que todos los miembros internos salgan durante horario laboral, es decir, por el desarrollo de actividades de campo, atención o soporte a otras áreas, necesidades personales u horario de descanso.

Por lo que se asignara a un encargado semanalmente llenando los siguientes campos:

Encargado de la Semana: Jonathan Rodrigo Pérez Del Río

Duración de la Semana: 19 Febrero al 23 de Febrero

Horario por cubrir: 9:00 hrs a 18:00 hrs

Veces que se ha responsabilizado: 1

Figura 247. Compromiso de asignación de encargado para el correcto cierre de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Compromiso de asignación de encargado para el correcto cierre de la UTIC. , 2024)

Vulnerabilidad Atendida enfocada a Seguridad Lógica

- Falta de copias de seguridad periódicas de los datos almacenados en los equipos.
- Ausencia de Copias de seguridad de sistemas y datos en un lugar externo seguro.

Recomendación

- Realizar copias de seguridad de los datos y la información relevante que contengan los equipos de cómputo internos.
- Almacenarlas en un lugar seguro y remoto, se puede recomendar almacenarlas en la nube para tener acceso a la información en cualquier lugar y en cualquier momento.
- Contratación del servicio de almacenamiento en la nube “OneDrive” de Microsoft.
- Realizar al menos una vez semanalmente las copias de seguridad de la información y datos relevantes de la UTIC.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC no realizan copias de seguridad de los datos e información manejada en los equipos de cómputo internos, por lo que no hay evidencia para comparar el estado actual ya que no existen copias de seguridad o bien, herramientas procesos para ello.

Después: Primero se propone que se contrate el servicio de One Drive de Microsoft para negocios, es un buen inicio para empezar con el proceso de copias de seguridad, después de que se pone en ejecución el uso de esta herramienta se les especifico que solo el Jefe de la Unidad puede realizar estos respaldos y manejar la cuenta de One Drive, además de solo asegurar información relevante y datos importantes al menos una vez por semana, por lo que se recomendó que los datos se almacenaran en carpetas comprimidos en carpetas comprimidas para ahorrar un poco de espacio al momento de subirlo a la nube, así ellos sabrán que datos asegurar o bien que información respaldarán.

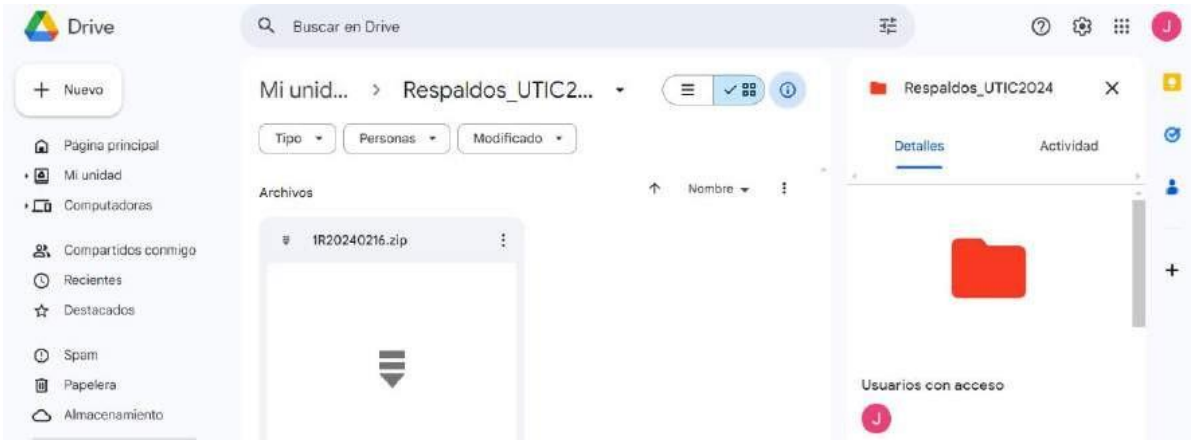


Figura 248. Respaldo en la nube de datos de la UTIC. Fuente: Google Drive. (Santos Ramírez & Moran Diego, 2024)

Vulnerabilidad Atendida enfocada a Servicios

- Los enchufes eléctricos no son los necesarios para satisfacer todos los equipos con los que cuenta la UTIC, implementando extensiones y provocando cables cruzados que comprometen la seguridad de los equipos.
- Sobrecargas por parte del uso de extensiones saturadas de equipos conectados.

Recomendación

- No sobrecargar con el uso de dispositivos las extensiones o “multicontactos” usados.
- Reemplazo y la implementación de Sistemas de Alimentación Ininterrumpida.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC usan extensiones regulares para satisfacer la ausencia de contactos eléctricos y poder abastecer todos los equipos con los que cuentan y usan para el desarrollo de sus actividades, por lo que hay ocasiones en las que se saturan dichas extensiones y ponen en riesgo los equipos por una posible sobrecarga.



Figura 249. Uso de extensiones en la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Uso de extensiones en la UTIC, 2023)



Figura 250. Uso de extensiones en la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Uso de extensiones en la UTIC, 2023)

Después: Se propuso reemplazar las extensiones regulares por Sistemas de Alimentación Ininterrumpida, principalmente para evitar que los equipos sufran algún desperfecto ya que el voltaje a veces puede variar según las instalaciones, por lo que una vez que accedieron a el uso de estos sistemas, se hizo la solicitud debidamente y se implementaron para así

tener un nivel más optimo en cuanto a la seguridad contra sobrecargas y apagones de equipos.



Figura 251. Cambio de extensiones por sistemas de alimentación ininterrumpidas. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cambio de extensiones por sistemas de alimentación ininterrumpidas, 2024)



Figura 252. Vista frontal del sistema de alimentación ininterrumpida. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista frontal del sistema de alimentación ininterrumpida, 2024)



Figura 253. Vista del No Break con código QR para saber sus características. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Vista del No Break con código QR para saber sus características, 2024)



Figura 254. Caja de los No Break implementados en la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Caja de los No Break implementados en la UTIC, 2024)



Figura 255. Características de los No Break implementados en la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Características de los No Break implementados en la UTIC, 2024)

Vulnerabilidad Atendida enfocada a Servicios

- Material inflamable debajo de los interruptores principales de la UTIC, es decir, el centro de carga (caja de fusibles y pastillas) que comprometen a una mayor propagación de incendio en caso de corto circuito.

Recomendación

- Colocar el extintor para circuitería ubicado en el interior del cuarto del site fijado contra la pared.
- En caso de no ser posible ubicar el extintor en un espacio visible al entrar al site y totalmente despejado para evitar tropiezos o accidentes.
- Despejar completamente el escenario considerado como peligroso y mencionado en los resultados de esta prueba.
- Mantener los activos, documentos o materiales con un mayor índice de ser inflamables, lejos de los contactos ubicados dentro del site.

Estrategia Implementada.

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que hay un escenario de alto riesgo dentro del cuarto del Site, pues hay material inflamable debajo de los interruptores eléctricos principales de la UTIC, se sabe que no hay espacio suficiente para almacenar todos sus archivos, sin embargo, pueden ubicarse en otro punto, además, el extintor está situado en el suelo por lo que no cumple con las normativas mencionadas.



Figura 256. Archivo debajo de interruptores eléctricos principales de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Archivo debajo de interruptores eléctricos principales de la UTIC, 2024)



Figura 257. Extintor mal ubicado dentro del site. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extintor mal ubicado dentro del site, 2024)

Después: Una vez atendidas las recomendaciones se puede percibir que el escenario donde estaban ubicados todos los archivos o bien materiales inflamables con mayor índice de propagación, han sido removidos y ubicados en otro punto, dejando despejada el área de los principales interruptores eléctricos de la UTIC, sin embargo, sobre el extintor, no fue posible fijarlo a la pared, dejándolo posicionado en el suelo, pero aislado de otros activos para fácil acceso.



Figura 258. Interruptores eléctricos despejados de archivos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Interruptores eléctricos despejados de archivos, 2024)



Figura 259. Extintor mejor ubicado dentro del site. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Extintor mejor ubicado dentro del site, 2024)

Vulnerabilidad Atendida enfocada a Servicios

- Bloqueo de entrada y salida con activos situados en el piso o bien por mobiliario cruzado en el paso.

Recomendación

- Designar un lugar específico para la ubicación de los activos que tienen situados en el suelo del área de trabajo.
- Ordenar los activos correctamente dentro del cuarto del site al no contar con algún otro espacio disponible.
- Quitar los activos situados a un costado del acceso principal para aumentar el espacio de entrada/salida.
- Retirar el “burlete” o “sello de puerta” colocado debajo de esta, ya que impide que la misma se abra en su totalidad y libremente.

Estrategia Implementada

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que hay activos situados en el piso, obstruyendo el correcto desplazamiento de los empleados internos a través de los pequeños espacios para moverse, además también estar ubicados a un costado del acceso principal impidiendo un acceso y salida correcto ya que abarca espacio, además del burlete debajo de la puerta que impide que esta se pueda abrir totalmente.



Figura 260. Activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)



Figura 261. Activos obstruyendo el acceso principal de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos obstruyendo el acceso principal de la UTIC, 2024)

Después: Luego de atender dichas debilidades se puede apreciar que los pequeños espacios para trasladarse han sido despejados al ya no tener activos situados justo en al paso de los empleados, además de que las cajas con equipos ubicadas a un costado del acceso principal fueron reubicadas y permite la libre salida y entrada al sitio con mayor movilidad.



Figura 262. Espacio del pasillo libre de activos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Espacio del pasillo libre de activos, 2024)



Figura 263. Acceso principal a la UTIC despejado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Acceso principal a la UTIC despejado, 2024)

Vulnerabilidad Atendida enfocada a Servicios

- No cuentan con todos los señalamientos de emergencia, por lo que no están al alcance de la vista de cualquier usuario.

Recomendación

- Colocar los señalamientos de emergencia con los que no cuentan, o al menos los más comunes y que pueden ayudar a los usuarios en su comportamiento durante una emergencia o evacuación.
- Solicitud o bien un comunicado donde reporte la falta de dichos señalamientos para que las autoridades correspondientes actúen ante la notable ausencia de estos.

Estrategia Implementada

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que no cuentan con la mayoría de los señalamientos de emergencia por lo que los usuarios visitantes en caso de alguna emergencia no sabrán como actuar ante la circunstancia ya que evidentemente no se encuentran a la vista de cualquier usuario, a continuación, se colocan imágenes de los señalamientos con los que cuentan:



Figura 264. Señalamiento de emergencia. Fuente: Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Salida de Emergencia, 2023)

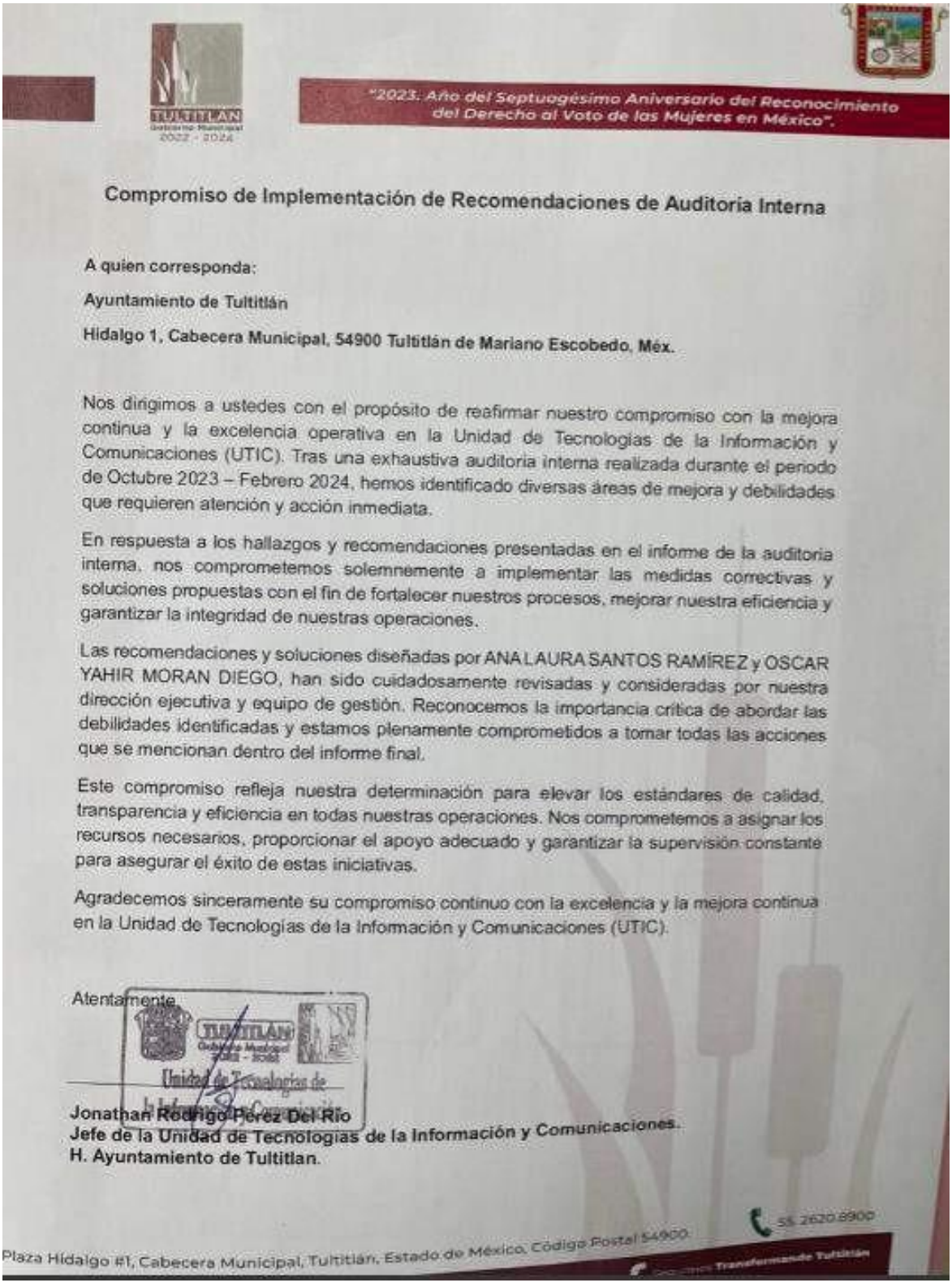


Figura 265 Señalamiento de emergencia. Fuente: Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Ruta de Evacuación, 2023)



Figura 266 Señalamiento de emergencia. Fuente: Ayuntamiento de Tultitlán. (Tultitlán. H. A., Señalamiento de Exintor, 2023)

Después: luego de implementar las recomendaciones mencionadas se puede concluir que aún no se colocan los señalamientos faltantes ya que es un proceso de aprobación por la dependencia bastante largo, sin embargo, se pudo mandar el oficio para hacer saber a los superiores la notable ausencia de dichos señalamientos, firmado por el jefe de la UTIC el cual se encargó de presentar el comunicado ante la dirección del Ayuntamiento como una solicitud de atención.



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Compromiso de Implementación de Recomendaciones de Auditoria Interna

A quien corresponda:

Ayuntamiento de Tultitlán

Hidalgo 1, Cabecera Municipal, 54900 Tultitlán de Mariano Escobedo, Méx.

Nos dirigimos a ustedes con el propósito de reafirmar nuestro compromiso con la mejora continua y la excelencia operativa en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC). Tras una exhaustiva auditoria interna realizada durante el periodo de Octubre 2023 – Febrero 2024, hemos identificado diversas áreas de mejora y debilidades que requieren atención y acción inmediata.

En respuesta a los hallazgos y recomendaciones presentadas en el informe de la auditoria interna, nos comprometemos solemnemente a implementar las medidas correctivas y soluciones propuestas con el fin de fortalecer nuestros procesos, mejorar nuestra eficiencia y garantizar la integridad de nuestras operaciones.

Las recomendaciones y soluciones diseñadas por ANA LAURA SANTOS RAMÍREZ y OSCAR YAHIR MORAN DIEGO, han sido cuidadosamente revisadas y consideradas por nuestra dirección ejecutiva y equipo de gestión. Reconocemos la importancia crítica de abordar las debilidades identificadas y estamos plenamente comprometidos a tomar todas las acciones que se mencionan dentro del informe final.

Este compromiso refleja nuestra determinación para elevar los estándares de calidad, transparencia y eficiencia en todas nuestras operaciones. Nos comprometemos a asignar los recursos necesarios, proporcionar el apoyo adecuado y garantizar la supervisión constante para asegurar el éxito de estas iniciativas.

Agradecemos sinceramente su compromiso continuo con la excelencia y la mejora continua en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

Atentamente

Unidad de Tecnologías de la Información y Comunicación

Jonathan Rodrigo Perez Del Rio
Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.
H. Ayuntamiento de Tultitlan.

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900 55 2620 8900

Figura 267 Compromiso firmado de implementación de recomendaciones de auditoría interna. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Compromiso Firmado de Implementacion de Recomendaciones de Auditoría Interna, 2024)

Vulnerabilidad Atendida enfocada a Infraestructura

- Activos situados en el suelo y el paso entre los escritorios de la UTIC que interponen con la libre movilidad de los empleados.

Recomendación

- Asignar un espacio con el rol de un almacén o bodega cerca del departamento donde solo los empleados de la UTIC tengan acceso, para ingresar todo activo que llegue o tengan que comprometa la libre movilidad en el área de trabajo.

Estrategia Implementada

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que no cuentan con el espacio suficiente para almacenar todos los activos que llegan o bien ingresan de otros departamentos, además de que el espacio destinado para almacenar activos en condiciones no tan favorables en general del ayuntamiento no está disponible para que la UTIC almacene dentro de él. No hay evidencia sobre dicho almacén ya que no permiten el ingreso a él, sin embargo, como se muestra en las pruebas de la Auditoría hay evidencia de como cuentan con activos situados en el suelo.



Figura 268 Activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)



Figura 269 Activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)



Figura 270 Activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)



Figura 271 Activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Activos ubicados en el suelo, 2023)

Después: Se optó por movilizar todos los activos situados en el suelo que comprometen el desplazamiento de los empleados en el interior de la unidad, así que se reubicaron dichos activos, equipos y demás al interior del cuarto del site con una mejor organización, de esta manera los pequeños espacios entre los escritorios no son obstruidos y existe un nivel mayor de movilidad.



Figura 272 Reubicación de los activos situados en el piso. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reubicación de los activos situados en el piso, 2024)



Figura 273 Reubicación de activos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reubicación de los activos situados en el piso, 2024)



Figura 274 Reubicación de activos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reubicación de los activos situados en el piso, 2024)



Figura 275 Reubicación de activos. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Reubicación de los activos situados en el piso, 2024)

Vulnerabilidad Atendida enfocada a Infraestructura

- Los contactos eléctricos están debidamente instalados, sin embargo, no son suficientes para todos los equipos funcionales con los que cuentan dentro de la UTIC, provocando el uso de extensiones mal ubicadas.
- Equipos enchufados y apagados sin ser utilizados provocan que los cables se crucen y exista confusión en el multi contacto.

Recomendación

- Identificar con etiquetas físicas de extremo a extremo el cableado de la UTIC.
- Agruparlos con cinchos sujeta-cables o velcro acorde al tipo de periférico (Mouse, teclado, bocinas, cable de corriente, cable ethernet, etc.).

Estrategia Implementada

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que no hay un ordenamiento de cables es decir que no están agrupados los cables de accesorios o periféricos, ni una identificación de cables de colores para ubicar que tipo de cable este enchufado en dichas extensiones y así no confundirse o provocar un apagón repentino en algún equipo de cómputo mientras se están usando, afectando así el trabajo de los empleados.



Figura 276 Cableado desordenado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado desordenado, 2023)



Figura 277 Cableado desordenado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Cableado desordenado, 2023)

Después: una vez implementadas las recomendaciones es notable que los cables de los periféricos y accesorios o componentes de los equipos son agrupados mostrando un mayor nivel de organización, además para los cables principales, es decir, los de corriente que alimentan los equipos de cómputo son marcados en el extremo donde se enchufan a la energía con un distintivo de color para evitar confusiones a la hora de desconectar y provocar algún apagón imprevisto en el horario laboral.



Figura 278 Identificación del cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)



Figura 279 Identificación del cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)

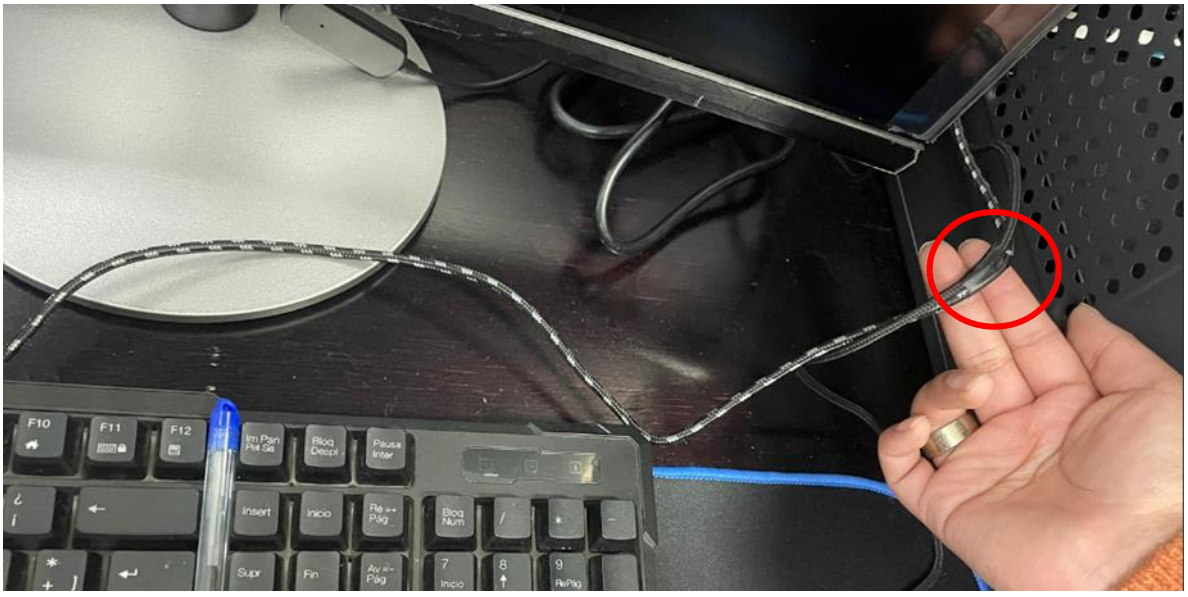


Figura 280 Identificación de cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)



Figura 281 Identificación de cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)



Figura 282 Identificación de cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)



Figura 283 Identificación de cableado. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Identificación del cableado, 2024)

Vulnerabilidad Atendida enfocada a Infraestructura

- No cuentan con reglas específicas para el uso de los routers, switches y servidores.

Recomendación

- Establecer el uso de los dispositivos de telecomunicaciones, así como responsabilidades y sanciones hacia aquel empleado o proveedor que realice mantenimiento preventivo y correctivo dentro de una política interna.

Estrategia Implementada

Antes: En las pruebas realizadas se encontró que usuarios internos de la UTIC se encontró que no cuentan con reglas sobre el uso debido de los dispositivos de redes, activos o demás, mucho menos con sanciones sobre el incumplimiento de las reglas, por lo que no hay evidencia que se pueda mostrar al tener la ausencia de este apartado en la política.

Después: Luego de implementar las recomendaciones mencionadas, se puso en práctica la política como una de las medidas principales con anterioridad, pues regula el comportamiento y uso de los activos internos de la UTIC, dentro de esta política se mencionan puntos relacionados con el correcto uso de los dispositivos de redes, o componentes en general, además de imponer sanciones para los empleados que no cumplan con dichas reglas.

Artículo 15. Son obligaciones del personal interno de la UTIC:

a) Mantener una imagen de responsabilidad y respeto que propicie una buena convivencia en los espacios de trabajo donde participen. Brindar el servicio con cortesía y respeto a los civiles, empleados y demás usuarios.

b) Proporcionar asesoría básica en el uso y manejo de paqueterías autorizadas por la dependencia.

c) Dar un uso adecuado al equipo y mobiliario de la UTIC para evitar daños y/o descomposturas.

d) Verificar y gestionar la reposición del equipo, mobiliario o cualquier otro dispositivo en caso de deterioro, pérdida total o parcial, el cual deberá ser sustituido por otro con las mismas o mejores características.

e) Publicar los horarios de trabajo de la UTIC.

f) Mantener los sistemas de los equipos de cómputo internos actualizados a la versión más reciente y no tener actualizaciones en espera u omitidas por la realización de actividades laborales.

g) Usar adecuadamente los dispositivos de red y los componentes de telecomunicaciones, evitando abolladuras, golpes, jalones de cables y todo lo que afecte la apariencia y rendimiento de los dispositivos.

Figura 284 Parte de la Política (revisar anexo 2). Fuente: Elaboración propia. (propia., Parte de la Política, 2024)

CAPITULO V

DE LAS SANCIONES

Artículo 17. Cualquier infracción a lo dispuesto en la presente política, generará la aplicación de sanciones, considerando ante todo la gravedad del hecho, sus consecuencias, así como la intencionalidad y reincidencia:

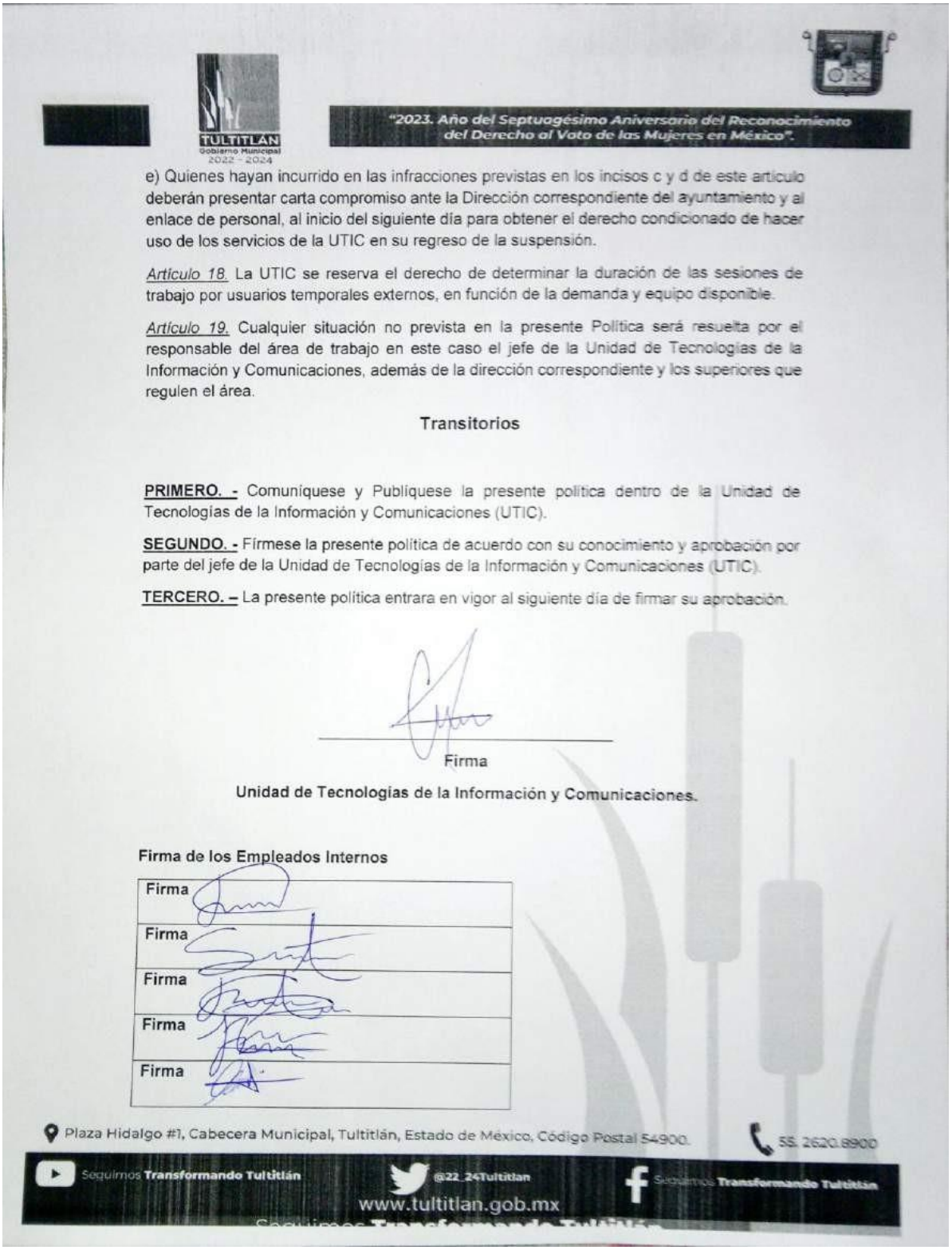
a) Se amonestará por escrito a todo usuario que viole el contenido del Artículo 16, en sus incisos b, g, h.

b) La acumulación de dos amonestaciones por escrito dará cabida a la suspensión de sus actividades dentro de la UTIC, hasta por tres días, dependiendo la gravedad de las amonestaciones.

c) La acumulación de tres amonestaciones escritas dará por suspendido al usuario de sus actividades dentro de la UTIC, hasta por 5 días, dependiendo la gravedad de las amonestaciones.

d) Será causa de suspensión inmediata de sus derechos y servicios por un tiempo determinado por las autoridades hasta por más de una semana a quien viole lo dispuesto por el Artículo 16, en sus incisos a, c y d.

Figura 285 Capitulo V de la política (revisar anexo 2). Fuente: Elaboración propia. (propia., Capitulo V de la política, 2024)



TULTITLÁN Gobierno Municipal 2022 – 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

e) Quienes hayan incurrido en las infracciones previstas en los incisos c y d de este artículo deberán presentar carta compromiso ante la Dirección correspondiente del ayuntamiento y al enlace de personal, al inicio del siguiente día para obtener el derecho condicionado de hacer uso de los servicios de la UTIC en su regreso de la suspensión.

Artículo 18. La UTIC se reserva el derecho de determinar la duración de las sesiones de trabajo por usuarios temporales externos, en función de la demanda y equipo disponible.

Artículo 19. Cualquier situación no prevista en la presente Política será resuelta por el responsable del área de trabajo en este caso el jefe de la Unidad de Tecnologías de la Información y Comunicaciones, además de la dirección correspondiente y los superiores que regulen el área.

Transitorios

PRIMERO. - Comuníquese y Publíquese la presente política dentro de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

SEGUNDO. - Fírmese la presente política de acuerdo con su conocimiento y aprobación por parte del jefe de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

TERCERO. – La presente política entrara en vigor al siguiente día de firmar su aprobación.

Firma

Unidad de Tecnologías de la Información y Comunicaciones.

Firma de los Empleados Internos

Firma
Firma
Firma
Firma
Firma

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 286 Política firmada por los empleados de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Política aprobada, 2024)

Vulnerabilidad Atendida enfocada a Infraestructura

- La falta de políticas y reglas dentro de la UTIC.

Recomendación

- Implementar políticas, acorde a la falta de reglas que regulen el lugar y hacer uso de sanciones a todo aquel que las incumpla.

Estrategia Implementada

Antes: Durante la inspección que se realizó a la UTIC, es notable la ausencia de una política que regule el comportamiento y buen uso de los equipos y activos internos de la UTIC al contar con usuarios temporales nuevos constantemente (servicio social y prácticas profesionales). Por lo que no se pude evidenciar la ausencia de dicha política.

Después: Se diseño la siguiente política enfocándose al correcto uso de los activos y al comportamiento de los usuarios dentro de la UTIC, por lo que abarca temas generales que puedan ser aplicados para todo tipo de usuario que quiera ingresar a la UTIC, además, de que dentro de dicha política se establecen sanciones para el incumplimiento de esta.



Figura 287 Contenido de la política (revisar anexo 2). Fuente: Elaboración propia. (propia., Contenido de la política, 2024)

CAPITULO V

DE LAS SANCIONES

Artículo 17. Cualquier infracción a lo dispuesto en la presente política, generará la aplicación de sanciones, considerando ante todo la gravedad del hecho, sus consecuencias, así como la intencionalidad y reincidencia:

a) Se amonestará por escrito a todo usuario que viole el contenido del Artículo 16, en sus incisos b, g, h.

b) La acumulación de dos amonestaciones por escrito dará cabida a la suspensión de sus actividades dentro de la UTIC, hasta por tres días, dependiendo la gravedad de las amonestaciones.

Figura 288 Capitulo V de la política (revisar anexo 2). Fuente: Elaboración propia. (propia., Capitulo V de la política, 2024)

Vulnerabilidad Atendida enfocada a Infraestructura

- Falta de explicación hacia los usuarios nuevos o externos sobre el buen uso interno que se le da a los equipos de cómputo o activos en general

Recomendación

- Establecer en las políticas que un empleado encargado debiera dar una breve explicación acerca de cómo se trabaja dentro de la UTIC y cual serian sus reglas y comportamientos que también debieran seguir y que se debiera de comunicar a los empleados y a las partes externas.

Estrategia Implementada

Antes: Durante la inspección que se realizó a la UTIC, es notable la ausencia de una política que regule el comportamiento y buen uso de los equipos y activos internos de la UTIC al contar con usuarios temporales nuevos constantemente (servicio social y prácticas profesionales). Por lo que no se pude evidenciar la ausencia de dicha política.

Después: Se diseño la siguiente política enfocándose al correcto uso de los activos y al comportamiento de los usuarios dentro de la UTIC, por lo que abarca temas generales que puedan ser aplicados para todo tipo de usuario que quiera ingresar a la UTIC, además, de que dentro de dicha política se establece un apartado mencionando que es necesario orientar a los usuarios nuevos o temporales con una pequeña asesoría sobre la forma de trabajo y el uso de dichos activos.



Figura 289 Contenido de la política (revisar anexo 2). Fuente: Elaboración propia. (propia., Contenido de la política, 2024)

Artículo 15. Son obligaciones del personal interno de la UTIC:

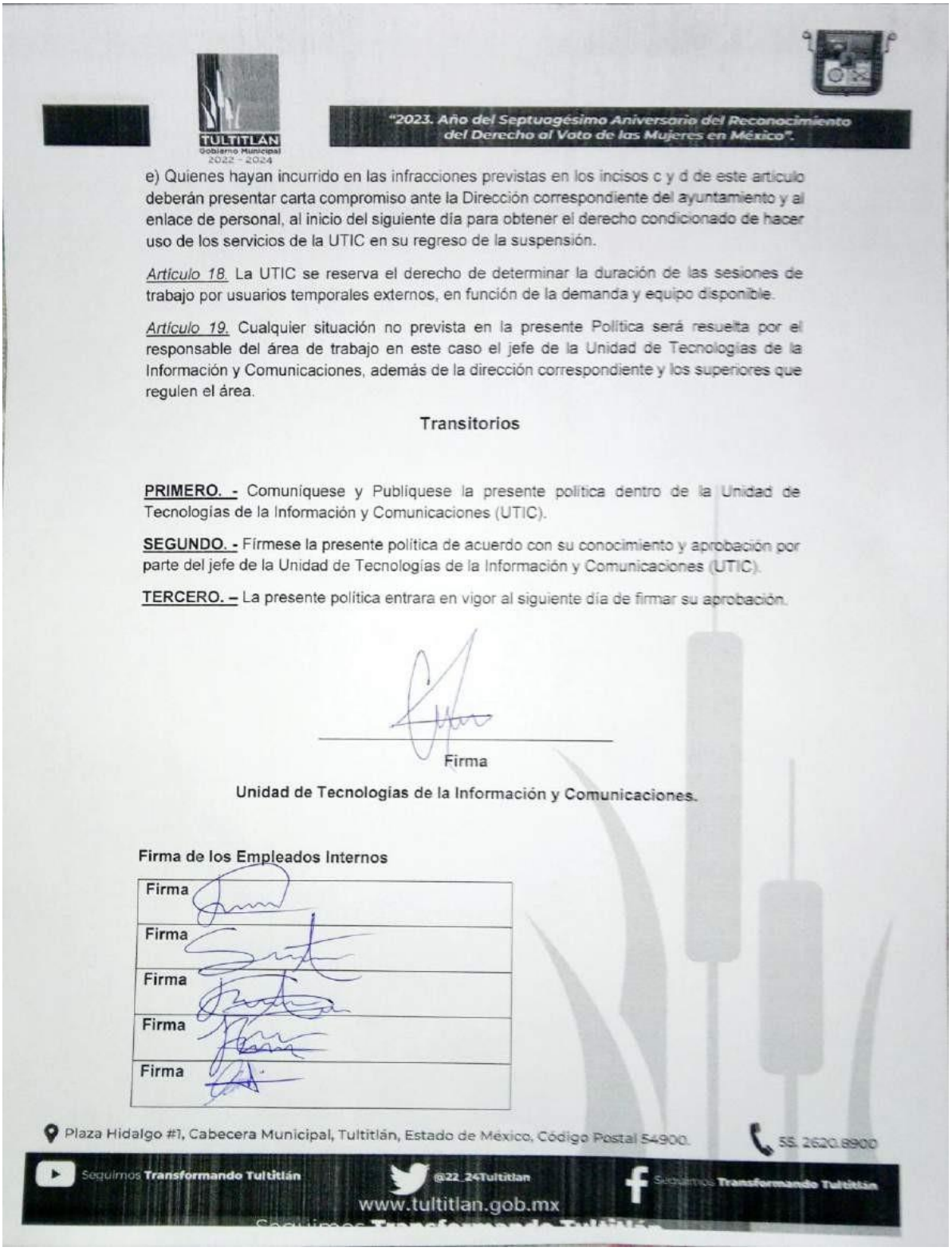
a) Mantener una imagen de responsabilidad y respeto que propicie una buena convivencia en los espacios de trabajo donde participen. Brindar el servicio con cortesía y respeto a los civiles, empleados y demás usuarios.

b) Proporcionar asesoría básica en el uso y manejo de los activos y dispositivos usados internamente, a usuarios temporales o prestadores de servicio social, prácticas profesionales o simplemente usuarios nuevos.

c) Dar un uso adecuado al equipo y mobiliario de la UTIC para evitar daños y/o descomposturas.

d) Verificar y gestionar la reposición del equipo, mobiliario o cualquier otro dispositivo en caso de deterioro, pérdida total o parcial, el cual deberá ser sustituido por otro con las mismas o mejores características.

Figura 290 Artículo 15 de la política (revisar anexo 2). Fuente: Elaboración propia. (propia., Artículo 15 de la política, 2024)



TULTITLÁN Gobierno Municipal 2022 – 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

e) Quienes hayan incurrido en las infracciones previstas en los incisos c y d de este artículo deberán presentar carta compromiso ante la Dirección correspondiente del ayuntamiento y al enlace de personal, al inicio del siguiente día para obtener el derecho condicionado de hacer uso de los servicios de la UTIC en su regreso de la suspensión.

Artículo 18. La UTIC se reserva el derecho de determinar la duración de las sesiones de trabajo por usuarios temporales externos, en función de la demanda y equipo disponible.

Artículo 19. Cualquier situación no prevista en la presente Política será resuelta por el responsable del área de trabajo en este caso el jefe de la Unidad de Tecnologías de la Información y Comunicaciones, además de la dirección correspondiente y los superiores que regulen el área.

Transitorios

PRIMERO. - Comuníquese y Publíquese la presente política dentro de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

SEGUNDO. - Fírmese la presente política de acuerdo con su conocimiento y aprobación por parte del jefe de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

TERCERO. – La presente política entrara en vigor al siguiente día de firmar su aprobación.

Firma

Unidad de Tecnologías de la Información y Comunicaciones.

Firma de los Empleados Internos

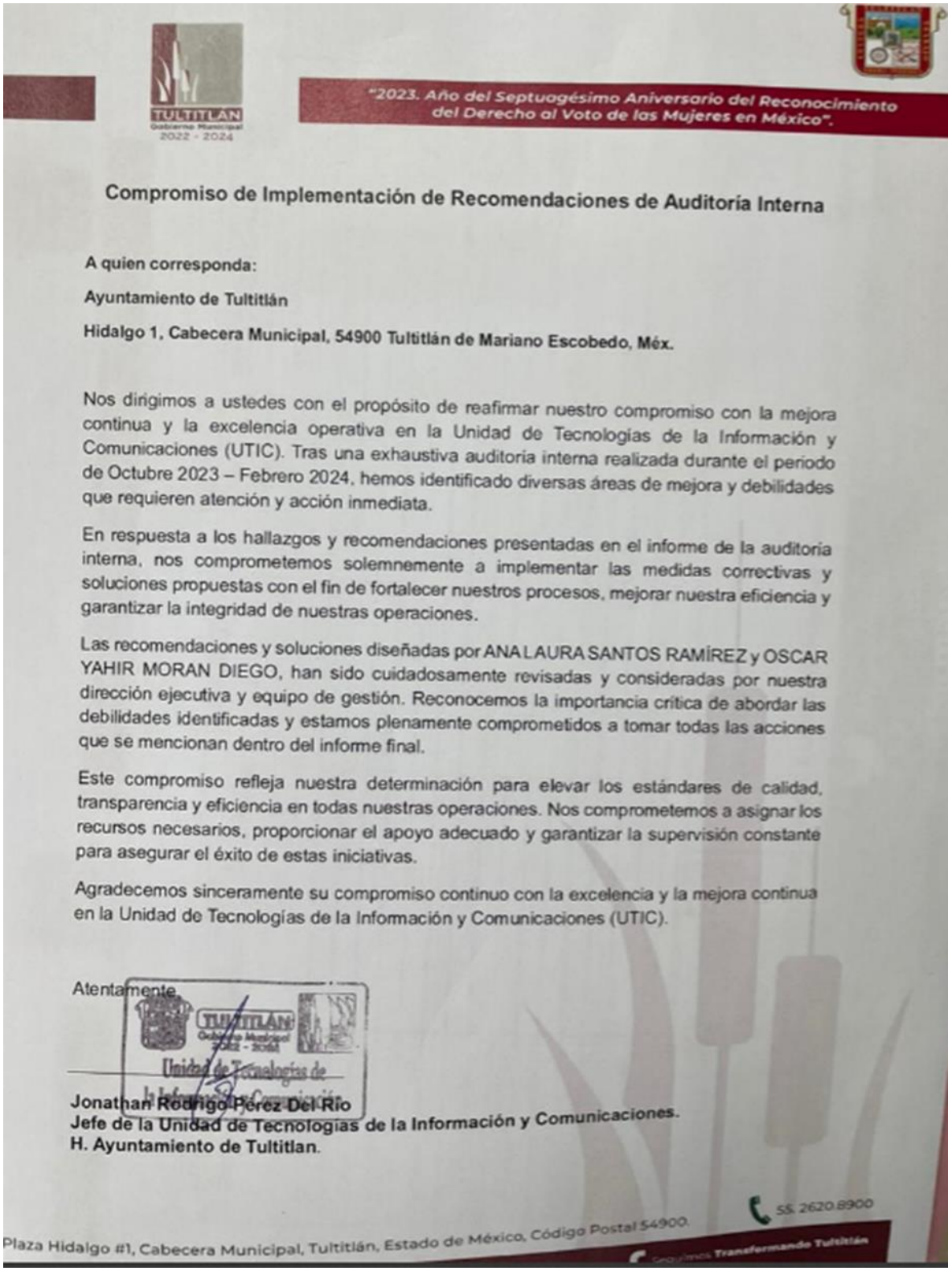
Firma
Firma
Firma
Firma
Firma

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 291 Política firmada por los empleados de la UTIC. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Política aprobada, 2024)



TULTITLÁN
Gobierno Municipal
2022 - 2024

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Compromiso de Implementación de Recomendaciones de Auditoría Interna

A quien corresponda:

Ayuntamiento de Tultitlán

Hidalgo 1, Cabecera Municipal, 54900 Tultitlán de Mariano Escobedo, Méx.

Nos dirigimos a ustedes con el propósito de reafirmar nuestro compromiso con la mejora continua y la excelencia operativa en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC). Tras una exhaustiva auditoria interna realizada durante el periodo de Octubre 2023 – Febrero 2024, hemos identificado diversas áreas de mejora y debilidades que requieren atención y acción inmediata.

En respuesta a los hallazgos y recomendaciones presentadas en el informe de la auditoría interna, nos comprometemos solemnemente a implementar las medidas correctivas y soluciones propuestas con el fin de fortalecer nuestros procesos, mejorar nuestra eficiencia y garantizar la integridad de nuestras operaciones.

Las recomendaciones y soluciones diseñadas por ANA LAURA SANTOS RAMÍREZ y OSCAR YAHIR MORAN DIEGO, han sido cuidadosamente revisadas y consideradas por nuestra dirección ejecutiva y equipo de gestión. Reconocemos la importancia crítica de abordar las debilidades identificadas y estamos plenamente comprometidos a tomar todas las acciones que se mencionan dentro del informe final.

Este compromiso refleja nuestra determinación para elevar los estándares de calidad, transparencia y eficiencia en todas nuestras operaciones. Nos comprometemos a asignar los recursos necesarios, proporcionar el apoyo adecuado y garantizar la supervisión constante para asegurar el éxito de estas iniciativas.

Agradecemos sinceramente su compromiso continuo con la excelencia y la mejora continua en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

Atentamente

TULTITLÁN Gobierno Municipal 2022 - 2024
Unidad de Tecnologías de la Información y Comunicación

Jonathan Rodrigo Pérez Del Río
Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.
H. Ayuntamiento de Tultitlan.

55 2620 8900

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900.

Transformando Tultitlán

Figura 292 Compromiso firmado de implementación de recomendaciones de auditoría interna. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Compromiso Firmado de Implementacion de Recomendaciones de Auditoría Interna, 2024)

Vulnerabilidad Atendida enfocada al Sistema de Inventario

- El sistema de inventario es de fácil acceso y consulta por parte de los usuarios internos y externos de la UTIC.

Recomendación

- Implementar un control de acceso en el sistema de inventario de acuerdo con los diferentes roles que tengan los empleados.

Estrategia Implementada

Antes: Durante la inspección que se realizó a la UTIC, es notable la ausencia de un sistema de inventario que funcione correctamente y que cumpla con características de seguridad para proteger la información, pues no cuenta con ninguna medida que regule el acceso al sistema de inventario usado actualmente pues solo acceden a una carpeta compartida del archivo usado con función de inventario.

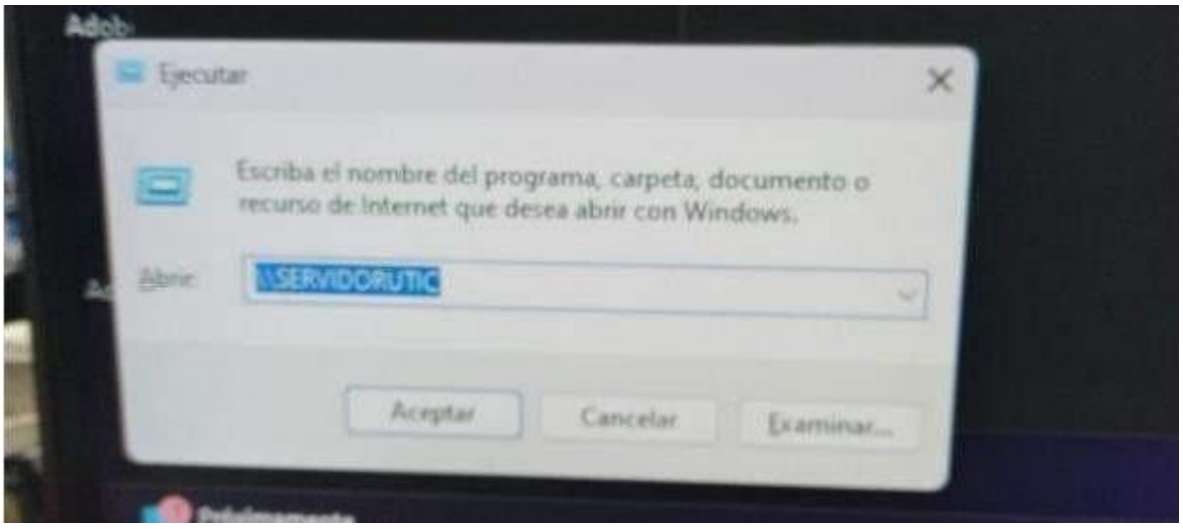


Figura 293 Acceso al inventario desde la herramienta 'Ejecutar'. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Acceso al inventario desde la herramienta 'Ejecutar', 2023)

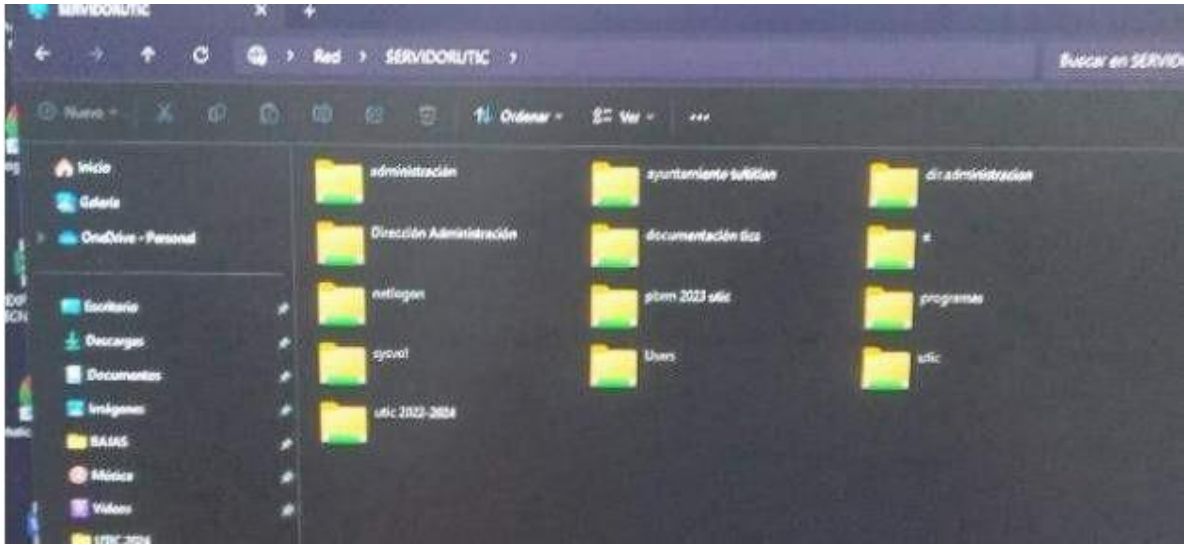


Figura 294 Carpetas en red donde se encuentra el inventario. Fuente: Equipos de Cómputo de la UTIC. (Comunicación. U. d., Carpetas en Red, 2023)

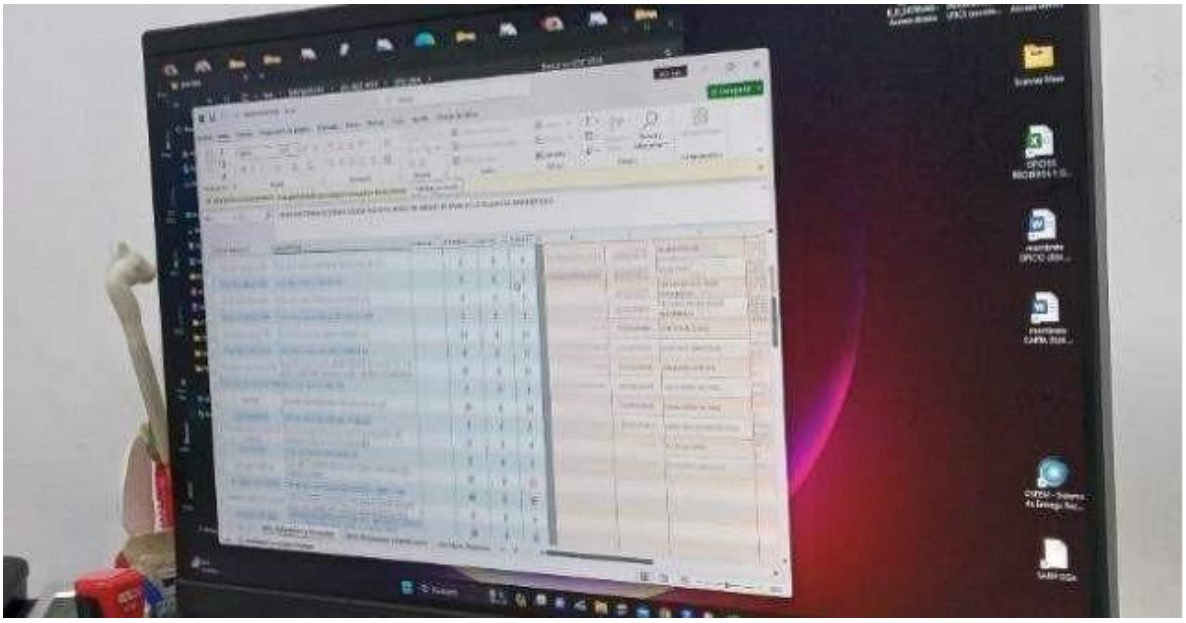


Figura 295 Inventario de la UTIC en hojas de cálculo. Fuente: Equipos de Cómputo de la UTIC. (Comunicación. U. d., Inventario de la UTIC en hojas de cálculo, 2023)

Después: Las medidas implementadas con base a las recomendaciones mencionadas son implementadas y se puso en uso un sistema de inventario desarrollado con base a las necesidades con las que cuenta la UTIC, por lo que se implementó y se desarrolló una medida de seguridad de acceso en este caso un formulario (login) para evitar que usuarios externos accedan a la información y los datos, pues requiere usuario y contraseña que cada uno de los empleados internos.

Para esto primero se deben instalar correctamente las herramientas necesarias en este caso son dos el apache NetBeans y SQL server para la base de datos.

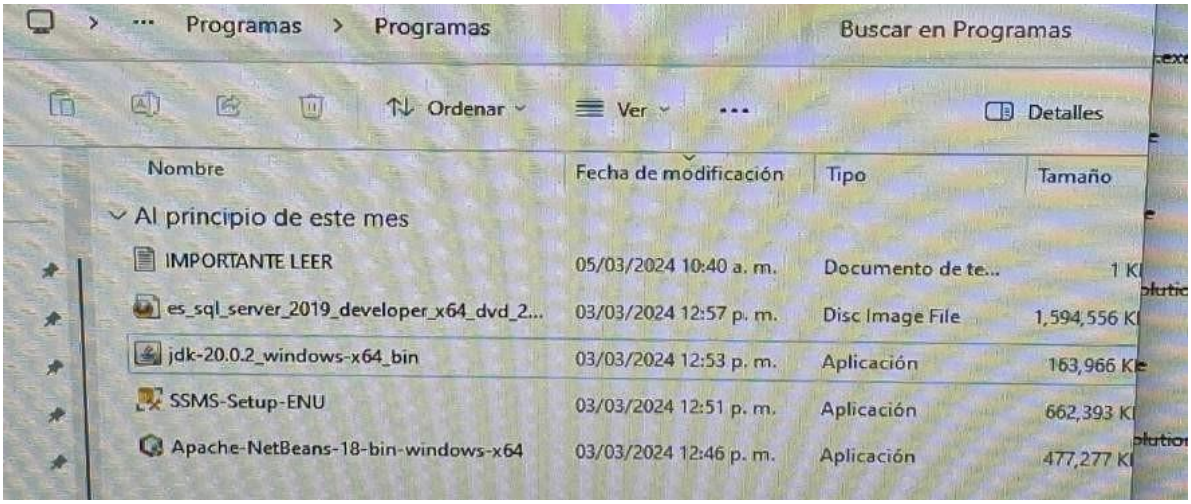


Figura 296 Lista de programas a instalar para la implementación del Sistema de Inventario. Fuente: Elaboración propia. (propia., Lista de programas a instalar para la implementación del Sistema de Inventario, 2024)

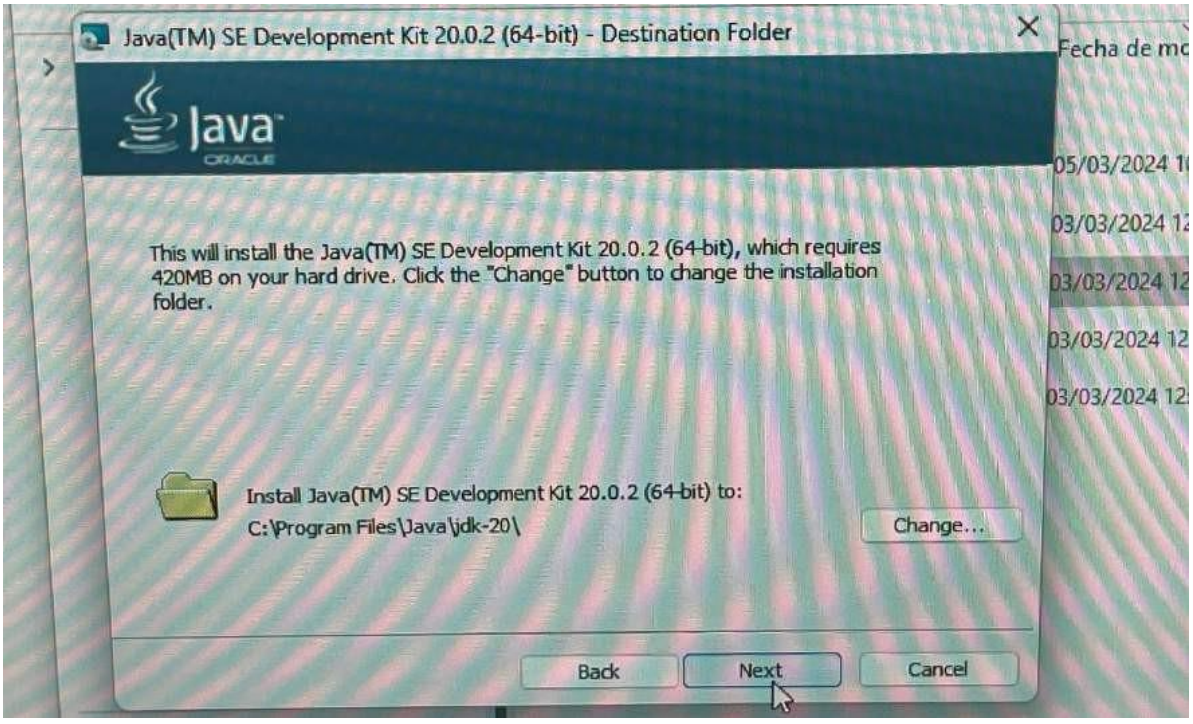


Figura 297 Instalación del JDK para NetBeans. Fuente: Elaboración propia. (propia., Instalación del JDK para NetBeans, 2024)

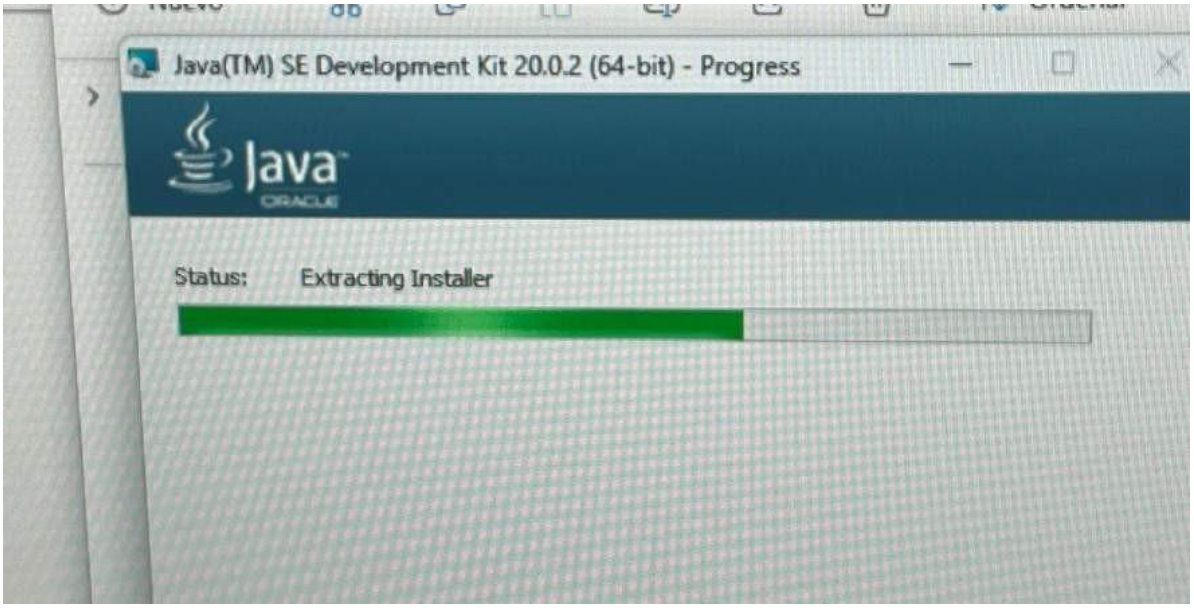


Figura 298 Instalación del JDK para NetBeans. Fuente: Elaboración propia. (propia., Instalación del JDK para NetBeans, 2024)

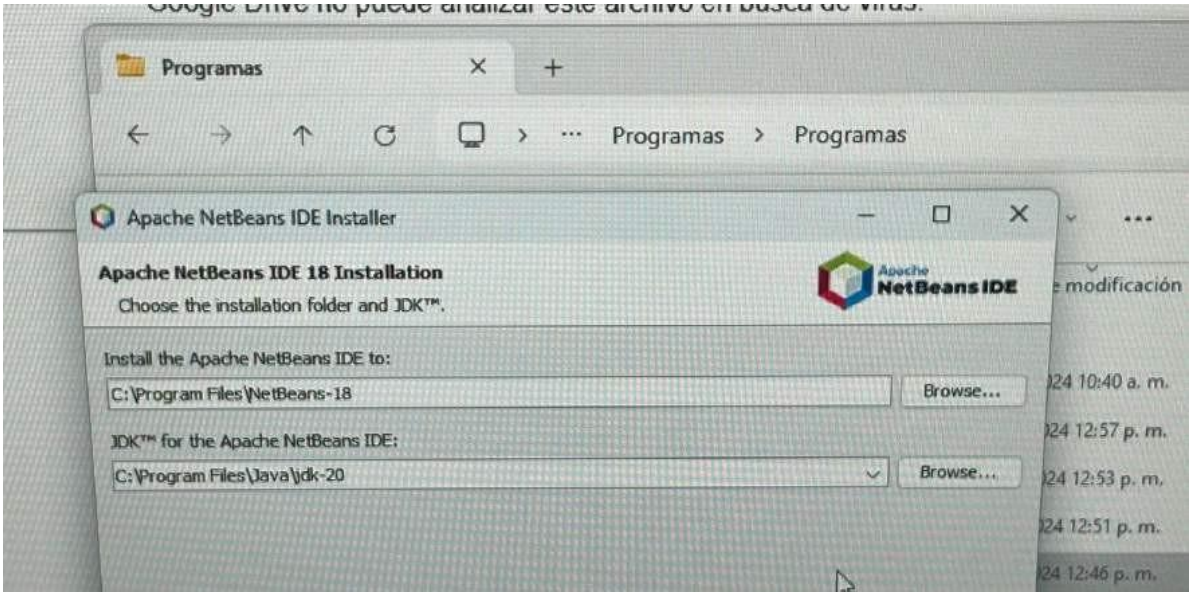


Figura 299 Instalación del lenguaje de programación Apache NetBeans. Fuente: Elaboración propia. (propia., Instalación del lenguaje de progrmación Apache NetBeans, 2024)

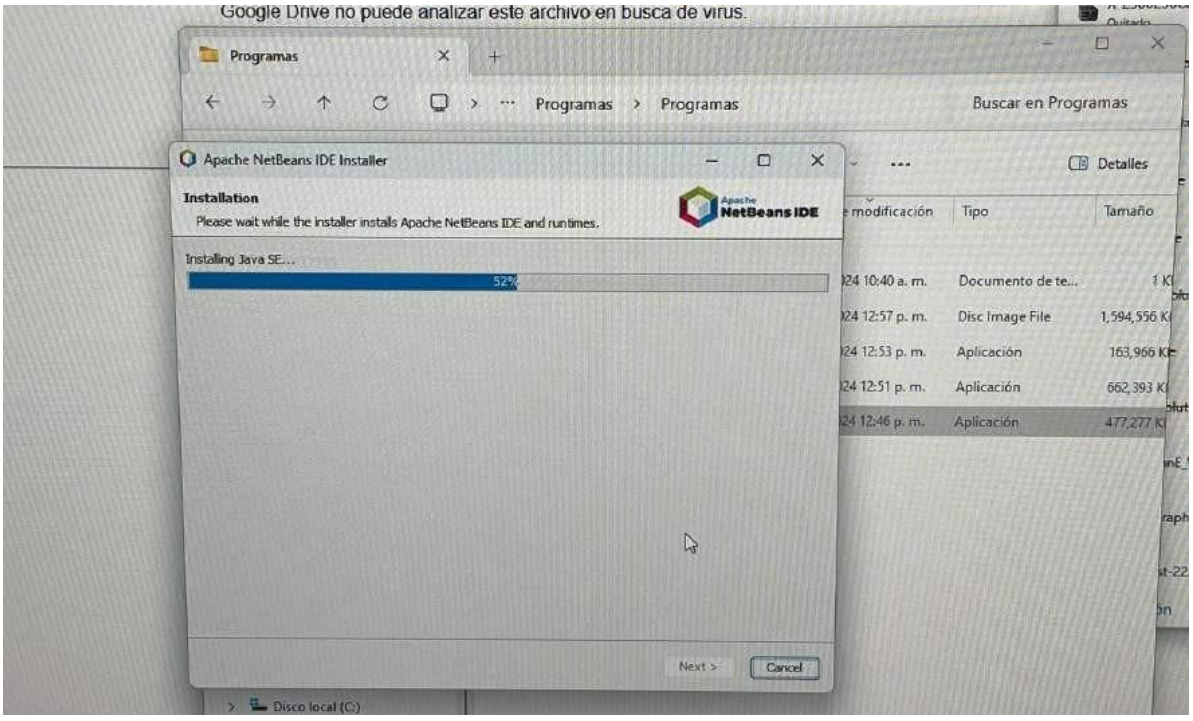


Figura 300 Instalación del JDK para NetBeans. Fuente: Elaboración propia. (propia., Instalación del JDK para NetBeans, 2024)



Figura 301 Instalación del Gestor de Base de Datos SQL Server. Fuente: Elaboración propia. (propia., Instalación del Gestor de Base de Datos SQL Server, 2024)



Figura 302 Instalación del Gestor de Base de Datos SQL Server. Fuente: Elaboración propia. (propia., Instalación del Gestor de Base de Datos SQL Server, 2024)

Después de instalar de manera correcta las herramientas es momento de instalar el sistema de inventario diseñado para la UTIC en la computadora principal del área. Esto se tuvo que realizar vía remota ya que el personal no contaba con espacios libres en el horario laboral por carga de trabajo, sin embargo, se logró correctamente y quedo implementado de la siguiente manera (revisar manual de usuario en el anexo 3).

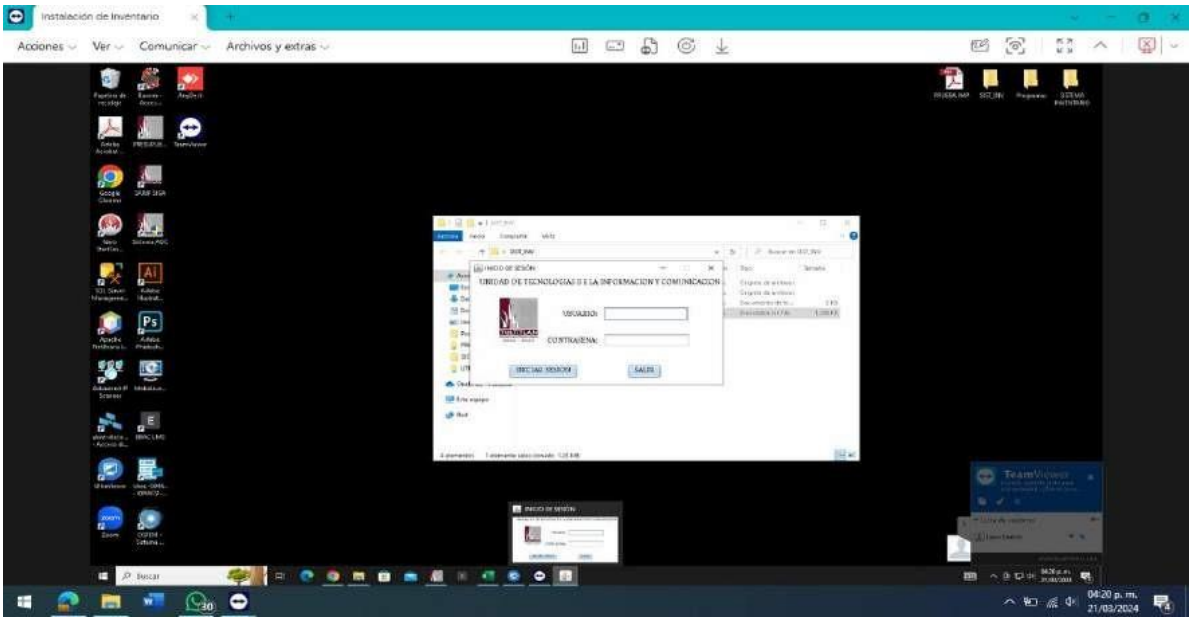


Figura 303 Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC. Fuente: Elaboración propia. (propia., Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC, 2024)

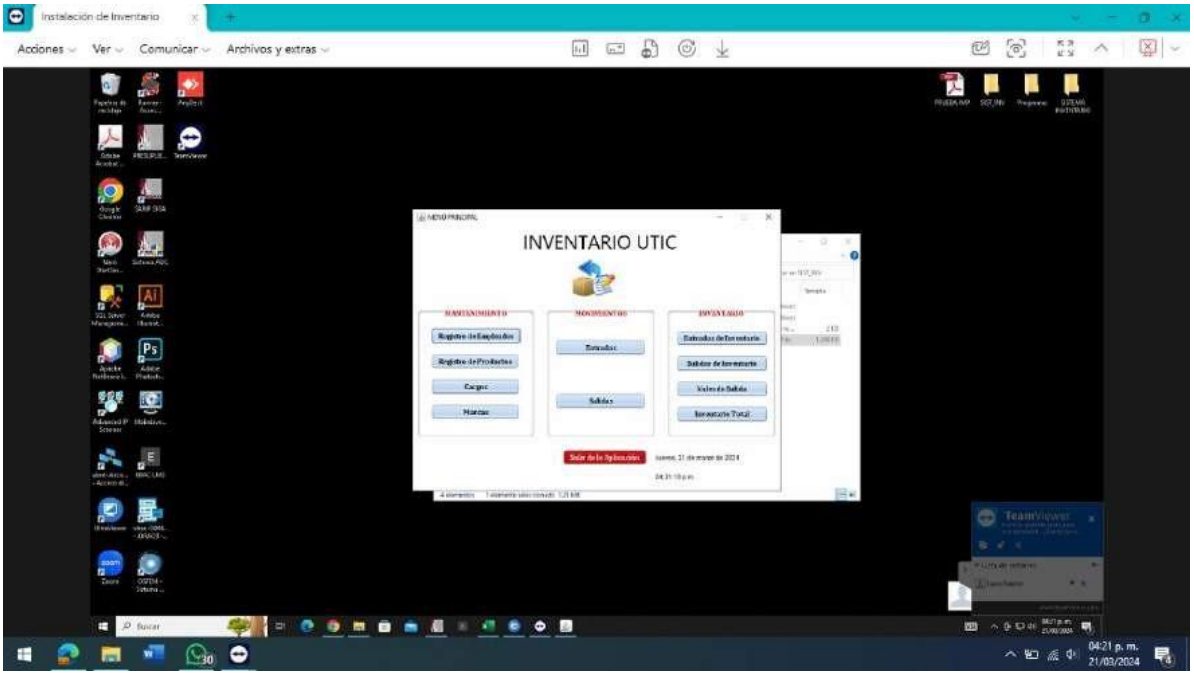


Figura 304 Interfaz Principal del Sistema de Inventario. Fuente: Elaboración propia. (propia., Interfaz Principal del Sistema de Inventario, 2024)

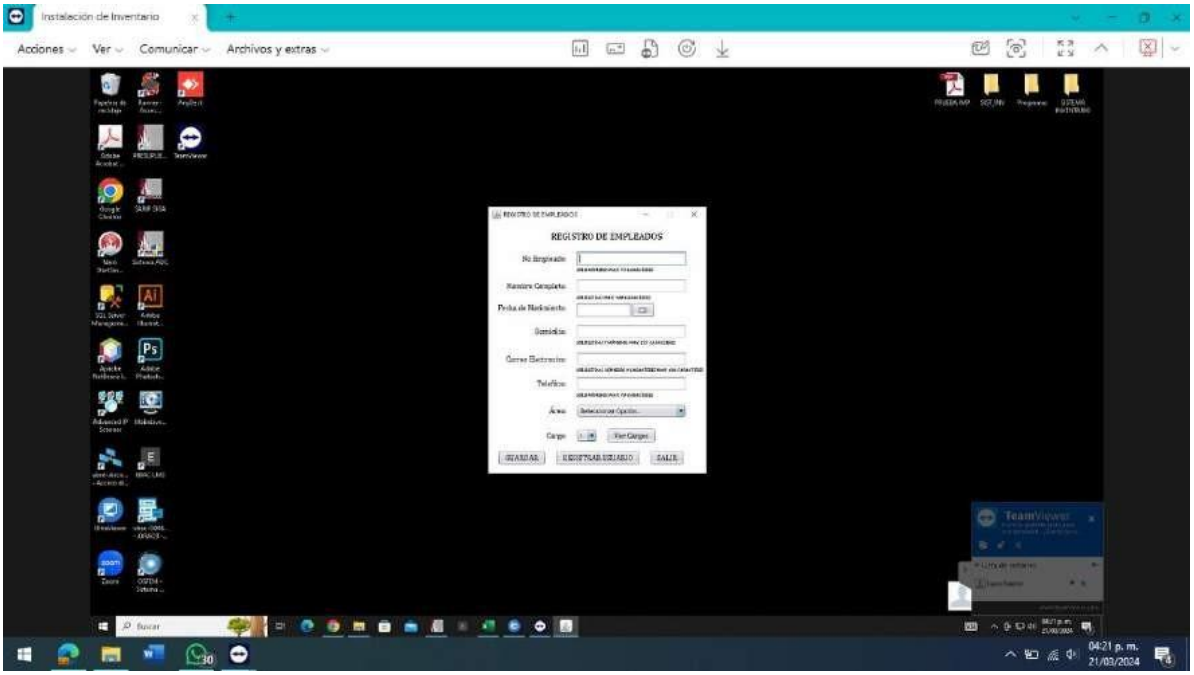


Figura 305 Interfaz de Registro de Empleados. Fuente: Elaboración propia. (propia., Interfaz de Registro de Empleados, 2024)

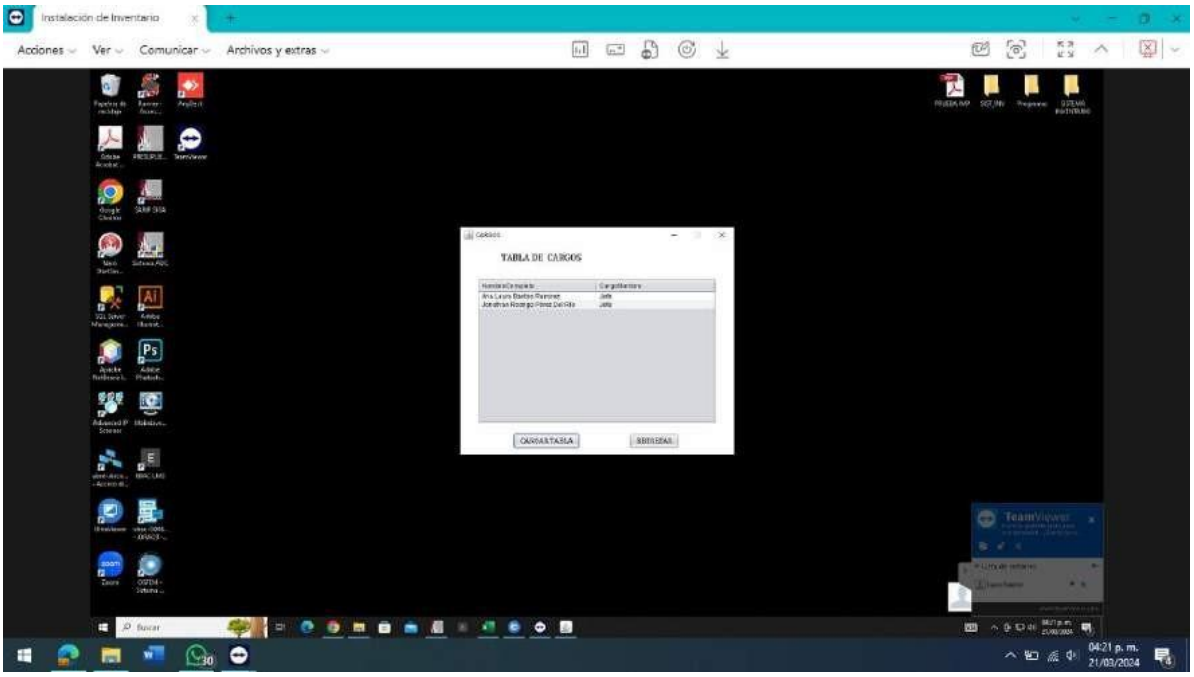


Figura 306 Interfaz de Cargos de los Empleados. Fuente: Elaboración propia. (propia., Interfaz de Cargos de los Empleados, 2024)

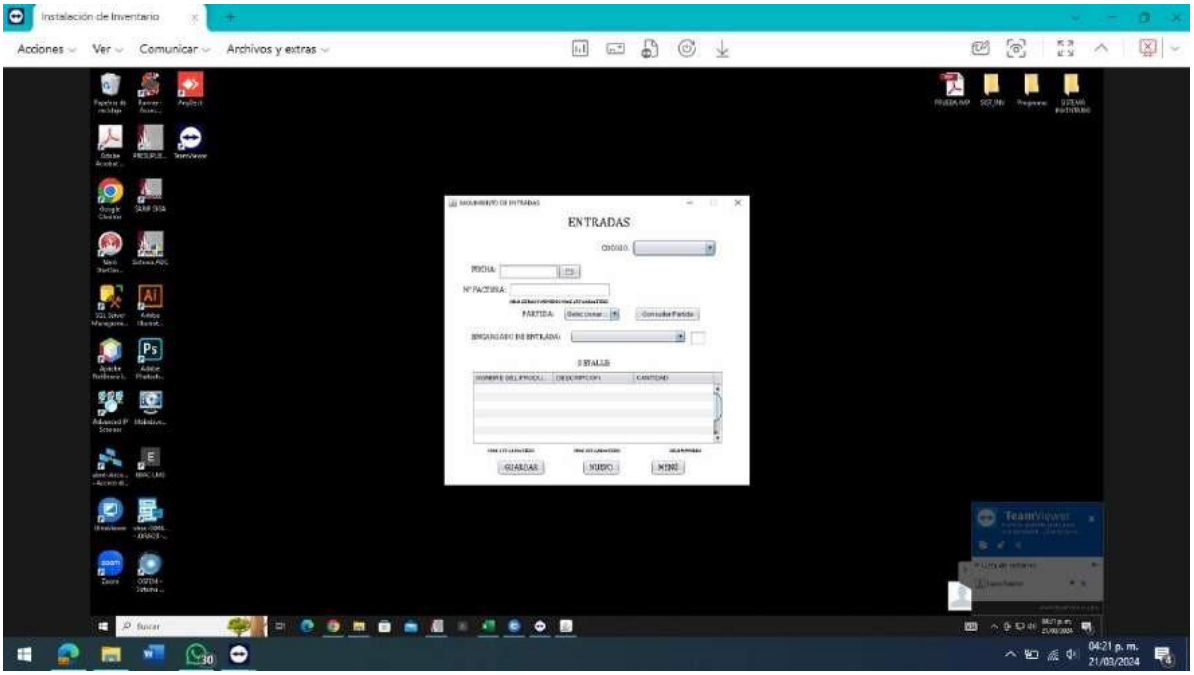


Figura 307 Interfaz de Registro de Entradas. Fuente: Elaboración propia. (propia., Interfaz de Registro de Entradas, 2024)

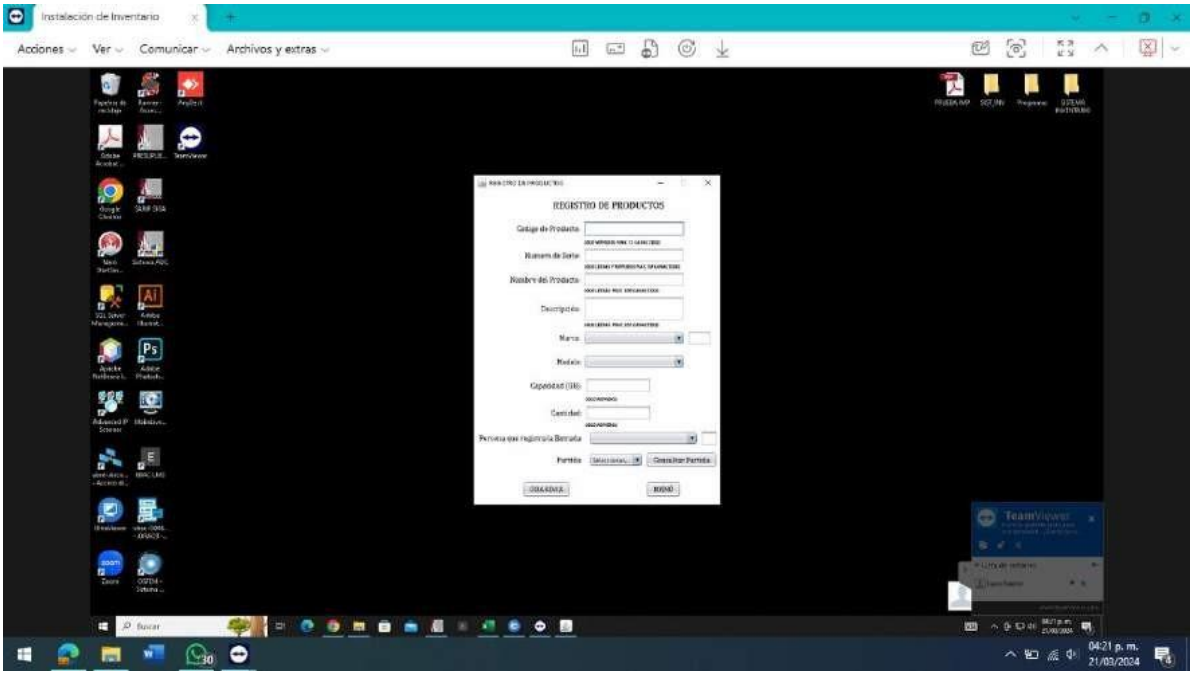


Figura 308 Interfaz de Registro de Productos. Fuente: Elaboración propia. (propia., Interfaz de Registro de Productos, 2024)

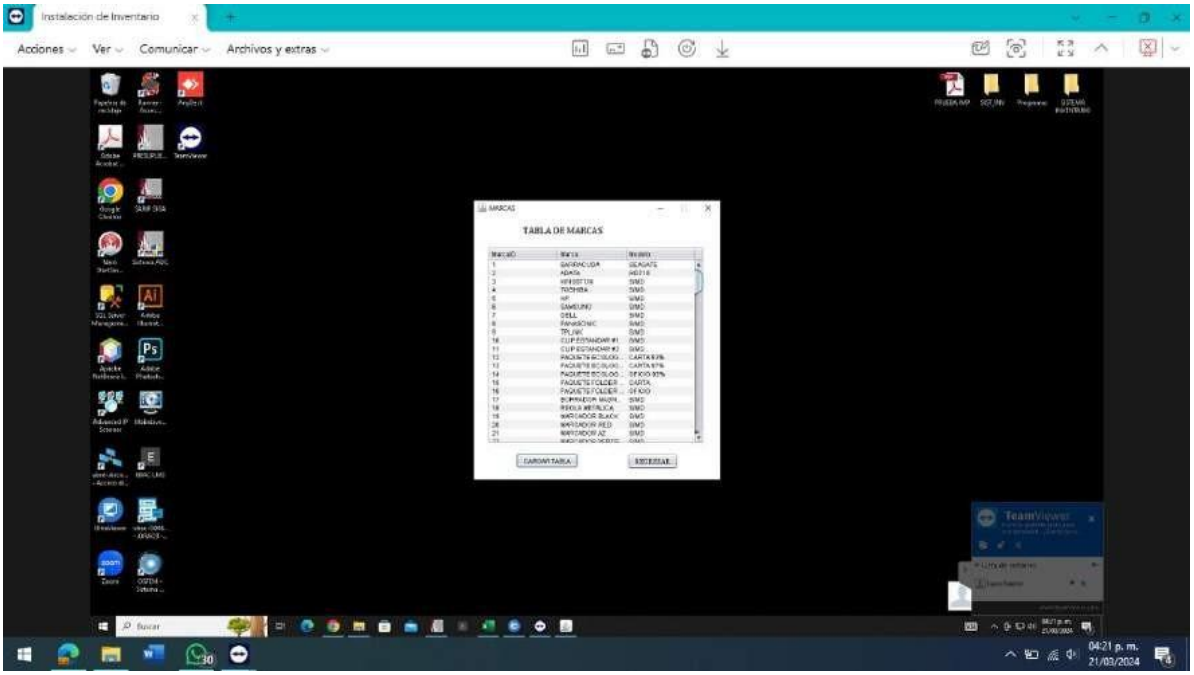


Figura 309 Interfaz de las Marcas manejadas de la UTIC. Fuente: Elaboración propia. (propia., Interfaz de las Marcas manejadas de la UTIC, 2024)

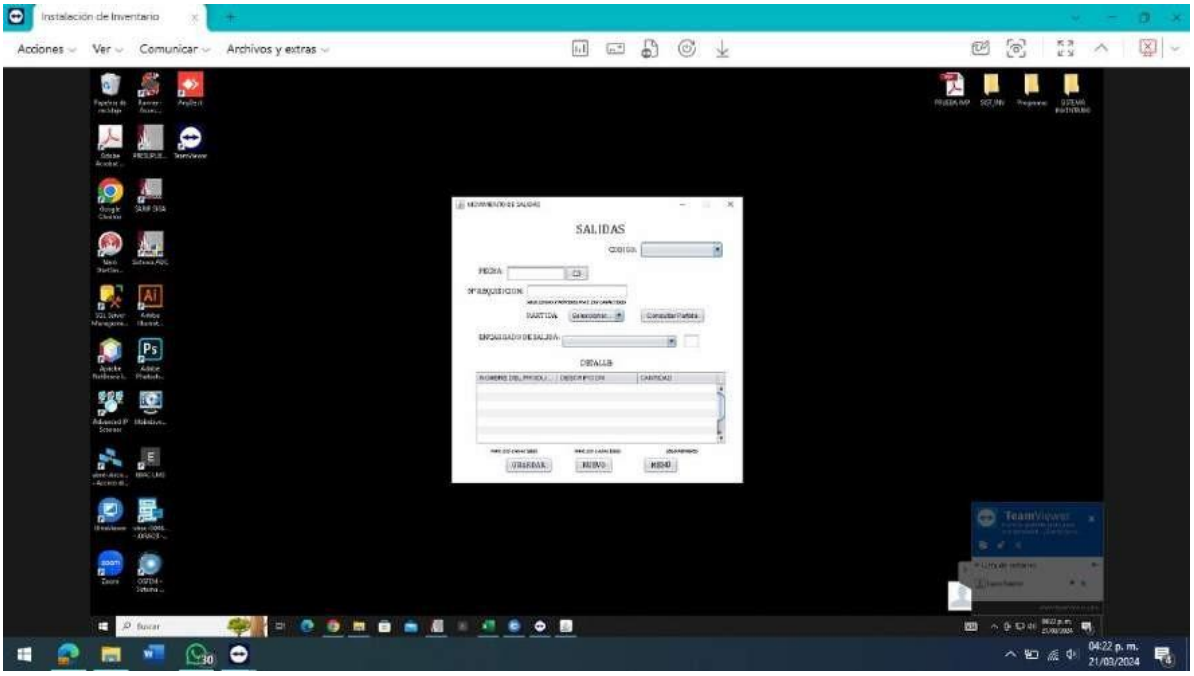


Figura 310 Interfaz de Registro de Salidas. Fuente: Elaboración propia. (propia., Interfaz de Registro de Salidas, 2024)

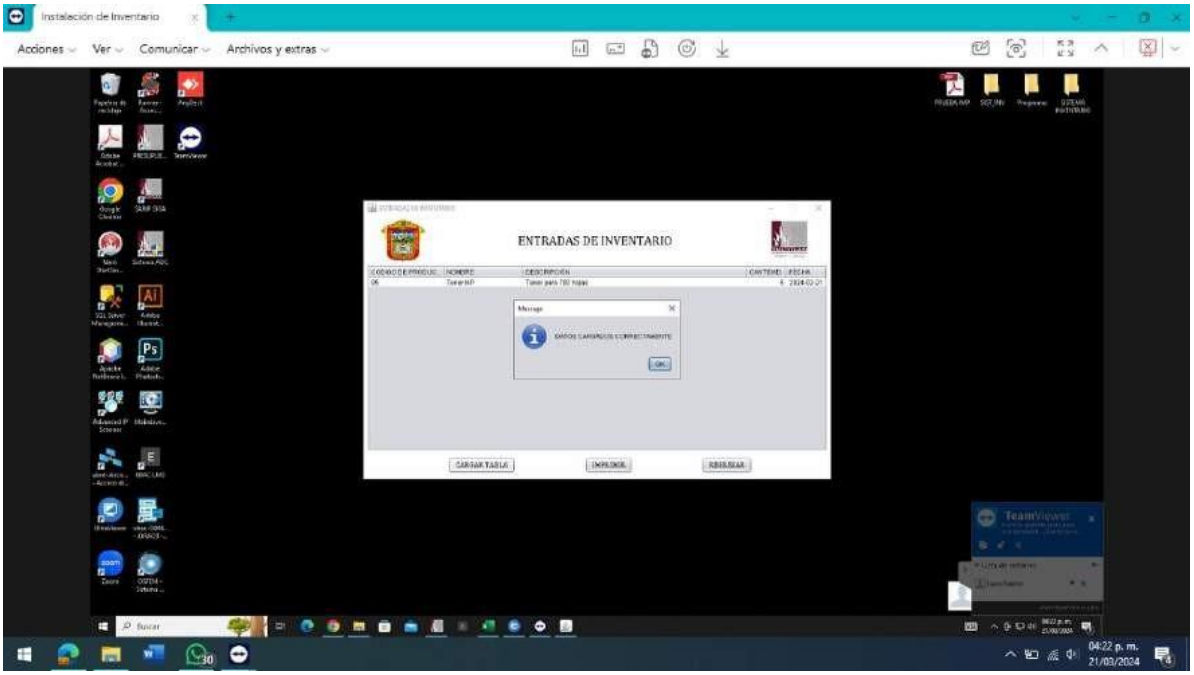


Figura 311 Interfaz de Consulta de las Entradas del Inventario. Fuente: Elaboración propia. (propia., Interfaz de Consulta de las Entradas del Inventario, 2024)

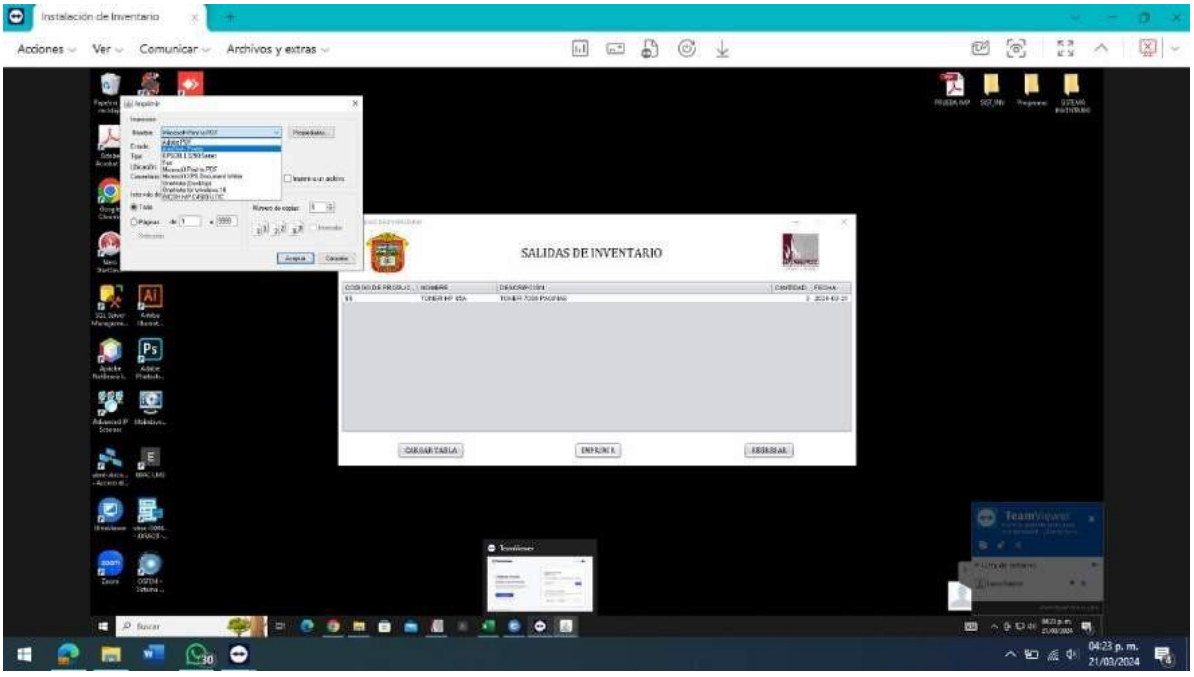


Figura 312 Interfaz de Consulta de las Salidas del Inventario. Fuente: Elaboración propia. (propia., Interfaz de Consulta de las Salidas del Inventario, 2024)

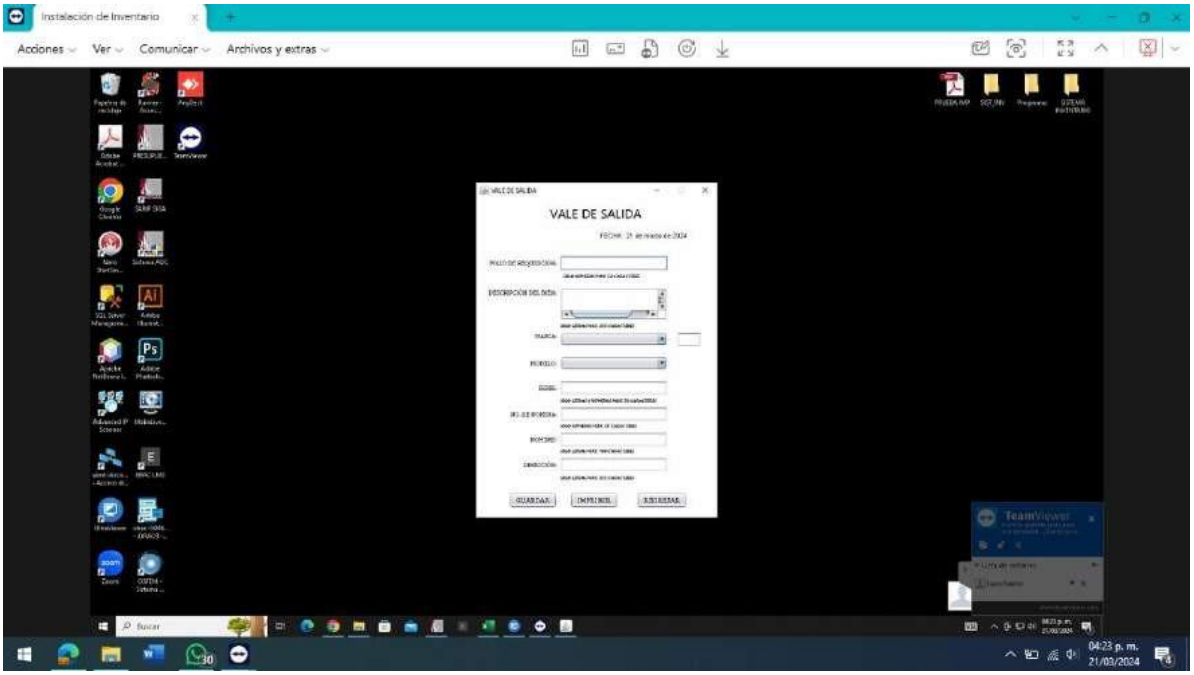


Figura 313 Interfaz del llenado del Vale de Salida. Fuente: Elaboración propia. (propia., Interfaz del llenado del Vale de Salida, 2024)

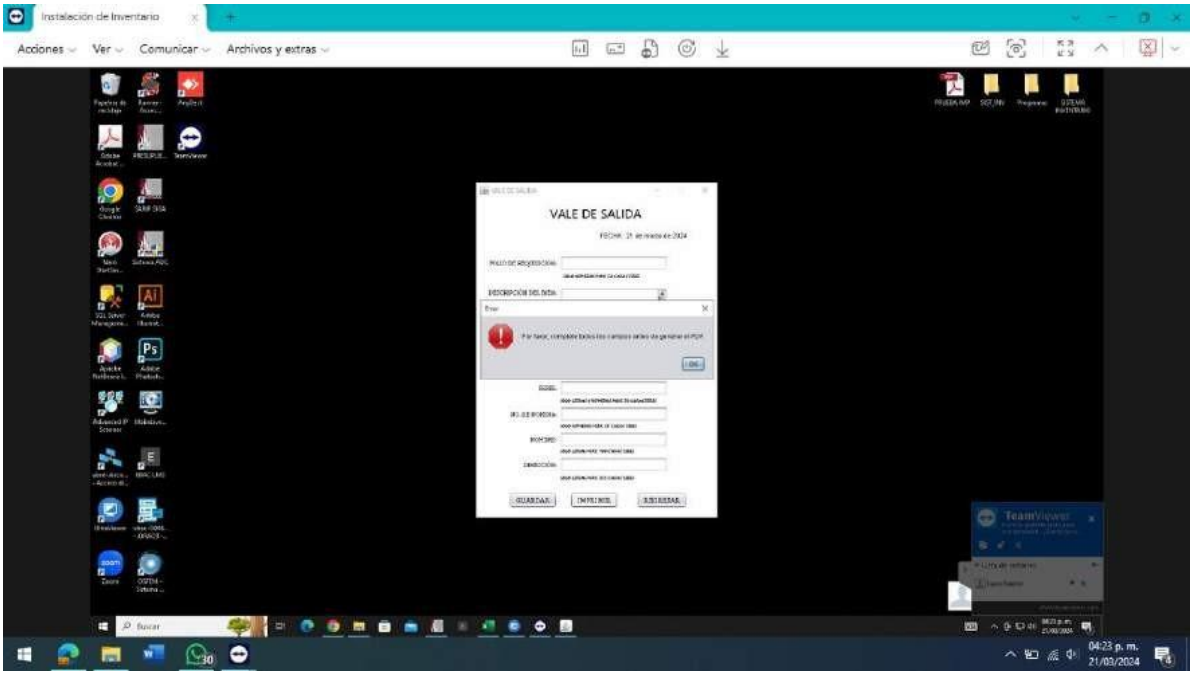


Figura 314 Mensaje de Advertencia si no se llena el Vale de Salida. Fuente: Elaboración propia. (propia., Mensaje de Advertencia si no se llena el Vale de Salida, 2024)

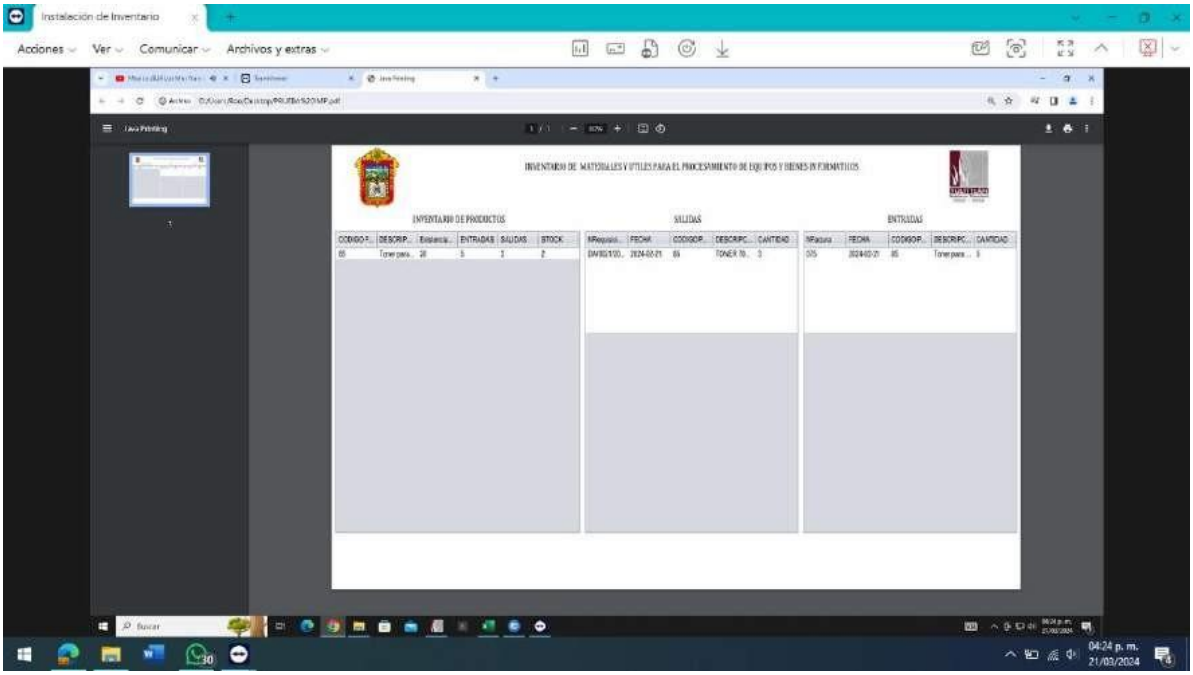


Figura 315 Vista preliminar de impresión del inventario total de la partida que se seleccione. Fuente: Elaboración propia. (propia., Vista preliminar de impresión del inventario total de la partida que se seleccione, 2024)

Vulnerabilidad Atendida enfocada al Sistema de Inventario

- El inventario con el que cuentan no está desarrollado en un sistema gestor de bases de datos.

Recomendación

- Migrar la información del inventario a un programa o software especializado o realizado a sus medidas y necesidades de la Unidad.
- Implementar sistema de inventario en conjunto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

Estrategia Implementada

Antes: Durante la inspección que se realizó a la UTIC, es notable el uso de un sistema de inventario en hojas de cálculo, el cual puede ser perjudicial para sus actividades al paso del tiempo, pues al usar archivos de Excel editables todos tienen acceso a ellos para la manipulación de la información y los datos que este contiene.

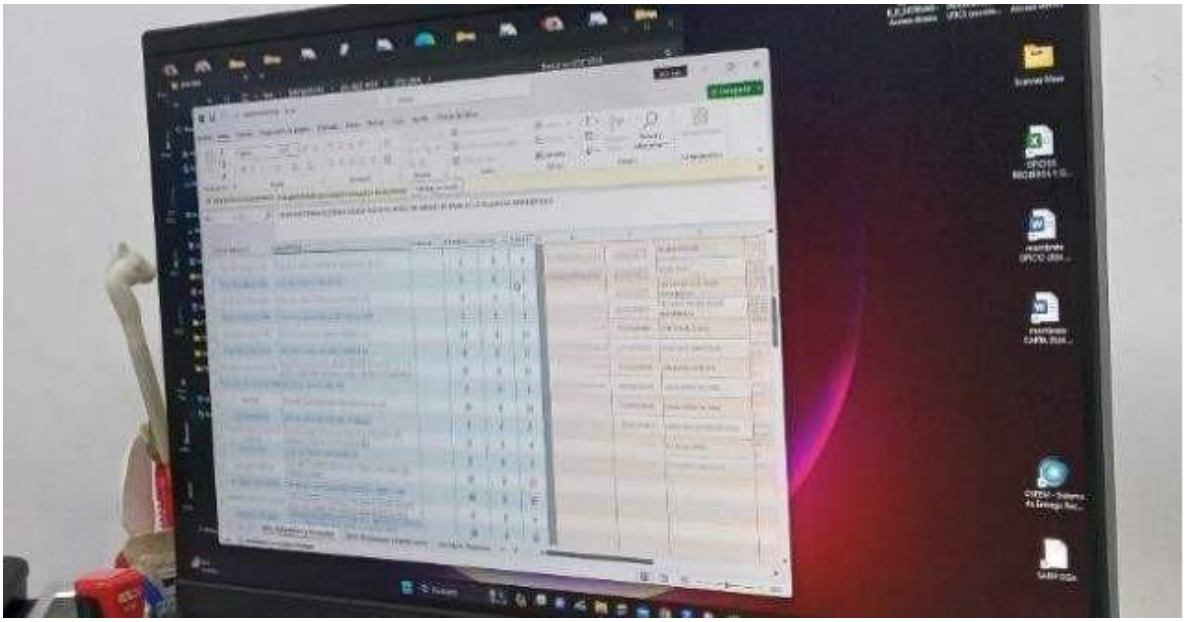


Figura 316 Inventario de la UTIC en hojas de cálculo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Inventario de la UTIC en hojas de cálculo, 2023)

Después: Se migro el sistema de inventario con el que trabajan a uno diseñados debidamente, programado y usando un sistema gestor de bases de datos en este caso (SQL Server) ya que tienen conocimiento previo en el uso de ese SGDB, por lo que ahora pueden editar el código y la base de datos de acuerdo con las necesidades o actualizaciones que vayan teniendo.

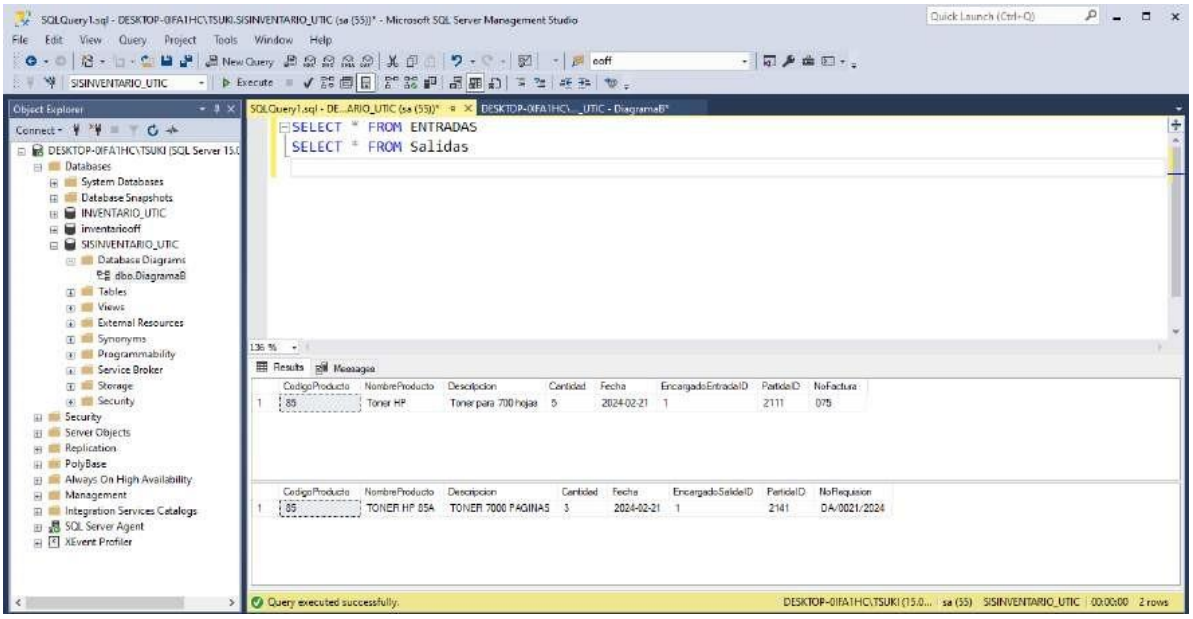


Figura 317 Consulta directa en la Base de Datos. Fuente: SQL Server. (Server., Consulta directa en la Base de Datos, 2024)

Vulnerabilidad Atendida enfocada al Sistema de Inventario

- Todos los usuarios internos de la UTIC pueden editar la información dentro del inventario ya que no cuentan con roles ni privilegios de acuerdo con su puesto.

Recomendación

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Establecer roles de usuario en el sistema de gestión de activos que reflejen los roles y responsabilidades de las personas dentro de la UTIC.
- Facilitar la identificación de activos en el ciclo de vida de la información a través del software.
- Implementar funcionalidades en el software que permitan la asignación de propiedad y clasificación para cada activo identificado.
- Proporcionar capacitación a los usuarios sobre el uso adecuado del software y los roles de privilegio asignados.

Estrategia Implementada

Antes: Durante la inspección que se realizó el sistema que usan con el rol de inventario dentro de UTIC se puede observar que no cuentan con roles ni privilegios, lo que permite que todos los usuarios puedan manipular la información sin restricción alguna, lo que es un riesgo pues no todos están capacitados o bien cuentan con el consentimiento para llegar a eliminar información, como se usan hojas de cálculo simulando el rol de inventario se anexa evidencia de la secuencia que se sigue sobre como acceder a la información.

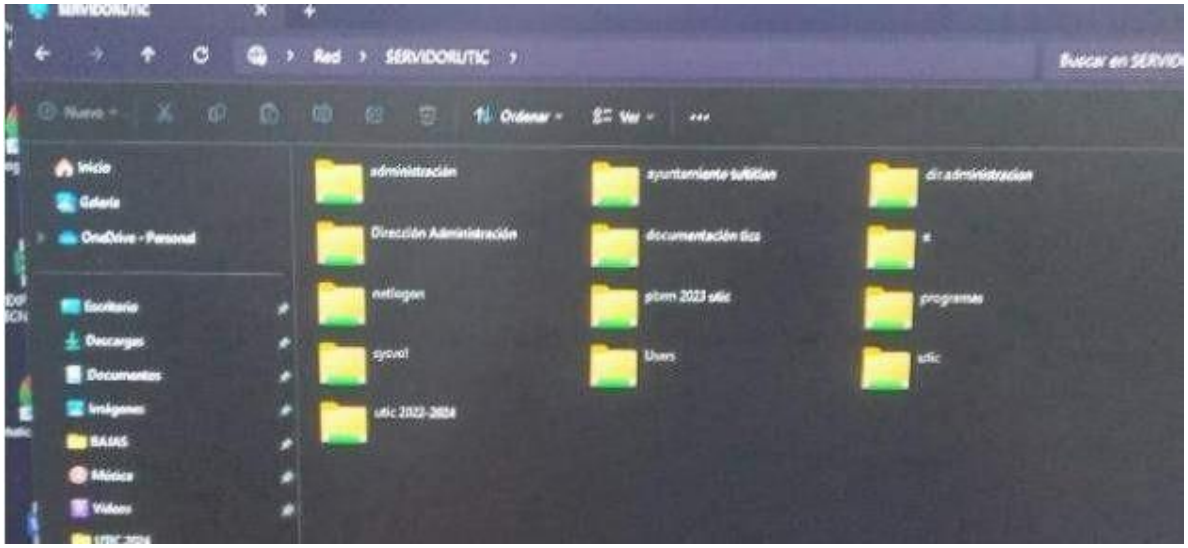


Figura 318 Carpetas en red donde se encuentra el inventario. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Carpetas en Red, 2023)

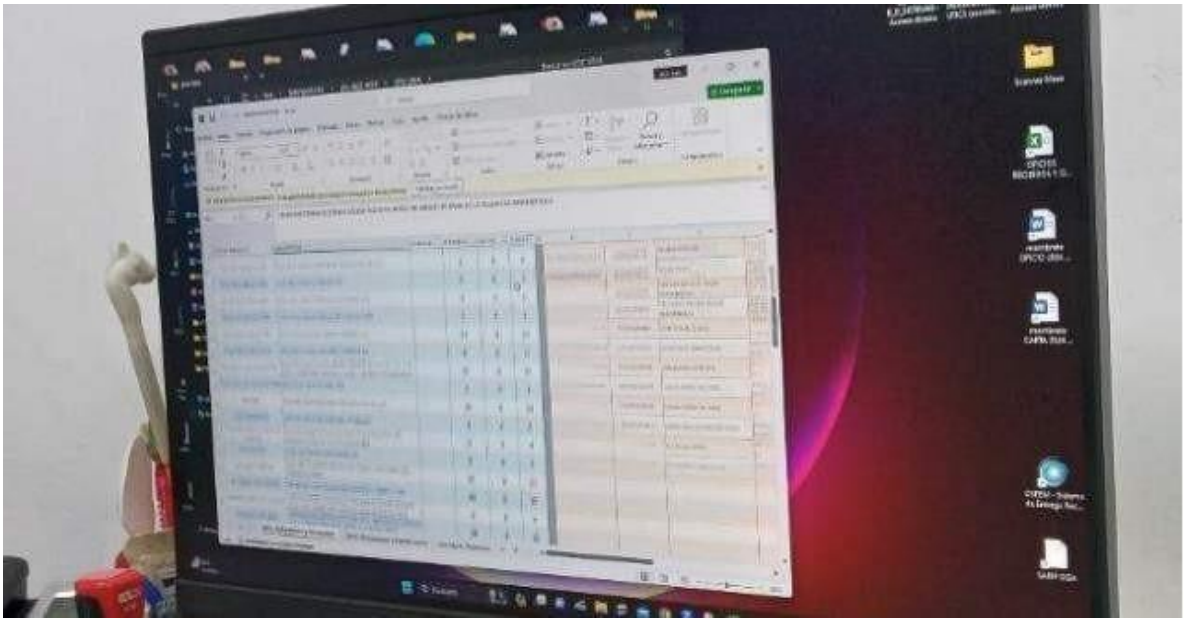


Figura 319 Inventario de la UTIC en hojas de cálculo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Inventario de la UTIC en hojas de cálculo, 2023)

Después: Una vez implementado el sistema de inventario, se les muestra a los empleados que a partir de ahora habrá un inicio de sesión para acceder a la información además de roles y con ellos privilegios sobre las acciones que podrán realizar de acuerdo con su puesto, se les asignación sus usuarios y contraseñas seguras temporales, así como una breve capacitación sobre cómo usar el sistema nuevo.



Figura 320 Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC. Fuente: Elaboración propia. (propia., Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC, 2024)

Vulnerabilidad Atendida enfocada al Sistema de Inventario

- Para la consulta de las distintas categorías de activos disponibles, deben acceder a diferentes archivos individuales para realizar consultas.

Recomendación

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Implementar sistema de inventario en conjunto con un Sistema Gestor de Base de Datos como lo puede ser SQL Server.

Estrategia Implementada

Antes: Durante la inspección que se realizó el sistema que usan con el rol de inventario dentro de UTIC se puede observar que no cuentan con un sistema que integre todos los datos, categorías, archivos, etc. En uno solo, pues al usar hojas de cálculo en Excel deben estar cambiando de página o archivo según sea la manipulación que requieran hacer y la categoría en donde se debe realizar.

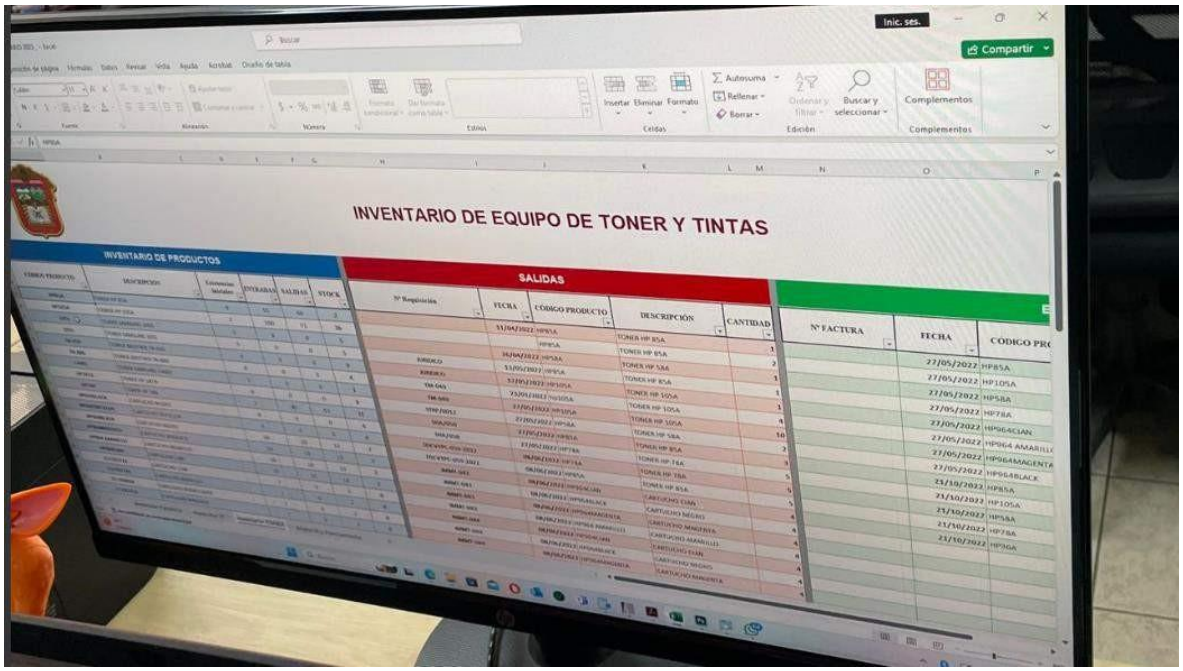


Figura 321 Inventario de la UTIC en hojas de cálculo. Fuente: Unidad de Tecnologías de la Información y Comunicación. (Comunicación. U. d., Inventario de la UTIC en hojas de cálculo, 2023)

Después: Luego de desarrollar el sistema de inventario que permite la creación y mantenimiento del de la información que manejan internamente, se logra emplear uno desarrollado en un sistema gestor de bases de datos el cual permite mediante tablas, y relación entre ellas que toda la información manejada se mantenga en un solo sistema manejando diferentes archivos y formatos.



Figura 322 Interfaz Principal del Sistema de Inventario. Fuente: Elaboración propia. (propia., Interfaz Principal del Sistema de Inventario, 2024)

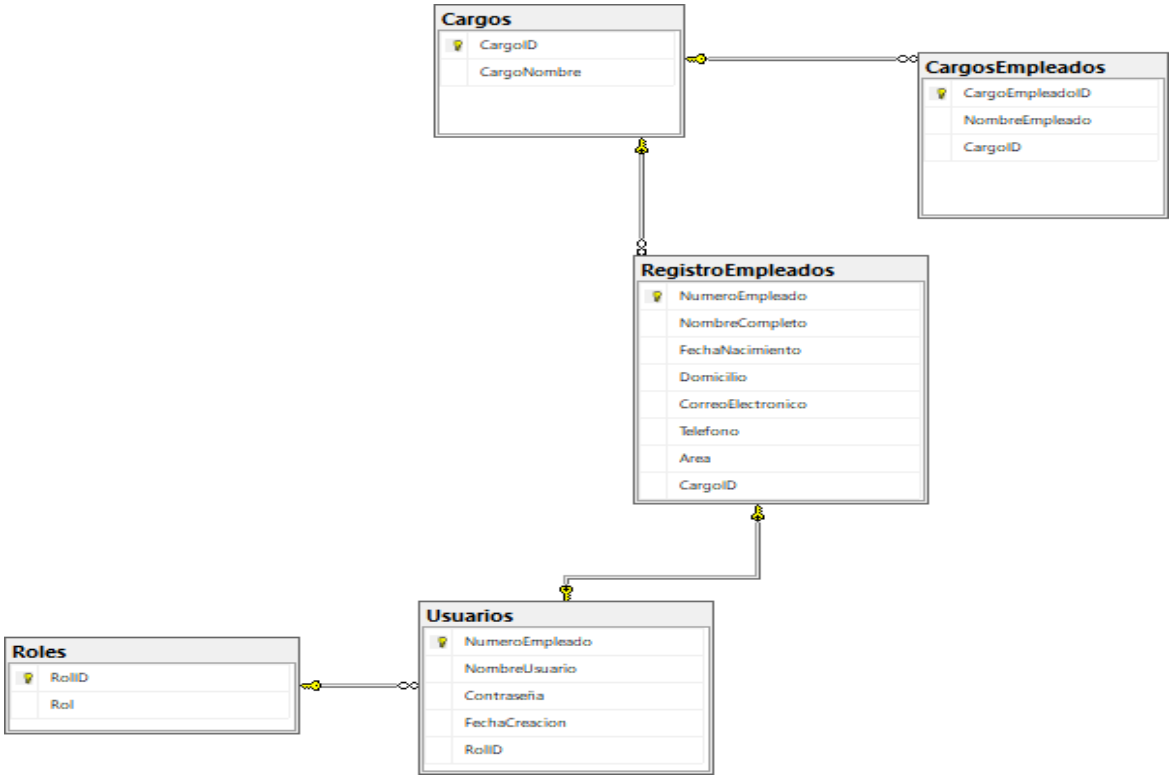


Figura 323 Tablas de la base de datos. Fuente: SQL Server. (Server., Tablas de la base de datos, 2024)

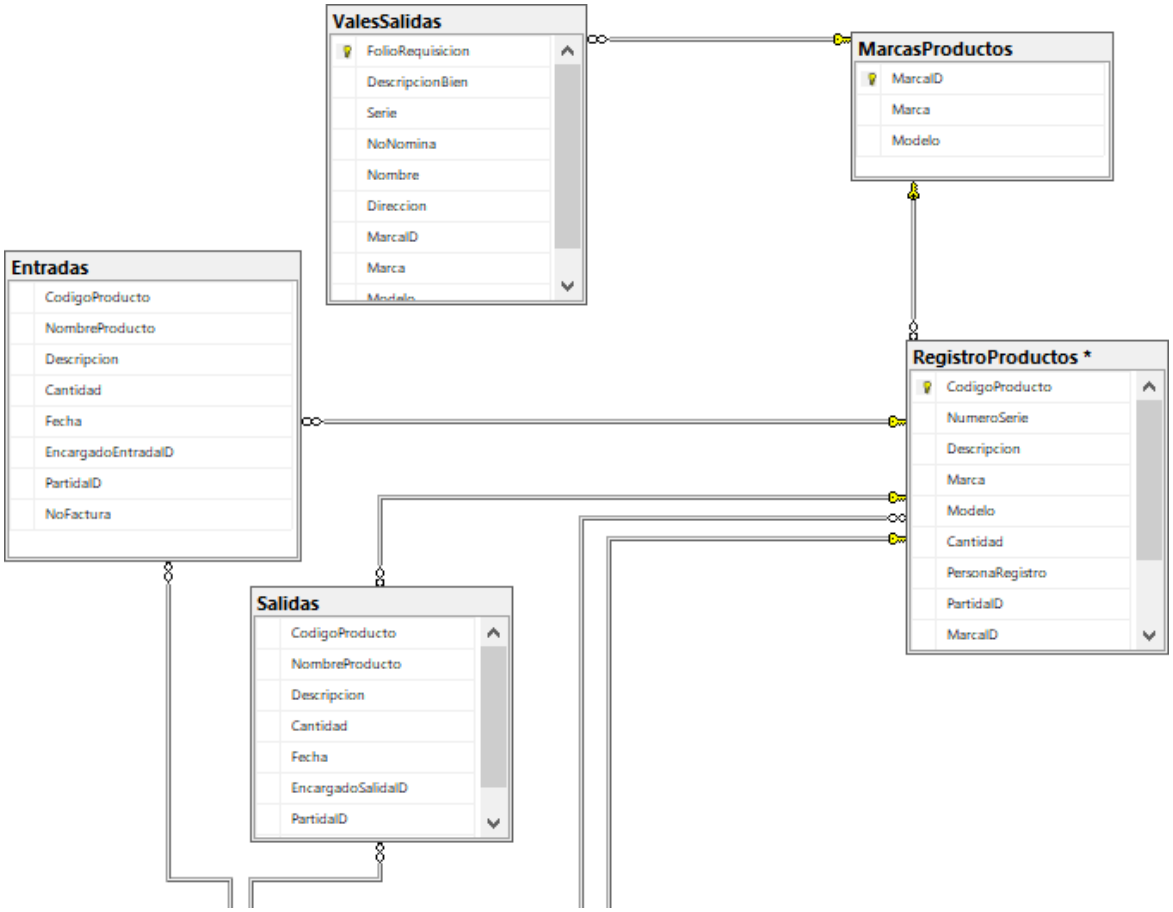


Figura 324 Tablas de la base de datos. Fuente: SQL Server. (Server., Tablas de la base de datos, 2024)



Figura 325 Tablas de la base de datos. Fuente: Sql Server. (Server., Tablas de la base de datos, 2024)

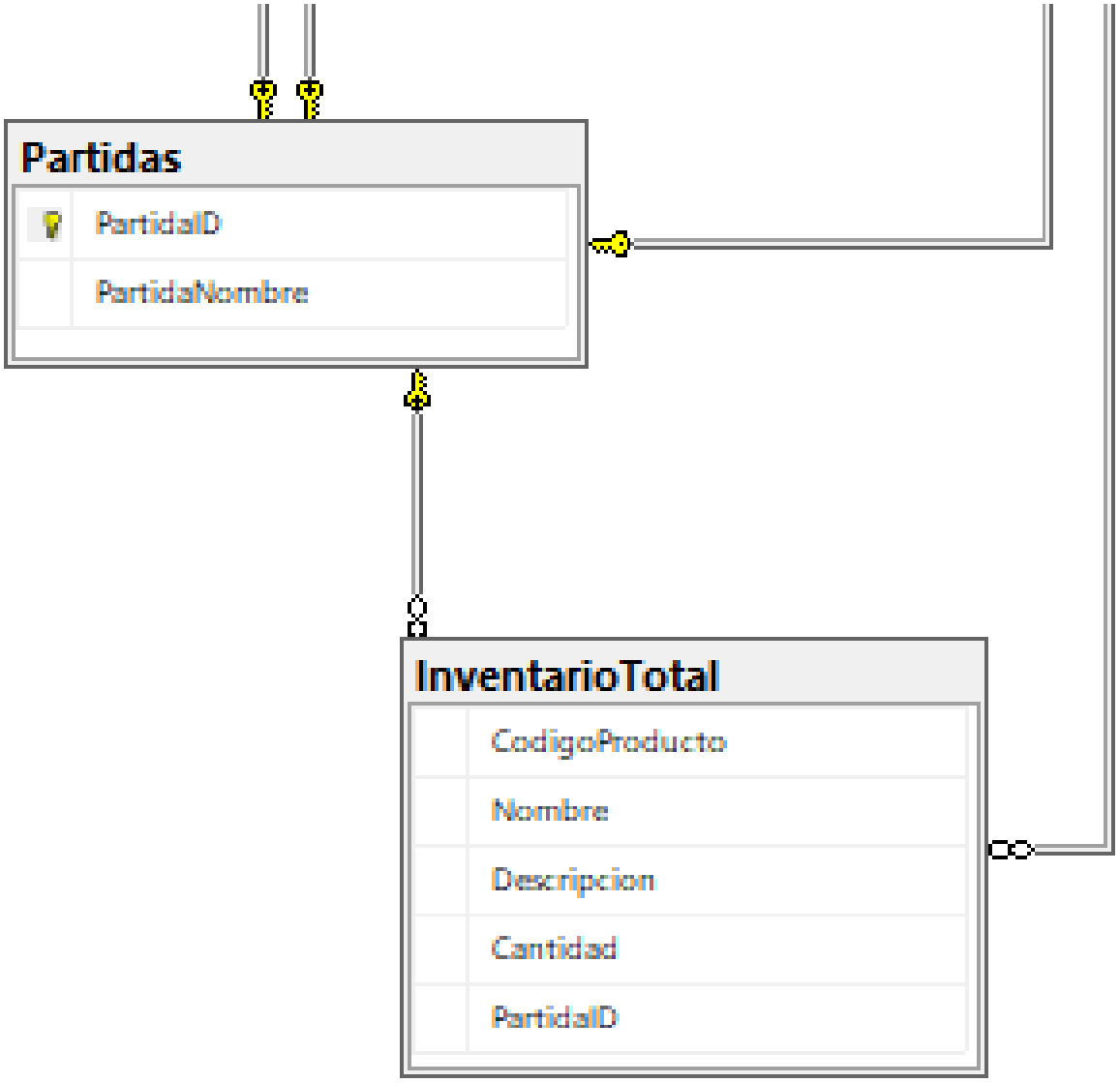


Figura 326 Tablas de la base de datos. Fuente: Sql Server. (Server., Tablas de la base de datos, 2024)

Vulnerabilidad Atendida enfocada al Sistema de Inventario

- El inventario empleado actualmente no cuenta con seguridad alguna, rol de usuarios ni contraseñas para acceder al mismo.
- El sistema no cuenta con ninguna medida de seguridad.
- Ausencia de usuarios y contraseñas para restringir el acceso a usuarios externos.

Recomendación

- Utilizar un sistema de gestión de activos que permita la creación y mantenimiento de un inventario de activos de información.
- Implementar un Inicio de sesión que restrinja el acceso a las diferentes funciones de pudiera llegar a tener este acorde a el rol, ocupación y tareas de cada empleado.
- Agregar estrategias de seguridad de la información que puedan ser útiles de acuerdo con el desarrollo de sus actividades y al manejo de la información en el sistema de inventario.

Estrategia Implementada

Antes: Durante la inspección que se realizó el sistema que usan con el rol de inventario dentro de UTIC se concluye que no cuenta con ninguna medida de seguridad, lo cual deja al descubierto la información y los datos que hay dentro del este, es decir no posee roles, ni privilegios, usuarios ni un control de acceso, por lo que es importante atender estas deficiencias, como son hojas de cálculo en Excel y en las vulnerabilidades anteriores ya se ha anexado evidencia de que no cuentan con seguridad alguna y el proceso para acceder a la información, no se anexa nuevamente evidencia ya que son los mismos procesos y se refleja lo mencionado en esta.

Después: Con el nuevo sistema de inventario implementado se puede observar que hay un acceso controlado de los usuarios pues solicita sus datos de empleado para acceder (usuario y contraseña), además cuenta con roles y privilegios, cabe mencionar que como estrategias para aun la seguridad de la información de acuerdo con sus actividades se implementó el no repudio dentro del sistema y condicionales para evitar que inserten datos si algún campo está vacío.



Figura 327 Interfaz de Consulta de las Entradas del Inventario. Fuente: Elaboración propia. (propia., Interfaz de Consulta de las Entradas del Inventario, 2024)

CONCLUSIONES

De acuerdo con los objetivos estipulados desde el comienzo del presente trabajo se consideró como el primero “planificar la Auditoría” el cual se cumple satisfactoriamente ya que se inició diseñando un plan de trabajo, el cual se proporcionó y se platicó con la UTIC para esclarecer los detalles de la forma en la que se planeaba trabajar, los tiempos, las herramientas o estrategias que se tenían en mente para poder indagar a cerca de la situación inicial de la dependencia. El segundo objetivo y el más extenso era “Ejecutar la Auditoría”, en este apartado se diseñaron formatos para recabar información sobre los puntos de interés y la situación actual en los procesos de la UTIC dando como resultado una notable carencia de estrategias entre ellas para la protección de la información principalmente, la protección de los equipos, la eficacia de los servicios y el uso de un sistema de inventario deficiente, por lo que realizadas cada una de las pruebas para inspeccionar apartados específicos de acuerdo a cada uno de los puntos mencionados, se obtuvieron las vulnerabilidades, posibles escenarios a los que están expuestos como centro de trabajo y las recomendaciones basadas en las normas y estándares citados en base al campo de estudio que se inspecciona, con la intención de que se sigan los parámetros que estipula cada estándar o bien tomen en cuenta las recomendaciones diseñadas bajo dichos parámetros.

Como último objetivo se tiene “entregar resultados” este objetivo es uno de los más importantes, ya que se debe analizar todo lo obtenido en el objetivo anterior para poder buscar soluciones ante las problemáticas que se presentan dentro de la UTIC, sin embargo, aun así se logra completar correctamente, ya que para la fácil consulta de los usuarios se optó por una opción que contenga todos los datos críticos de las pruebas, es decir la realización de un informe ejecutivo el cual de manera precisa y clara concentra las vulnerabilidades presentes, los escenarios que implican, las recomendaciones de los estándares pero al mismo tiempo las recomendaciones diseñadas en base a las normas y estándares para poder realizar cambio y evitar o prevenir problemáticas o eventos desafortunados, además de la elaboración de un apartado en donde se pueden apreciar las estrategias implementadas y los cambios que tare consigo una vez funcionando dentro de la UTIC.

COMPETENCIAS DESARROLLADAS

Las siguientes competencias Generales y específicas de la especialidad en Auditoría y Seguridad en Aplicaciones, con las consideradas como puestas en práctica y desarrolladas con éxito durante el desarrollo del presente trabajo, ordenadas de acuerdo con la asignatura en la que tienen relevancia y con una pequeña descripción de cómo es que se desarrolló.

Tabla 77 Competencias Desarrolladas. Fuente Temario.

Materia	Competencia.
Fundamentos de Base de Datos:	• Analiza requerimientos y diseña bases de datos para generar soluciones al tratamiento de información basándose en modelos y estándares.
Implementación: Se analizan las especificaciones que la dependencia argumenta de acuerdo con sus necesidades por lo que se genera una solución enfocada a una base de datos que almacena y permite manejar la información que controlan de una manera mucho más ágil.	
Taller de base de datos:	• Implementa bases de datos para apoyar la toma de decisiones considerando las reglas de negocio.
Implementación: Se deja implementada una base de datos para cumplir con el rol de un inventario, de la mano de un sistema diseñado de acuerdo con las especificaciones brindadas por la dependencia, gracias al conocimiento en gestores de bases de datos previo dentro del plan de estudios.	

Tabla 77 (continuación)

Administración de Base de Datos:	• Instala, configura y administra un gestor de base de datos para el manejo de la información de una organización, optimizando la infraestructura computacional existente.
Implementación: Una vez diseñada la base de datos y debidamente instalada se diseña un manual de usuario donde se especifica como administrarla para que los usuarios no tengan inconvenientes con su función.	
Tópicos Avanzados de Programación:	• Desarrolla soluciones de software para resolver problemas en diversos contextos utilizando programación concurrente, acceso a datos, que soporten interfaz gráfica de usuario y consideren dispositivos móviles.
Implementación: Se diseña el sistema de inventario conectado a una base de datos, construyendo interfaces graficas para una experiencia más dinamina y visual además de intuitiva, instalado en distintos dispositivos de cómputo dentro de la dependencia.	
Taller de investigación I:	• Elabora un protocolo de investigación en el que presenta soluciones científico - tecnológicas a problemáticas relacionadas con su campo profesional en diversos contextos.
Implementación: Se realiza una investigación previa sobre la situación actual de la dependencia en donde como resultado surgen vulnerabilidades y problemáticas internas, para ello se desarrollan soluciones y estrategias que atiendan dichas debilidades, siempre basadas y con la perspectiva de un ingeniero en sistemas computacionales.	

Tabla 77 (continuación)

Taller de investigación II:	Consolida el protocolo para ejecutar la investigación y obtener productos para su exposición, defensa y gestión de su transcendencia.
Implementación: Después de la investigación y el diseño de las estrategias que solucionen las problemáticas internas, se ejecutan pruebas y métodos que ayudan a la obtención de resultados, los cuales ayudan a entender mejor el funcionamiento interno y la percepción de antes y después de la implementación.	
Toma de Decisiones:	Conocer la importancia que tiene la toma de las decisiones como una alternativa en la solución de problemas del mundo real, las técnicas que existen para su manejo y herramientas que apoyan el diseño de estos modelos.
Implementación: Una vez identificadas las vulnerabilidades internas, se diseñan estrategias que las atiendan, pero se requiere tomar la mejor decisión o bien aquella que sea más efectiva y funcional, ya que el propósito es optimizar y aumentar el nivel en conjunto de la dependencia.	

Tabla 77 (continuación)

Legislación Informática:	• Identifica los principales conceptos sobre el derecho aplicados al ámbito informático. • Analiza los distintos lineamientos sobre regímenes y legislaciones para aplicar el derecho informático en el ámbito nacional como internacional. • Conoce los procedimientos para legalizar y registrar un software. • Reconoce los procesos e implicaciones para el registro del derecho de autor. • Analiza el contenido de los contratos informáticos y reconoce los puntos clausulares de los mismos. • Conoce las responsabilidades jurídicas de las acciones ilegales al manipular los dispositivos informáticos a su cargo. • Conoce y analiza los derechos que le son aplicables en situaciones reales al estar dentro del campo laboral.
Implementación: Es necesario conocer derechos, lineamientos jurídicos al realizar el desarrollo de una sistema, pues cuando es realizado para una dependencia nunca se sabe si esta hará un uso simplemente interno o lo compartirá, en caso de esto es necesario registrarlo para evitar un mal uso u alteración, además de conocer las partes de un contrato, o bien acuerdos, en este caso se diseñaron distintos documentos que respaldan la implementación de distintas estrategias, cada uno de ellos respaldados por la firma y aprobación del personal interno para el departamento al cual se diseñaron.	

Tabla 77 (continuación)

Administración y Seguridad en Aplicaciones:	• Establece políticas y normas para su uso antes, durante y después de alguna amenaza a los sistemas de información. • Conoce las normas, marcos y estándares utilizados para la auditoría informática. • Identifica los principios de control interno y su relación con la auditoría informática. • Conoce las propiedades ACID en las bases de datos. • Identifica conceptos básicos de Sistemas de Información con bases de datos. • Implementa perfiles de usuario para acceso a un servidor de base de datos.
Implementación: Una de las problemáticas internas de la dependencia donde se realizó dicho proyecto es la falta de reglas y políticas internas, por lo que se diseñaron para un mejor uso de activos y comportamiento de los empleados internos, de igual forma se implementaron recomendaciones en base a normas ISO, en el desarrollo de la base de datos y el sistema de inventario se tuvo en cuenta las propiedades ACID (atomicidad, coherencia, aislamiento y durabilidad.) para que puedan tener un manejo de la información eficaz, se implementaron perfiles de usuarios para los empleados internos además de un control de acceso al sistema para evitar alteraciones y modificaciones no deseadas.	

Tabla 77 (continuación)

Administración de la Función Informática:	• Manejo de los fundamentos teóricos de seguridad informática para su aplicación en casos prácticos. • Uso e interpretación de los lineamientos, estándares y marcos referenciales que complemente el conocimiento de la asignatura. • Uso de técnicas y herramientas de software para comprender el ambiente de seguridad. • Proponer medidas de seguridad basadas en lineamientos y estándares actuales.
Implementación: Dentro del proyecto implementado hay fundamentos teóricos sobre la seguridad informática que son referenciados de acuerdo a las problemáticas de la dependencia, como guía para entender mejor la compatibilidad y parentescos de estos con otros proyectos similares, además de los estándares y normas referenciadas para la mejor interpretación y diseño de soluciones, además se técnicas para el desarrollo del software con el rol de sistema de inventario, que garantizan la seguridad de la información, roles de seguridad, contraseñas seguridad, acceso controlado, restricciones en la información ingresada en las interfaces, además de recomendaciones de seguridad basadas en normas ISO para tener un mejor control del sistema.	

Tabla 77 (continuación)

Auditoría Informática de Desarrollo de Proyectos y Aplicaciones:	• Manejo de los fundamentos teóricos de auditoría general, informática y tecnologías de información, así como su integración para su aplicación en el entorno práctico. • Identifica interpretación y uso de lineamientos, estándares, marcos referenciales, técnicas y otros conceptos que complemente la unión del conocimiento para la posterior aplicación de la Auditoría informática. • Describe la terminología propia de la Auditoría a fin de aplicarla en la planificación, ejecución y entrega de resultados del proceso de Auditoría informática que incluya la selección de herramientas, técnicas, y las propuestas de actividades de control. • Comprende del entorno del control interno en las empresas y su concepción en una normativa internacional. • Argumenta las metodologías para el control interno, seguridad y Auditoría informática, a fin de incorporar en el proceso de la Auditoría.
Implementación: El uso de lineamientos, estándares y normas dentro del proyecto fue indispensable ya que en un Auditoría es necesario referenciarlos para conocer los requerimientos oficiales y poder verificar si cumplen actualmente con lo estipulado, en caso contrario se diseñan soluciones basadas en estas reglas oficiales, además se incorpora información sobre lo que es Auditoría para que el proyecto tenga una mejor interpretación y análisis, además las metodologías usadas en la investigación y desarrollo del proyecto garantizan una seguridad de la información en todo momento al priorizarla.	

Tabla 77 (continuación)

Normalización de Software y Hardware:	• Analiza y compara los distintos lineamientos actuales sobre el hardware, software y telecomunicaciones para aplicar su uso. • Conoce los procesos y estándares relacionados con la ingeniería del software. • Valora los modelos y estándares de evaluación y mejora de los procesos de software. • Identifica los contenidos de los estándares generales de hardware enfocándose principalmente en las mejores prácticas y normas en almacenamiento, memorias, microprocesadores y periféricos.
Implementación: Para el desarrollo de la Auditoría es necesario el conocimiento de estándares que se concentren en el desarrollo y uso de software, de este modo es que se compara la situación actual con lo requerido y se generan propuesta de soluciones respetando dichos estándares y normas.	

FUENTES DE INFORMACIÓN

Acronis. (s.f.). Obtenido de Acronis: https://www.acronis.com/es-mx/blog/posts/data-integrity/

Ávila Funes, D. J. (25 de Abril de 2013). *INCMNSZ*. Obtenido de INCMNSZ: https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

Comunicación., U. d. (12 de Diciembre de 2023). "Remachado" del tubo de drenaje.

Comunicación., U. d. (16 de Noviembre de 2023). Acceso al inventario desde la herramienta 'Ejecutar'.

Comunicación., U. d. (14 de Diciembre de 2023). Achivos de la Carpeta UTIC 2022-2024.

Comunicación., U. d. (11 de Diciembre de 2023). Activos sobre el pasillo.

Comunicación., U. d. (7 de Diciembre de 2023). Activos ubicados en el suelo.

Comunicación., U. d. (11 de Diciembre de 2023). Activos, Materiales, Archivos de la UTIC.

Comunicación., U. d. (11 de Diciembre de 2023). Activos, Materiales, Archivos, Equipos de Impresión.

Comunicación., U. d. (6 de Diciembre de 2023). Actualización Postergada.

Comunicación., U. d. (6 de Diciembre de 2023). Actualización Postergada en otro equipo.

Comunicación., U. d. (8 de Diciembre de 2023). Archivos Físicos bajo la corriente alterna de la UITC.

Comunicación., U. d. (12 de Diciembre de 2023). Asientos de la UTIC.

Comunicación., U. d. (8 de Diciembre de 2023). Bajada del contacto eléctrico.

Comunicación., U. d. (8 de Diciembre de 2023). Bajada del contacto eléctrico.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 1.

Comunicación., U. d. (12 de Diciembre de 2023). Cableado 1 del Rack.

Comunicación., U. d. (113 de Diciembre de 2023). Cableado 10.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 11.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 2.

Comunicación., U. d. (12 de Diciembre de 2023). Cableado 2 del Rack.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 3.

Comunicación., U. d. (12 de Diciembre de 2023). Cableado 3 del Rack.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 4.

Comunicación., U. d. (12 de Diciembre de 2023). Cableado 4 del Rack.

Comunicación., U. d. (12 de Diciembre} de 2023). Cableado 5 del Rack.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 6.

Comunicación., U. d. (12 de Diciembre de 2023). Cableado 6 del Rack.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 7.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 8.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado 9.

Comunicación., U. d. (30 de Noviembre de 2023). Cableado desordenado.

Comunicación., U. d. (11 de Diciembre de 2023). Cableado5.

Comunicación., U. d. (4 de Diciembre de 2023). Cámara Interna de la UTIC.

Comunicación., U. d. (14 de Diciembre de 2023). Carpetas en Red.

Comunicación., U. d. (12 de Diciembre de 2023). Dispositivos de telecomunicciones.

Comunicación., U. d. (6 de Diciembre de 2023). Equipo 1 con contraseña.

Comunicación., U. d. (6 de Diciembre de 2023). Equipo 2 sin contraseña.

Comunicación., U. d. (6 de Diciembre de 2023). Equipo 3 sin contraseña.

Comunicación., U. d. (6 de Diciembre de 2023). Equipo 4 sin contraseña.

Comunicación., U. d. (6 de Diciembre de 2023). Equipo 5 con contraseña.

Comunicación., U. d. (4 de Diciembre de 2023). Equipo de Impresión Multifuncional.

Comunicación., U. d. (11 de Diciembre de 2023). Equipo en proceso de reparación.

Comunicación., U. d. (8 de Diciembre de 2023). Etiquetado 1.

Comunicación., U. d. (8 de Diciembre de 2023). Etiquetado 2.

Comunicación., U. d. (8 de Diciembre de 2023). Etiquetado 3.

Comunicación., U. d. (8 de Diciembre de 2023). Etiquetado 4.

Comunicación., U. d. (8 de Diciembre de 2023). Etiquetado 5.

Comunicación., U. d. (8 de Diciembre de 2023). Extensiones eléctricas.

Comunicación., U. d. (8 de Diciembre de 2023). Extensiones eléctricas.

Comunicación., U. d. (8 de Diciembre de 2023). Extensiones eléctrticas.

Comunicación., U. d. (8 de Diciembre de 2023). Extintor 1.

Comunicación., U. d. (8 de Diciembre de 2023). Extintor 2.

Comunicación., U. d. (8 de Diciembre de 2023). Extintor fuera de la UTIC.

Comunicación., U. d. (12 de Diciembre de 2023). Formato 1 de Vale de Entrega.

Comunicación., U. d. (12 de Diciembre de 2023). Formato 1 de Vale de Salida.

Comunicación., U. d. (12 de Diciembre de 2023). Formato 2 de Vale de Entrega.

Comunicación., U. d. (14 de Diciembre de 2023). Función Ejecutar de Windows.

Comunicación., U. d. (4 de Diciembre de 2023). Imagen de la Cámara de Videovigilancia.

Comunicación., U. d. (16 de Noviembre de 2023). Inventario de la UTIC en hojas de cálculo.

Comunicación., U. d. (6 de Diciembre de 2023). Lista de aplicaciones que contiene el equipo.

Comunicación., U. d. (7 de Diciembre de 2023). Materiales ubicados en el suelo.

Comunicación., U. d. (6 de Octubre de 2023). Oficina de la UTIC sin vigilancia.

Comunicación., U. d. (12 de Diciembre de 2023). Protección de la puerta principal de la UTIC.

Comunicación., U. d. (11 de Diciembre de 2023). Reparación de equipos fuera de la UTIC.

Comunicación., U. d. (16 de Noviembre de 2023). Uso de extensiones en la UTIC.

Comunicación., U. d. (8 de Diciembre de 2023). Vista 1 de los contactos eléctricos.

Comunicación., U. d. (7 de Diciembre de 2023). Vista 1 del Aire Acondicionado.

Comunicación., U. d. (12 de Diciembre de 2023). Vista 1 del techo falso de la UTIC.

Comunicación., U. d. (8 de Diciembre de 2023). Vista 2 de los contactos eléctricos.

Comunicación., U. d. (7 de Diciembre de 2023). Vista 2 del Aire Acondicionado.

Comunicación., U. d. (14 de Diciembre de 2023). Vista 2 del Sistema de Inventario.

Comunicación., U. d. (12 de Diciembre de 2023). Vista 2 del techo falso de la UTIC.

Comunicación., U. d. (8 de Diciembre de 2023). Vista 3 de los contactos eléctricos.

Comunicación., U. d. (7 de Diciembre de 2023). Vista 3 del Aire Acondicionado.

Comunicación., U. d. (14 de Diciembre de 2023). Vista 3 del Sistema de Inventario.

Comunicación., U. d. (12 de Diciembre de 2023). Vista 3 del techo falso de la UTIC.

Comunicación., U. d. (12 de Diciembre de 2023). Vista del cableado.

Comunicación., U. d. (12 de Diciembre de 2023). Vista del Drenaje.

Comunicación., U. d. (11 de Diciembre de 2023). Vista del escitorio principal.

Comunicación., U. d. (11 de Diciembre de 2023). Vista del escritorio 1.

Comunicación., U. d. (11 de Diciembre de 2023). Vista del escritorio 2.

Comunicación., U. d. (12 de Diciembre de 2023). Vista del Servidor.

Comunicación., U. d. (14 de Diciembre de 2023). Vista del Sistema de Inventario de la UTIC.

Comunicación., U. d. (11 de Diciembre de 2023). Vista General de la UTIC.

Comunicación., U. d. (12 de Diciembre de 2023). Vsita interior 1 del rack.

Comunicación., U. d. (23 de Febrero de 2024). Acceso principal a la UTIC despejado.

Comunicación., U. d. (22 de Febrero de 2024). Activos obstruyendo el acceso principal de la UTIC.

Comunicación., U. d. (23 de Febrero de 2024). Archivo debajo de interruptores eléctricos principales de la UTIC.

Comunicación., U. d. (21 de Febrero de 2024). Bitácora del uso de la impresora en uso.

Comunicación., U. d. (22 de Febrero de 2024). Caja de los No Break implementados en la UTIC.

Comunicación., U. d. (22 de Febrero de 2024). Cambio de extensiones por sistemas de alimentación ininterrumpidas.

Comunicación., U. d. (22 de Febrero de 2024). Características de los No Break implementados en la UTIC.

Comunicación., U. d. (15 de Febrero de 2024). Compromiso de asignación de encargado para el correcto cierre de la UTIC. .

Comunicación., U. d. (15 de Enero de 2024). Compromiso Firmado de Implementacion de Recomendaciones de Auditoría Interna.

Comunicación., U. d. (15 de Enero de 2024). Compromiso firmado de uso de contraseñas seguras.

Comunicación., U. d. (15 de Febrero de 2024). Compromiso formado de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC.

Comunicación., U. d. (18 de Enero de 2024). Equipo aleatorio mostrando mensaje de actulización.

Comunicación., U. d. (15 de Enero de 2024). Equipo mostrando mensaje de actualización.

Comunicación., U. d. (22 de Febrero de 2024). Espacio del pasillo libre de activos.

Comunicación., U. d. (21 de Febrero de 2024). Extintor mal ubicado dentro del site.

Comunicación., U. d. (23 de Febrero de 2024). Extintor mejor ubicado dentro del site.

Comunicación., U. d. (23 de Febrero de 2024). Identificación del cableado.

Comunicación., U. d. (23 de Febrero de 2024). Interruptores eléctricos despejados de archivos.

Comunicación., U. d. (15 de Enero de 2024). Política aprobada.

Comunicación., U. d. (23 de Febrero de 2024). Reubicación de los activos situados en el piso.

Comunicación., U. d. (22 de Febrero de 2024). Vista del No Break con código QR para saber sus características.

Comunicación., U. d. (22 de Febrero de 2024). Vista frontal del sistema de alimentación ininterrumpida.

Desconocido. (22 de Marzo de 2021). *idc Online*. Obtenido de idc Online: https://idconline.mx/corporativo/2021/03/19/diferencia-entre-nom-y-estandar

Desconocido. (20 de Diciembre de 2021). *Universidad Europea*. Obtenido de Universidad Europea: https://universidadeuropea.com/blog/que-es-hardware-ordenador/

Editorial, E. (27 de Diciembre de 2018). *Significados*. Obtenido de Significados: https://www.significados.com/evaluacion/

Equipo editorial, E. (1 de Septiembre de 2020). *Concepto.de*. Obtenido de Concepto.de: https://concepto.de/infraestructura/

Equipo editorial, E. (14 de Febrero de 2022). *Concepto*. Obtenido de Concepto: https://concepto.de/gestion/

Gabarró Sust, J. (s.f.). *normes ISO*. Obtenido de normes ISO: https://iso.cat/es/como-elaborar-un-plan-de-auditoria-interna/

ibaiscanbit.com. (04 de Septiembre de 2022). Obtenido de ibaiscanbit.com: https://ibaiscanbit.com/ibaiscanbit/auditoria-informatica-de-sistemas-que-es-y-sus-ventajas/

IBM. (08 de Marzo de 2021). Obtenido de IBM: https://www.ibm.com/docs/es/i/7.1?topic=availability-roadmap

ISEC, U. d. (08 de Marzo de 2022). *Universidad de Negocios ISEC*. Obtenido de Universidad de Negocios ISEC: https://uneg.edu.mx/para-que-sirven-las-tecnologias-de-la-informacion/

Maps, G. (01 de Septiembre de 2023). *Google Maps*. Obtenido de Google Maps: https://www.google.com.mx/maps/place/Palacio+Municipal+de+Tultitl%C3%A1n/@19.6514517,-99.1764874,14z/data=!4m6!3m5!1s0x85d1f595bd69bf73:0xf0cc5ee2592bcf8e!8m2!3d19.6474177!4d-99.1691902!16s%2Fg%2F11g73b2f84?entry=ttu&g_ep=EgoyMDI0MTAyNy4wIKXMDSoASAFQAw%3D

Martínez, A. (14 de Junio de 2023). *conceptodefinicion*. Obtenido de conceptodefinicion: https://conceptodefinicion.de/analisis/

Pérez Porto, J., & Gardey, A. (1 de Noviembre de 2018). *Definición.de*. Obtenido de Definición.de: https://definicion.de/examinar/

Pérez Porto, J., & Gardey, A. (24 de Agosto de 2021). *Definición.de*. Obtenido de Definición.de: https://definicion.de/seguridad/

Pérez Porto, J., & Gardey, A. (2 de Julio de 2024). *Definicion.de*. Obtenido de Definicion.de: https://definicion.de/software/

Pérez Porto, J., & Merino, M. (21 de Septiembre de 2021). *Definición.de*. Obtenido de Definición.de: https://definicion.de/inspeccion/

Personal., D. d. (6 de Diciembre de 2023). Abatelenguas del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Agua Oxigenada del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Cubrebocas KNY-95 del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Gafas de Protección del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Gasas del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Glúcometro del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Isopos de algodón del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Jabón Germicida Líquido del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Lampara de Diagnóstico del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Oxímetro de Pulso del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Pinzas de Kelly rectas del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Tela Adhesiva del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Termómetro digital del botiquín médico.

Personal., D. d. (6 de Diciembre de 2023). Vendas del botiquín médico.

propia, E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 3.

propia, E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 17.

propia., E. (6 de Noviembre de 2023). Acceso Principal a UTIC.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 1.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 10.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 11.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 12.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 13.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 14.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 15.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 2.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 4.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 5.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 6.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 7.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 8.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Amenaza 9.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 3.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 1.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 10.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 11.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 12.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 13.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 14.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 15.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 16.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 18.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 2.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 4.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 5.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 6.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 7.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 8.

propia., E. (29 de Noviembre de 2023). Análisis de Riesgos, Infraestructura Vulnerabilidad 9.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 1.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 2.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 3.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 4.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 5.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 6.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 7.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 8.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Amenaza 9.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 1.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 10.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 11.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 12.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 13.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 14.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 2.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 3.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 4.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 5.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 6.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 7.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 8.

propia., E. (1 de Diciembre de 2023). Análisis de Riesgos, Inventario Vulnerabilidad 9.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 1.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 10.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 11.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 2.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 3.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 4.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 5.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 6.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 7.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 8.

propia., E. (22 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Amenaza 9.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 1.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 2.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 3.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 3.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 4.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 5.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 6.

propia., E. (20 de Noviembre de 2023). Análisis de Riesgos, Seguridad Física Vulnerabilidad 7.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 1.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 2.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 3.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 4.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 5.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Amenaza 6.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 1.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 2.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 3.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 4.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 5.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 6.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 7.

propia., E. (24 de Noviembre de 2023). Análisis de Riesgos, Seguridad Lógica Vulnerabilidad 8.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 1.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 2.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 3.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 4.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 5.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 6.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 7.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Amenaza 8.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 1.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 2.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 3.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 4.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 5.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 6.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 7.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 8.

propia., E. (27 de Noviembre de 2023). Análisis de Riesgos, Servicios Vulnerabilidad 9.

propia., E. (18 de Diciembre de 2023). Escrito firmado de la asignación del encargado de la UTIC.

propia., E. (18 de Diciembre de 2023). Formato de Asignacion de Cierre.

propia., E. (18 de Diciembre de 2023). Formato de Bitácora.

propia., E. (18 de Diciembre de 2023). Formato de llenado de la Asignacion de Cierre.

propia., E. (18 de Diciembre de 2023). Formato de llenado de la Bitácora.

propia., E. (18 de Enero de 2024). Artículo 15 de la política.

propia., E. (18 de Enero de 2024). Capitulo V de la política.

propia., E. (8 de Enero de 2024). Caratula de la política.

propia., E. (18 de Enero de 2024). Compromiso de asignación de encargado para el monitoreo de los sistemas de los equipos de cómputo en la UTIC.

propia., E. (15 de Enero de 2024). Compromiso de uso de contraseñas seguras.

propia., E. (18 de Enero de 2024). Contenido de la política.

propia., E. (15 de Enero de 2024). Datos de Inicio de sesión con contraseñas seguras.

propia., E. (21 de Marzo de 2024). Inicio de Sesión del Sistema de Inventario desarrollado para la UTIC.

propia., E. (29 de Enero de 2024). Instalación del Gestor de Base de Datos SQL Server.

propia., E. (29 de Enero de 2024). Instalación del JDK para NetBeans.

propia., E. (29 de Enero de 2024). Instalación del lenguaje de progrmación Apache NetBeans.

propia., E. (21 de Marzo de 2024). Interfaz de Cargos de los Empleados.

propia., E. (21 de Marzo de 2024). Interfaz de Consulta de las Entradas del Inventario.

propia., E. (21 de Marzo de 2024). Interfaz de Consulta de las Salidas del Inventario.

propia., E. (21 de Marzo de 2024). Interfaz de las Marcas manejadas de la UTIC.

propia., E. (21 de Marzo de 2024). Interfaz de Registro de Empleados.

propia., E. (21 de Marzo de 2024). Interfaz de Registro de Entradas.

propia., E. (21 de Marzo de 2024). Interfaz de Registro de Productos.

propia., E. (21 de Marzo de 2024). Interfaz de Registro de Salidas.

propia., E. (21 de Marzo de 2024). Interfaz del llenado del Vale de Salida.

propia., E. (21 de Marzo de 2024). Interfaz Principal del Sistema de Inventario.

propia., E. (29 de Enero de 2024). Lista de programas a instalar para la implementación del Sistema de Inventario.

propia., E. (21 de Marzo de 2024). Mensaje de Advertencia si no se llena el Vale de Salida.

propia., E. (18 de Enero de 2024). Parte de la Política.

propia., E. (21 de Marzo de 2024). Vista preliminar de impresión del inventario total de la partida que se seleccione.

Santos Ramírez, A. L., & Moran Diego, O. Y. (18 de Enero de 2024). *Google Drive*. Obtenido de Google Drive: https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fdrive.google.com%2Fdrive%2Fsearch%3Fhl%3Des%26q%3Dtype%3Apdf&followup=https%3A%2F%2Fdrive.google.com%2Fdrive%2Fsearch%3Fhl%3Des%26q%3Dtype%3Apdf&hl=es-419&ifkv=AcMMx-dRWZkg4pQJ4ZDPSbP

Segura Martínez, J. (2012). *Departamento de Informática y Sistemas*. Obtenido de Departamento de Informática y Sistemas: http://dis.um.es/~lopezquesada/documentos/IES_1213/SAD/curso/UT4/ActividadesAlumnos/12/index.html

Server., S. (21 de Marzo de 2024). Consulta directa en la Base de Datos.

Server., S. (31 de Enero de 2024). Tablas de la base de datos.

Tultitlán, D. d. (14 de Septiembre de 2023). Organigrama del Palacio Municipal.

Tultitlán., H. A. (4 de Septiembre de 2023). Acceso a la UTIC.

Tultitlán., H. A. (6 de Diciembre de 2023). Acceso al botiquín médico.

Tultitlán., H. A. (4 de Diciembre de 2023). Cerraduras de la puerta de la UTIC.

Tultitlán., H. A. (4 de Diciembre de 2023). Oficina de la UTIC.

Tultitlán., H. A. (4 de Diciembre de 2023). Segunda Vista de la Cerradura del Acceso Principal a la UTIC.

Tultitlán., H. A. (4 de Diciembre de 2023). Segundo acceso hacia la UTIC.

Tultitlán., H. A. (8 de Diciembre de 2023). Señalamiento de Exintor.

Tultitlán., H. A. (8 de Diciembre de 2023). Señalamiento de Ruta de Evacuación.

Tultitlán., H. A. (8 de Diciembre de 2023). Señalamiento de Salida de Emergencia.

Tultitlán., H. A. (4 de Diciembre de 2023). Tercera Vista de la Cerradura del Acceso Principal a la UTIC.

Tultitlán., H. A. (4 de Diciembre de 2023). Vista de la Cerradura del Acceso Principal a la UTIC.

Tultitlán., H. A. (4 de Diciembre de 2023). Vista trasera al Acceso a la UTIC.

Tultitlán., H. A. (6 de Diciembre de 2024). Acceso al botiquín médico.

Tultitlán., I. d. (3 de Noviembre de 2023). Ubicación Física de la Unidad de Tecnologías de la Información y Comunicación (UTIC).

UCSP, P. (s.f.). *Postgrado UCSP*. Obtenido de Postgrado UCSP: https://postgrado.ucsp.edu.pe/articulos/que-es-auditoria-externa/

valuekeep. (s.f.). Obtenido de valuekeep: https://valuekeep.com/es/gestion-de-activos/

Vélez Martínez, C. (s.f.). *Instituto de Ingeniería UNAM*. Obtenido de Instituto de Ingeniería UNAM: https://www.iingen.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadfísica.aspx

ANEXOS

Anexo 1

Tabla 78. Anexo 1. Cronograma de Reuniones. Fuente: Elaboración propia.

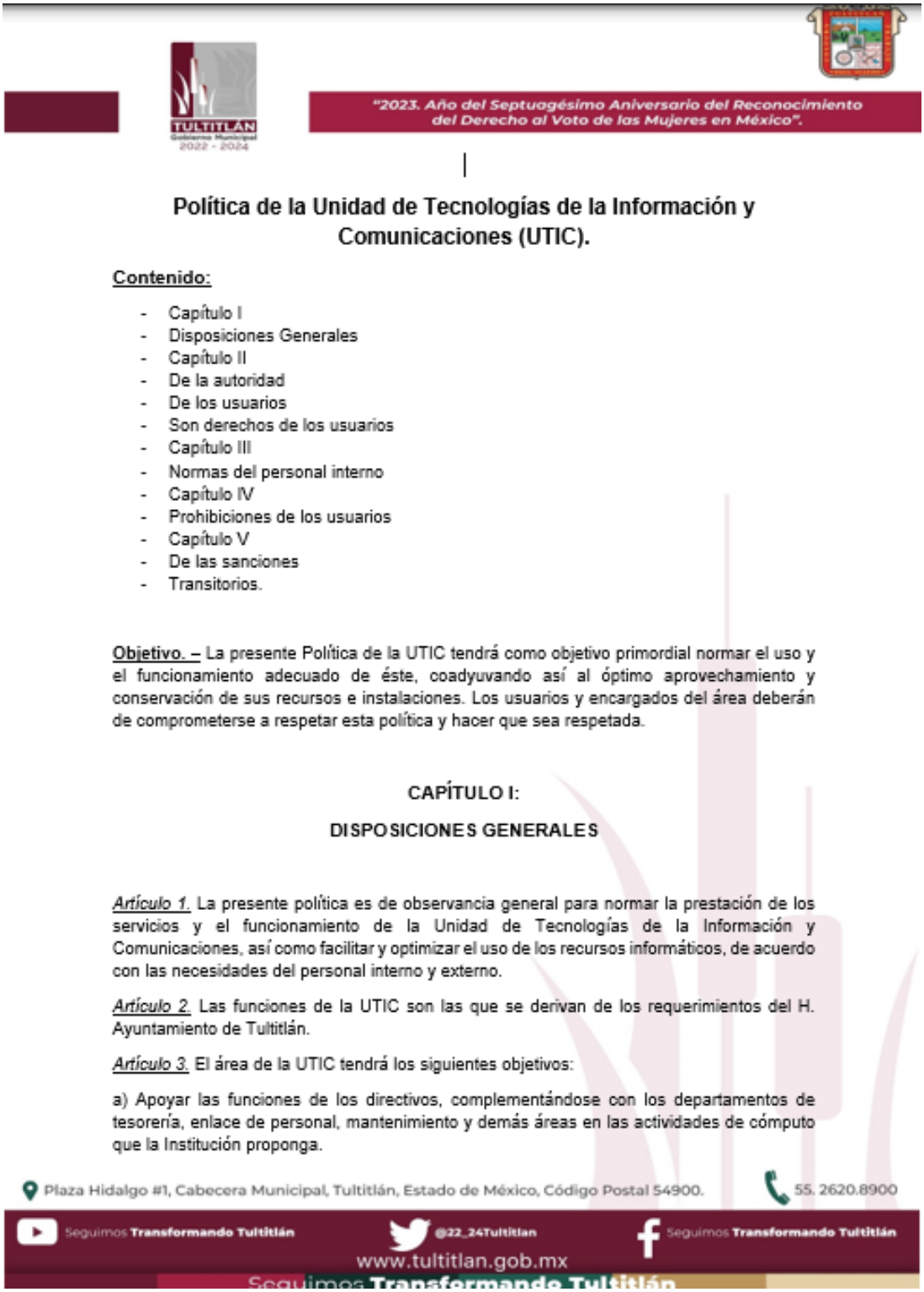
REUNIONES	FECHA	HORARIO	LUGAR	ASISTENTES	PROPÓSITO
Reunión de Apertura	14/10/2023	09:00 am – 10:30 am	Unidad de Tecnologías de la Información y Comunicación (UTIC), Ayuntamiento de Tultitlán	Equipo Auditor, Encargado de TI, Personal de la UTIC	Dar a conocer el propósito y objetivo que se planea cumplir en la Auditoría y la forma de trabajo
Reunión de Auditores	14/10/2023	15:00 pm --16:00 pm	Tecnológico de Estudios Superiores de Coacalco	Equipo Auditor	Compartir y definir las estrategias que se implementaran, tiempos y repartición de tareas entre el equipo Auditor
Reunión de avance de Auditoría	02/11/2023	09:00 am – 10:30 am	Unidad de Tecnologías de la Información y Comunicación (UTIC), Ayuntamiento de Tultitlán)	Equipo Auditor, Encargado de TI, Personal de la UTIC	Mostrar el avance logrado del objetivo a lograr, comparando el antes y el ahora trabajo implementado
Reunión Revisión de	24/11/2023	08:00 am – 10:00 am	Tecnológico de Estudios Superiores de Coacalco	Equipo Auditor	Recopilar toda la documentación generada hasta el

Documentación					momento, verificar que todo cumpla con las normas y empezar a formar el escrito final
Reunión visualización de resultados	20/12/2023	08:00 am – 10:00 am	Tecnológico de Estudios Superiores de Coacalco	Equipo Auditor	Revisar detalladamente que todo esté en orden y resolver problemas generados en la última etapa
Reunión de Cierre y Entrega de Resultados	02/02/2024	08:00 am – 09:00 am	Unidad de Tecnologías de la Información y Comunicación (UTIC), Ayuntamiento de Tultitlán	Equipo Auditor	Preparar la documentación y herramientas que se usaran en la entrega de resultados finales

Tabla 78 (continuación)

Reunión de Cierre y Entrega de Resultados	02/02/2024	09:00 am – 11:00 am	Unidad de Tecnologías de la Información y Comunicación (UTIC), Ayuntamiento de Tultitlán)	Equipo Auditor, Encargado de TI, Personal de la UTIC	Entregar el diagnostico final, exponer los motivos por los cuales se obtuvieron dichos resultados y dar cierre al proyecto de Auditoría

Anexo 2



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Política de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

Contenido:

- Capítulo I
- Disposiciones Generales
- Capítulo II
- De la autoridad
- De los usuarios
- Son derechos de los usuarios
- Capítulo III
- Normas del personal interno
- Capítulo IV
- Prohibiciones de los usuarios
- Capítulo V
- De las sanciones
- Transitorios.

Objetivo. – La presente Política de la UTIC tendrá como objetivo primordial normar el uso y el funcionamiento adecuado de éste, coadyuvando así al óptimo aprovechamiento y conservación de sus recursos e instalaciones. Los usuarios y encargados del área deberán de comprometerse a respetar esta política y hacer que sea respetada.

CAPÍTULO I:

DISPOSICIONES GENERALES

Artículo 1. La presente política es de observancia general para normar la prestación de los servicios y el funcionamiento de la Unidad de Tecnologías de la Información y Comunicaciones, así como facilitar y optimizar el uso de los recursos informáticos, de acuerdo con las necesidades del personal interno y externo.

Artículo 2. Las funciones de la UTIC son las que se derivan de los requerimientos del H. Ayuntamiento de Tultitlán.

Artículo 3. El área de la UTIC tendrá los siguientes objetivos:

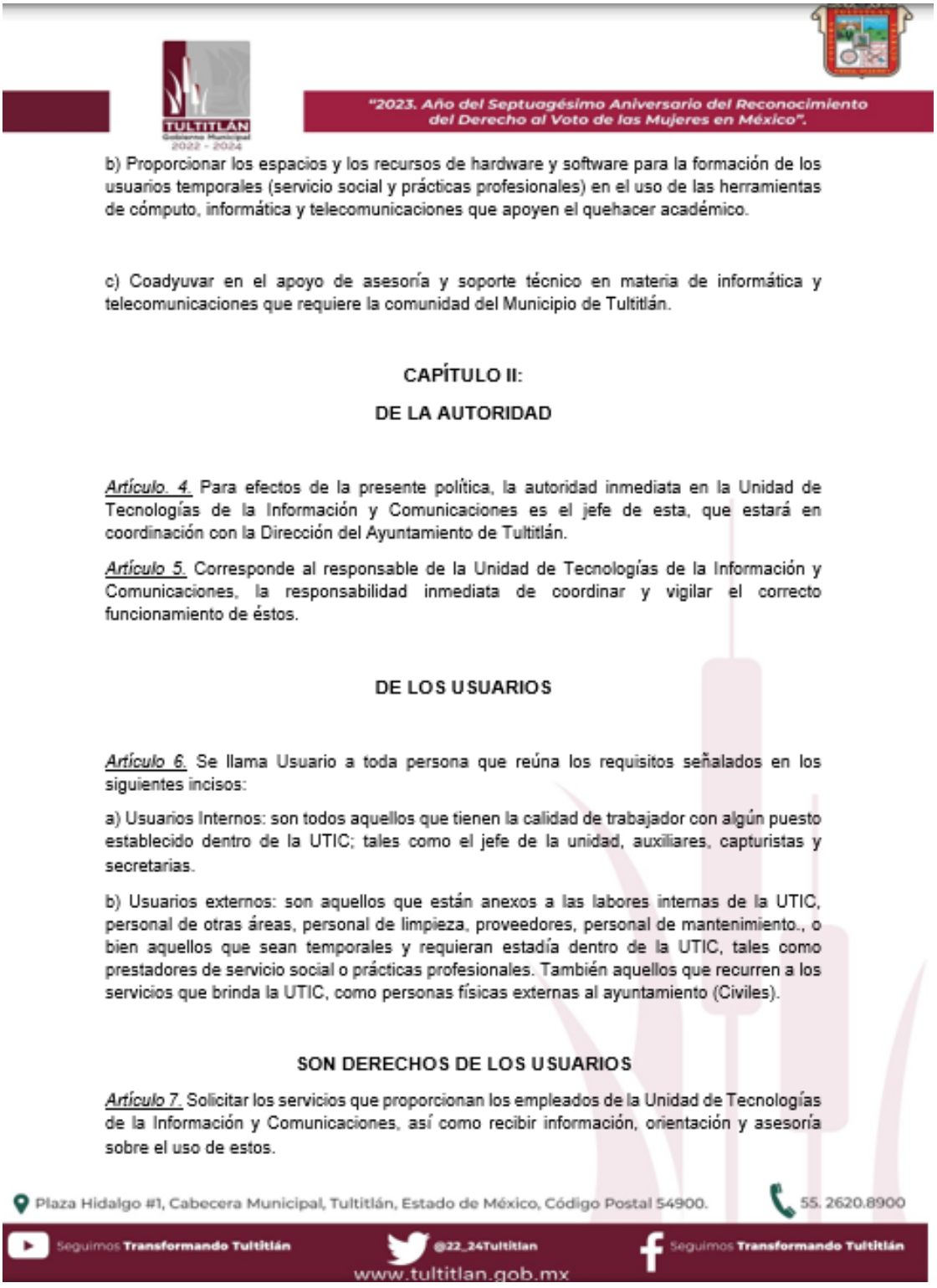
a) Apoyar las funciones de los directivos, complementándose con los departamentos de tesorería, enlace de personal, mantenimiento y demás áreas en las actividades de cómputo que la Institución proponga.

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 328 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo I politica de seguridad, 2024).



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

b) Proporcionar los espacios y los recursos de hardware y software para la formación de los usuarios temporales (servicio social y prácticas profesionales) en el uso de las herramientas de cómputo, informática y telecomunicaciones que apoyen el quehacer académico.

c) Coadyuvar en el apoyo de asesoría y soporte técnico en materia de informática y telecomunicaciones que requiere la comunidad del Municipio de Tultitlán.

CAPÍTULO II:

DE LA AUTORIDAD

Artículo 4. Para efectos de la presente política, la autoridad inmediata en la Unidad de Tecnologías de la Información y Comunicaciones es el jefe de esta, que estará en coordinación con la Dirección del Ayuntamiento de Tultitlán.

Artículo 5. Corresponde al responsable de la Unidad de Tecnologías de la Información y Comunicaciones, la responsabilidad inmediata de coordinar y vigilar el correcto funcionamiento de éstos.

DE LOS USUARIOS

Artículo 6. Se llama Usuario a toda persona que reúna los requisitos señalados en los siguientes incisos:

a) Usuarios Internos: son todos aquellos que tienen la calidad de trabajador con algún puesto establecido dentro de la UTIC; tales como el jefe de la unidad, auxiliares, capturistas y secretarias.

b) Usuarios externos: son aquellos que están anexos a las labores internas de la UTIC, personal de otras áreas, personal de limpieza, proveedores, personal de mantenimiento., o bien aquellos que sean temporales y requieran estadía dentro de la UTIC, tales como prestadores de servicio social o prácticas profesionales. También aquellos que recurren a los servicios que brinda la UTIC, como personas físicas externas al ayuntamiento (Civiles).

SON DERECHOS DE LOS USUARIOS

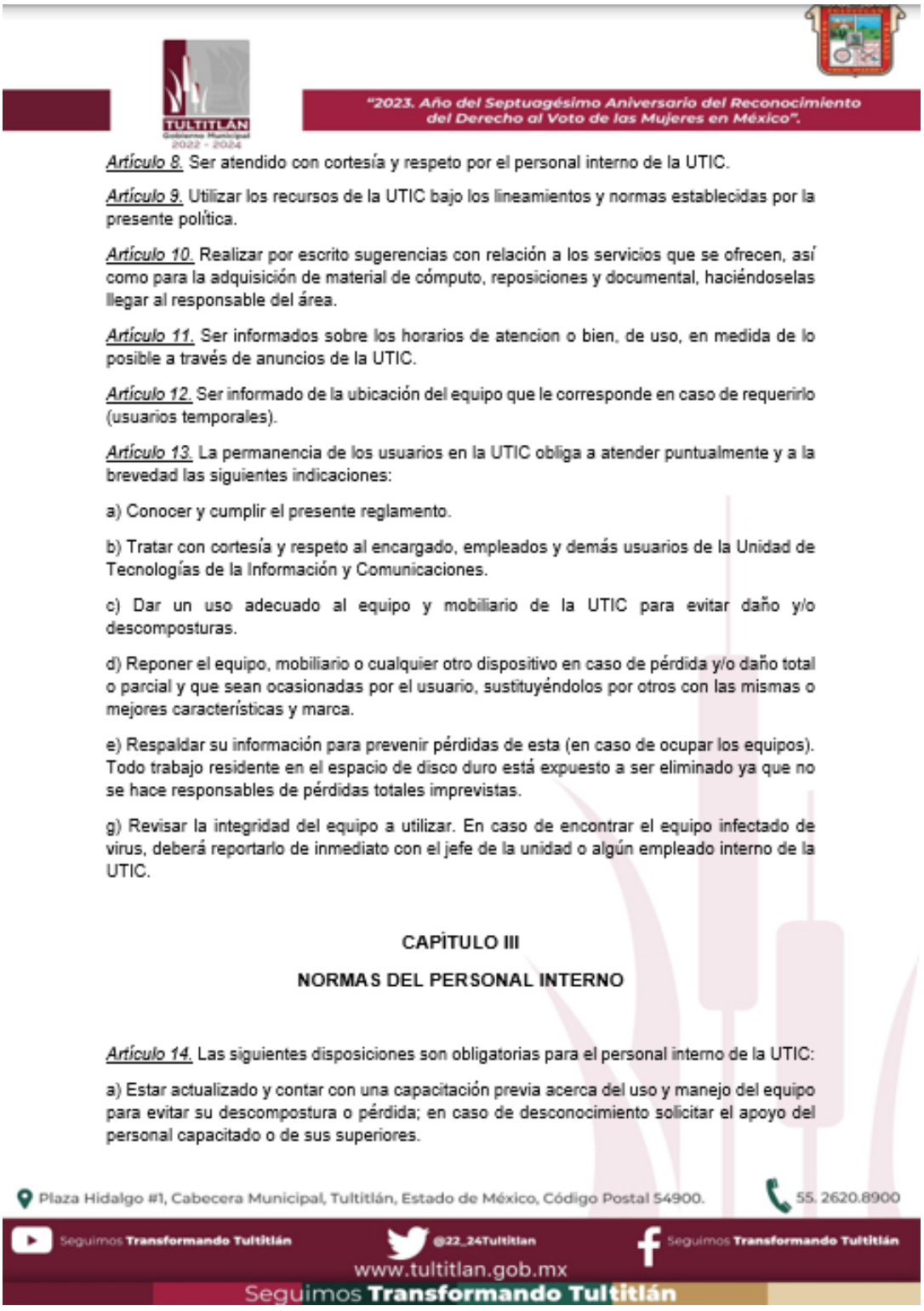
Artículo 7. Solicitar los servicios que proporcionan los empleados de la Unidad de Tecnologías de la Información y Comunicaciones, así como recibir información, orientación y asesoría sobre el uso de estos.

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Figura 329 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo 2 politica de seguridad, 2024).



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Artículo 8. Ser atendido con cortesía y respeto por el personal interno de la UTIC.

Artículo 9. Utilizar los recursos de la UTIC bajo los lineamientos y normas establecidas por la presente política.

Artículo 10. Realizar por escrito sugerencias con relación a los servicios que se ofrecen, así como para la adquisición de material de cómputo, reposiciones y documental, haciéndoselas llegar al responsable del área.

Artículo 11. Ser informados sobre los horarios de atencion o bien, de uso, en medida de lo posible a través de anuncios de la UTIC.

Artículo 12. Ser informado de la ubicación del equipo que le corresponde en caso de requerirlo (usuarios temporales).

Artículo 13. La permanencia de los usuarios en la UTIC obliga a atender puntualmente y a la brevedad las siguientes indicaciones:

a) Conocer y cumplir el presente reglamento.

b) Tratar con cortesía y respeto al encargado, empleados y demás usuarios de la Unidad de Tecnologías de la Información y Comunicaciones.

c) Dar un uso adecuado al equipo y mobiliario de la UTIC para evitar daño y/o descomposturas.

d) Reponer el equipo, mobiliario o cualquier otro dispositivo en caso de pérdida y/o daño total o parcial y que sean ocasionadas por el usuario, sustituyéndolos por otros con las mismas o mejores características y marca.

e) Respaldar su información para prevenir pérdidas de esta (en caso de ocupar los equipos). Todo trabajo residente en el espacio de disco duro está expuesto a ser eliminado ya que no se hace responsables de pérdidas totales imprevistas.

g) Revisar la integridad del equipo a utilizar. En caso de encontrar el equipo infectado de virus, deberá reportarlo de inmediato con el jefe de la unidad o algún empleado interno de la UTIC.

CAPÍTULO III

NORMAS DEL PERSONAL INTERNO

Artículo 14. Las siguientes disposiciones son obligatorias para el personal interno de la UTIC:

a) Estar actualizado y contar con una capacitación previa acerca del uso y manejo del equipo para evitar su descompostura o pérdida; en caso de desconocimiento solicitar el apoyo del personal capacitado o de sus superiores.

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Seguimos Transformando Tultitlán

Figura 330 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo 3 politica de seguridad, 2024).



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

b) Mantener el orden y supervisar que los compañeros internos y usuarios temporales en caso de aplicar hagan uso adecuado de programas y equipo de cómputo, en las sesiones reservadas para los equipos.

c) Asistir con puntualidad a los horarios de trabajo impuestos por la UTIC. Transcurridos cinco minutos de tiempo de tolerancia, el responsable del acceso principal requerirá llegar minutos antes que los demás trabajadores para tener el acceso a la UTIC abierto.

d) Reportar inmediatamente al jede de la unidad, cualquier desperfecto que presente el equipo, evitando que se le responsabilice por el daño encontrado.

e) Verificar que al término de la sesión los componentes y el equipo de cómputo estén completos y en buenas condiciones, absteniéndose de intercambiar estos, notificando el estado que guardan al jefe de la UTIC antes de retirarse.

Artículo 15. Son obligaciones del personal interno de la UTIC:

a) Mantener una imagen de responsabilidad y respeto que propicie una buena convivencia en los espacios de trabajo donde participen. Brindar el servicio con cortesía y respeto a los civiles, empleados y demás usuarios.

b) Proporcionar asesoría básica en el uso y manejo de los activos y dispositivos usados internamente, a usuarios temporales o prestadores de servicio social, prácticas profesionales o simplemente usuarios nuevos.

c) Dar un uso adecuado al equipo y mobiliario de la UTIC para evitar daños y/o descomposturas.

d) Verificar y gestionar la reposición del equipo, mobiliario o cualquier otro dispositivo en caso de deterioro, pérdida total o parcial, el cual deberá ser sustituido por otro con las mismas o mejores características.

e) Publicar los horarios de trabajo de la UTIC.

f) Mantener los sistemas de los equipos de cómputo internos actualizados a la versión más reciente y no tener actualizaciones en espera u omitidas por la realización de actividades laborales.

g) Usar adecuadamente los dispositivos de red y los componentes de telecomunicaciones, evitando abolladuras, golpes, jalones de cables y todo lo que afecte la apariencia y rendimiento de los dispositivos.

CAPÍTULO IV

PROHIBICIONES A LOS USUARIOS

Artículo 16. Queda prohibido a los usuarios de los Laboratorios de Cómputo:

a) Introducir, consumir o presentarse bajo los efectos de bebidas embriagantes o cualquier tipo de droga, en el espacio de trabajo de la UTIC.

Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Seguimos Transformando Tultitlán

Figura 331 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo 4 politica de seguridad, 2024).



"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

b) Fumar, introducir o consumir alimentos cerca de los equipos de cómputo y/o bebidas en botellas que no sean de taparrosca o con sello en la tapa, en los espacios de trabajo de la UTIC.

c) Introducir armas de fuego, punzocortantes o de cualquier otro tipo, que pudieran poner en peligro la vida o salud de los usuarios de la UTIC. (en caso de ser herramientas que se usaran para reparaciones de equipos, se debe reportar ante el jefe de la unidad)

d) Dañar intencionalmente cualquier componente del equipo de cómputo, así como extraer, borrar o cambiar la forma de operación del programa instalado en las computadoras.

e) Desconectar o cambiar de lugar o remplazar sin aviso los elementos o periféricos conectados a las computadoras.

f) Utilizar los recursos de la UTIC para acceder a equipos locales o remotos a los cuales el usuario no tenga autorización explícita en su uso o intente violar la seguridad de acceso.

g) Cambiar la configuración de los equipos que se encuentran en el área de trabajo de la UTIC.

h) Instalar software sin autorización previa del responsable del área de trabajo, en este caso, del jefe de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

i) Alterar las condiciones de higiene, limpieza y disciplina del Laboratorio de Cómputo.

j) Sustraer equipo o periféricos sin autorización.

CAPITULO V

DE LAS SANCIONES

Artículo 17. Cualquier infracción a lo dispuesto en la presente política, generará la aplicación de sanciones, considerando ante todo la gravedad del hecho, sus consecuencias, así como la intencionalidad y reincidencia:

a) Se amonestará por escrito a todo usuario que viole el contenido del Artículo 16, en sus incisos b, g, h.

b) La acumulación de dos amonestaciones por escrito dará cabida a la suspensión de sus actividades dentro de la UTIC, hasta por tres días, dependiendo la gravedad de las amonestaciones.

c) La acumulación de tres amonestaciones escritas dará por suspendido al usuario de sus actividades dentro de la UTIC, hasta por 5 días, dependiendo la gravedad de las amonestaciones.

d) Será causa de suspensión inmediata de sus derechos y servicios por un tiempo determinado por las autoridades hasta por más de una semana a quien viole lo dispuesto por el Artículo 16, en sus incisos a, c y d.

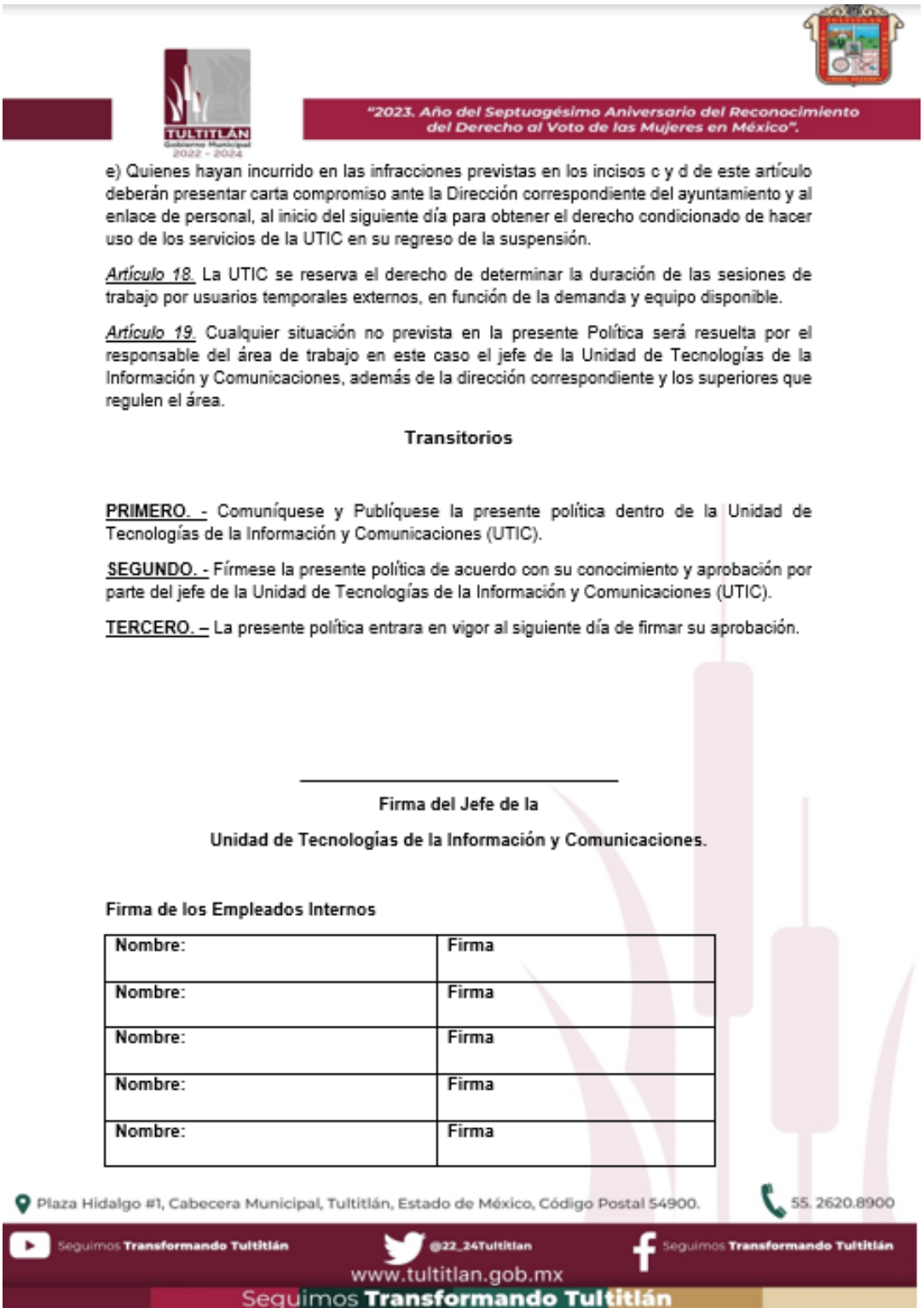
Plaza Hidalgo #1, Cabecera Municipal, Tultitlán, Estado de México, Código Postal 54900. 55. 2620.8900

Seguimos Transformando Tultitlán @22_24Tultitlan Seguimos Transformando Tultitlán

www.tultitlan.gob.mx

Seguimos Transformando Tultitlán

Figura 332 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo 5 politica de seguridad, 2024).



e) Quienes hayan incurrido en las infracciones previstas en los incisos c y d de este artículo deberán presentar carta compromiso ante la Dirección correspondiente del ayuntamiento y al enlace de personal, al inicio del siguiente día para obtener el derecho condicionado de hacer uso de los servicios de la UTIC en su regreso de la suspensión.

Artículo 18. La UTIC se reserva el derecho de determinar la duración de las sesiones de trabajo por usuarios temporales externos, en función de la demanda y equipo disponible.

Artículo 19. Cualquier situación no prevista en la presente Política será resuelta por el responsable del área de trabajo en este caso el jefe de la Unidad de Tecnologías de la Información y Comunicaciones, además de la dirección correspondiente y los superiores que regulen el área.

Transitorios

PRIMERO. - Comuníquese y Publíquese la presente política dentro de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

SEGUNDO. - Fírmese la presente política de acuerdo con su conocimiento y aprobación por parte del jefe de la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).

TERCERO. – La presente política entrara en vigor al siguiente día de firmar su aprobación.

_____

Firma del Jefe de la

Unidad de Tecnologías de la Información y Comunicaciones.

Firma de los Empleados Internos

Nombre:	**Firma**
Nombre:	**Firma**
Nombre:	**Firma**
Nombre:	**Firma**
Nombre:	**Firma**

Figura 333 Política de Seguridad UTIC. Fuente: Elaboración propia. (propia., capitulo 5 politica de seguridad, 2024).

MANUAL DE USUARIO PARA EL USO DEL SISTEMA DE INVENTARIO

Anexo 3

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Bienvenido al Manual de Usuario

Estimado usuario,

Nos complace darte la bienvenida a este manual, diseñado para ofrecerte una guía completa y detallada sobre el funcionamiento y uso óptimo del sistema de inventario. Este manual ha sido elaborado con el objetivo de proporcionarte la información esencial que necesitas para aprovechar al máximo las características y capacidades de este inventario.

Te recomendamos que leas este manual en su totalidad antes de utilizar el sistema de inventario, ya que contiene información valiosa que te permitirá disfrutar de una experiencia sin inconvenientes. Además, no dudes en consultar el índice para encontrar rápidamente la información que necesitas.

¡Que tengas una experiencia excepcional con el sistema de inventario!

Atentamente,

Moran Diego Oscar Yahir

Santos Ramírez Ana Laura

Ficha Técnica

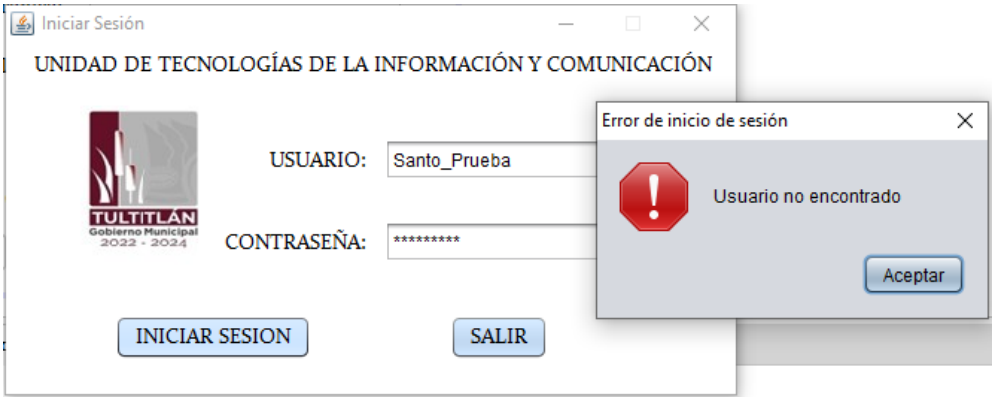
NOMBRE	**SISTEMA DE INVENTARIO UTIC**
LENGUAJE DE PROGRAMACION	Apache NetBeans 18
GESTOR DE BASE DE DATOS	SQL Server 2019

INICIO DE SESIÓN

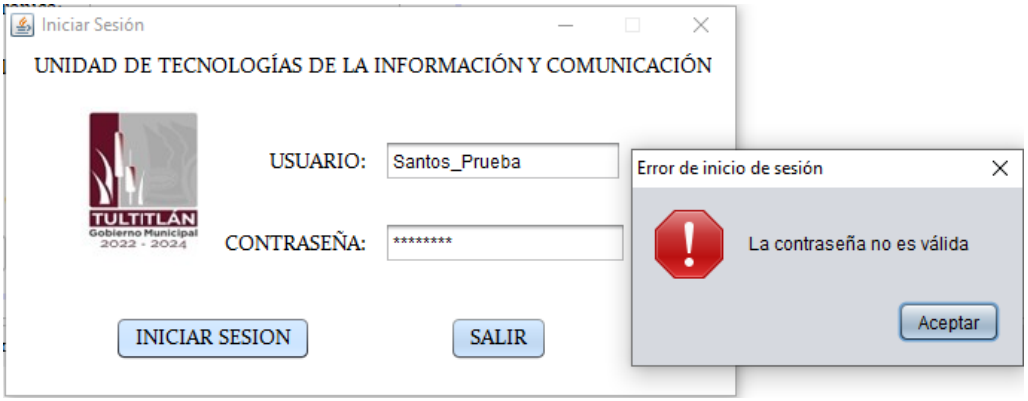
Al iniciar el Sistema de Inventario se abrirá una ventana emergente como la siguiente:



En caso de que tu usuario y contraseña no coincida te arrojara un mensaje emergente como el siguiente:



En este caso el usuario si coincide, pero la contraseña no:



Deberá ingresar tu usuario y tu contraseña que previamente se te brindo, al ingresar con tus datos proporcionados podrás visualizar la siguiente ventana seccionada en tres partes, la primera sección tiene como nombre ‘MANTENIMIENTO’ donde se podrá registrar a empleados nuevos, registrar productos que ingresen, consultar los cargos de los empleados y las marcas que la UTIC maneja. En la segunda sección llamada ‘MOVIMIENTOS’ se podrá registrar las entradas y salidas de los productos que se distribuyan en el área o en otras cuando se soliciten, y en la última sección llamada ‘INVENTARIO’ se podrá consultar las entradas y salidas e imprimir lo que se encuentre en estos apartados, además de llenar un vale de salida e imprimirlo si es necesario y por último el inventario total de todas las partidas que se manejan y la consulta de estos productos.



REGISTRO DE EMPLEADOS

Al hacer clic en el botón ‘Registro de Empleados’ se abrirá una ventana emergente como la siguiente:



Como se puede observar los campos cuentan con instrucciones específicas de su llenado, le indica si puede ingresar solo números o en su defecto letras y con una cantidad máxima de caracteres esto es con la finalidad de que los datos sean íntegros. A continuación, se muestra un ejemplo de llenado de este formulario:

Como se observa al llegar al apartado del Cargo te pedirá que selecciones del número 1 al número 4, si tiene duda de cuál es el cargo que corresponde cada número en el botón ‘Ver Cargos’ puede visualizarlos para seleccionar el cargo que maneja el empleado a registrar.



Si por equivocación das clic en el botón ‘Guardar’ sin haber llenado los campos se arrojará un mensaje de advertencia como se muestra a continuación:



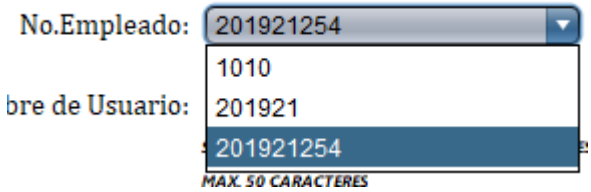
Una vez llenado el formulario, al seleccionar el botón ‘Guardar’ se aparecerá un mensaje emergente para corroborar que la información sea la correcta.



Al seleccionar la opción ‘Si’, se abrirá otro mensaje emergente donde se le preguntará si deseas registrar su usuario del empleado, si no lo deseas registrar en ese momento puedes volver a ingresar a la opción ‘Registro de Empleados’ en el botón ‘Registrar Usuario’.

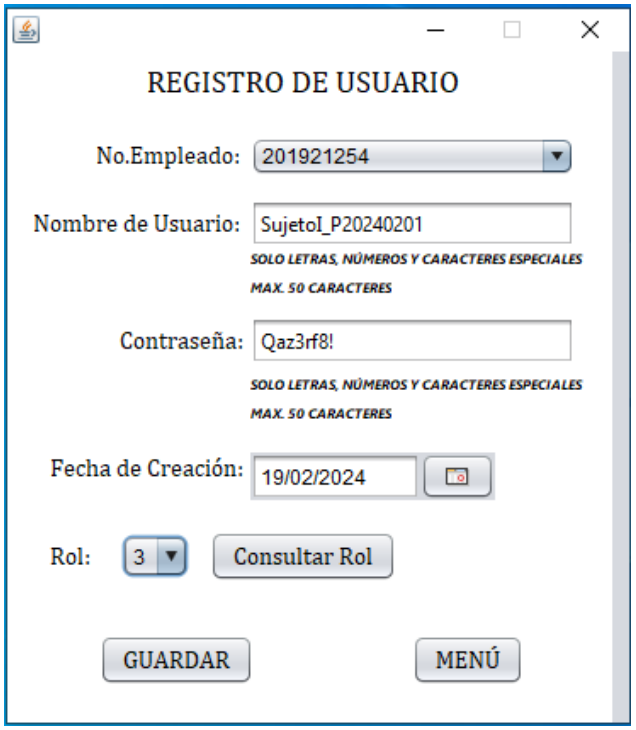


En caso contrario si selecciona la opción ‘Si’, se abrirá una ventada para registrar el usuario, para seleccionar el Numero de Empleado selecciona la parte central del recuadro que se te muestra a continuación:

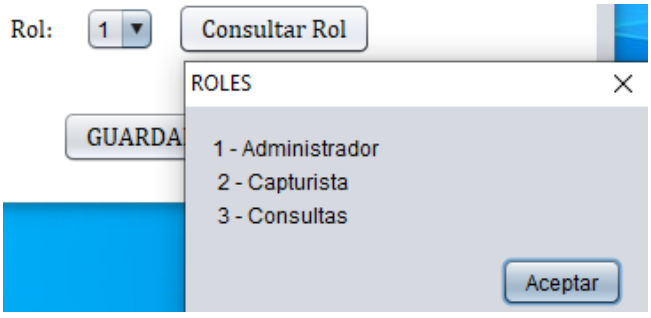


Ya que si lo selecciona de la flecha que se encuentra de la parte derecha no te mostrara el Número de Empleado.

Este es un ejemplo del llenado del formulario para registrar el usuario:



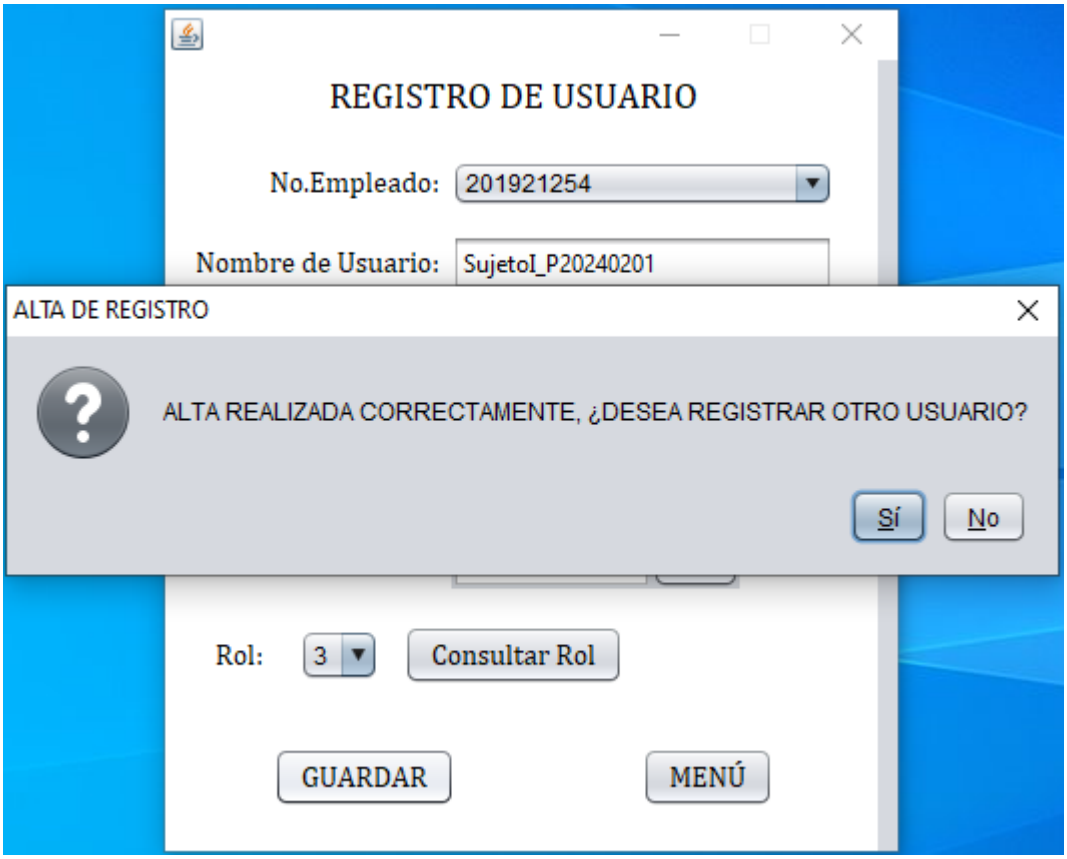
Al seleccionar el rol que tendrá el empleado aparecerá una numeración del 1 al 3, para consultar que rol corresponde a cada número, puede consultarlo del botón ‘Consultar Rol’ y se te mostrará la siguiente información



Una vez llenado el formulario al seleccionar el botón ‘Guardar’ aparecerá un mensaje emergente para corroborar si los datos son correctos.



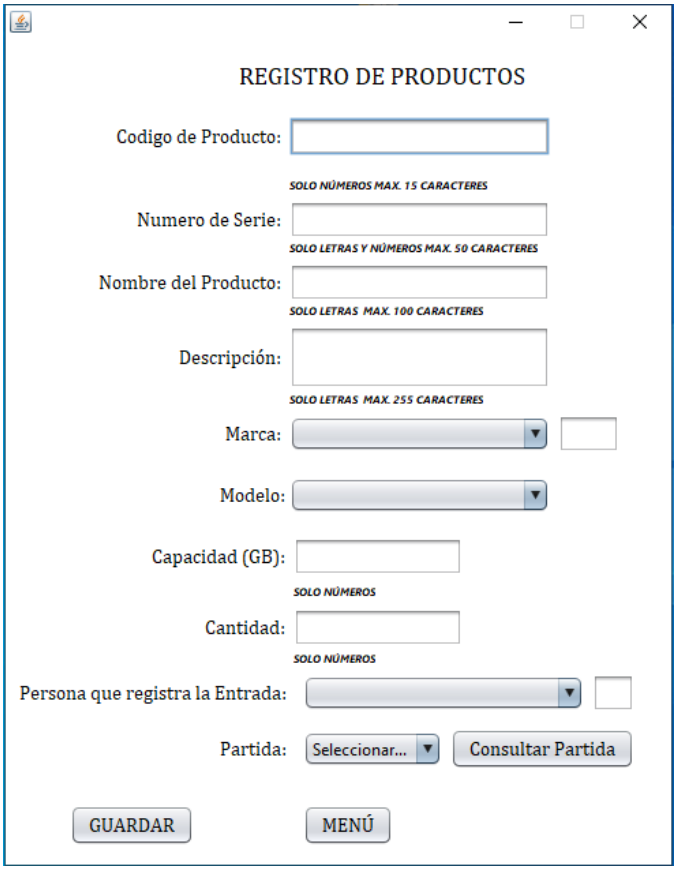
Al seleccionar ‘Si’ se abrirá otro mensaje emergente por si desea registrar otro usuario:



Si seleccionamos la opción ‘No’ se vaciará el formulario y una vez vaciado puede regresar a la pantalla de inicio.

REGISTRO DE PRODUCTOS

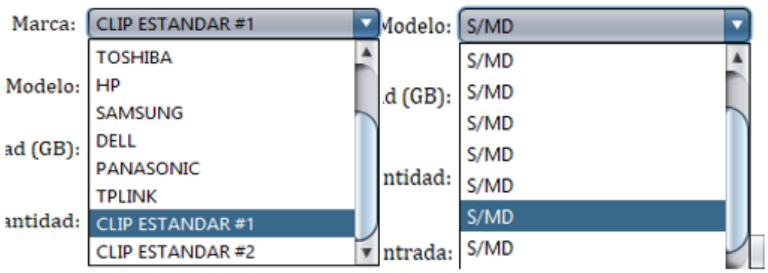
Al seleccionar la opción de ‘Registro de Productos’ se tendrá la siguiente interfaz:



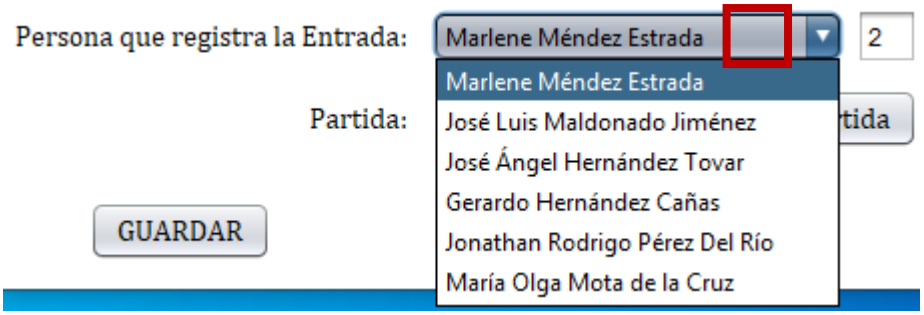
Se recomienda que el código de producto empiece por los dígitos de la partida correspondiente:



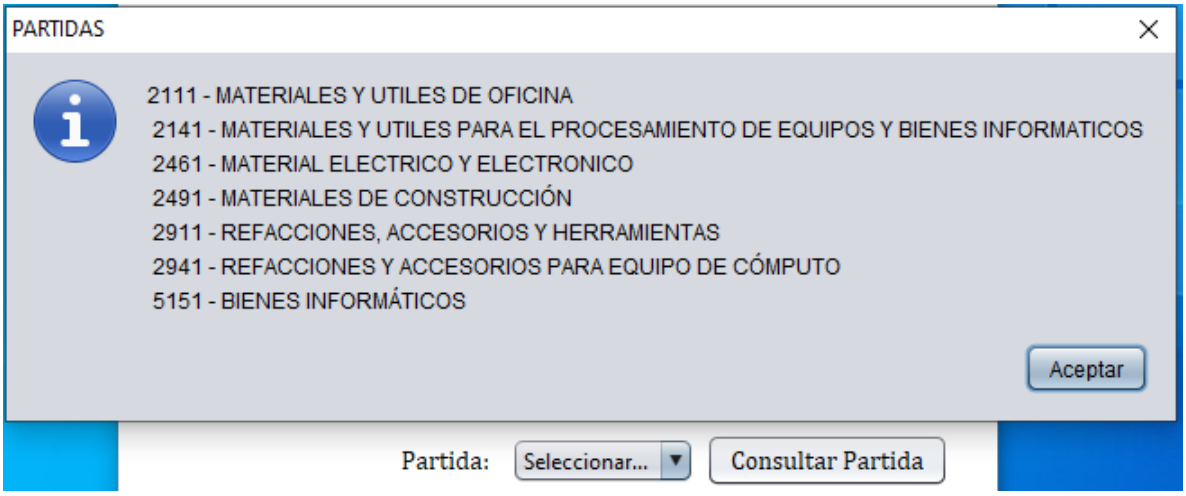
De igual manera seleccione la marca de la parte central del recuadro para que pueda visualizar las Marcas, mismo caso para el Modelo, cabe mencionar que al seleccionar la marca debe corroborar si aparece un numero como se observa en el círculo rojo de la anterior imagen.



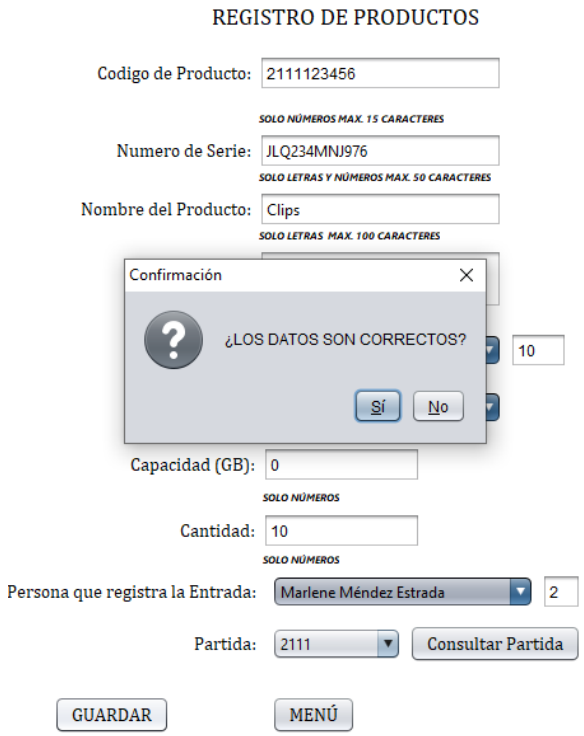
De la misma manera seleccione de la parte central el recuadro para que se despliegue la lista de los empleados, además debe de corroborar que se dibuje un numero como en el recuadro color rojo de la siguiente imagen:



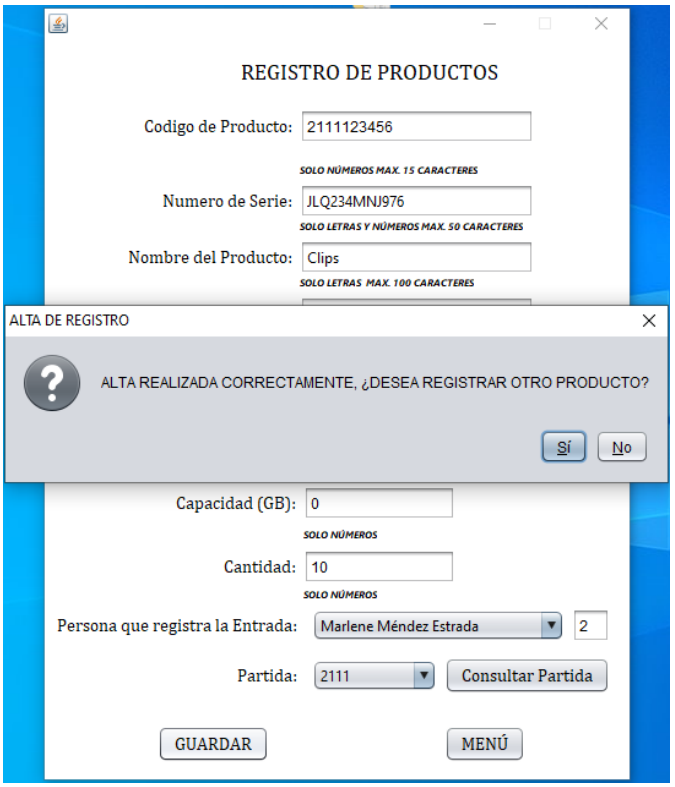
Ademas si desea consultar que partida corresponde a cada número, con ayuda del boton ‘Consultar Partida’ se le desplegara la informacion necesaria.



Una vez llenado todos los campos, se aparecerá un mensaje para corroborar si todos los datos son correctos para evitar cualquier equivocación.

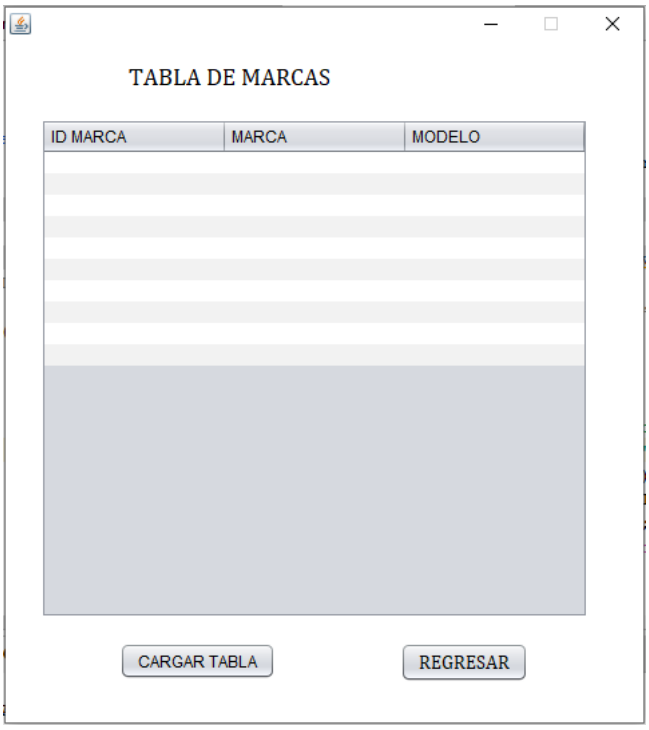


Una vez guardada la información le solicitara si desea registrar otro producto. En caso de ser ‘Si’ se limpiara el formulario en caso de ser ‘No’ se cerrará el mensaje y podrá regresar al Menú Principal con ayuda del botón ‘Menú’.



CONSULTA DE MARCAS

Al seleccionar la opción de ‘Marcas’ en el Menú, se aparecerá una ventana con lo siguiente:

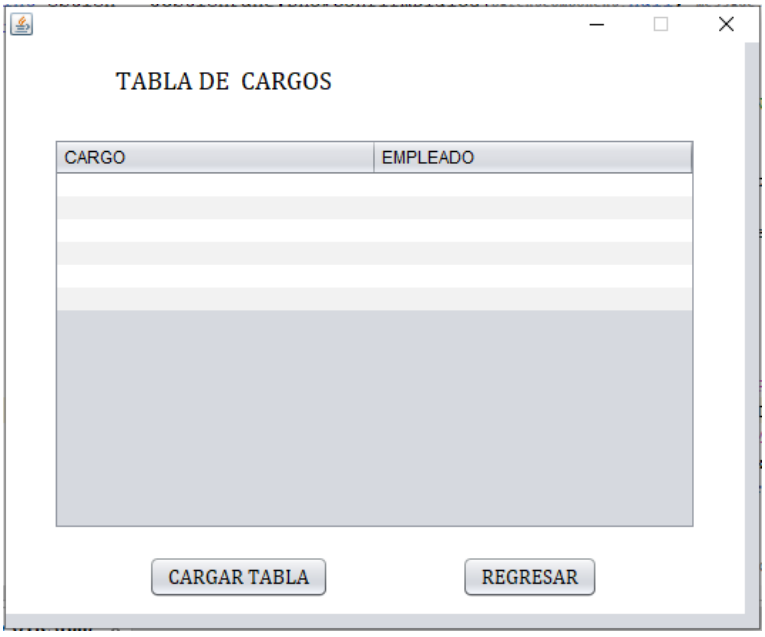


Para visualizar la información seleccione el botón ‘Cargar Tabla’ y se la marca junto con su modelo que previamente se ingresaron a la Base de Datos.

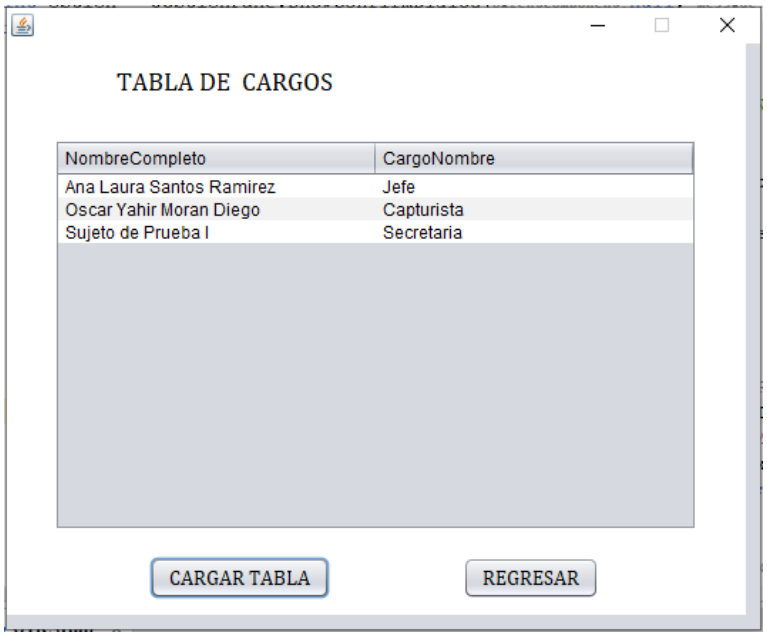


CONSULTA DE CARGOS

Al seleccionar la opción de ‘Cargos’ en el Menú, se aparecerá una ventana con lo siguiente:



Para visualizar la información selecciona el botón ‘Cargar Tabla’ y se observa el Empleado que se registró anteriormente con su respectivo cargo.



REGISTRO DE ENTRADA

Para el registro de entrada tendrá la siguiente interfaz donde podrá seleccionar el Código que se ingresó previamente en el formulario de Registro de productos, de igual manera seleccione de la parte central el recuadro para que se despliegue la lista de los códigos, además también podrá seleccionar la fecha de la entrada , la partida, si no conoce la partida con ayuda del botón consultar partida se le desplegara la información necesaria, además de seleccionar nuevamente de la parte central el recuadro perteneciente a la persona que registra la entrada y esperar a que se refleje un numero como se observa en el recuadro color azul de la siguiente imagen:



Además, en la tabla de detalle podrá ingresar la información que se te solicita.

Al insertar todos los campos y guardarlos le arrojara el mensaje de confirmación para corroborar que todos los datos sean correctos:



Al seleccionar ‘Si’ se arrojara un mensaje exitoso:

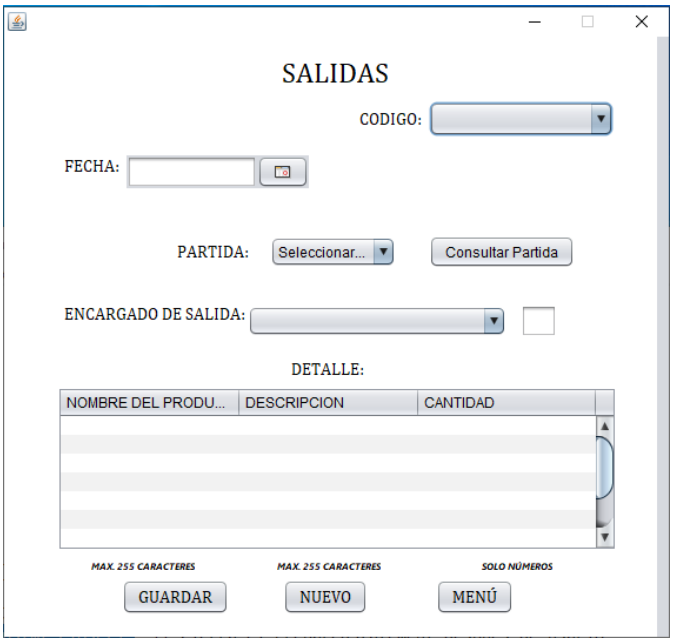


Al darle clic al botón nuevo se limpiarán los campos como lo son la fecha y la tabla de ‘Detalle’

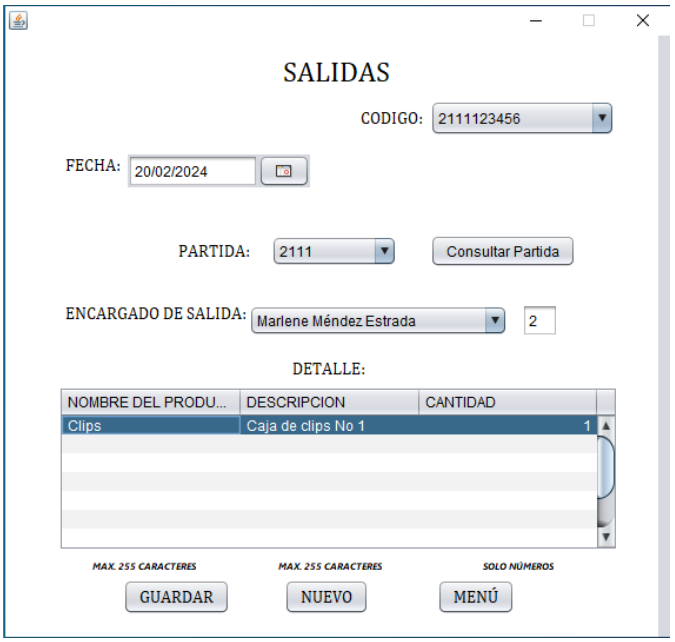


REGISTRO DE SALIDA

Al ingresar a la opción Salidas se verá reflejada una ventana similar a la de Entradas, el llenado del formulario será el mismo:



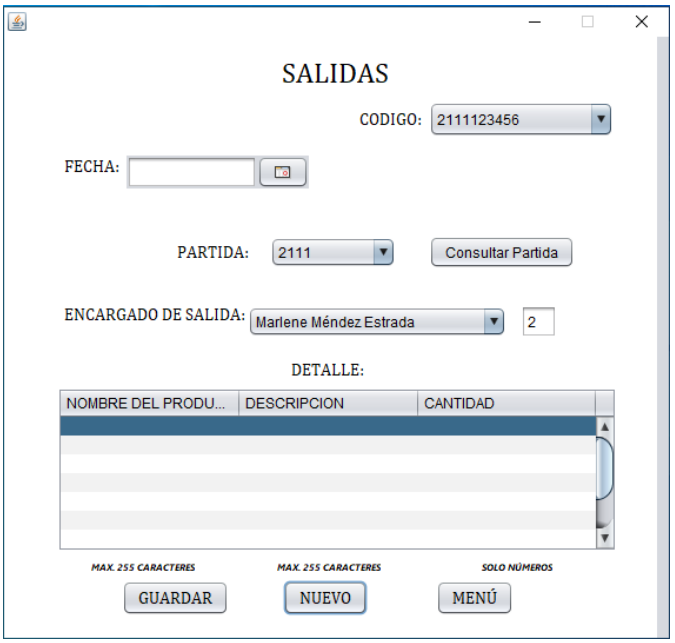
A continuación, veras un ejemplo de cómo llenar el formulario de Salidas:



De la misma manera al guardar los datos, se arrojará un mensaje de éxito:



Al seleccionar el botón ‘Nuevo’ se limpiará el formulario como se muestra a continuación:



CONSULTAS DE ENTRADAS

Al seleccionar la opción de ‘Entradas de Inventario’ se abrirá una ventana como se muestra a continuación:

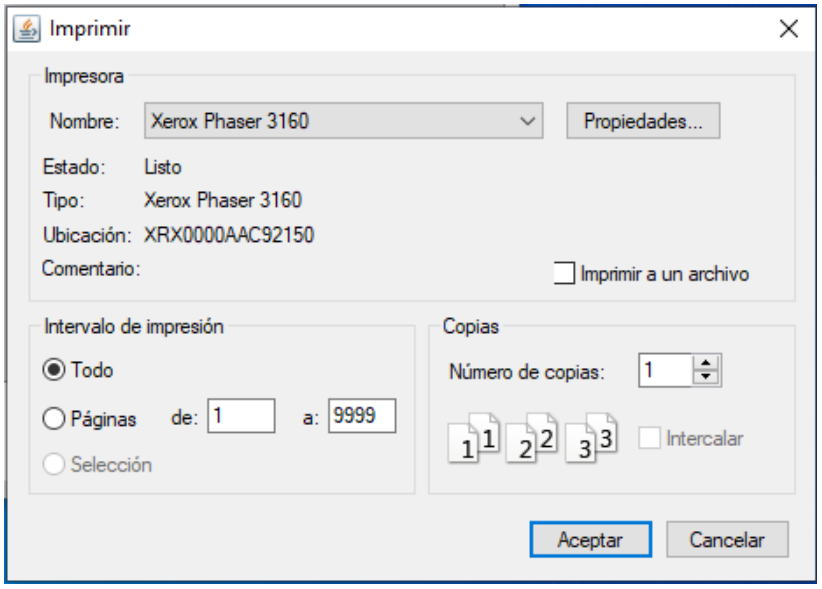


Al seleccionar el botón ‘Cargar Tabla’ se verá reflejada la información que previamente se ingresó en las Entradas:

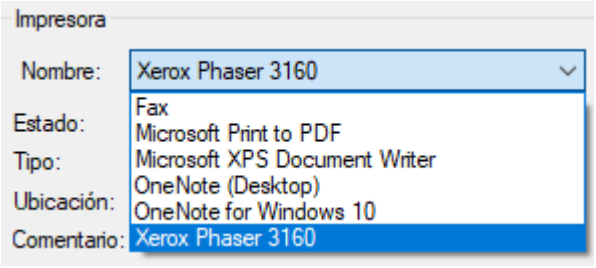


Instrucciones para imprimir

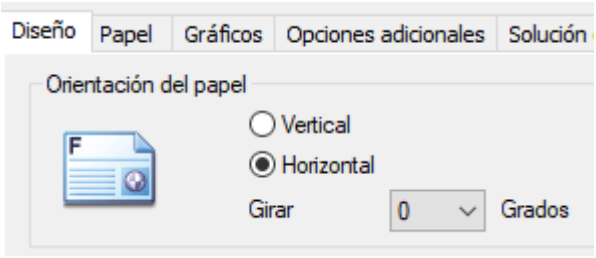
Para imprimir la tabla ‘Entradas de Inventario’ seleccione el botón ‘Imprimir’ y a continuación se verá reflejada una ventana como la siguiente:



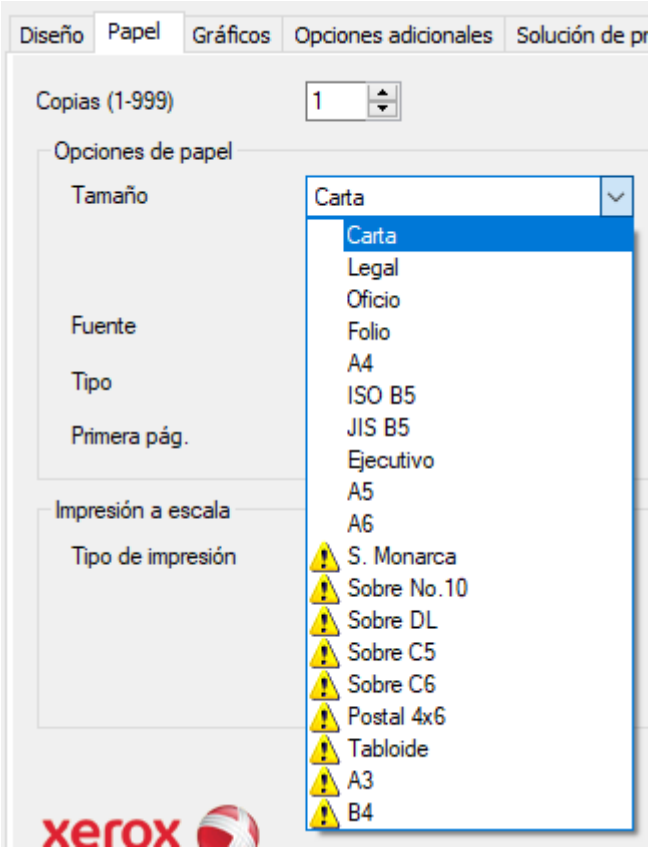
Aquí podrá seleccionar su impresora de interés, en este caso para la prueba se utilizó la impresora domestica llamada ‘Xerox Phaser 3160’:



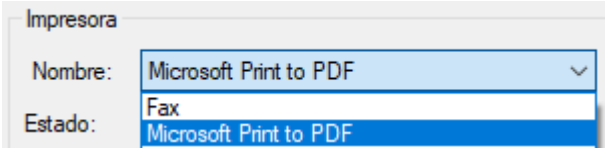
En el botón propiedades “propiedades” podrá seleccionar la orientación del papel para una mejor visualización se recomienda que la orientación sea horizontal:



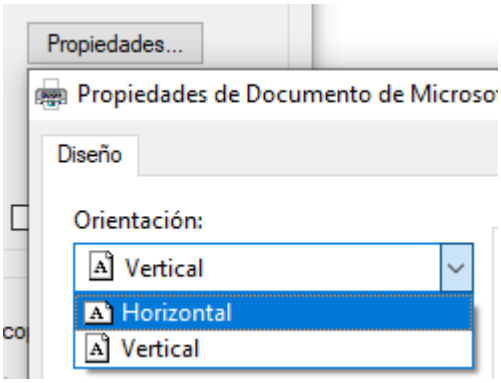
Además, en la pestaña ‘Papel’ podrá seleccionar el tipo de papel en donde se desea imprimir, para esta prueba se utilizó el tamaño Oficio:



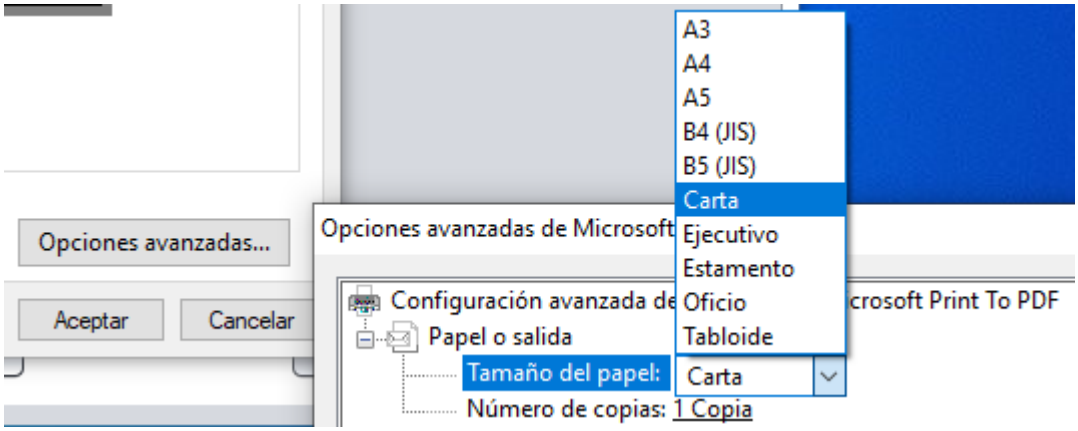
O en su defecto si deseas guardarla como PDF, selecciona la siguiente opción:



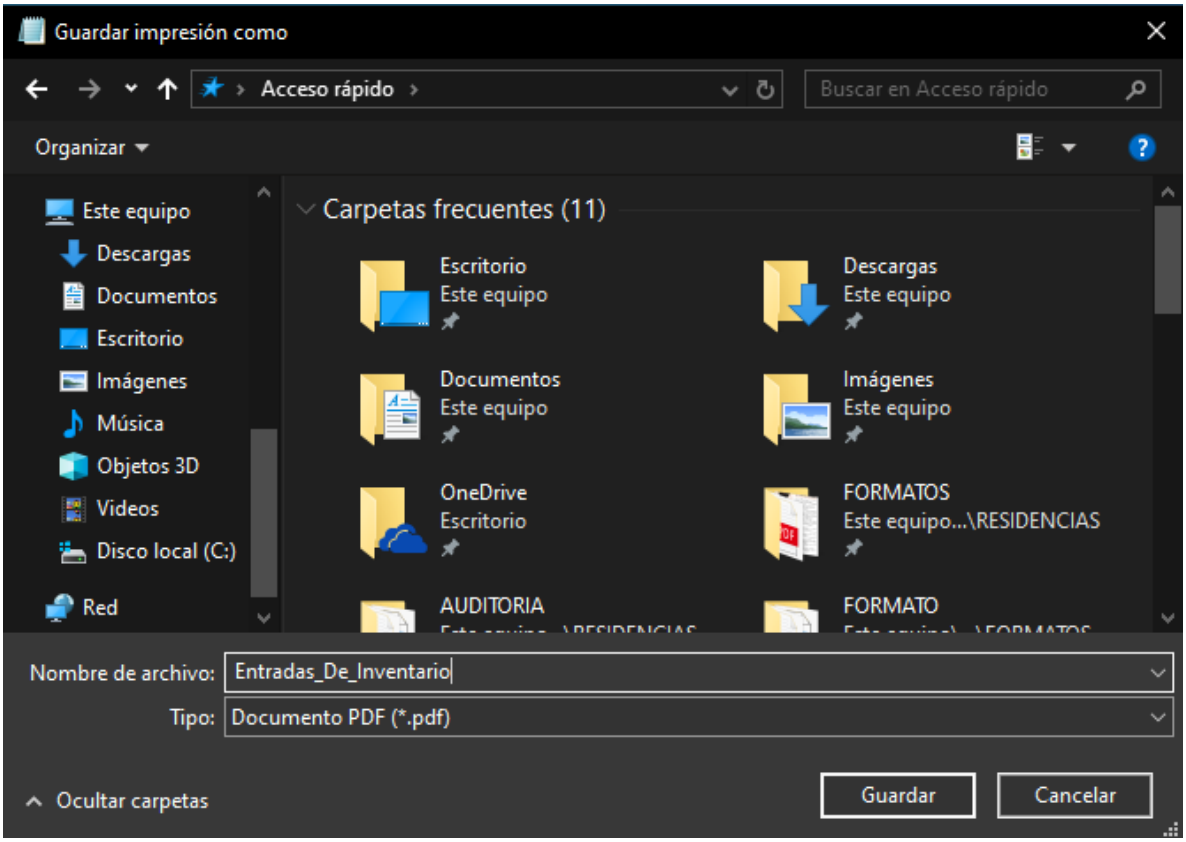
En el botón propiedades “propiedades” selecciona la opción de orientación como horizontal



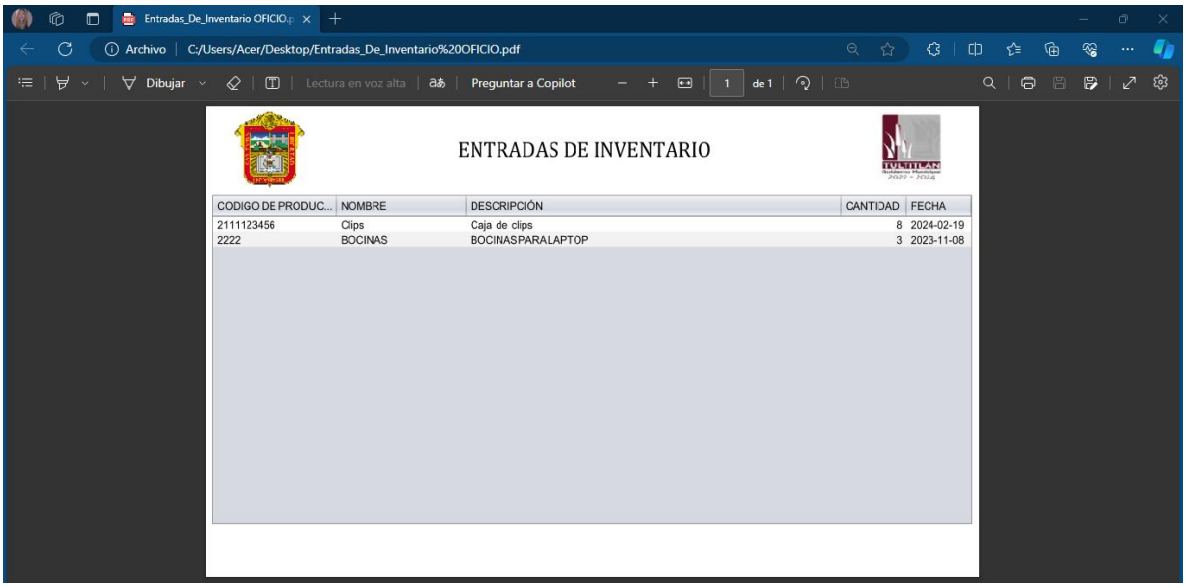
Además, en opciones avanzadas podrá seleccionar el tamaño del papel:



Al seleccionar la opción Aceptar se abrirá una ventana en donde seleccionará la ubicación del archivo:



Así se visualiza el documento, como se observa no tiene ningún botón al momento de guardarlo como PDF así mismo al momento de imprimirlo no se visualizará ningún botón:



CONSULTAS DE SALIDAS

Al seleccionar la opción de ‘Salidas de Inventario’ se abrirá una ventana como se muestra a continuación:

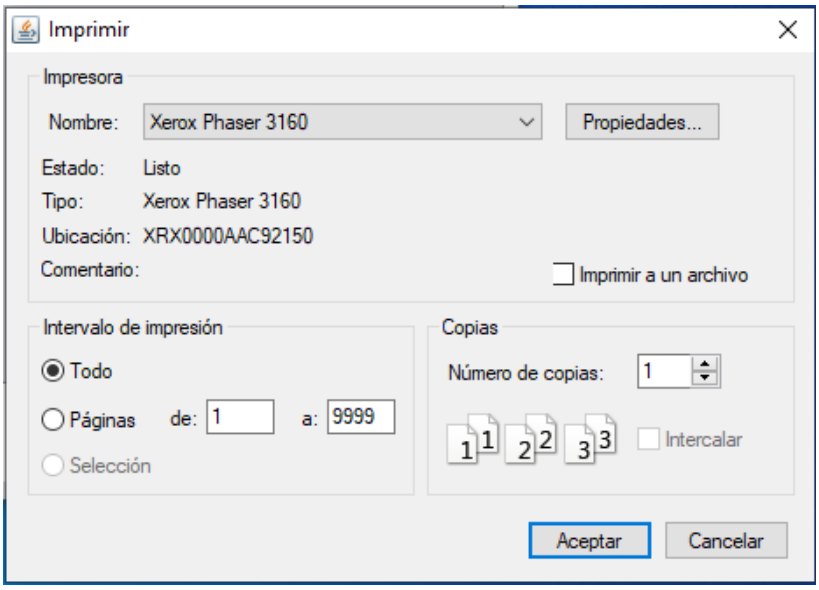


Al seleccionar el botón ‘Cargar Tabla’ se verá reflejada la información que previamente se ingresó en las Salidas:

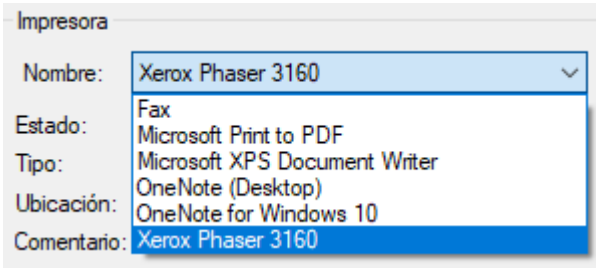


Instrucciones para imprimir

Para imprimir la tabla ‘Salidas de Inventario’ seleccione el botón ‘Imprimir’ y a continuación se verá reflejada una ventana como la siguiente:

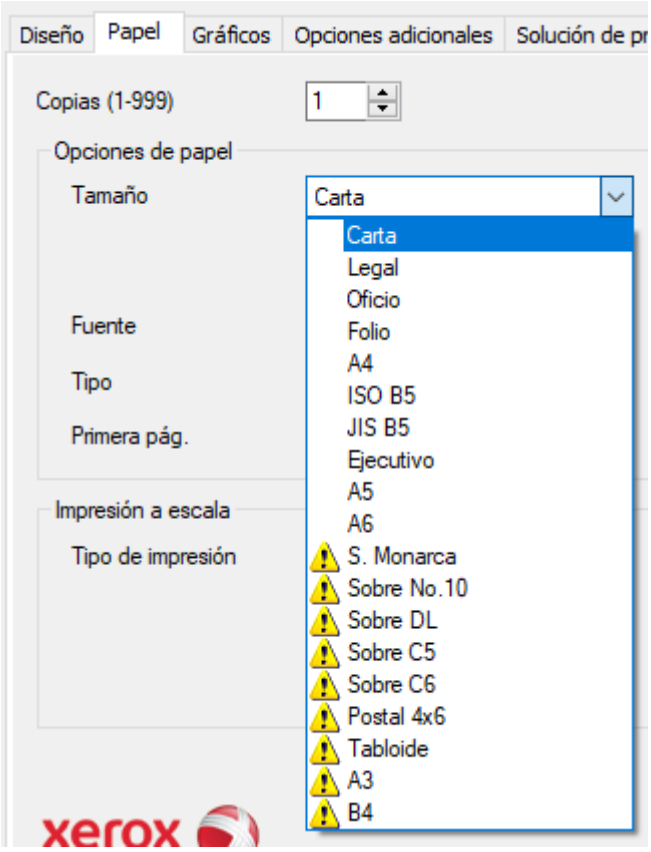


Aquí podrá seleccionar su impresora de interés, en este caso para la prueba se utilizó la impresora domestica llamada ‘Xerox Phaser 3160’:

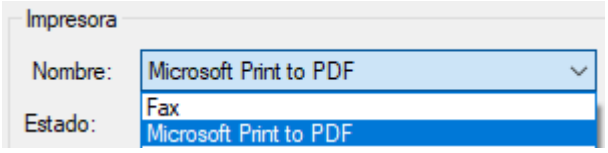


En el botón propiedades “propiedades” podrá seleccionar la orientación del papel para una mejor visualización se recomienda que la orientación sea horizontal:

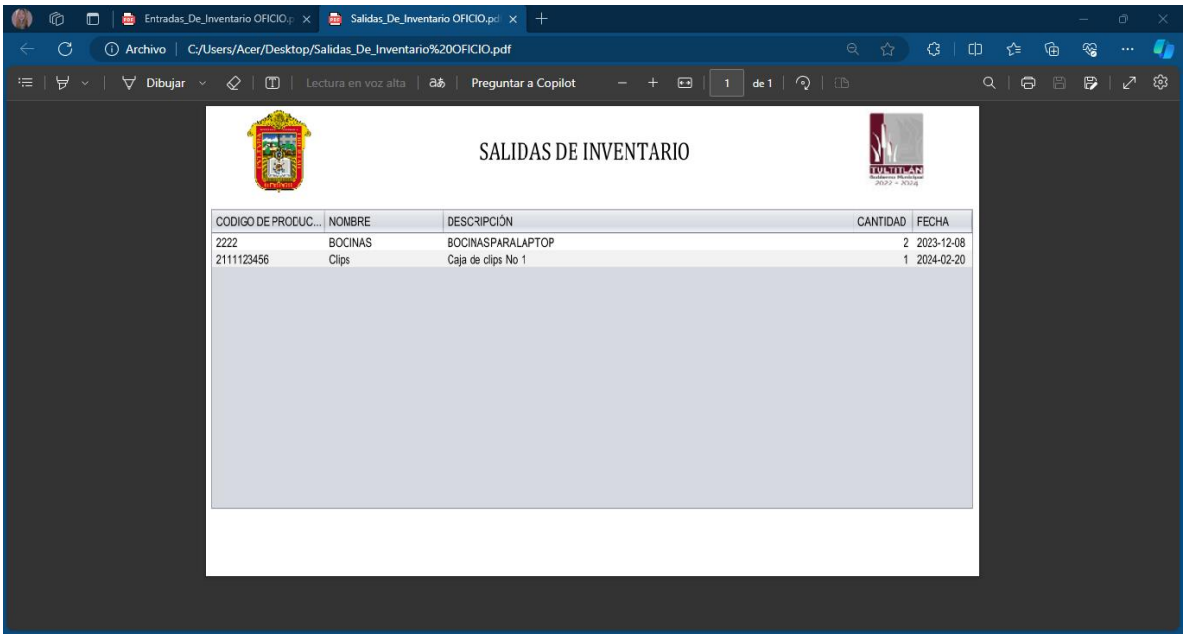
Además, en la pestaña ‘Papel’ podrá seleccionar el tipo de papel en donde se desea imprimir, para esta prueba se utilizó el tamaño Oficio:



O en su defecto si deseas guardarla como PDF, selecciona la siguiente opción:

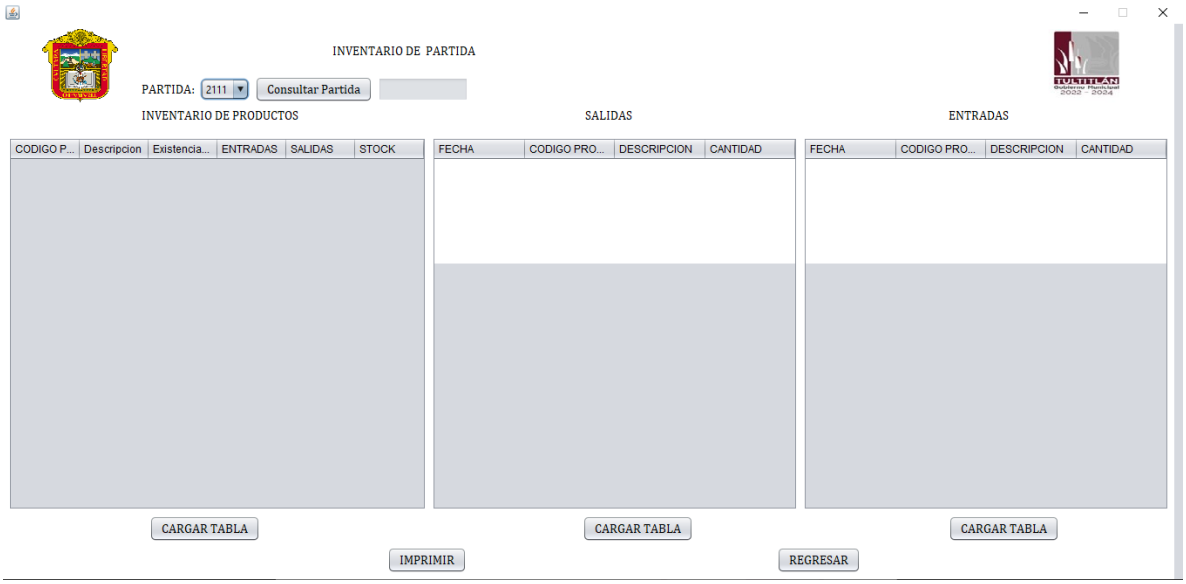


Así se visualiza el documento, como se observa no tiene ningún botón al momento de guardarlo como PDF así mismo al momento de imprimirlo no se visualizará ningún botón:

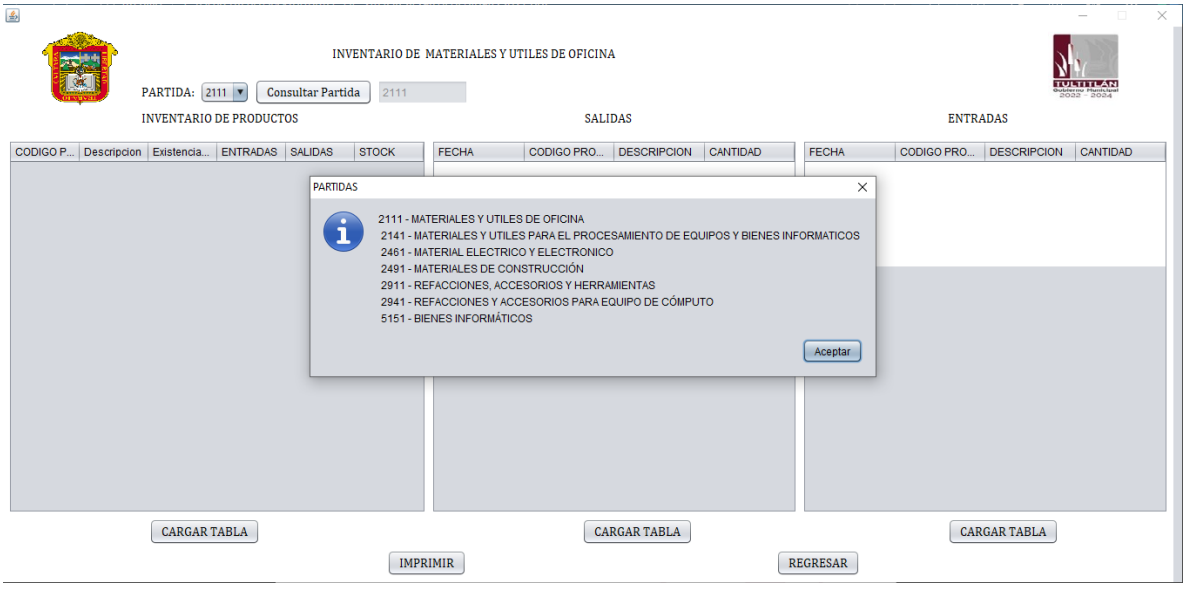


CONSULTA DEL INVENTARIO TOTAL

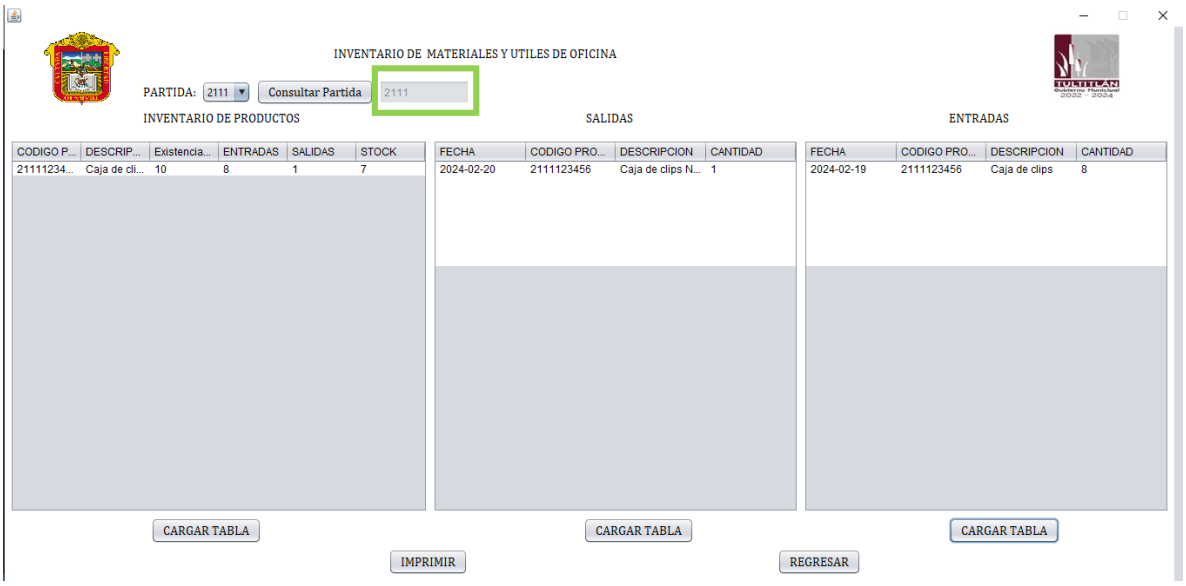
Al seleccionar la opción ‘Inventario Total’ podrá visualizar la siguiente ventana:



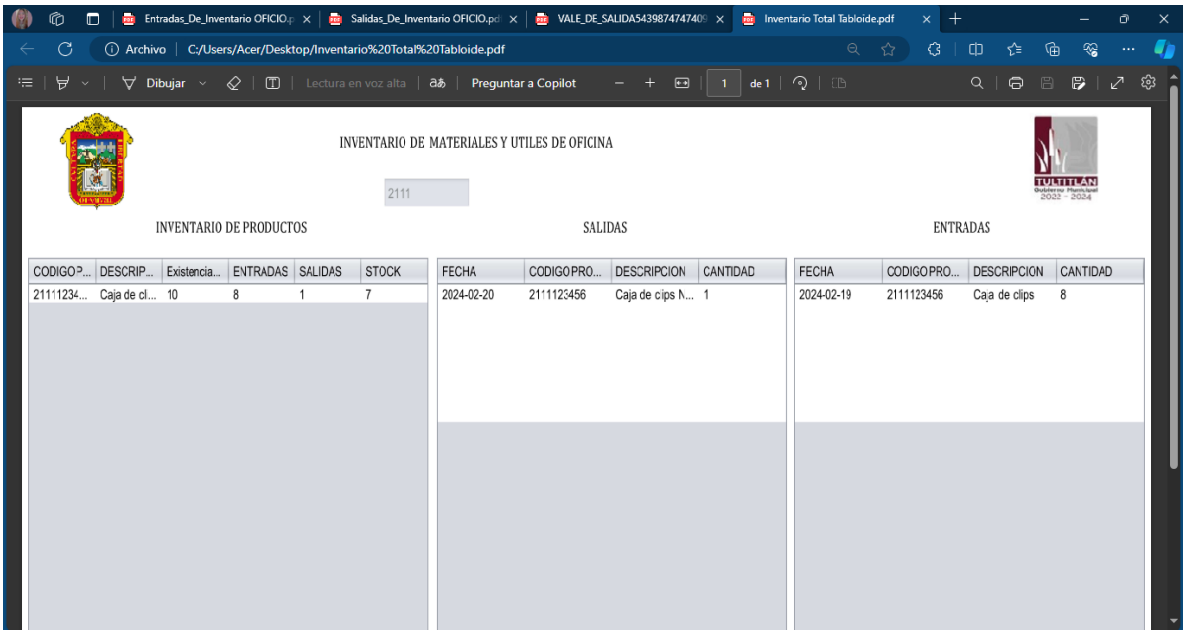
Si desea consultar a que numero corresponde la partida, con ayuda del botón ‘Consultar Partida’ se desplegara la información necesaria:



Al seleccionar la partida podrá visualizar que en el recuadro color verde se verá reflejada la partida seleccionada, una vez realizado esto procede a seleccionar los botones de ‘Cargar Tabla’ que se encuentran debajo de las mismas.

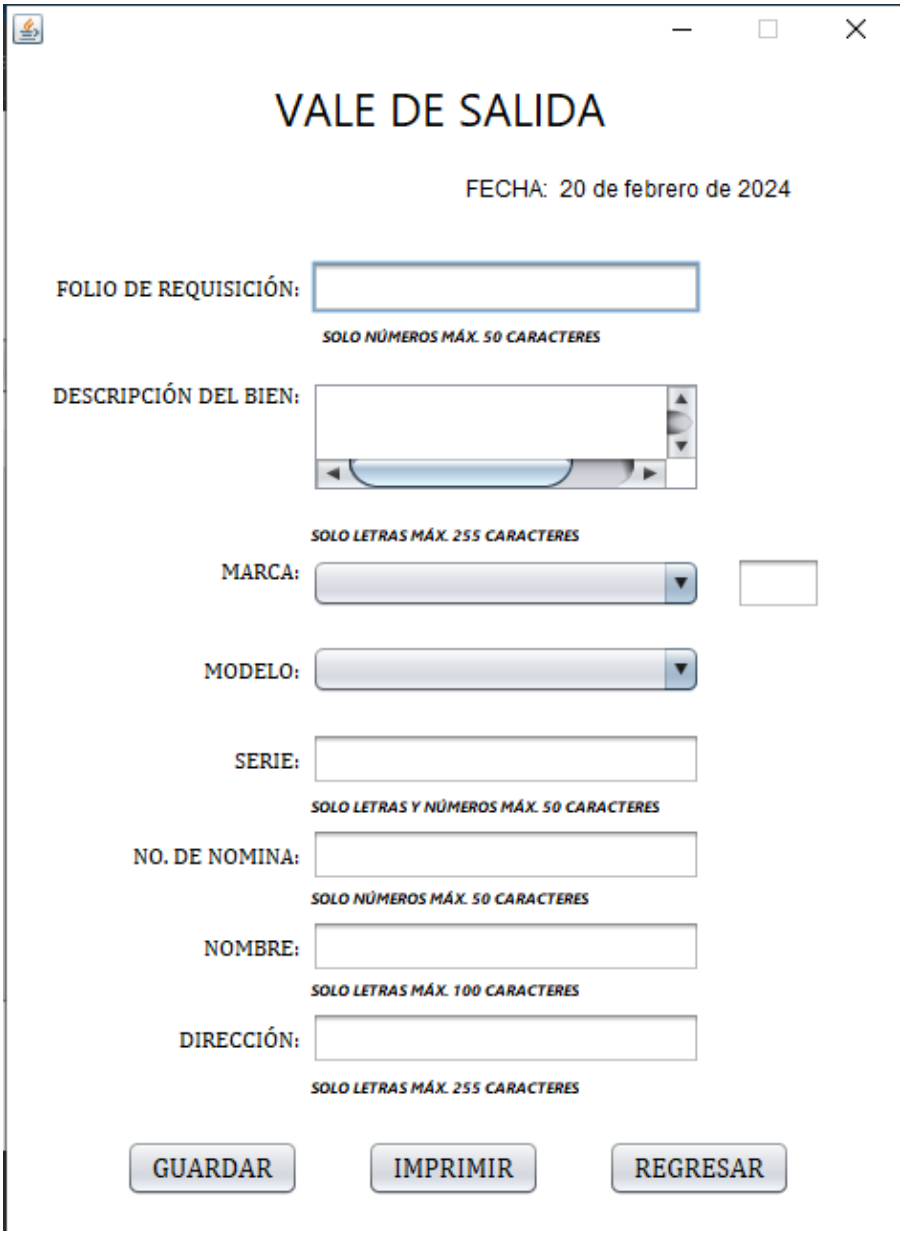


El proceso de impresión es el mismo que se mencionó anteriormente, así como el proceso de guardado como PDF, una vez guardado el PDF en la ruta que designo se podrá visualizar como se muestra a continuación:

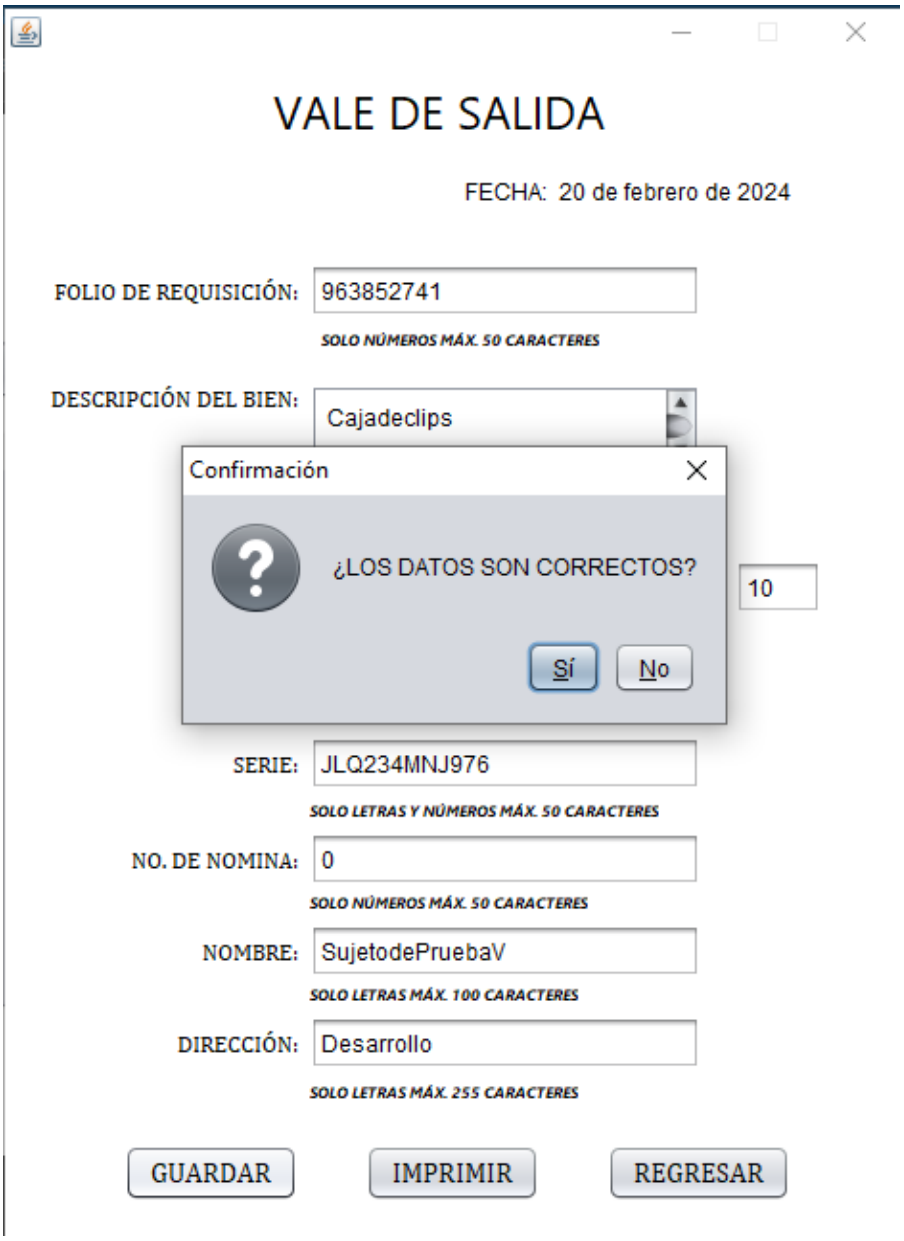


VALE DE SALIDA

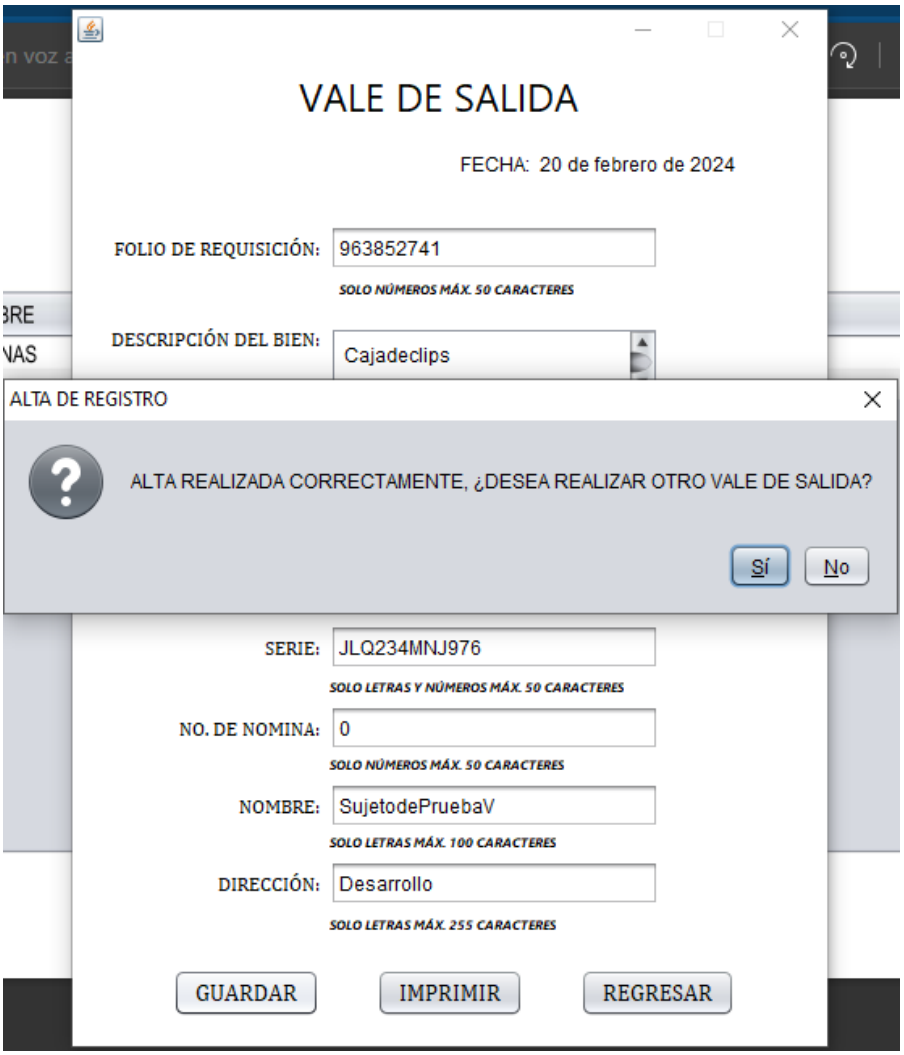
Al seleccionar la opción ‘Vale de Salida’ se abrirá una ventana como se muestra a continuación, los campos cuentan con etiquetas de su llenado ya que algunos campos solo van a permitir letras o números, para la opción de Marca y Modelo se debe de seleccionar de la parte central para que despliegue la información así mismo en el recuadro del lado derecho se debe de visualizar un número, una vez llenado seleccione la opción ‘Guardar’ para que posteriormente se imprima el vale de salida.



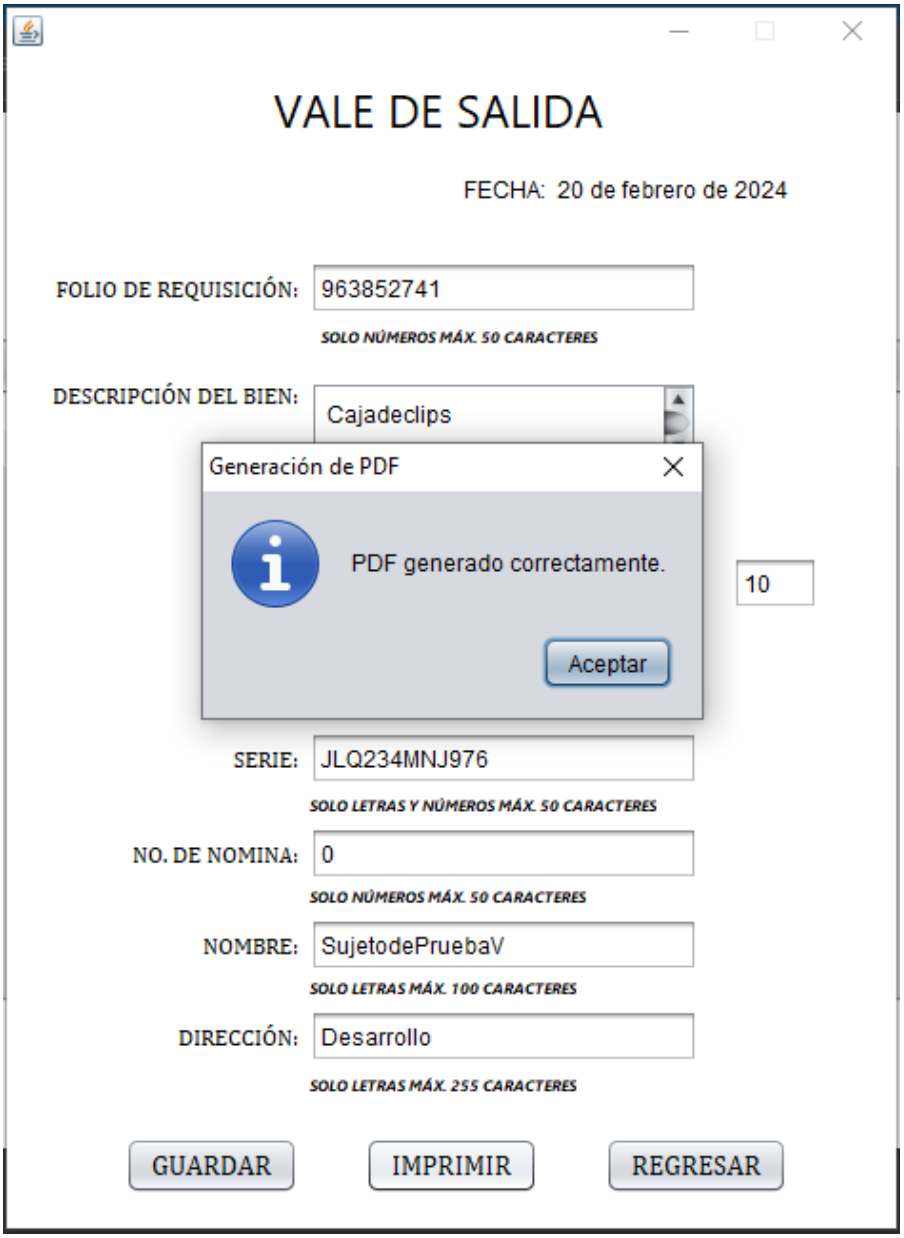
Una vez llenado todos los campos, al seleccionar la opción ‘Guardar’ se arrojará un mensaje de confirmación para corroborar que todos los datos ingresados sean los correctos.



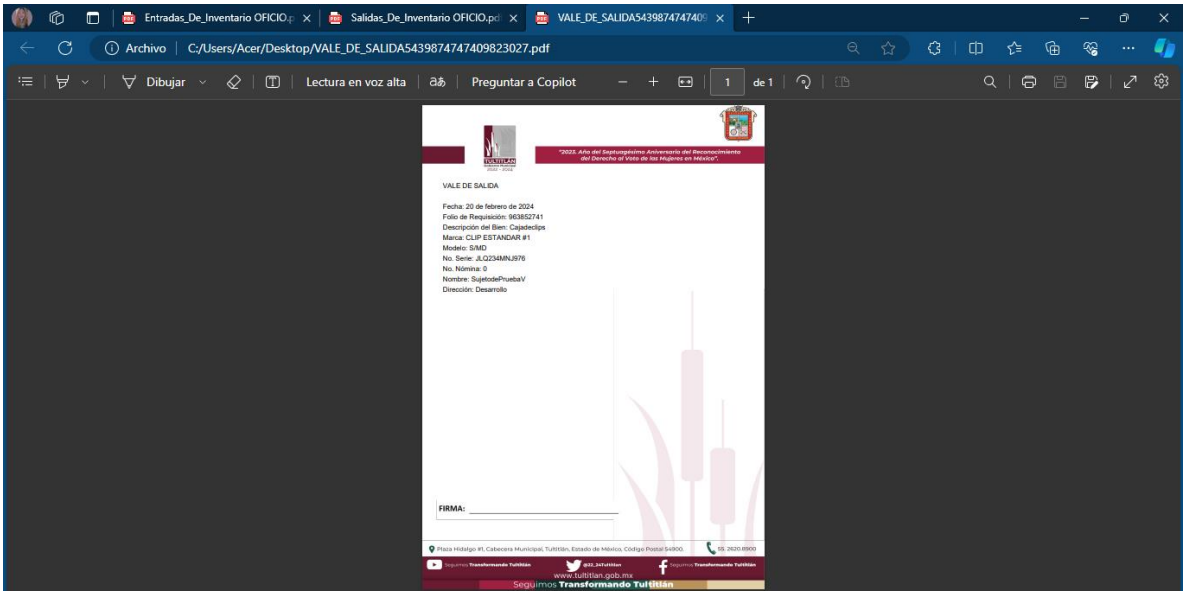
Una vez realizado el guardado, se mostrará otro mensaje emergente por si desea realizar otro vale de salida, lo más recomendable es que imprimas primeramente vale por vale.



Cuando seleccione la opción ‘Imprimir’ se genera un pdf automáticamente en el escritorio de la computadora.



De la siguiente manera es como se visualiza el vale de salida como archivo PDF:



ADMINISTRADOR

CAMBIAR IMAGEN DEL LOG IN

En el código fuente encontrara un JFrame llamado ‘LOG_IN_UTIC’ perteneciente al paquete llamado ‘INTERFACES’, de las líneas de código 267 a 272 está el método donde se dibuja la imagen en la JLabel llamada ‘imagen’:

```
private void SetImageLbel(JLabel labelName, String root) {
        ImageIcon image = new ImageIcon(root);
        Icon icon = new
ImageIcon(image.getImage().getScaledInstance(labelName.getWidth(),
labelName.getHeight(), Image.SCALE_DEFAULT));
        labelName.setIcon(icon);
        this.repaint();
    }
```

Ahora en la línea 17 encontrara la siguiente línea:

SetImageLbel(imagen, "src/img/Logo2.jpg"); donde se manda a llamar el método donde se dibuja la imagen en la JLabel ademas de asignarle como atributo el nombre de la variable de la JLabel en este caso llamada ‘imagen’ más la ruta donde se encuentra la imagen en este caso está dentro del proyecto del inventario en una carpeta llamada ‘IMG’. No olvides revisar la extensión de la imagen ya que puede variar entre ‘jpg’, ‘png’, etc.



CAMBIAR IMAGEN DE LAS CONSULTAS DE ENTRADAS Y SALIDAS E INVENTARIO TOTAL

En el código fuente encontrara en el paquete ‘INVENTARIO’ en el JFrame llamado ‘Entradas_Inventario’ en la línea 257 a la 261 encontrara el mismo método que se maneja en el JFrame ‘LOG_IN_UTIC’, ahora en las líneas del código 24 y 25 está el método donde se dibuja la imagen más sus atributos asignados, que en este caso son el nombre de las variables de las JLabel

SetImageLbel(ESCUDO_MEX, "src/img/escudo_estado_mexico.png");
SetImageLbel(LOGO, "src/img/Logo2.jpg");

La ubicación de las imágenes se encuentra dentro del proyecto, mencionado anteriormente, cabe mencionar que debes revisar la extensión de tu imagen.

Ahora en el mismo paquete llamado ‘INVENTARIO’ en el JFrame llamado ‘Salidas_inventario’ en la línea 209 a 214 está el método donde se dibuja la imagen en el JLabel, y en las líneas 20 y 21 esta implementado el método:

SetImageLbel(ESCUDO_MEX, "src/img/escudo_estado_mexico.png");
SetImageLbel(LOGO, "src/img/Logo2.jpg");

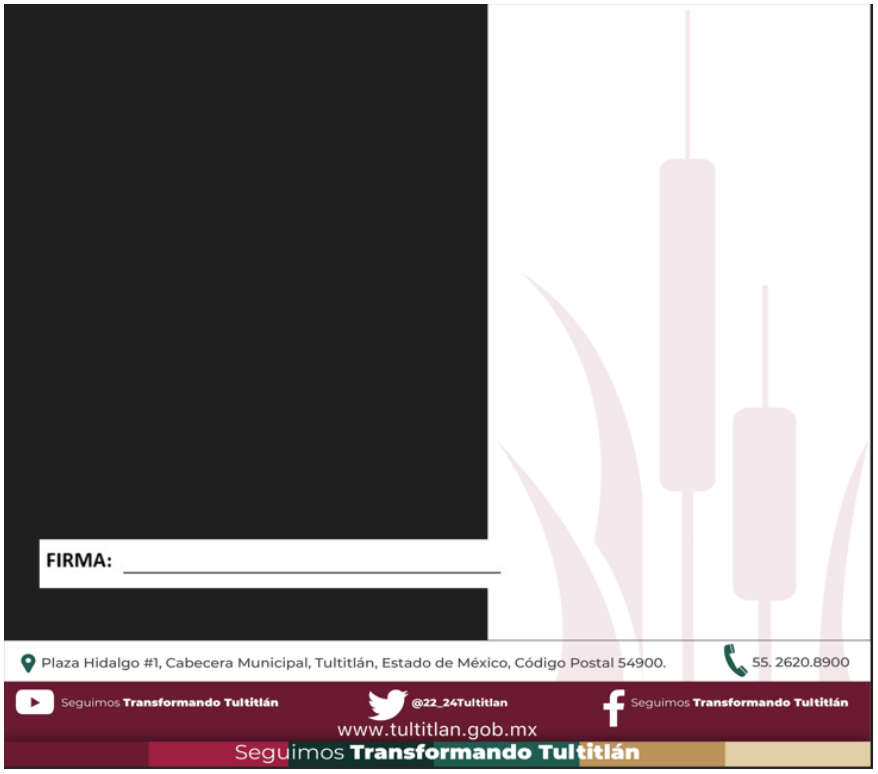
Ahora en el JFrame llamado ‘Inventario_Total’ de la línea 634 a 639 está el método que ayuda dibujar la imagen en el JLabel y en las líneas 23 y 24 esta implementado el método:

SetImageLbel(Escudo_EDOMEX, "src/img/escudo_estado_mexico.png");
SetImageLbel(Logo_Municipio, "src/img/Logo2.jpg");

Este procedimiento se repetirá en el paquete llamado ‘CONSULTAS’.

CAMBIAR IMAGEN DEL ENCABEZADO Y PIE DE PAGINA DEL VALE DE SALIDA

Para el vale de salida que está en el paquete llamado ‘INVENTARIO’ en las líneas 40 a 74 se encuentra el método ‘PdfHeaderFooter’ que ayuda a implementar las imágenes del encabezado del documento asi como el pie de página, exactamente en la línea 45 está la ruta de la imagen del encabezado así como en la línea 66 está la ruta donde se encuentra la imagen del pie de página, en este caso se debe de asegurar que la imagen que se implemente en el pie de página sea como la siguiente:



Ya que al contrario si se implementa completa a la hora de imprimir un vale de salida parte de la información se verá afectada y no se logrará visualizar completamente.

Este procedimiento se repetirá en el en el paquete llamado ‘CAPTURISTA’.