



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

“Plan de continuidad de negocio con el estándar ISO 17799
para la gestión de los recursos de TI y seguridad en la
Universidad Mexiquense del Bicentenario Tultitlán.”

INFORME TÉCNICO DE RESIDENCIAS PROFESIONALES PARA OBTENER EL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

Presenta:

Mikael Ceja Lopez

Saúl Lazo Plata

Michael Alexis Moreno Rivero

Coacalco de Berriozábal, Enero 2024.

AGRADECIMIENTOS

Queremos expresar nuestro más sincero agradecimiento a todas las personas que han contribuido de manera significativa al éxito de nuestro proyecto de Plan de Continuidad de Negocio en la Universidad Mexiquense del Bicentenario, Tultitlán.

En primer lugar, queremos agradecer a nuestra asesora interna, la Mtra. Diana Marisol Prado Oseguera. Su dedicación, orientación y profundo conocimiento en el área fueron fundamentales para el desarrollo y la calidad del plan. Su paciencia y apoyo constante fueron una fuente de inspiración para todo el equipo.

A nuestro asesor externo M. en C. E Juan Raúl Vargas Hernández, le extendemos nuestro agradecimiento más sincero. Su experiencia y visión estratégica han sido invaluable para la formulación y ejecución efectiva del plan. Su compromiso y asesoramiento continuo fueron esenciales para alcanzar los estándares de excelencia que nos propusimos.

No podemos pasar por alto el esfuerzo y la colaboración del personal de la Universidad Mexiquense del Bicentenario, cuya dedicación ha sido esencial en la implementación y consolidación de este proyecto. Cada miembro del equipo ha contribuido con su experiencia y compromiso, lo cual ha fortalecido enormemente nuestro enfoque integral hacia la continuidad de negocio.

En conjunto, hemos logrado crear un plan sólido y efectivo que responde a las necesidades específicas de nuestra institución. Estamos profundamente agradecidos por la oportunidad de trabajar con profesionales tan dedicados y comprometidos, y esperamos que este proyecto sirva como base para fortalecer la resiliencia de la Universidad Mexiquense del Bicentenario en el futuro. A todos, gracias por su arduo trabajo, apoyo y compromiso.

Atentamente.

Ceja López Mikael

Lazo Plata Saúl

Moreno Rivero Michael Alexis

Estudiantes del Tecnológico de Estudios Superiores de Coacalco

15 de Enero de 2024.

RESUMEN

La Universidad Mexiquense del Bicentenario enfrenta importantes retos en la protección de sus activos digitales y la integridad de sus servicios educativos y administrativos debido a la falta de controles adecuados en la gestión de TI y procedimientos sólidos para enfrentar desastres. La institución, que ofrece cuatro carreras principales, ha experimentado incidentes como el robo de equipos de cómputo, lo que evidenció la necesidad de un plan de contingencia efectivo.

Para abordar esta problemática, se desarrolló un Plan de Continuidad del Negocio alineado con el estándar ISO 17799. El objetivo principal es mejorar la seguridad de los datos de estudiantes y personal, asegurar la integridad de los servicios educativos y administrativos, y mantener la calidad educativa ante interrupciones tecnológicas.

El proceso metodológico incluyó una revisión de las estrategias previas, un Análisis de Impacto para identificar y priorizar los procesos críticos, y un Análisis de Riesgos para detectar amenazas y vulnerabilidades específicas. Con base en estos análisis, se desarrollaron estrategias para la recuperación eficiente de los procesos críticos y se estableció un Plan de Reanudación de Operaciones con protocolos claros para mantener la continuidad operacional.

Finalmente, se implementaron estrategias de seguimiento y control para asegurar la efectividad y adaptabilidad del plan frente a desafíos emergentes. El fortalecimiento de controles y la implementación de este plan personalizado aumentarán la eficiencia y resiliencia de la universidad, garantizando una respuesta rápida en emergencias y preservando su reputación académica.

ÍNDICE DE CONTENIDOS

CAPÍTULO I. GENERALIDADES DEL PROYECTO.....	12
INTRODUCCIÓN	13
DESCRIPCIÓN DE LA EMPRESA.....	14
PROBLEMA QUE RESOLVER	18
OBJETIVOS	19
JUSTIFICACIÓN	20
CAPÍTULO II. MARCO TEÓRICO	21
2.1 ESTADO DEL ARTE.....	22
2.2 MARCO CONCEPTUAL.....	26
2.3 MARCO METODOLÓGICO	31
CAPÍTULO III. DESARROLLO.....	40
INTRODUCCIÓN	41
OBJETIVO 0. Analizar Requisitos: Indagar sobre las condiciones de las estrategias ya existentes para apoyar la misión de la institución.....	41
ACTIVIDAD 0.1.....	41
ACTIVIDAD 0.2.....	43
OBJETIVO 1. Analizar Impacto: Identificar aquellos procesos relacionados con apoyar la misión de la institución y el impacto que habría si fuesen interrumpidos, como resultado de un desastre.	45
ACTIVIDAD 1.1.....	45
ACTIVIDAD 1.2.....	48
ACTIVIDAD 1.3.....	58
ACTIVIDAD 1.4.....	60
ACTIVIDAD 1.5.....	65
ACTIVIDAD 1.6.....	70
ACTIVIDAD 1.7.....	79
ACTIVIDAD 1.8.....	82
OBJETIVO 2. Analizar Riesgos: Analizar las amenazas y vulnerabilidades de la institución para controlar o reducir los riesgos de un posible desastre.	86
ACTIVIDAD 2.1.....	86
ACTIVIDAD 2.2.....	90
ACTIVIDAD 2.3.....	93
ACTIVIDAD 2.4.....	101

ACTIVIDAD 2.6.....	136
ACTIVIDAD 2.7.....	143
OBJETIVO 3. Desarrollar Estrategias de Plan de Continuidad de Negocio: Valorar los requerimientos y opciones para la recuperación de procesos críticos y sus recursos en un escenario de interrupción por un desastre.	154
ACTIVIDAD 3.1.....	154
ACTIVIDAD 3.2.....	162
ACTIVIDAD 3.3.....	178
ACTIVIDAD 3.4.....	197
CAPÍTULO IV. RESULTADOS.....	200
OBJETIVO 4. Desarrollar un Plan de Reanudación de Operaciones: Desarrollar un plan para mantener la continuidad del desempeño de la institución, específicamente en la “gestión del riesgo” y en los puntos anteriores.	201
ACTIVIDAD 4.1.....	201
ACTIVIDAD 4.2.....	214
OBJETIVO 5. Realizar las Estrategias Propuestas: Implementar un sistema de seguimiento y control para supervisar continuamente las estrategias de la institución y garantizar su efectividad.	221
ACTIVIDAD 5.1.....	221
ACTIVIDAD 5.2.....	224
ACTIVIDAD 5.3.....	240
ACTIVIDAD 5.4.....	245
CONCLUSIONES	249
COMPETENCIAS DESARROLLADAS	250
FUENTES DE INFORMACIÓN.....	252
ANEXOS.....	254
ANEXO A. INVENTARIO DE LOS ACTIVOS DE TI DE LA INSTITUCIÓN.	255
ANEXO B. CARTA DE JUSTIFICACION DE LA AUSENCIA DE EVIDENCIA DE LOS SISTEMAS DE CONTROL.	271
ANEXO C. EVIDENCIAS DEL SISTEMA DE CONTROL NÚMERO 3. USO DE UN ACCESS POINT PARA EXTENDER LA RED EXISTENTE POR WIFI.	272
ANEXO D. EVIDENCIAS DEL SISTEMA DE CONTROL NÚMERO 4. USO DEL EXTINTOR DESIGNADO.....	274
ANEXO E. TABLA DE UBICACIÓN DE LOS EXTINTORES EN LA INSTITUCIÓN.	277
ANEXO F. PROPUESTA DE BITÁCORA DE INCIDENTES DE TI.	278
ANEXO G. PROPUESTA DE LISTA DE ASISTENCIA PARA LA PRESENTACIÓN DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA.....	279

ANEXO H. PROPUESTA DE LISTA DE ASISTENCIA PARA EL CURSO CONCIENCIACIÓN SOBRE LA SEGURIDAD INFORMÁTICA.....	280
ANEXO I. PROPUESTA DE LISTA DE ASISTENCIA PARA EL CURSO COMO CREAR CONTRASEÑAS SEGURAS Y SU IMPORTANCIA.....	281
ANEXO J. EVIDENCIA DE LA IMPLEMENTACIÓN DE LOS PRODUCTOS SELECCIONA	282
ANEXO K. POLÍTICA DE SEGURIDAD INFORMÁTICA.....	290
ANEXO L. CURSO DE CONCIENCIACIÓN SOBRE SEGURIDAD INFORMÁTICA.....	321
ANEXO M. CURSO PARA LA CREACIÓN DE CONTRASEÑAS SEGURAS Y SU IMPORTANCIA.....	325

ÍNDICE DE TABLAS

Tabla 1. Estado del Arte de los Proyectos Similares o Previos a este.....	22
Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto.....	33
Tabla 3. Recuento de todos los activos de TI de la institución	44
Tabla 4. Departamentos y procesos identificados en la Institución	45
Tabla 5. Impacto financiero identificado por cada uno de los procesos que ejecuta la institución...	49
Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución.	53
Tabla 7. Identificación de los procesos críticos de acuerdo con el impacto financiero y operacional.	58
Tabla 8. Tiempo Máximo Tolerable de inactividad determinado por cada proceso crítico	61
Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados....	65
Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados.	70
Tabla 11. Determinación del punto objetivo de recuperación para cada uno de los procesos identificados.	79
Tabla 12. Identificación de los procesos alternos para cada uno de los procesos	82
Tabla 13. Identificación de los activos de TI asignados a cada uno de los procesos críticos.	86
Tabla 14. Identificación de las amenazas a los activos de TI asignados a cada uno de los procesos críticos.....	90
Tabla 15. Identificación de las vulnerabilidades de los activos de TI asignados a cada uno de los procesos críticos.....	93
Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos	96
Tabla 17. Análisis preguntas 1.1 y 1.2	107
Tabla 18. Análisis preguntas 2.1 y 2.2	108
Tabla 19. Análisis preguntas 3.1 y 3.2	108
Tabla 20. Análisis preguntas 4.1 y 4.2	109
Tabla 21. Análisis preguntas 5.1 y 5.2	110
Tabla 22. Análisis preguntas 6.1 y 6.2	110
Tabla 23. Análisis preguntas 7.1 y 7.2	111
Tabla 24. Análisis preguntas 8.1 y 8.2	112
Tabla 25. Análisis preguntas 9.1 y 9.2	112
Tabla 26. Análisis preguntas 10.1 y 10.2	113
Tabla 27. Análisis preguntas 11.1 y 11	114
Tabla 28. Análisis preguntas 12.1 y 12.2	114
Tabla 29. Análisis preguntas 13.1 y 13.2	115
Tabla 30. Análisis preguntas 14.1 y 14.2.	116
Tabla 31. Análisis preguntas 15.1 y 15.2.	116
Tabla 32. Análisis preguntas 16.1 y 16.2	117
Tabla 33. Análisis preguntas 17.1 y 17.2	118
Tabla 34. Análisis preguntas 18.1 y 18.2	118
Tabla 35. Análisis preguntas 19.1 y 19.2	119
Tabla 36. Análisis preguntas 20.1 y 20.2	120
Tabla 37. Análisis preguntas 21.1 y 21.2	120
Tabla 38. Análisis preguntas 22.1 y 22.2	121

Tabla 39. Análisis preguntas 23.1 y 23.2	122
Tabla 40. Análisis preguntas 24.1 y 24.2	123
Tabla 41. Análisis preguntas 25.1 y 25.2	123
Tabla 42. Análisis preguntas 26.1 y 26.2	124
Tabla 43. Análisis preguntas 27.1 y 27.2	125
Tabla 44. Análisis preguntas 28.1 y 28.2	125
Tabla 45. Análisis preguntas 29.1 y 29.2	126
Tabla 46. Análisis preguntas 30.1 y 30.2	127
Tabla 47. Análisis preguntas 31.1 y 31.2	127
Tabla 48. Análisis preguntas 32.1 y 32.2	128
Tabla 49. Análisis preguntas 33.1 y 33.2	129
Tabla 50. Análisis preguntas 34.1 y 34.2	129
Tabla 51. Análisis preguntas 35.1 y 35.2	130
Tabla 52. Análisis preguntas 36.1 y 36.2	131
Tabla 53. Análisis preguntas 37.1 y 37.2	131
Tabla 54. Análisis preguntas 38.1 y 38.2	132
Tabla 55. Análisis preguntas 39.1 y 39.2	133
Tabla 56. Análisis preguntas 40.1 y 40.2	133
Tabla 57. Análisis preguntas 41.1 y 41.2	134
Tabla 58. Análisis preguntas 42.1 y 42.2	135
Tabla 59. Cuadro de la prioridad del riesgo acorde al impacto y probabilidad de este.....	136
Tabla 60. Priorización de las Amenazas de acuerdo con el impacto y la probabilidad.....	137
Tabla 61. Priorización de las Vulnerabilidades de acuerdo con el impacto y la probabilidad	140
Tabla 62. Evaluación de los sistemas de control. Control Número 1. Parte 1	144
Tabla 63. Evaluación de los sistemas de control. Control Número 1. Parte 2	145
Tabla 64. Evaluación de los sistemas de control. Control Número 2. Parte 1	146
Tabla 65. Evaluación de los sistemas de control. Control Número 2. Parte 2	147
Tabla 66. Evaluación de los sistemas de control. Control Número 3. Parte 1	148
Tabla 67. Evaluación de los sistemas de control. Control Número 3. Parte 2	149
Tabla 68. Evaluación de los sistemas de control. Control Número 4. Parte 1	150
Tabla 69. Evaluación de los sistemas de control. Control Número 4. Parte 2	151
Tabla 70. Evaluación de los sistemas de control. Control Número 5. Parte 1	152
Tabla 71. Evaluación de los sistemas de control. Control Número 5. Parte 2	153
Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799.....	155
Tabla 73. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 1er conjunto ...	162
Tabla 74. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 2do conjunto ..	164
Tabla 75. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 3er conjunto ...	165
Tabla 76. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 4to conjunto ...	167
Tabla 77. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 5to conjunto ...	168
Tabla 78. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 6to conjunto ...	170
Tabla 79. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 7mo conjunto .	171
Tabla 80. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 8vo conjunto ..	173
Tabla 81. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 9no conjunto ..	174

Tabla 82. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 10mo conjunto.	176
Tabla 83. Cuadro de evaluación de viabilidad	179
Tabla 84. Cuadro de las tecnologías utilizadas para el desarrollo del sistema.....	226
Tabla 85. Inventario completo de todos los Activos de TI de la Institución.....	255
Tabla 86. Ubicación de los extintoras en la Institución. Resultado de la evaluación del sistema de control Número 4	277
Tabla 87. Cuadro de asignación de personal para ejecutar la Política. Elemento 3 de la Política .	310

ÍNDICE DE FIGURAS

Figura 1. Ubicación de la Institución	14
Figura 2. Organigrama de la Institución.....	15
Figura 3. Diagrama de las Fases que componen un PCN.....	31
Figura 4. Grafica de Gantt de las Actividades a Desarrollar	39
Figura 5. Croquis de la institución donde marca la ubicación de la TI localizada	43
Figura 6. Valores del riesgo acorde a la probabilidad/impacto.	136
Figura 7. Diagrama de Procedimientos. Proceso No. 1.....	204
Figura 8. Diagrama de Procedimientos. Proceso No. 2.....	205
Figura 9. Diagrama de Procedimientos. Proceso No. 3.....	206
Figura 10. Diagrama de Procedimientos. Proceso No. 4.....	207
Figura 11. Diagrama de Procedimientos. Proceso No. 5.....	208
Figura 12. Diagrama de Procedimientos. Proceso No. 6.....	209
Figura 13. Diagrama de Procedimientos. Proceso No. 7.....	210
Figura 14. Diagrama de Procedimientos. Proceso No. 8.....	211
Figura 15. Diagrama de Procedimientos. Proceso No. 9.....	212
Figura 16. Diagrama de Procedimientos. Proceso No. 10.....	213
Figura 17. Color. #86B13A: Dark moderate green	226
Figura 18. Color. #EEE1C8: Light grayish orange	227
Figura 19. Diagrama de la Base de Datos en SQL Server Managment Studio	227
Figura 20. Ventana de Inicio de Sesión.....	229
Figura 21. Ventana del Panel de Control	230
Figura 22. Ventana de Visualización de los Activos.....	231
Figura 23. Ventana para Registrar un Activo.....	232
Figura 24. Ventana para Eliminar un Activo	233
Figura 25. Ventana para Agregar un Activo	234
Figura 26. Ventana para Asignar un Software a un Activo.....	235
Figura 27. Ventana para Eliminar un Software de un Activo	236
Figura 28. Ventana Panel de Control de Admin	237
Figura 29. Ventana para Registro Múltiples de Activos	237
Figura 30. Ventana para Eliminar Múltiples de Activos.....	238
Figura 31. Ventana para Asignar Departamento.....	238
Figura 32. Material del Curso. Imagen de apoyo para el curso de Concienciación sobre la Seguridad informática	241
Figura 33. Material del Curso. Infografía sobre Seguridad Informática	242
Figura 34. Material del Curso. Prueba de Aprendizaje sobre el curso para la Concienciación sobre la Seguridad Informática. Parte 1.....	243
Figura 35. Material del Curso. Prueba de Aprendizaje sobre el curso para la Concienciación sobre la Seguridad Informática. Parte 2.....	244
Figura 36. Material del Curso. Imagen de apoyo para el curso de creación de contraseñas seguras y su importancia.	246
Figura 37. Material del Curso. Prueba de Aprendizaje sobre el curso para la Creación de Contraseñas Seguras y su Importancia. Parte 1.....	247

Figura 38. Material del Curso. Prueba de Aprendizaje sobre el curso para la Creación de Contraseñas Seguras y su Importancia. Parte 2.....	248
Figura 39. Carta de justificación de la ausencia de evidencia de los sistemas de control.....	271
Figura 40. Sistema de Control Número 3. Evidencia 1. Salida del cable ethernet del Access Point por la pared.....	272
Figura 41. Sistema de Control Número 3. Evidencia 2. Cruce del cable ethernet por el pacillo	272
Figura 42. Sistema de Control Número 3. Evidencia 3. Conexión del cable ethernet a la terminal de red del laboratorio de cómputo.....	273
Figura 43. Sistema de Control Número 3. Evidencia 4. Foto completa del cable ethernet.....	273
Figura 44. Sistema de Control Número 4. Evidencia 1. Foto de ausencia de extintor en el laboratorio D1.....	274
Figura 45. Sistema de Control Número 4. Evidencia 2. Foto de ausencia de extintor en el laboratorio C6.....	274
Figura 46. Sistema de Control Número 4. Evidencia 3. Foto del extintor número 1.....	275
Figura 47. Sistema de Control Número 4. Evidencia 4. Foto del extintor número 2.....	275
Figura 48. Sistema de Control Número 4. Evidencia 5. Foto del extintor número 3.....	276
Figura 49. Sistema de Control Número 4. Evidencia 6. Foto del extintor número 4.....	276
Figura 50. Propuesta de Bitácora de Incidentes de TI.....	278
Figura 51. Propuesta de lista de asistencia para la presentación de la Política de Seguridad Informática.....	279
Figura 52. Propuesta de lista de asistencia para el curso “Concienciación sobre la Seguridad Informática”.....	280
Figura 53. Propuesta de lista de asistencia para el curso “Como crear contraseñas seguras y su importancia”.....	281
Figura 54. Aprobación por parte de todos los involucrados de la Política de Seguridad Informática.....	282
Figura 55. Aplicación de la versión recortada de la Política de Seguridad Informática en el Laboratorio C6.....	283
Figura 56. Ejecución del Sistema de Inventario de TI. Parte 1.....	283
Figura 57. Ejecución del Sistema de Inventario de TI. Parte 2.....	284
Figura 58. Lista de asistencia al curso de “Concienciación sobre seguridad informática”.....	285
Figura 59. Captura de pantalla del aquellos que respondieron el cuestionario del curso de “Concienciación sobre seguridad informática”.....	286
Figura 60. Lista de asistencia al curso de “Creación de contraseñas seguras y su importancia”	287
Figura 61. Captura de pantalla del aquellos que respondieron el cuestionario del curso de “Creación de contraseñas seguras y su importancia”.....	288
Figura 62. Distribución de las puntuaciones totales del curso de “Concienciación sobre seguridad informática”.....	289
Figura 63. Distribución de las puntuaciones totales del curso de “Creación de contraseñas seguras y su importancia”.....	289

CAPÍTULO I. GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

La Universidad Mexiquense del Bicentenario se enfrenta a desafíos críticos en la gestión de su Tecnología de la Información (TI) y la continuidad de sus operaciones esenciales. Esta institución, que desempeña un papel crucial en la formación de recursos humanos y cuenta con una amplia gama de procesos críticos en la gestión académica, administrativa y de recursos, ha identificado la necesidad urgente de fortalecer sus controles internos y desarrollar un Plan de Continuidad del Negocio que esté alineado con estándares internacionales.

Este trabajo se centra en desarrollar un plan de continuidad de negocio conforme al estándar ISO 17799, un marco reconocido para la gestión de recursos de TI y seguridad. La relevancia de este proyecto radica no solo en su potencial para mejorar la seguridad de datos y la integridad de los servicios educativos y administrativos, sino también en su capacidad para fomentar un entorno académico donde la continuidad y la calidad educativa sean resilientes frente a interrupciones tecnológicas.

Para abordar estos desafíos de manera estructurada y efectiva, se ha adoptado una metodología integral que incluye el análisis de estrategias existentes, la evaluación del impacto y los riesgos, y el desarrollo de estrategias específicas para la continuidad de las operaciones críticas y la gestión del riesgo. Este enfoque metódico asegura no solo la implementación de un sistema robusto de seguimiento y control para garantizar la efectividad de las estrategias, sino también la adaptación del plan a las necesidades específicas de la universidad, abarcando desde la gestión de activos y el control de acceso hasta la gestión de incidentes.

Este proyecto, por tanto, no solo representa una iniciativa para abordar las vulnerabilidades actuales y mejorar la gestión de TI, sino que también es un paso hacia la transformación de la institución en un entorno académico más seguro, eficiente y resiliente.

DESCRIPCIÓN DE LA EMPRESA

Nombre o razón social

“Universidad Mexiquense del Bicentenario”

Ubicación

“Avenida Ex Hacienda los Portales SN, Colonia Villa Esmeralda, 54910 Tultitlán de Mariano Escobedo, Tultitlán, Estado de México. Frente Soriana, Coppel y Central de Abastos Tultitlán”



Figura 1. Ubicación de la Institución. [Fuente: Google Maps (2023)].

Organigrama

A continuación, se muestra una imagen de la estructura organizacional de la Universidad Mexiquense del Bicentenario, para el momento en el que fue publicado este trabajo.

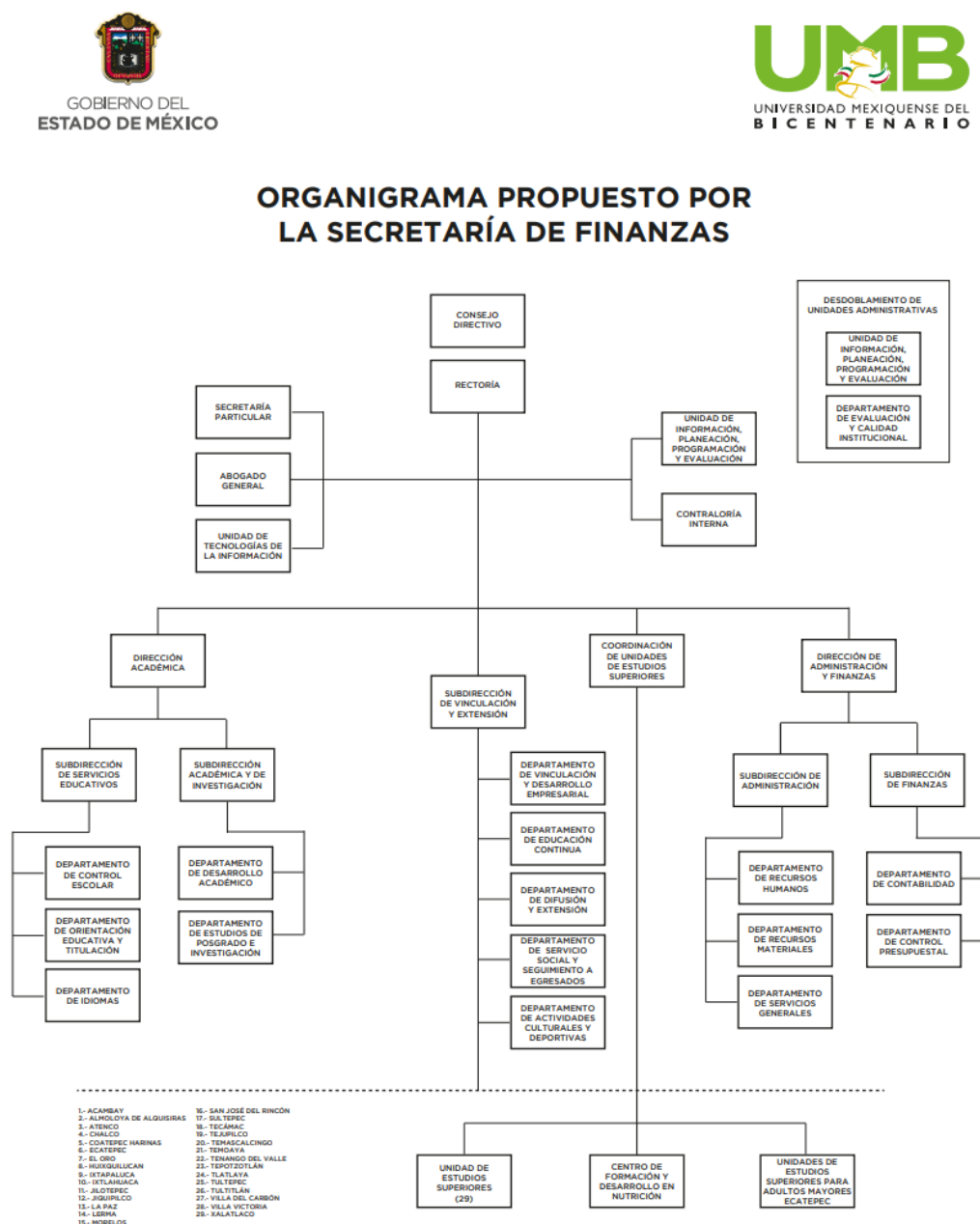


Figura 2. Organigrama de la Institución. [Fuente: UMB (2023)].

Sector productivo de la empresa

Servicios.

Misión, Visión, Filosofía y/o Valores

Misión

“La Universidad Mexiquense del Bicentenario es una institución de carácter público, en busca de la excelencia académica, enfocada a la formación integral de profesionistas con conocimientos, habilidades, competencias, vocación de transformación social y un amplio sentido de la vida; con plena conciencia de la situación regional, estatal y nacional, capaces de desempeñarse eficientemente, con valores universitarios y comprometidos con el desarrollo sustentable, económico, científico, tecnológico y cultural de la humanidad”.

Visión

“Ser la Institución de Educación Superior del Estado de México reconocida por su excelencia académica, comprometida con las necesidades, intereses y requerimientos de la sociedad, contribuyendo al desarrollo regional, estatal y nacional”.

Valores

Humanismo

Se fundamenta en el valor de los seres humanos, dándole mayor importancia al pensamiento crítico y a lo racional, impulsando las potencialidades de la comunidad universitaria para ofrecer a la sociedad profesionales más justos, de trato equitativo, que fomenten los valores humanos, ante los procesos culturales y sociales.

Verdad

Es el fundamento del auténtico conocimiento y de la persona en la que no hay doblez. Indispensable para una Institución Educativa.

Compromiso

Comprometerse va más allá de cumplir con una obligación, es poner en juego nuestras capacidades para sacar adelante todo aquello que se nos ha confiado. Es un aspecto fundamental del emprendedor.

Lealtad

Cumplimiento de lo que exigen las leyes de la fidelidad y las del honor, es el amor y la gratitud que muestran las personas hacia sus amigos, padres, compañeros, etc. Aspecto fundamental para la persona del siglo XXI.

Servicio

Brindar ayuda de manera espontánea en los detalles pequeños de manera diligente; habla de nuestro alto sentido de colaboración para hacer la vida más ligera a los demás. Fundamento de la auténtica vocación.

Trascendencia

Fundamento para rebasar los paradigmas establecidos y buscar nuevos significados del conocimiento, la verdad, la belleza. Es el detonante de una auténtica espiritualidad.

Breve historia de la empresa.

Nuestra casa de estudios surge como una respuesta para replantear el sistema educativo estatal y nacional, para revisar y proponer un modelo educativo, pedagógico, que se aparte de los paradigmas de la recepción, que promueva la creatividad, la autodisciplina, la necesidad de la formación permanente en cada uno de sus egresados y de las personas que quieran ser parte de este proyecto educativo.

PROBLEMA QUE RESOLVER

“Universidad Mexiquense del Bicentenario” es una institución de educación superior que desempeña un papel fundamental en la formación de recursos humanos, la institución cuenta con una gran cantidad de procesos críticos como gestión académica, administrativa y de recursos que requieren el uso activo de la TI. La universidad cuenta con 4 carreras, 2 pertenecientes al área de ingeniería (Química y Civil) así como dos licenciaturas (contaduría y psicología industrial).

La universidad tiene una falta de control adecuado en cuanto a la gestión de la TI con la que cuenta, aunado a ello, la ausencia de procedimientos solidos en caso de desastres provoca que la institución se encuentre expuesta a la amenaza de perder su TI y por lo tanto ver interrumpidos los procesos académicos, así como administrativos que esta desempeña. Además de resaltar que toda el área administrativa se ve rodeada de una falta de conciencia en cuanto a las amenazas a las que se encuentra expuesta la TI y los procesos de la institución, generando que aumente el riesgo de una falla catastrófica que pueda dejar inoperable a gran parte de la institución en un periodo de tiempo perjudicioso, lo que haría que la Universidad se vea afectada tanto en su desempeño como en su reputación como institución académica de grado superior. Así mismo se tiene el precedente de un percance que la Universidad sufrió no hace mucho donde fueron robados varios equipos de cómputo de uno de los laboratorios y al no existir algún proceso o estrategia de recuperación fue necesario cerrar dicho laboratorio afectando directamente al desempeño académico; este incidente no es más que una prueba clara de la falta de un control generalizado para toda la TI con la que se cuenta. Por esta razón y por la gran preocupación de la coordinadora que está a cargo de la institución de que una situación parecida o inclusive peor a la anteriormente mencionada, se repita, es imperativo la implementación de un Plan de Continuidad del Negocio.

OBJETIVOS

Objetivo general

Desarrollar un plan de continuidad de negocio conforme al estándar ISO 17799 para la gestión de recursos de TI y seguridad en la Universidad Mexiquense del Bicentenario Tultitlán.

Objetivos específicos

0. Analizar Requisitos. -Indagar sobre las condiciones de las estrategias ya existentes para apoyar la misión de la institución.
1. Analizar Impacto. - Identificar aquellos procesos relacionados con apoyar la misión de la institución y el impacto que habría si fuesen interrumpidos, como resultado de un desastre.
2. Analizar Riesgos. - Analizar las amenazas y vulnerabilidades de la institución para controlar o reducir los riesgos de un posible desastre.
3. Desarrollar Estrategias de Plan de Continuidad de Negocio. - Valorar los requerimientos y opciones para la recuperación de procesos críticos y sus recursos en un escenario de interrupción por un desastre.
4. Desarrollar un Plan de Reanudación de Operaciones. - Desarrollar un plan para mantener la continuidad del desempeño de la institución, específicamente en la “gestión del riesgo” y en los puntos anteriores.
5. Realizar las Estrategias Propuestas. - Implementar un sistema de seguimiento y control para supervisar continuamente las estrategias de la institución y garantizar su efectividad.

JUSTIFICACIÓN

La Universidad Mexiquense del Bicentenario enfrenta desafíos significativos en relación con la seguridad de la tecnología de la información (TI) y la continuidad de sus operaciones críticas. Al fortalecer los controles internos, la institución protegerá sus activos digitales, mejorará la seguridad de datos de estudiantes y personal, y mantendrá la integridad de los servicios educativos y administrativos. La adopción de medidas proactivas resultará en una operación más eficiente y confiable, fomentando un entorno académico donde la continuidad y la calidad educativa son inmunes a las interrupciones tecnológicas. Un plan de contingencia consolidado servirá como salvaguarda ante emergencias, permitiendo una recuperación rápida y ordenada que minimiza el tiempo de inactividad y preserva la reputación de la universidad. Estas mejoras estratégicas son fundamentales para sostener la excelencia y competitividad de la Universidad Mexiquense del Bicentenario. La implementación de estas acciones culminará en la creación de un plan de continuidad de negocio sólido y adaptado a las necesidades específicas de la universidad.

CAPÍTULO II. MARCO TEÓRICO

A continuación, se presenta el Marco Teórico, el cual inicia con el Estado del Arte el cual ofrece una visión actualizada de los trabajos que precedieron a este. El Marco Conceptual que proporciona la estructura teórica esencial para comprender los resultados y definiendo conceptos clave. Por último, el Marco Metodológico que delinea las estrategias utilizadas, así como los recursos consultados para desarrollar el proyecto.

2.1 ESTADO DEL ARTE

La gestión efectiva de la continuidad en las operaciones universitarias es esencial para preservar la estabilidad académica y administrativa en situaciones de emergencia. Este análisis del estado del arte se enfoca en revisar trabajos y estudios previos que abordan la planificación de la continuidad en universidades. Examinaremos enfoques innovadores y mejores prácticas, destacando las áreas de investigación emergentes y los desafíos pendientes. El objetivo es comprender el panorama actual y señalar oportunidades para el avance en la preparación ante eventos disruptivos en el ámbito académico.

Tabla 1. Estado del Arte de los Proyectos Similares o Previos a este. [Fuente: Elaboración propia].

Autor	Nombre del trabajo	Año de publicación	Métodos Utilizados	Resultados
Rojas Bustamante, Jairo David	Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador	2017	• Análisis del contexto. • Definición de las características organizacionales. • Identificación de procesos organizacionales y sus interrelaciones. • Análisis de impacto en el negocio.	Se lograron identificar los incidentes que pueden atentar contra los procesos, posibilitando identificar los tiempos críticos de recuperación, así mismo, se identificaron los controles para cada amenaza, además de establecerse los informes que resultan de los análisis y verificaciones realizadas.

Tabla 1. Estado del Arte de los Proyectos Parecidos o Previos a este. [Fuente: Elaboración propia]. (Continuación).

Autor	Nombre del trabajo	Año de publicación	Métodos Utilizados	Resultados
Malaver Duarte, Jeimy Carolina	Diseño e implementación del plan de continuidad de negocio en Bancompartir	2020	• Análisis de involucrados. • Generación de un árbol de problemas. • Generación de un árbol de objetivos. • Identificación de acciones y alternativas.	Se estableció una estrategia de continuidad del negocio basada en los procesos críticos y en los recursos como personal, aplicativos, costos y tecnología que son necesarios para que puedan operar, todo enfocado a mantener el servicio en caso de un evento de indisponibilidad.
Yolanda Pérez (directora del área de Gobierno, Riesgo y Cumplimiento (GRC) en KPMG)	La nueva era de los planes de continuidad de negocio	2021	• Reflexión sobre la importancia de los BCPs especialmente en respuesta a la pandemia.	No especificados, pero discute la necesidad de tener BCPs bien establecidos.
Plan de continuidad de negocio en las universidades	Plan de continuidad de negocio en las universidades	2022	• Identificación de servicios críticos y análisis de riesgos. • Determinación de estrategias de recuperación. • Documentación de la estrategia de continuidad. • Diseño y realización de pruebas de eficacia. Formación del personal involucrado.	Se logro establecer un PCN robusto, con un énfasis en la preparación y respuesta a incidentes, la recuperación de servicios y la minimización del impacto en caso de interrupciones.

Tabla 1. Estado del Arte de los Proyectos Parecidos o Previos a este. [Fuente: Elaboración propia]. (Continuación).

Autor	Nombre del trabajo	Año de publicación	Métodos Utilizados	Resultados
Joaquín Canca Cuenca.	Plan de Continuidad de Negocio Universidad de Málaga	2022	• Entrevistas estructuradas con administradores universitarios. • Análisis de documentos institucionales, incluyendo planes de continuidad de negocio existentes. • Revisión de casos de estudio de interrupciones pasadas en otras instituciones educativas.	Identificación de áreas críticas de vulnerabilidad en los planes de continuidad de negocio universitarios. Evaluación de la efectividad de las estrategias de recuperación implementadas en casos previos. Recomendaciones para mejorar la preparación y respuesta ante posibles interrupciones.
Mora Yomayaza David Felipe	Plan de Continuidad de Negocio Como Base del Éxito Organizacional - Universidad Piloto de Colombia		• Encuestas a personal universitario para evaluar la percepción y conocimiento sobre planes de continuidad. • Análisis de tecnologías utilizadas en planes de continuidad en universidades de referencia. • Estudio de casos detallado sobre la implementación exitosa de tecnologías específicas en situaciones de crisis.	Identificación de la importancia de la tecnología en la eficacia de los planes de continuidad. Evaluación de las tecnologías emergentes utilizadas en la planificación de continuidad. Desarrollo de recomendaciones para la integración efectiva de la tecnología en futuros planes de continuidad.

En este análisis, se examinan y proponen mejoras clave para fortalecer los planes de continuidad de negocios en el ámbito universitario. Basándonos en la información detallada en la tabla, se identificaron áreas de oportunidad para optimizar la preparación ante posibles interrupciones, ya sean de origen tecnológico, académico o derivadas de eventos imprevistos.

Las siguientes sugerencias se presentan con el propósito de mejorar la resiliencia de la universidad, asegurando la eficacia de los planes de continuidad y promoviendo la adaptabilidad a entornos cambiantes.

Centralización de Recursos Tecnológicos.

Considerar la centralización de recursos tecnológicos, como servidores y sistemas de respaldo, para mejorar la eficiencia en la gestión de la infraestructura tecnológica.

Implementación de Herramientas de Colaboración.

Introducir y promover el uso de herramientas de colaboración en línea y plataformas de comunicación para garantizar una rápida transición a entornos virtuales en casos de emergencia.

Pruebas y Simulacros Regulares.

Realizar pruebas y simulacros regulares del plan de continuidad para evaluar la efectividad de las medidas adoptadas.

Colaboración con Empresas y Organizaciones Externas.

Establecer alianzas y colaboraciones con empresas y organizaciones externas para compartir recursos y experiencias en la gestión de la continuidad.

2.2 MARCO CONCEPTUAL

El presente marco conceptual es esencial para contextualizar y comprender la interconexión de conceptos que se aplicarán en el desarrollo del proyecto. Ofrece una visión integral de los términos y relaciones teóricas que se utilizan para abordar la continuidad de negocio en un entorno educativo y específicamente en el ámbito de TI de la institución UMB Tultitlán.

A lo largo de este documento, se explorarán conceptos clave, tales como la gestión de riesgos, la recuperación ante desastres, las normativas de seguridad, y otros elementos que contribuyen a la elaboración y ejecución de un plan de continuidad de negocio efectivo en el contexto educativo.

1. Auditoría Informática

Es un proceso que consiste en recopilar, agrupar y evaluar evidencias que permiten determinar si el sistema informático utilizado por una empresa mantiene la integridad de los datos, cumple con los protocolos establecidos, hace un uso eficiente de los recursos, cumple con las normativas y leyes establecidas que regulan la materia (Ponce, 2023).

Características Principales

El tipo de evaluación específica que se lleva a cabo en el área de Tecnología de la Información.

- La auditoría informática, debe funcionar como una imagen de confianza sobre la digitalización del flujo de trabajo empresarial.
- La evaluación no solo requiere el estudio de los activos informáticos físicos de una empresa, sino que debe ir más allá, englobando las prácticas y uso de las herramientas de trabajo
- Debe haber un seguimiento constante de las actualizaciones informáticas del mercado y su aplicación empresarial (Ponce, 2023).

2. Plan de Continuidad de Negocio

Un plan de continuidad de negocios o BCP, por sus siglas en inglés (Business Continuity Planning), es un documento que describe los procesos y sistemas de la empresa, sus posibles fallas y cómo atenderlas.

Incluye planes de contingencia para los problemas que puedan presentarse en diferentes ámbitos de la compañía, bien sea por ciberataques, desastres naturales o cualquier error que ponga en riesgo su correcto funcionamiento (LISA Institute, 2023).

❖ Características de un Plan de Continuidad de Negocio

Identificar y ordenar las amenazas. Puede usarse una lista con los incidentes capaces de interrumpir la actividad de la compañía. Aquí hay que considerar fenómenos naturales y situaciones provocadas por personas.

Analizar el impacto en la empresa, luego de determinar las áreas de la compañía que serían críticas para su supervivencia. En este punto también es importante calcular cuánto podría resistir la empresa antes de que la falta de una función específica pueda provocar un impacto grave. Esto ayudará a establecer prioridades acerca de las funciones que no pueden parar ante una crisis.

Crear un plan de respuesta y recuperación. Como extensión del análisis previo, hay que recabar datos de los bienes que estén involucrados en las funciones críticas. En cuanto a los equipos, es muy importante tener sus números de serie, los acuerdos de licencia, las garantías y la información de los contactos para saber a quién habría que llamar en cada categoría de incidente. En esta parte, el BCR se relaciona con otro tipo de plan: el de comunicación de crisis, para tener en consideración quién es vocero de la compañía y podría dar un mensaje público si fuera necesario.

Probar el plan y evaluar el análisis. Los expertos en administración de BCR recomiendan evaluar el plan y probarlo con simulaciones por lo menos una vez al año. Aquí es necesario hacer análisis paso a paso de las situaciones que podrían presentarse y hacer simulaciones (Serafin, 2020).

• Análisis de Riesgo

El análisis de riesgos es una forma de encontrar y tratar problemas que podrían perjudicar a proyectos o iniciativas empresariales importantes. Sin embargo, también puede aplicarse a proyectos no empresariales, como la planificación de eventos o incluso la compra de una vivienda.

Para realizar un análisis de riesgos, primero debes identificar las amenazas potenciales a las que te enfrentas, después estimar sus consecuencias probables si se producen y, por último, calcular la probabilidad de que estas amenazas se produzcan (Ortega, 2023).

• Gestión de Riesgos

La gestión de riesgos de los proyectos, también conocida como Risk Management, es la práctica de identificar, analizar y responder de manera proactiva a diferentes tipos de riesgos potenciales de un proyecto. Un riesgo de un proyecto es todo aquello que pueda afectar al éxito del proyecto, puede ser algo que cause retrasos en el cronograma del proyecto, que haga que se exceda el presupuesto previsto o cualquier cosa que derive en la disminución del rendimiento del equipo de un modo u otro (Asana, Inc, 2023).

- **Manejo de Crisis**

Indica los pasos para manejar las comunicaciones y minimizar el impacto en la imagen.

Cabe destacar que existen dos tipos de crisis que se puede enfrentar, aquellas que se dan internamente dentro de su operación, las cuales no son de importancia pública y se pueden solucionar rápidamente y aquellas que afectan de forma directa la imagen de la empresa, así como sus partes interesadas generando un efecto negativo en los clientes y afectando la imagen (Disaster Recovery, 2018).

- **Evaluación de Impacto**

Identificar los procesos más críticos para la organización los cuales, le puedan permitir seguir la operación para entregar el producto y servicios aún en un nivel más bajo pero sin afectación considerable, identificar los recursos necesarios y al mismo tiempo determinar los periodos máximos en los cuales la empresa puede continuar si ese proceso se detiene por una afectación grave y dar un nivel de impacto por cada proceso con estos datos se pueden analizar y conocer las operaciones y/o procesos más críticos y los tiempos de recuperación para la empresa (Disaster Recovery, 2018).

- **Recuperación de Desastres**

En esta etapa determinar los recursos necesarios en la realización de esos procesos críticos identificados anteriormente, en cuestión de equipo de cómputo incluir software y hardware, proveedores e información sensible que se utilice. Crear tu árbol de llamadas, documentado y más importante mantenerlo actualizado, para que en el momento del incidente sean notificados de alguna forma ya sea manual o automática (a través de algún sistema automatizado de notificación) para que este grupo inicie las actividades de respuesta y determinar el inicio de las actividades del vocero oficial para la interacción con los medios, clientes y partes interesadas durante el incidente para que dependiendo de su nivel de evento y escenario de contingencias pueda continuar sus operaciones de forma aceptable en los tiempos requeridos, o en su caso puedan continuar operando en un sitio alternativo (Disaster Recovery, 2018).

- **Capacidad de Recuperación**

Después de las acciones de respuesta, se deben detallar las acciones que se llevarán a cabo para recuperar la normalidad dentro del plan de continuidad del negocio o BCP Es importante definir los pasos que se seguirán, así como el nivel de intervención de cada persona, sus respectivos roles, evitando al máximo la improvisación (Riveros, Pasos para implementar un plan de continuidad de negocio, 2023).

3. Normativas y Estándares de Seguridad

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento (Martin, 2021).

4. Resiliencia Operativa

En el ámbito organizacional, la resiliencia operativa se puede definir como la habilidad de una organización para perseguir su misión y aprovechar oportunidades, incluso en circunstancias no idóneas o adversas como un incidente de seguridad o una crisis financiera. Esta habilidad tiene como propósito fundamental mantener los procesos de negocio y los servicios que soportan de manera directa la misión de la organización (Mendoza, 2015).

❖ Importancia de la Resiliencia Operativa

La resiliencia no puede ser determinada en términos de lo que no ha sucedido o se desconoce, y aunque resulta importante identificar el ambiente de riesgo actual en la organización, es más relevante determinar la capacidad de la empresa para predecir su comportamiento ante una situación de estrés. En otras palabras, estimar qué tan bien se va a desempeñar la organización ante un cambio en el ambiente de riesgos (Mendoza, 2015).

❖ ¿Cómo puede ser aplicada la Resiliencia Operativa?

La aplicación de un modelo para la resiliencia operativa es el punto de partida para aprovechar la convergencia entre seguridad, continuidad del negocio y las actividades de operaciones de TI.

Además, puede ser la base para evaluar las capacidades de la organización y mejorar las áreas donde no han alcanzado el estado deseado; mejorar las actividades de seguridad de la información, cumplimiento, operaciones de TI, de continuidad y recuperación ante desastres, así como evaluar las actividades de protección de la infraestructura crítica (Mendoza, 2015).

5. Recuperación Rápida

En la etapa de respuesta se define qué y cómo se llevará a cabo las acciones definidas si ocurriera uno de los sucesos detallados en el PCN.

La etapa de recuperación describe el proceso que llevará a cabo el restablecimiento de las actividades tal y como se llevaban a cabo antes de darse el escenario que ha afectado la continuidad de negocio (Riveros, Pasos para implementar un plan de continuidad de negocio, 2023).

Objetivos de Tiempo de Recuperación (RTOs):

El RTO es una métrica esencial que le ayudará a calcular el tiempo que toma restaurar su sistema o aplicación después de un período de tiempo fuera de servicio con una interrupción mínima de las operaciones comerciales. En resumen, es la cantidad de tiempo fuera de servicio que su empresa puede manejar cómodamente (Veritas, 2023).

6. Plan de Contingencia

La planificación de contingencias significa preparar a una organización para que esté lista para responder de manera efectiva en caso de una emergencia (IFCR, 2023).

2.3 MARCO METODOLÓGICO

En este apartado se presentan todas las metodologías que implementan en el proyecto tomándose como referencia para el desarrollo de las actividades propuestas y el cumplimiento de los objetivos.

METODOLOGÍA PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO CON ENFOQUE AL 27001

El libro “Diseño de un sistema de gestión de seguridad informática” escrito por Alberto G. Alexander propone una metodología para el desarrollo de un plan de continuidad del negocio con enfoque al 27001 para saber cómo proceder al implantar en cualquier empresa un Sistema de Gestión de Seguridad de Información (SGSI), que les permita a las organizaciones minimizar los riesgos y asegurar una continuidad en sus operaciones. En el capítulo 4 del libro, “Gestión de la continuidad del negocio”, se enfoca en cómo las empresas pueden prepararse para situaciones imprevistas que puedan afectar su capacidad para operar normalmente. El capítulo describe cómo los sistemas de gestión de seguridad de la información pueden ayudar a las empresas a identificar y evaluar los riesgos, y cómo pueden desarrollar planes para garantizar la continuidad del negocio en caso de interrupciones. En dicho capítulo se habla de las fases que compone un plan de continuidad del negocio las cuales se pueden apreciar en el siguiente diagrama:

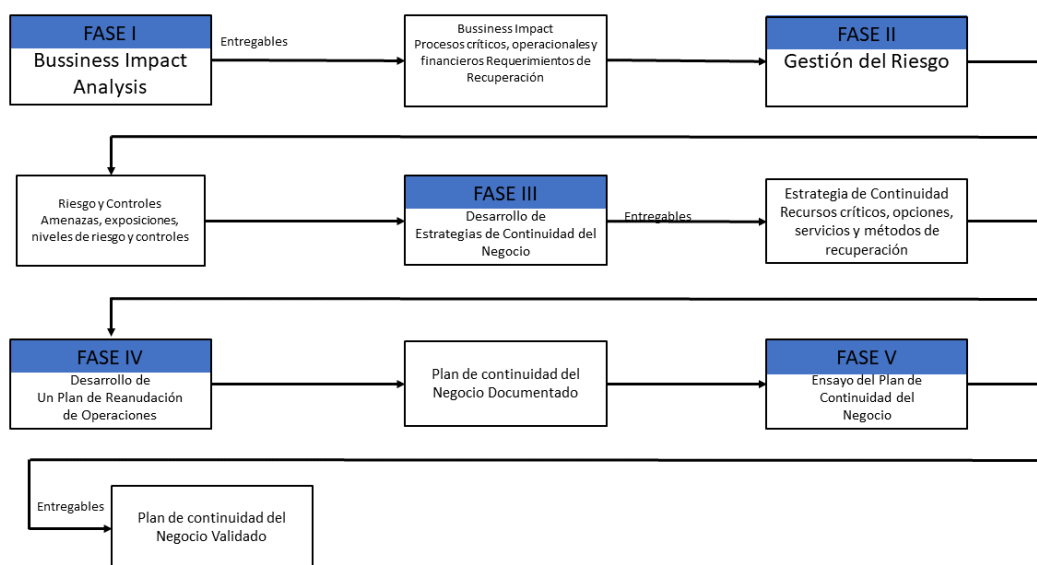


Figura 3. Diagrama de las Fases que componen un PCN. [Fuente: Alexander (2007)].

El proyecto desarrollado en este reporte sigue los pasos y ejemplos descritos en el capítulo cuatro de este libro, tomando como punto de partida las instrucciones mostradas en las seis fases del plan de continuidad del negocio descrito en el libro (Alexander, 2007).

NORMA ISO/IEC 17799

La norma ISO/IEC 17799, conocida por establecer directrices para la gestión de seguridad de la información, es crucial para el desarrollo del PCN de la UMB Tultitlán. Su aplicación garantiza la protección de la información académica y administrativa, abarcando desde la gestión de activos y el control de acceso hasta la gestión de incidentes. Para este proyecto, se adoptarán sus prácticas recomendadas en control de accesos, gestión de comunicaciones y operaciones, y la continuidad del negocio, asegurando la resiliencia y recuperación efectiva de las operaciones de la institución frente a interrupciones (ISO/IEC JTC 1/SC 27, 2005).

METODOLOGÍA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE SEGUIMIENTO EN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN

Esta metodología aborda la importancia crítica de la seguridad de la información y las tecnologías que la respaldan en las empresas. Se identifica una carencia generalizada de conocimiento en seguridad de la información dentro del ámbito de las Tecnologías de Información (TI), lo que resulta en una menor priorización de esta área crucial. Para abordar este desafío, la tesis propone una metodología específica destinada a empresas que buscan mejorar su seguridad de la información o evitar riesgos asociados con el conocimiento insuficiente en esta materia. La metodología se centra en el establecimiento de objetivos y actividades que refuercen la seguridad en la información manejada por las TI. La metodología detalla cada fase de la metodología propuesta, incluyendo las actividades que la complementan, y finaliza con un ejemplo práctico de su aplicación. Para este proyecto se toma como referencia todo lo abarcado en la Fase 3, Actividad 3.1, para el desarrollo del objetivo 2 (Prado, 2009).

CUADRO METODOLÓGICO INTEGRAL PARA EL DESARROLLO DEL PROYECTO

La siguiente tabla proporciona un conjunto integral de estrategias para abordar diversos riesgos identificados en la institución educativa.

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia].

Actividades	Técnicas	Herramienta	Metas
0.1. Entrevistar al personal correspondiente sobre la existencia de estrategias implementadas que apoyen la misión de la institución referido a la TI.	-Entrevista con personal clave en el uso de las TIC's -Revisión de documentos organizacionales	-Documentos organizacionales - Entrevistas	-Identificar las funciones críticas de Ti que sustentan las operaciones clave para la institución -Mapear los procesos esenciales relacionados con la implementación de estrategias de TI
0.2. Realizar un recuento sobre los activos de TI con los que cuenta la institución.	-Inventario físico -Revisión de documentos -Entrevista a personal de TI	-Documentos de Inventarios	-Obtener un inventario completo y preciso de todos los activos de TI de la institución. -Identificar activos críticos y aquellos que podrían necesitar actualizaciones o reemplazos.
1.1 Identificar funciones y procesos de la institución.	-Revisión de documentos organizacionales -Entrevistas con personal clave para mapear procesos	-Documentos organizacionales -entrevistas -diagramas de flujo	-Determinar las funciones y procesos esenciales que sostienen las operaciones críticas de la institución
1.2. Evaluar los impactos financieros y operacionales.	-Análisis de impacto en el negocio para cuantificar efectos de interrupciones	-Análisis manual -entrevistas con el departamento financiero	-Comprender el impacto potencial de las interrupciones en la continuidad operativa y financiera

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia]. (Continuación).

Actividades	Técnicas	Herramienta	Metas
1.3. Identificar los procesos críticos.	-Identificación y priorización de procesos basados en su criticidad -Reuniones con líderes de proceso -análisis de documentos de operación	-Cuestionarios -Procesador de texto.	-Seleccionar y priorizar procesos críticos para la continuidad del negocio
1.4. Establecer los tiempos de recuperación.	-Entrevistas con el personal sobre el tiempo de recuperación en cada una de sus actividades	-Plantillas de continuidad de negocio en papel,	-Establecer marcos de tiempo para la recuperación operativa tras un incidente
1.5. Identificar los requerimientos de recursos de TI.	-Evaluación de necesidades tecnológicas para el funcionamiento de procesos críticos	-Inventario físico -listas de control manual	-Asegurar la disponibilidad de los recursos de TI necesarios para mantener la continuidad
1.6 Determinar el tiempo objetivo de recuperación.	-Revisión de incidentes anteriores -discusiones con cada departamento sobre tiempos de parada aceptables -análisis de acuerdos de nivel de servicio (SLAs) existentes	-Tablas de tiempo de recuperación	-Establecer el tiempo máximo aceptable para recuperar las operaciones tras una interrupción
1.7. Determinar el punto objetivo de recuperación.	-Evaluación de capacidad de respaldo de datos -Análisis de tolerancia de pérdida de datos -Pruebas de restauración	-Registros de respaldo -listas de verificación de datos	-Definir el umbral máximo de datos que la institución puede permitirse perder en caso de desastre

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia]. (Continuación).

Actividades	Técnicas	Herramienta	Metas
1.8. Identificar los procedimientos alternos.	-Evaluación de procedimientos actuales -Análisis de requerimientos para realizar dichos procesos y la razón por la que existen	-Documentos de procedimientos alternativos -Esquemas de procesos	-Crear un plan de acción para operar en modo contingencia si los procesos estándar no están disponibles
2.1. Identificar los activos de TI de la institución.	- Análisis de inventario de activos. -Conteo de equipos de cómputo y complementos	- Herramienta de inventario de TI -Cuestionarios	- Obtener una lista completa de activos de TI de la Institución y quien lo opera.
2.2. Identificar las amenazas a la TI de la institución.	- Análisis de riesgos y revisión de incidentes pasados. -Realizar entrevista a personal de la institución para recopilar información de amenazas posibles.	- Matriz de riesgos -Cuestionarios	- Identificar y priorizar las amenazas que existan o puedan darse en la institución.
2.3. Identificar las vulnerabilidades de los activos de TI de la institución.	- Evaluación de vulnerabilidades y auditorías de seguridad.	- Escáner de vulnerabilidades -Cuestionarios	- Mejorar la seguridad y controles existentes.
2.4. Aplicar una encuesta al personal administrativo para poder calcular la exposición al riesgo.	- Análisis de datos con la ayuda de encuestas realizadas en el plantel.	-Cuestionarios -Procesador de texto	- Visualizar el riesgo que tienen los docentes al hacer uso de sus equipos de cómputo.
2.5. Análisis de los resultados de las encuestas.	- Análisis cuantitativo de riesgos. -Realizar conteo de diversos riesgos	- Herramienta de gestión de riesgos -Cuestionarios	- Cuantificar el impacto y probabilidad.

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia]. (Continuación).

Actividades	Técnicas	Herramienta	Metas
2.6. Priorizar riesgos	-Análisis de riesgos -Matriz de riesgos -Evaluación de impacto y probabilidad.	-Software de gestión de riesgos, -Hojas de cálculo	-Identificar y clasificar los riesgos según su impacto y probabilidad, priorizar los riesgos para centrarse en los más críticos.
2.7. Evaluar los sistemas de control con los que cuenta la institución	-Revisión de documentos -Auditorías internas.	-Cuestionarios estructurados -Documentación de procesos.	-Identificar y documentar los sistemas de control existentes, evaluar su eficacia, identificar posibles brechas en los controles existentes.
3.1. Identificar las opciones de recuperación.	-Análisis de escenarios de riesgo y recuperación.	- Documentación de procesos	-Listar todas las opciones viables de recuperación de TI. -Priorizar las opciones según eficacia y eficiencia.
3.2. Identificar los requerimientos para la recuperación.	-Análisis de requerimientos. -Revisión de documentos de políticas y procedimientos de TI existentes.	-Cuestionarios	- Establecer una lista clara de necesidades y requerimientos para la recuperación.
3.3. Evaluar la viabilidad de implementar las estrategias, a partir de la disponibilidad de recursos, restricciones operativas y el tiempo de implementación.	-Análisis coste-beneficio. -Evaluación de capacidad y recursos disponibles.	-Herramientas de análisis. -Inventarios de recursos	-Determinar la factibilidad de las estrategias propuestas. -Identificar posibles limitaciones o desafíos en la implementación.

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia]. (Continuación).

Actividades	Técnicas	Herramienta	Metas
3.4 Descripción de las propuestas seleccionadas por la institución.	- Documentación detallada de propuestas.	- Procesador de Texto. - Internet.	-Tener un documento claro y detallado de las propuestas seleccionadas. -Asegurar que todas las partes interesadas comprendan y estén de acuerdo con las propuestas.
4.1. Redactar un plan de reanudación de operaciones para los procesos críticos.	- Redacción clara y concisa - Revisión y aprobación por parte de los responsables de TI y la dirección	- Procesador de texto. - Internet.	-Crear un plan detallado y accionable para la reanudación de operaciones. -Asegurar que el plan sea revisado, aprobado y comprendido por todas las partes relevantes.
4.2. Propuesta de División de Tecnologías de la Información (TI)	- Análisis de roles y responsabilidades. - Sesiones de planificación de recursos humanos.	- Procesador de texto.	-Designar roles en equipos de Ti -Conformar diversos objetivos a cada rol
5.1. Redactar una política de seguridad para los laboratorios de informática de la institución.	- Redacción clara y con concisa. - Uso de diagramas representativos. - Consulta de normativas y mejores prácticas en seguridad informática.	- Procesador de texto. - Guías de estándares de seguridad informática. - Herramientas de colaboración y documentación.	-Establecer una política de seguridad comprensiva y adaptada a las necesidades de la institución. -Asegurar que la política sea aprobada, publicada y comunicada eficazmente a todo el personal y estudiantes.

Tabla 2. Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Fuente: Elaboración propia]. (Continuación).

Actividades	Técnicas	Herramienta	Metas
5.2. Desarrollar un sistema de inventario para gestionar todos los activos de TI de la institución.	- Desarrollo de sistemas informáticos. - Integración de bases de datos y sistemas de inventario existentes.	- Plataformas de gestión de bases de datos. - Software de desarrollo e integración de sistemas.	-Crear un sistema de inventario que permita un seguimiento eficiente y preciso de todos los activos de TI. -Facilitar la gestión, actualización y mantenimiento de los activos de TI de forma centralizada y automatizada.
5.3 Desarrollar un curso para concienciación sobre la Seguridad Informática.	-Uso de ejemplos prácticos y estudios de caso para ilustrar amenazas y defensas de seguridad informática.	-Plataforma de Forms para la entrega y gestión del curso.	-Aumentar la conciencia sobre la importancia de la seguridad informática entre el personal y los estudiantes.
5.4 Desarrollar un curso para la creación de contraseñas seguras y su importancia.	-Desarrollo de contenidos que enfatizan la importancia de las contraseñas seguras mediante ejemplos y consecuencias de contraseñas débiles.	-Herramientas de creación de cursos en línea para la elaboración de materiales didácticos interactivos. -Software de simulación para practicar la creación de contraseñas seguras.	-Capacitar al personal y a los estudiantes en la creación y manejo de contraseñas seguras. -Reducir la incidencia de brechas de seguridad causadas por contraseñas débiles o comprometidas.

					Septiembre				Octubre				Noviembre				Diciembre				Enero			
Etapa	Actividad	S1	S2	S3	S4	S1	S2	S3	S4	S5	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4		
0.Analizar Requisitos	0.1. Entrevistar al personal correspondiente sobre la existencia de estrategias implementadas que apoyen la misión de la institución referido a la TI.																							
	0.2. Realizar un recuento sobre los activos de TI con los que cuenta la institución.																							
Fase I. Analizar Impacto	1.1. Identificar funciones y procesos de la institución.																							
	1.2.Evaluar los impactos financieros y operacionales.																							
	1.3.Identificar los procesos críticos.																							
	1.4.Establecer los tiempos de recuperación.																							
	1.5.Identificar los requerimientos de recursos de TI.																							
	1.6.Determinar el tiempo objetivo de recuperación.																							
	1.7.Determinar del punto objetivo de recuperación.																							
	1.8.Identificar los procedimientos alternos.																							
Fase II. Analizar Riesgos	2.1.Identificar los activos de TI de la institución.																							
	2.2.Identificar las amenazas a la TI de la institución.																							
	2.3.Identificar las vulnerabilidades y sistemas de control.																							
	2.4. Aplicar una encuesta al personal administrativo para poder calcular la exposición al riesgo.																							
	2.5. Análisis de los resultados de las encuestas.																							
	2.6. Priorizar riesgos																							
	2.7. Evaluar los sistemas de control con los que cuenta la institución																							
Fase III. Proponer Estrategias de Plan de Continuidad de Negocio	3.1. Identificar las opciones de recuperación.																							
	3.2. Identificar los requerimientos para la recuperación.																							
	3.3. Evaluar la viabilidad de implementar las estrategias, a partir de la disponibilidad de recursos, restricciones operativas y el tiempo de implementación.																							
	3.4 Descripción de las propuestas seleccionadas por la institución.																							
Fase IV. Desarrollar un Plan de Renaudación de Operaciones	4.1. Redactar un plan de reanudación de operaciones para los procesos críticos.																							
	4.2. Propuesta de División de Tecnologías de la Información (TI)																							
Fase V. Realizar las Estrategias Propuestas	5.1. Redactar una política de seguridad para los laboratorios de informática de la institución.																							
	5.2. Desarrollar un sistema de inventario para gestionar todos los activos de TI de la institución.																							
	5.3 Desarrollar un curso para concienciación sobre la Seguridad Informática.																							
	5.4 Desarrollar un curso para la creación de contraseñas seguras y su importancia.																							

Así mismo, en conjunto con el marco metodológico, se puede ver la siguiente ilustración de una gráfica de Gantt con la planeación del proyecto dividida por etapas, las actividades correspondientes a las etapas y las semanas previstas para realizar de cada actividad.

Figura 4. Grafica de Gantt de las Actividades a Desarrollar. [Fuente: Elaboración propia].

CAPÍTULO III. DESARROLLO

INTRODUCCIÓN

En el presente capítulo se realizan los objetivos, así como las actividades propuestas con anterioridad utilizando como referencia para su desarrollo las metodologías previamente mencionadas en el marco metodológico. Donde se realiza primero la adquisición de toda la información posible sobre la Institución, con respecto a su estructura de TI y los procesos que realiza; para posteriormente realizar un análisis de dicha información con la intención de determinar los procesos y activos de TI más importantes para que la institución pueda operar correctamente, seguido de ello se busca evaluar el riesgo al que se exponen los activos asociados a los procesos más importantes. Y finalmente proponer soluciones preventivas o correctivas para poder resguardar dichos activos de TI, que dependiendo de los que escoja la Universidad serán los que se implantaran y permitieran la redacción del PCN. Además, como añadido, tal como lo dice el último objetivo se demostrará como fueron realizados los entregables.

OBJETIVO 0. Analizar Requisitos: Indagar sobre las condiciones de las estrategias ya existentes para apoyar la misión de la institución.

ACTIVIDAD 0.1

Entrevistar al personal correspondiente sobre la existencia de estrategias implementadas que apoyen la misión de la institución referido a la TI.

DESCRIPCIÓN DE LA ACTIVIDAD

Para esta actividad se realiza un cuestionario para aplicarlo en entrevistas al personal de educación dual, control escolar, al administrativo de titulación, al secretario de la directora, a la directora, etc. de forma presencial en la institución. Dichas entrevistas se realizarán conforme a lo sugerido en el capítulo 4 del libro escrito por Alberto G. Alexander “Diseño de un Sistema de Gestión de Seguridad de Información” para el desarrollo del BIA (Business Impact Analysis) donde se busca la obtención de información acerca de los procesos con los que cuenta actualmente la institución, quienes son los responsables de estos y si es que previamente se ha aplicado un plan de continuidad del negocio o productos similares que apoyen a la seguridad informática de la institución; y con ellos poder realizar un análisis detallado que se mostrara en el análisis de impacto que es abarcado en todo el objetivo 1.

RESULTADO DE LA ACTIVIDAD

El cuestionario generado fue el siguiente:

1. ¿Qué actividades administrativas realiza utilizando el equipo de cómputo de su oficina?
2. ¿Qué aplicaciones de su equipo de cómputo utiliza para poder realizar esas actividades?
3. En caso de que el equipo no esté operativo por alguna falla, tales como: corte de luz, internet o daño al equipo de cómputo en sí; ¿Cuánto tiempo podría permanecer sin realizar dichas tareas sin que afecte su trabajo y a la institución? Coloque el tiempo (en horas, días o semanas) por cada actividad.
4. ¿La institución experimenta alguna pérdida en caso de usted no realice esas actividades? (pérdida financiera, reputación, procesos académicos, etc.) De ser así, explique por cada actividad.
5. ¿Cuenta con la posibilidad de realizar esas mismas actividades sin su equipo de cómputo? Si es así, describa como.
6. ¿Qué procedimiento lleva a cabo para reanudar su trabajo? En caso de fallas en su equipo de cómputo.

ACTIVIDAD 0.2

Realizar un recuento sobre los activos de TI con los que cuenta la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

De acuerdo con las sugerencias planteadas en el contexto general del ISO 27001 se realizará un recuento sobre los activos de TI con los que cuenta la institución debido a que en las visitas previas se pudo observar que la universidad no cuenta con un conteo claro sobre los activos con los que cuenta. Así mismo al generar este recuento se podrán realizar con mayor precisión las recomendaciones en actividades posteriores además de poder entregarle a la institución un sistema de inventario de TI desarrollado en Java como parte de uno de los entregables finales del proyecto. El resultado de esta actividad es un croquis generado a partir de una imagen extraída de Google Maps de toda la institución para poder señalar los laboratorios o departamentos donde se encuentra concentrada la TI de la institución; para posteriormente plasmar en una tabla la cantidad de dispositivos que se encuentran en cada uno de los lugares señalados en la imagen. Revisar Anexo para ver el inventario de TI completo.

RESULTADO DE LA ACTIVIDAD

Con ello se obtuvo el siguiente resultado:



Figura 5. Croquis de la institución donde marca la ubicación de la TI localizada. [Fuente: Google Maps (2023)].

Tabla 3. Recuento de todos los activos de TI de la institución. [Fuente: Elaboración propia].

Lugar	PC	Router	Modem	Switch	Server	NAS	Proyector	Televisor	Impresora
E1	40	2	3	4	1	1	0	0	1
E2 P1	27	2	1	2	1	1	1	0	1
E2 P2	8	0	0	0	0	0	2	0	5
E2 P3	0	0	0	0	0	0	5	0	0
E3	0	0	0	0	0	0	0	6	0
E4 P1	36	1	2	0	1	0	1	0	1
E4 P2	2	0	0	0	0	0	0	2	0
Total	113	5	6	6	3	2	9	8	8

La tabla anterior contiene el inventario de activos informáticos de la UMB, se puede observar que la mayoría de los equipos de cómputo se encuentran en el E1 y E4. Para ver el inventario completo que incluye el conteo realizado en esta actividad revisar el Anexo A. Inventario de los Activos de TI de la Institución.

OBJETIVO 1. Analizar Impacto: Identificar aquellos procesos relacionados con apoyar la misión de la institución y el impacto que habría si fuesen interrumpidos, como resultado de un desastre.

ACTIVIDAD 1.1

Identificar funciones y procesos de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Con la información recabada del cuestionario generado y aplicado en el objetivo 0.1, se realiza una tabla que se compone de los departamentos identificados, así como los procesos que se realizan en dichos departamentos. Realizar esto tiene como propósito la identificación y clasificación de los procesos que ejecuta la Institución para posteriormente determinar cuáles son los de mayor importancia para la Universidad a través de la evaluación de impacto financiero, así como operacional que se ve en la siguiente actividad.

RESULTADO DE LA ACTIVIDAD

Tabla 4. Departamentos y procesos identificados en la Institución. [Fuente: Alexander (2007)].

Departamento	Procesos Identificados
Dirección	1. Redacción de reportes
	2. Uso de base de datos para administración de recursos
	3. Gestión de comunicaciones internas y externas mediante plataformas digitales
	4. Monitoreo y análisis de datos institucionales para la toma de decisiones
Control Escolar	1. Realización de reportes académicos y administrativos
	2. Uso de plataforma institucional para gestión de cursos y calificaciones
	3. Administración de registros académicos en sistemas de información
	4. Coordinación de horarios y asignaciones docentes a través de herramientas digitales
	5. Inscripciones de nuevos alumnos mediante sistemas en línea
	6. Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales

Tabla 4. Departamentos y procesos identificados en la Institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Procesos Identificados
Educación Dual	1. Elaboración de oficios y documentación oficial a través de sistemas automatizados
	2. Comunicación con empresas y otras instituciones por medios digitales
	3. Gestión de proyectos de trabajos estudiantiles en plataformas colaborativas
	4. Administración y monitoreo de equipamiento y software de laboratorios
	5. Coordinación de prácticas de laboratorio y seguimiento en línea
Laboratorios de Cómputo	1. Administración y monitoreo de equipamiento y software de laboratorios
	2. Gestión de accesos y seguridad en sistemas de laboratorio
	3. Coordinación de prácticas de laboratorio y reservaciones en línea
	4. Desarrollo y mantenimiento de plataformas para prácticas virtuales
	5. Soporte técnico y actualizaciones de software y hardware
Titulación	1. Procesamiento de solicitudes de titulación a través de sistemas automatizados
	2. Administración de expedientes académicos digitales para procesos de titulación
	3. Coordinación de evaluaciones de titulación mediante plataformas en línea
	4. Comunicación con egresados y seguimiento post-graduación a través de plataformas digitales
	5. Generación de certificados y documentos oficiales en formato digital
Coordinación de Inglés	1. Gestión de programas de idiomas y recursos digitales
	2. Coordinación de exámenes y certificaciones en línea
	3. Administración de plataformas de aprendizaje virtual
	4. Seguimiento y evaluación del progreso de los estudiantes mediante herramientas de análisis de datos
	5. Comunicación interactiva con estudiantes y docentes a través de plataformas en línea

Tabla 4. Departamentos y procesos identificados en la Institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Procesos Identificados
Coordinación de Ingeniería Civil	1. Administración de software especializado para diseño y cálculo estructural
	2. Coordinación de proyectos de investigación y desarrollo en plataformas colaborativas
	3. Gestión de recursos digitales y bases de datos técnicas
	4. Organización de talleres y seminarios virtuales
	5. Evaluación y seguimiento de prácticas profesionales mediante herramientas digitales
Coordinación de Ingeniería Química	1. Manejo de bases de datos de seguridad y procedimientos químicos
	2. Coordinación de experimentos y proyectos en laboratorios virtuales
	3. Administración de plataformas educativas para enseñanza de procesos químicos
	4. Gestión de inventarios y recursos de laboratorios mediante software especializado
	5. Evaluación de desempeño y seguimiento de estudiantes en actividades prácticas
Coordinación de Licenciatura en Contaduría	1. Uso de sistemas contables y de gestión financiera integrados
	2. Coordinación de auditorías internas y externas mediante herramientas digitales
	3. Gestión de presupuestos y pronósticos financieros en software especializado
	4. Capacitación en herramientas digitales para contabilidad y finanzas
	5. Seguimiento y análisis de tendencias económicas a través de plataformas de análisis de datos
Coordinación de Licenciatura en Psicología Industrial	1. Gestión de encuestas y estudios de clima organizacional en plataformas digitales
	2. Coordinación de programas de bienestar y desarrollo personal en línea
	3. Análisis de datos para la mejora del ambiente laboral y educativo
	4. Implementación de sistemas para seguimiento y apoyo a estudiantes y personal
	5. Desarrollo de programas de capacitación y desarrollo profesional en entornos virtuales

Esta tabla resume los departamentos y procesos identificados en la institución como parte de la Actividad 1.1. Se basa en la información recabada a través del cuestionario y entrevistas realizadas durante la Actividad 0.1. Cada departamento se enlista junto con sus procesos correspondientes, proporcionando una visión clara de las funciones críticas dentro de la escuela.

ACTIVIDAD 1.2

Evaluar los impactos financieros y operacionales.

DESCRIPCIÓN DE LA ACTIVIDAD

Con los procesos identificados y enlistados por departamento en la actividad pasada se realiza una evaluación de los impactos tanto financieros como operacionales que puede sufrir la institución dependiendo del proceso que se vea interrumpido. Dicha evaluación se realiza utilizando también la información obtenida en los resultados de las encuestas de la actividad 0.1. Para ello se realizan dos tablas, la primera contiene: El departamento, proceso ejecutado, pérdida diaria, nivel de severidad.

Correspondiente al nivel de severidad de acuerdo con el autor Alberto G. Alexander en su libro “Diseño de un Sistema de Gestión de Seguridad de Información”, menciona que los niveles de severidad van del 0 al 3, donde:

- Nivel de severidad 0 (no hay impacto)
- Nivel de severidad 1 (menor impacto)
- Nivel de severidad 2 (impacto intermedio)
- Nivel de severidad 3 (impacto mayor)

Por lo que se aplicará esa métrica para la tabla de pérdida financiera. Además, se contempla una segunda métrica cualitativa para la evaluación de la columna “pérdida diaria” de acuerdo con las cifras en dinero que podría perder la institución, sin embargo, no se añadieron las cifras como tal por solicitud de la institución.

Así mismo la segunda tabla contiene el departamento, el proceso ejecutado; y el apartado del impacto operacional donde se contempla: La competitividad, satisfacción del alumnado y calidad de la educación. Dicho apartado será medido un esquema de jerarquización cualitativo, tal como: bajo, medio, alto, crítico y ninguno.

Realizar esta evaluación tiene como propósito poder encontrar de entre todos los procesos identificados cuales son los de importancia crítica de acuerdo con el impacto financiero y operacional que se refleja en las dos siguientes tablas.

RESULTADOS DE LA ACTIVIDAD

Tabla 5. Impacto financiero identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)].

Departamento	Proceso Ejecutado	Pérdida Diaria (Estimada)	Nivel de Severidad
Dirección	Redacción de reportes	Baja	1
	Uso de base de datos para administración de recursos	Moderada	2
	Gestión de comunicaciones internas y externas	Moderada	2
	Monitoreo y análisis de datos institucionales	Alta	3
Control Escolar	Realización de reportes académicos y administrativos	Baja	1
	Uso de plataforma institucional para gestión de cursos y calificaciones	Moderada	2
	Administración de registros académicos en sistemas de información	Moderada	2
	Inscripciones de nuevos alumnos mediante sistemas en línea	Moderada	2
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	Moderada	2
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	Baja	1

Tabla 5. Impacto financiero identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Pérdida Diaria (Estimada)	Nivel de Severidad
Educación Dual	Gestión de convenios y programas de educación dual	Alta	3
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	Moderada	2
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	Moderada	2
	Monitoreo del desempeño estudiantil	Moderada	2
	Comunicación y gestión de recursos para la educación dual	Baja	1
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	Alta	3
	Gestión de accesos y seguridad en sistemas de laboratorio	Moderada	2
	Coordinación de prácticas de laboratorio y reservaciones en línea	Moderada	2
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	Baja	1
	Soporte técnico y actualizaciones de software y hardware	Baja	1
Titulación	Procesamiento de solicitudes de titulación	Moderada	2
	Administración de expedientes académicos digitales	Baja	1
	Coordinación de evaluaciones de titulación en línea	Moderada	2
	Comunicación con egresados y seguimiento post-graduación	Baja	1
	Generación de certificados y documentos oficiales digitales	Baja	1

Tabla 5. Impacto financiero identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Pérdida Diaria (Estimada)	Nivel de Severidad
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Moderada	2
	Coordinación de exámenes y certificaciones en línea	Moderada	2
	Administración de plataformas de aprendizaje virtual	Baja	1
	Seguimiento y evaluación del progreso estudiantil	Moderada	2
	Comunicación interactiva con estudiantes y docentes	Baja	1
Coordinación de Ingeniería Civil	Administración de software especializado	Alta	3
	Coordinación de proyectos de investigación y desarrollo	Moderada	2
	Gestión de recursos digitales y bases de datos técnicas	Moderada	2
	Organización de talleres y seminarios virtuales	Baja	1
	Evaluación y seguimiento de prácticas profesionales	Moderada	2
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Alta	3
	Coordinación de experimentos y proyectos en laboratorios virtuales	Alta	3
	Administración de plataformas educativas	Moderada	2
	Gestión de inventarios y recursos de laboratorios	Moderada	2
	Evaluación de desempeño y seguimiento de estudiantes	Baja	1

Tabla 5. Impacto financiero identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Pérdida Diaria (Estimada)	Nivel de Severidad
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Alta	3
	Coordinación de auditorías internas y externas	Alta	3
	Gestión de presupuestos y pronósticos financieros	Moderada	2
	Capacitación en herramientas digitales	Baja	1
	Seguimiento y análisis de tendencias económicas	Moderada	2
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Moderada	2
	Coordinación de programas de bienestar y desarrollo personal	Baja	1
	Análisis de datos para la mejora del ambiente laboral	Baja	1
	Implementación de sistemas de seguimiento y apoyo	Moderada	2
	Desarrollo de programas de capacitación en entornos virtuales	Baja	1

Esta tabla evalúa los impactos financieros potenciales en la institución por la interrupción de sus procesos. Enumera cada departamento y sus procesos específicos, seguidos por la estimación de la pérdida financiera diaria y el nivel de severidad de la interrupción, basándose en la métrica de Alberto G. Alexander.

IMPACTO OPERACIONAL

Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)].

Departamento	Impacto Operacional			
	Proceso Ejecutado	Competitividad	Satisfacción del Alumnado	Calidad de la Educación
Dirección	Redacción de reportes	Medio	Bajo	Medio
	Uso de base de datos para administración de recursos	Alto	Medio	Alto
	Inscripciones de nuevos alumnos mediante sistemas en línea	Alto	Alto	Alto
	Gestión de comunicaciones internas y externas	Alto	Alto	Alto
	Monitoreo y análisis de datos institucionales	Crítico	Alto	Crítico
Control Escolar	Realización de reportes académicos y administrativos	Bajo	Bajo	Medio
	Uso de plataforma institucional para gestión de cursos y calificaciones	Medio	Alto	Alto
	Administración de registros académicos en sistemas de información	Medio	Alto	Alto
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	Medio	Medio	Alto
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	Bajo	Medio	Medio

Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Impacto Operacional			
	Proceso Ejecutado	Competitividad	Satisfacción del Alumnado	Calidad de la Educación
Educación Dual	Gestión de convenios y programas de educación dual	Crítico	Crítico	Alto
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	Alto	Alto	Alto
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	Alto	Alto	Alto
	Monitoreo del desempeño estudiantil	Alto	Alto	Alto
	Comunicación y gestión de recursos para la educación dual	Medio	Medio	Medio
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	Alto	Medio	Crítico
	Gestión de accesos y seguridad en sistemas de laboratorio	Medio	Medio	Alto
	Coordinación de prácticas de laboratorio y reservaciones en línea	Medio	Alto	Alto
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	Bajo	Bajo	Medio
	Soporte técnico y actualizaciones de software y hardware	Bajo	Bajo	Medio

Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Impacto Operacional			
	Proceso Ejecutado	Competitividad	Satisfacción del Alumnado	Calidad de la Educación
Titulación	Procesamiento de solicitudes de titulación	Medio	Alto	Alto
	Administración de expedientes académicos digitales	Bajo	Medio	Medio
	Coordinación de evaluaciones de titulación en línea	Medio	Alto	Alto
	Comunicación con egresados y seguimiento posgraduación	Bajo	Medio	Medio
	Generación de certificados y documentos oficiales digitales	Bajo	Bajo	Bajo
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Medio	Alto	Alto
	Coordinación de exámenes y certificaciones en línea	Medio	Medio	Alto
	Administración de plataformas de aprendizaje virtual	Bajo	Medio	Medio
	Seguimiento y evaluación del progreso estudiantil	Medio	Alto	Alto
	Comunicación interactiva con estudiantes y docentes	Bajo	Bajo	Medio

Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Impacto Operacional			
	Proceso Ejecutado	Competitividad	Satisfacción del Alumnado	Calidad de la Educación
Coordinación de Ingeniería Civil	Administración de software especializado	Alto	Medio	Crítico
	Coordinación de proyectos de investigación y desarrollo	Medio	Alto	Alto
	Gestión de recursos digitales y bases de datos técnicas	Medio	Medio	Alto
	Organización de talleres y seminarios virtuales	Bajo	Bajo	Medio
	Evaluación y seguimiento de prácticas profesionales	Medio	Alto	Alto
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Alto	Alto	Crítico
	Coordinación de experimentos y proyectos en laboratorios virtuales	Alto	Medio	Crítico
	Administración de plataformas educativas	Medio	Alto	Alto
	Gestión de inventarios y recursos de laboratorios	Medio	Medio	Alto
	Evaluación de desempeño y seguimiento de estudiantes	Bajo	Bajo	Medio

Tabla 6. Impacto operacional identificado por cada uno de los procesos que ejecuta la institución. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Impacto Operacional			
	Proceso Ejecutado	Competitividad	Satisfacción del Alumnado	Calidad de la Educación
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Crítico	Alto	Crítico
	Coordinación de auditorías internas y externas	Alto	Medio	Crítico
	Gestión de presupuestos y pronósticos financieros	Medio	Alto	Alto
	Capacitación en herramientas digitales	Bajo	Bajo	Medio
	Seguimiento y análisis de tendencias económicas	Medio	Alto	Alto
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Medio	Alto	Alto
	Coordinación de programas de bienestar y desarrollo personal	Bajo	Medio	Medio
	Análisis de datos para la mejora del ambiente laboral	Bajo	Bajo	Medio
	Implementación de sistemas de seguimiento y apoyo	Medio	Alto	Alto
	Desarrollo de programas de capacitación en entornos virtuales	Bajo	Medio	Medio

Esta tabla centra su atención en los impactos operacionales dentro de la institución, relacionados con la interrupción de procesos. Incluye departamentos y procesos, con un análisis del impacto en aspectos clave como la competitividad, la satisfacción del alumnado y la calidad de la educación.

ACTIVIDAD 1.3

Identificar los procesos críticos.

DESCRIPCIÓN DE LA ACTIVIDAD

Una vez determinado el impacto financiero y operacional se pueden identificar cuáles son los procesos críticos de los cuales la Institución depende para funcionar correctamente, los cuales fueron identificados como los que más afectan a la institución en caso de ser interrumpidos provocando pérdidas financieras o daños operacionales. Dichos procesos críticos se plasman en una tabla de tres columnas que contempla: Departamento, proceso critico identificado 1 y proceso critico identificado 2. Así mismo el propósito identificar estos procesos se verá más adelante en las actividades del objetivo 2, donde en términos generales se determina el riesgo que existe de que dichos procesos se vean interrumpidos lo cual será muy importante para posteriormente generar las recomendaciones para prevenirlo o solucionarlo que se ven en las actividades del objetivo 3.

RESULTADO DE LA ACTIVIDAD

Tabla 7. Identificación de los procesos críticos de acuerdo con el impacto financiero y operacional. [Fuente: Elaboración propia].

Departamento	Proceso Crítico Identificado 1	Proceso Crítico Identificado 2
Dirección	Monitoreo y análisis de datos institucionales	Gestión de comunicaciones internas y externas
Control Escolar	Administración de registros académicos en sistemas de información	Uso de plataforma institucional para gestión de cursos y calificaciones
Educación Dual	Gestión de convenios y programas de educación dual	Monitoreo del desempeño estudiantil
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	Coordinación de prácticas de laboratorio y reservaciones en línea
Titulación	Procesamiento de solicitudes de titulación	Generación de certificados y documentos oficiales digitales
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Coordinación de exámenes y certificaciones en línea

Tabla 7. Identificación de los procesos críticos de acuerdo con el impacto financiero y operacional. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso Crítico Identificado 1	Proceso Crítico Identificado 2
Coordinación de Ingeniería Civil	Administración de software especializado	Coordinación de proyectos de investigación y desarrollo
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Coordinación de experimentos y proyectos en laboratorios virtuales
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Coordinación de auditorías internas y externas
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Implementación de sistemas de seguimiento y apoyo

Esta tabla detalla los procesos críticos identificados en cada departamento de la institución, utilizando los resultados obtenidos de las actividades 1.1 y 1.2. Presenta una lista de departamentos junto con los procesos críticos asociados, proporcionando una visión clara de las operaciones esenciales que son fundamentales para el funcionamiento de la institución.

ACTIVIDAD 1.4

Establecer los tiempos de recuperación.

DESCRIPCIÓN DE LA ACTIVIDAD

Esta actividad se aborda la determinación aproximada de los tiempos de recuperación para los todos procesos identificados en la actividad 1.1 a través del análisis de la información recabada durante la actividad 0.1. Para esta actividad se genera una tabla con el departamento, proceso crítico, el MTD o Tiempo Máximo Tolerable de inactividad el cual es el límite temporal máximo que la institución puede tolerar para la inactividad de un proceso crítico antes de que las consecuencias sean inaceptables generalmente medido en horas y la prioridad asignada a cada proceso crítico de acuerdo con las opiniones de los administrativos según su experiencia en su puesto y conocimiento sobre el proceso. La prioridad es evaluada de acuerdo con el autor Alberto G. Alexander en su libro “Diseño de un Sistema de Gestión de Seguridad de Información” siendo contemplada de la siguiente forma:

Alta Prioridad: Procesos críticos cuya interrupción tendría consecuencias significativas e inmediatas para la institución.

Media Prioridad: Procesos críticos con impacto sustancial pero que permiten cierta flexibilidad en los tiempos de recuperación.

Baja Prioridad: Procesos críticos cuya interrupción tiene un impacto moderado y se pueden recuperar en un marco de tiempo más extendido.

Esta actividad tiene como propósito generar una comprensión sobre los tiempos de recuperación y prioridad que tiene cada proceso en caso de verse interrumpidos, lo que permitirá en la actividad 1.6 poder determinar de forma clara el tiempo objetivo de recuperación.

RESULTADO DE LA ACTIVIDAD

Tabla 8. Tiempo Máximo Tolerable de inactividad determinado por cada proceso crítico. [Fuente: Alexander (2007)].

Departamento	Proceso Ejecutado	MTD (Estimado)	Prioridad
Dirección	Redacción de reportes	8 horas	Media
	Uso de base de datos para administración de recursos	4 horas	Alta
	Inscripciones de nuevos alumnos mediante sistemas en línea	2 horas	Alta
	Gestión de comunicaciones internas y externas	2 horas	Alta
	Monitoreo y análisis de datos institucionales	4 horas	Alta
Control Escolar	Realización de reportes académicos y administrativos	6 horas	Media
	Uso de plataforma institucional para gestión de cursos y calificaciones	3 horas	Alta
	Administración de registros académicos en sistemas de información	4 horas	Alta
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	5 horas	Media
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	3 horas	Alta
Educación Dual	Gestión de convenios y programas de educación dual	5 horas	Alta
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	4 horas	Alta
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	6 horas	Media
	Monitoreo del desempeño estudiantil	4 horas	Alta
	Comunicación y gestión de recursos para la educación dual	6 horas	Media

Tabla 8. Tiempo Máximo Tolerable de inactividad determinado por cada proceso crítico. [Fuente: Alexander (2007)].
(Continuación).

Departamento	Proceso Ejecutado	MTD (Estimado)	Prioridad
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	6 horas	Alta
	Gestión de accesos y seguridad en sistemas de laboratorio	4 horas	Media
	Coordinación de prácticas de laboratorio y reservaciones en línea	4 horas	Alta
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	8 horas	Baja
	Soporte técnico y actualizaciones de software y hardware	4 horas	Media
Titulación	Procesamiento de solicitudes de titulación	4 horas	Alta
	Administración de expedientes académicos digitales	6 horas	Media
	Coordinación de evaluaciones de titulación en línea	3 horas	Alta
	Comunicación con egresados y seguimiento posgraduación	8 horas	Baja
	Generación de certificados y documentos oficiales digitales	2 horas	Alta
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	5 horas	Alta
	Coordinación de exámenes y certificaciones en línea	4 horas	Alta
	Administración de plataformas de aprendizaje virtual	6 horas	Media
	Seguimiento y evaluación del progreso estudiantil	4 horas	Alta
	Comunicación interactiva con estudiantes y docentes	8 horas	Baja

Tabla 8. Tiempo Máximo Tolerable de inactividad determinado por cada proceso crítico. [Fuente: Alexander (2007)].
(Continuación).

Departamento	Proceso Ejecutado	MTD (Estimado)	Prioridad
Coordinación de Ingeniería Civil	Administración de software especializado	6 horas	Alta
	Coordinación de proyectos de investigación y desarrollo	5 horas	Alta
	Gestión de recursos digitales y bases de datos técnicas	4 horas	Media
	Organización de talleres y seminarios virtuales	8 horas	Baja
	Evaluación y seguimiento de prácticas profesionales	4 horas	Alta
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	6 horas	Alta
	Coordinación de experimentos y proyectos en laboratorios virtuales	5 horas	Alta
	Administración de plataformas educativas	6 horas	Media
	Gestión de inventarios y recursos de laboratorios	4 horas	Media
	Evaluación de desempeño y seguimiento de estudiantes	8 horas	Baja
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	5 horas	Alta
	Coordinación de auditorías internas y externas	6 horas	Alta
	Gestión de presupuestos y pronósticos financieros	4 horas	Alta
	Capacitación en herramientas digitales	8 horas	Baja
	Seguimiento y análisis de tendencias económicas	4 horas	Media

Tabla 8. Tiempo Máximo Tolerable de inactividad determinado por cada proceso crítico. [Fuente: Alexander (2007)].
(Continuación).

Departamento	Proceso Ejecutado	MTD (Estimado)	Prioridad
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	4 horas	Alta
	Coordinación de programas de bienestar y desarrollo personal	6 horas	Media
	Análisis de datos para la mejora del ambiente laboral	5 horas	Media
	Implementación de sistemas de seguimiento y apoyo	3 horas	Alta
	Desarrollo de programas de capacitación en entornos virtuales	8 horas	Baja

Esta tabla proporciona una evaluación detallada de los tiempos de recuperación para cada proceso crítico identificado en los departamentos de la institución. Incluye el departamento, el proceso crítico específico, el Tiempo Máximo Tolerable de Inactividad (MTD) medido en horas, y la prioridad asignada a cada proceso. La prioridad de los procesos se clasifica como alta, media o baja, basándose en las consecuencias de su interrupción y en la experiencia y conocimiento de los administrativos de la institución.

ACTIVIDAD 1.5

Identificar los requerimientos de recursos de TI.

DESCRIPCIÓN DE LA ACTIVIDAD

En esta actividad se aborda la identificación de los recursos de tecnología de la información (TI) necesarias para realizar los procesos identificados en la actividad 1.1 y de las que se sabe que son utilizadas por el personal debido a los resultados de las encuestas y entrevistas aplicados en la actividad 0.1. El resultado de esta actividad es una tabla con el departamento, proceso ejecutado y la TI que se utiliza para desarrollar dicho proceso. Identificar estos requerimientos de recursos de TI permite que más adelante, en el objetivo 3, las propuestas de solución tanto preventivas como correctivas tengan congruencia al no recomendar usar una tecnología que ya se esté utilizando.

RESULTADO DE LA ACTIVIDAD

Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados. [Fuente: Alexander (2007)].

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados
Dirección	Redacción de reportes	Software de procesamiento de texto, sistema de gestión documental, portal de reportes internos
	Uso de base de datos para administración de recursos	Sistemas de gestión de bases de datos, software ERP, herramientas de análisis de datos
	Inscripciones de nuevos alumnos mediante sistemas en línea	Portal de inscripciones en línea, sistema de gestión de estudiantes, base de datos central
	Gestión de comunicaciones internas y externas	Plataformas de correo electrónico, sistemas de mensajería instantánea, software de gestión de CRM
	Monitoreo y análisis de datos institucionales	Herramientas de Business Intelligence, sistemas de análisis de datos, dashboard de control

Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados
Control Escolar	Realización de reportes académicos y administrativos	Software de generación de reportes, sistemas de información académica, bases de datos de estudiantes
	Uso de plataforma institucional para gestión de cursos y calificaciones	Plataforma de gestión educativa, sistema de seguimiento de calificaciones, herramientas de análisis académico
	Administración de registros académicos en sistemas de información	Sistema de gestión de registros académicos, bases de datos seguras, software de archivo digital
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	Software de planificación de horarios, sistema de asignación de recursos, plataforma de gestión de personal
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	Sistema de tramitación de solicitudes, software de generación de documentos, portal de servicios estudiantiles
Educación Dual	Gestión de convenios y programas de educación dual	Plataforma de gestión de convenios, sistemas de seguimiento de programas duales, herramientas de colaboración en línea
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	Sistema de gestión de prácticas, herramientas de seguimiento en línea, plataformas de comunicación con empresas
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	Software de gestión de relaciones, plataformas de networking, sistemas de comunicación corporativa
	Monitoreo del desempeño estudiantil	Herramientas de seguimiento del rendimiento, sistemas de evaluación, bases de datos educativas
	Comunicación y gestión de recursos para la educación dual	Sistemas de gestión de recursos, plataformas de comunicación interna, herramientas de planificación estratégica

Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados
Titulación	Procesamiento de solicitudes de titulación	Sistema de gestión de titulación en línea, base de datos de egresados, software de procesamiento de documentos
	Administración de expedientes académicos digitales	Sistemas de archivo digital, plataformas de gestión documental, bases de datos seguras
	Coordinación de evaluaciones de titulación en línea	Plataforma de evaluación en línea, sistema de gestión de exámenes, herramientas de colaboración virtual
	Comunicación con egresados y seguimiento posgraduación	Plataformas de redes sociales, sistemas de seguimiento de egresados, herramientas de email marketing
	Generación de certificados y documentos oficiales digitales	Software de generación de documentos, sistemas de firma digital, herramientas de verificación de documentos
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Plataformas de aprendizaje de idiomas en línea, sistemas de gestión de contenido, herramientas de evaluación de idiomas
	Coordinación de exámenes y certificaciones en línea	Sistema de gestión de exámenes en línea, plataformas de certificación, bases de datos de resultados
	Administración de plataformas de aprendizaje virtual	Sistemas de gestión del aprendizaje (LMS), herramientas de creación de contenido, plataformas de videoconferencia
	Seguimiento y evaluación del progreso estudiantil	Herramientas de análisis de datos estudiantiles, sistemas de seguimiento académico, dashboards de rendimiento
	Comunicación interactiva con estudiantes y docentes	Sistemas de mensajería instantánea, plataformas de comunicación interna, foros en línea

Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados
Coordinación de Ingeniería Civil	Administración de software especializado	Software de diseño y cálculo estructural, herramientas de modelado BIM, plataformas de simulación
	Coordinación de proyectos de investigación y desarrollo	Sistemas de gestión de proyectos, herramientas de colaboración en línea, bases de datos de investigación
	Gestión de recursos digitales y bases de datos técnicas	Sistemas de gestión de bases de datos técnicas, plataformas de almacenamiento en la nube, herramientas de acceso remoto
	Organización de talleres y seminarios virtuales	Plataformas de webinar, herramientas de videoconferencia, sistemas de gestión de eventos
	Evaluación y seguimiento de prácticas profesionales	Herramientas de seguimiento de prácticas, plataformas de evaluación en línea, sistemas de gestión de feedback
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Sistemas de gestión de información química, bases de datos de seguridad, herramientas de documentación de procedimientos
	Coordinación de experimentos y proyectos en laboratorios virtuales	Software de simulación de laboratorio, plataformas de gestión de proyectos de investigación, bases de datos de resultados experimentales
	Administración de plataformas educativas	Sistemas de gestión del aprendizaje (LMS), herramientas de creación de contenido educativo, plataformas de colaboración virtual
	Gestión de inventarios y recursos de laboratorios	Software de gestión de inventarios, sistemas de seguimiento de recursos, herramientas de pedido y suministro
	Evaluación de desempeño y seguimiento de estudiantes	Herramientas de seguimiento del rendimiento estudiantil, sistemas de evaluación, bases de datos educativas

Tabla 9. Identificación de los recursos de TI necesarios para realizar los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Software de contabilidad y finanzas, herramientas de análisis financiero, sistemas de reporte de gestión
	Coordinación de auditorías internas y externas	Plataformas de auditoría, herramientas de análisis de datos financieros, sistemas de documentación de auditoría
	Gestión de presupuestos y pronósticos financieros	Software de planificación financiera, herramientas de modelado de presupuestos, sistemas de proyección y pronóstico
	Capacitación en herramientas digitales	Plataformas de e-learning, sistemas de gestión del conocimiento, herramientas de capacitación en línea
	Seguimiento y análisis de tendencias económicas	Herramientas de Business Intelligence, sistemas de análisis de tendencias, plataformas de visualización de datos
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Herramientas de encuestas en línea, sistemas de análisis de datos, plataformas de feedback de empleados
	Coordinación de programas de bienestar y desarrollo personal	Plataformas de gestión de bienestar, sistemas de seguimiento de desarrollo personal, herramientas de e-learning
	Análisis de datos para la mejora del ambiente laboral	Software de análisis de datos, herramientas de visualización de datos, sistemas de gestión de feedback
	Implementación de sistemas de seguimiento y apoyo	Sistemas de soporte estudiantil y de empleados, plataformas de asistencia en línea, herramientas de seguimiento y monitorización
	Desarrollo de programas de capacitación en entornos virtuales	Plataformas de e-learning, herramientas de creación de contenido educativo, sistemas de gestión del conocimiento

Esta tabla compila los recursos de TI requeridos para los procesos ejecutados en cada departamento de la institución, identificados en la Actividad 1.1. Se presenta una lista clara que relaciona cada departamento con sus respectivos procesos y los recursos de TI asociados necesarios para su ejecución, se puede concluir que la TI es un aspecto importante en cada proceso crítico de la UMB.

ACTIVIDAD 1.6

Determinar el tiempo objetivo de recuperación.

DESCRIPCIÓN DE LA ACTIVIDAD

En esta actividad se lleva a cabo la identificación del Recovery Time Objective (RTO) el cual es el tiempo entre el desastre y la recuperación de los recursos. Indica el tiempo disponible para recuperar recursos transformados. Y el WorkRecovery Time (WRT) que es el tiempo entre la recuperación de sistema y la normalización del procesamiento. Es el tiempo invertido en buscar datos perdidos y realizar reparaciones de todos los procesos identificados en la actividad 1.1; y que se complementa con los resultados obtenidos en la actividad 1.4.

El resultado de esta actividad es una tabla donde se contempla el departamento, proceso ejecutado, las TI utilizadas, el RTO y WRT. Así mismo el RTO y el WRT que se identifican en esta actividad servirán para tomarse en cuenta para las soluciones que se proponen más adelante en el objetivo 3 pues su implementación y ejecución debe de acercarse a los tiempos identificados en esta actividad.

RESULTADOS DE LA ACTIVIDAD

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)].

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Dirección	Redacción de reportes	Software de procesamiento de texto, sistema de gestión documental, portal de reportes internos	2 horas	1 hora
	Uso de base de datos para administración de recursos	Sistemas de gestión de bases de datos, software ERP, herramientas de análisis de datos	4 horas	2 horas
	Inscripciones de nuevos alumnos mediante sistemas en línea	Portal de inscripciones en línea, sistema de gestión de estudiantes, base de datos central	2 horas	2 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Dirección	Gestión de comunicaciones internas y externas	Plataformas de correo electrónico, sistemas de mensajería instantánea, software de gestión de CRM	1 hora	1 hora
	Monitoreo y análisis de datos institucionales	Herramientas de Business Intelligence, sistemas de análisis de datos, dashboard de control	3 horas	2 horas
Control Escolar	Realización de reportes académicos y administrativos	Software de generación de reportes, sistemas de información académica, bases de datos de estudiantes	3 horas	1 hora
	Uso de plataforma institucional para gestión de cursos y calificaciones	Plataforma de gestión educativa, sistema de seguimiento de calificaciones, herramientas de análisis académico	4 horas	2 horas
	Administración de registros académicos en sistemas de información	Sistema de gestión de registros académicos, bases de datos seguras, software de archivo digital	4 horas	2 horas
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	Software de planificación de horarios, sistema de asignación de recursos, plataforma de gestión de personal	5 horas	3 horas
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	Sistema de tramitación de solicitudes, software de generación de documentos, portal de servicios estudiantiles	3 horas	2 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Educación Dual	Gestión de convenios y programas de educación dual	Plataforma de gestión de convenios, sistemas de seguimiento de programas, herramientas de colaboración en línea	5 horas	3 horas
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	Sistema de gestión de prácticas, herramientas de seguimiento en línea, plataformas de comunicación con empresas	4 horas	2 horas
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	Software de gestión de relaciones, plataformas de networking, sistemas de comunicación corporativa	6 horas	3 horas
	Monitoreo del desempeño estudiantil	Herramientas de seguimiento del rendimiento, sistemas de evaluación, bases de datos educativas	4 horas	2 horas
	Comunicación y gestión de recursos para la educación dual	Sistemas de gestión de recursos, plataformas de comunicación interna, herramientas de planificación estratégica	6 horas	4 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software	Software de monitoreo de laboratorio, herramientas de acceso remoto, sistemas de gestión de inventarios	6 horas	4 horas
	Gestión de accesos y seguridad en sistemas de laboratorio	Sistemas de control de acceso, software de seguridad, herramientas de monitoreo en tiempo real	4 horas	2 horas
	Coordinación de prácticas de laboratorio y reservaciones en línea	Plataformas de reservación en línea, sistemas de gestión de laboratorios, herramientas de seguimiento de prácticas	4 horas	2 horas
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	Herramientas de desarrollo de software, sistemas de gestión de proyectos, plataformas de colaboración virtual	8 horas	5 horas
	Soporte técnico y actualizaciones de software y hardware	Sistemas de ticketing para soporte técnico, herramientas de gestión de hardware, software de actualización automática	4 horas	3 horas
Titulación	Procesamiento de solicitudes de titulación	Sistema de gestión de titulación en línea, base de datos de egresados, software de procesamiento de documentos	4 horas	2 horas
	Administración de expedientes académicos digitales	Sistemas de archivo digital, plataformas de gestión documental, bases de datos seguras	6 horas	3 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Titulación	Coordinación de evaluaciones de titulación en línea	Plataforma de evaluación en línea, sistema de gestión de exámenes, herramientas de colaboración virtual	3 horas	2 horas
	Comunicación con egresados y seguimiento posgraduación	Plataformas de redes sociales, sistemas de seguimiento de egresados, herramientas de email marketing	8 horas	4 horas
	Generación de certificados y documentos oficiales digitales	Software de generación de documentos, sistemas de firma digital, herramientas de verificación de documentos	2 horas	1 hora
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Plataformas de aprendizaje de idiomas en línea, sistemas de gestión de contenido, herramientas de evaluación de idiomas	5 horas	2 horas
	Coordinación de exámenes y certificaciones en línea	Sistema de gestión de exámenes en línea, plataformas de certificación, bases de datos de resultados	4 horas	2 horas
	Administración de plataformas de aprendizaje virtual	Sistemas de gestión del aprendizaje (LMS), herramientas de creación de contenido, plataformas de videoconferencia	6 horas	3 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Coordinación de Ingles	Seguimiento y evaluación del progreso estudiantil	Herramientas de análisis de datos estudiantiles, sistemas de seguimiento académico, dashboards de rendimiento	4 horas	2 horas
	Comunicación interactiva con estudiantes y docentes	Sistemas de mensajería instantánea, plataformas de comunicación interna, foros en línea	8 horas	4 horas
Coordinación de Ingeniería Civil	Administración de software especializado	Software de diseño y cálculo estructural, herramientas de modelado BIM, plataformas de simulación	6 horas	4 horas
	Coordinación de proyectos de investigación y desarrollo	Sistemas de gestión de proyectos, herramientas de colaboración en línea, bases de datos de investigación	5 horas	3 horas
	Gestión de recursos digitales y bases de datos técnicas	Sistemas de gestión de bases de datos técnicas, plataformas de almacenamiento en la nube, herramientas de acceso remoto	4 horas	2 horas
	Organización de talleres y seminarios virtuales	Plataformas de webinar, herramientas de videoconferencia, sistemas de gestión de eventos	8 horas	5 horas
	Evaluación y seguimiento de prácticas profesionales	Herramientas de seguimiento de prácticas, plataformas de evaluación en línea, sistemas de gestión de feedback	4 horas	3 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Sistemas de gestión de información química, bases de datos de seguridad, herramientas de documentación de procedimientos	6 horas	3 horas
	Coordinación de experimentos y proyectos en laboratorios virtuales	Software de simulación de laboratorio, plataformas de gestión de proyectos de investigación, bases de datos de resultados experimentales	5 horas	4 horas
	Administración de plataformas educativas	Sistemas de gestión del aprendizaje (LMS), herramientas de creación de contenido educativo, plataformas de colaboración virtual	6 horas	3 horas
	Gestión de inventarios y recursos de laboratorios	Software de gestión de inventarios, sistemas de seguimiento de recursos, herramientas de pedido y suministro	4 horas	2 horas
	Evaluación de desempeño y seguimiento de estudiantes	Herramientas de seguimiento del rendimiento estudiantil, sistemas de evaluación, bases de datos educativas	8 horas	5 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Software de contabilidad y finanzas, herramientas de análisis financiero, sistemas de reporte de gestión	5 horas	3 horas
	Coordinación de auditorías internas y externas	Plataformas de auditoría, herramientas de análisis de datos financieros, sistemas de documentación de auditoría	6 horas	4 horas
	Gestión de presupuestos y pronósticos financieros	Software de planificación financiera, herramientas de modelado de presupuestos, sistemas de proyección y pronóstico	4 horas	2 horas
	Capacitación en herramientas digitales	Plataformas de e-learning, sistemas de gestión del conocimiento, herramientas de capacitación en línea	8 horas	5 horas
	Seguimiento y análisis de tendencias económicas	Herramientas de Business Intelligence, sistemas de análisis de tendencias, plataformas de visualización de datos	4 horas	3 horas

Tabla 10. Determinación del tiempo objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	Tecnologías de la Información Utilizados	RTO (Estimado)	WRT (Estimado)
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Herramientas de encuestas en línea, sistemas de análisis de datos, plataformas de feedback de empleados	4 horas	2 horas
	Coordinación de programas de bienestar y desarrollo personal	Plataformas de gestión de bienestar, sistemas de seguimiento de desarrollo personal, herramientas de e-learning	6 horas	3 horas
	Análisis de datos para la mejora del ambiente laboral	Software de análisis de datos, herramientas de visualización de datos, sistemas de gestión de feedback	5 horas	4 horas
	Implementación de sistemas de seguimiento y apoyo	Sistemas de soporte estudiantil y de empleados, plataformas de asistencia en línea, herramientas de seguimiento y monitorización	3 horas	2 horas
	Desarrollo de programas de capacitación en entornos virtuales	Plataformas de e-learning, herramientas de creación de contenido educativo, sistemas de gestión del conocimiento	8 horas	5 horas

Esta tabla proporciona una evaluación detallada del Recovery Time Objective (RTO) y el Work Recovery Time (WRT) para cada proceso crítico en los departamentos de la institución. Incluye el departamento, el proceso crítico, las tecnologías de información utilizadas, el RTO y el WRT, basados en las estimaciones del personal administrativo concluyendo que la universidad no dispone de mucha holgura de tiempo a la hora de presentar un problema en su Ti, teniendo un máximo de 8 horas.

ACTIVIDAD 1.7

Determinar del punto objetivo de recuperación.

DESCRIPCIÓN DE LA ACTIVIDAD

En esta actividad a partir de los procesos identificados en la actividad 1.1, la información obtenida en la actividad 0.1 y tomando como referencia los tiempos identificados en la actividad anterior se establece el punto de recuperación objetivo también conocido como RPO por sus siglas en ingles Recovery Point Object, el cual establece la tolerancia máxima del tiempo que los datos o procesos pueden estar perdidos o detenidos sin afectar el desempeño de la institución. El resultado es una tabla con el departamento, proceso ejecutado y el RPO. Además de mencionar que al igual que varias actividades previas los tiempos determinados se toman en cuenta para las propuestas de solución desarrolladas en el objetivo 3 pues el tiempo de ejecución de dichas soluciones, principalmente las correctivas, no deben de exceder el RPO.

RESULTADO DE LA ACTIVIDAD

Tabla 11. Determinación del punto objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)].

Departamento	Proceso Ejecutado	RPO (Estimado)
Dirección	Redacción de reportes	4 horas
	Uso de base de datos para administración de recursos	2 horas
	Inscripciones de nuevos alumnos mediante sistemas en línea	1 hora
	Gestión de comunicaciones internas y externas	2 horas
	Monitoreo y análisis de datos institucionales	1 hora
Control Escolar	Realización de reportes académicos y administrativos	4 horas
	Uso de plataforma institucional para gestión de cursos y calificaciones	3 horas
	Administración de registros académicos en sistemas de información	2 horas
	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	4 horas
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	2 horas

Tabla 11. Determinación del punto objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	RPO (Estimado)
Educación Dual	Gestión de convenios y programas de educación dual	6 horas
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	4 horas
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	6 horas
	Monitoreo del desempeño estudiantil	4 horas
	Comunicación y gestión de recursos para la educación dual	6 horas
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software	8 horas
	Gestión de accesos y seguridad en sistemas de laboratorio	6 horas
	Coordinación de prácticas de laboratorio y reservaciones en línea	4 horas
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	8 horas
	Soporte técnico y actualizaciones de software y hardware	4 horas
Titulación	Procesamiento de solicitudes de titulación	2 horas
	Administración de expedientes académicos digitales	4 horas
	Coordinación de evaluaciones de titulación en línea	2 horas
	Comunicación con egresados y seguimiento posgraduación	6 horas
	Generación de certificados y documentos oficiales digitales	1 hora
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	4 horas
	Coordinación de exámenes y certificaciones en línea	3 horas
	Administración de plataformas de aprendizaje virtual	4 horas
	Seguimiento y evaluación del progreso estudiantil	4 horas
	Comunicación interactiva con estudiantes y docentes	8 horas
Coordinación de Ingeniería Civil	Administración de software especializado	6 horas
	Coordinación de proyectos de investigación y desarrollo	5 horas
	Gestión de recursos digitales y bases de datos técnicas	4 horas
	Organización de talleres y seminarios virtuales	8 horas
	Evaluación y seguimiento de prácticas profesionales	4 horas

Tabla 11. Determinación del punto objetivo de recuperación para cada uno de los procesos identificados. [Fuente: Alexander (2007)]. (Continuación).

Departamento	Proceso Ejecutado	RPO (Estimado)
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	6 horas
	Coordinación de experimentos y proyectos en laboratorios virtuales	5 horas
	Administración de plataformas educativas	4 horas
	Gestión de inventarios y recursos de laboratorios	6 horas
	Evaluación de desempeño y seguimiento de estudiantes	8 horas
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	4 horas
	Coordinación de auditorías internas y externas	6 horas
	Gestión de presupuestos y pronósticos financieros	4 horas
	Capacitación en herramientas digitales	8 horas
	Seguimiento y análisis de tendencias económicas	4 horas
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	4 horas
	Coordinación de programas de bienestar y desarrollo personal	6 horas
	Análisis de datos para la mejora del ambiente laboral	5 horas
	Implementación de sistemas de seguimiento y apoyo	3 horas
	Desarrollo de programas de capacitación en entornos virtuales	8 horas

Esta tabla detalla el Recovery Point Objective (RPO) para cada proceso crítico en los distintos departamentos de la institución. Se concluye que el RTO máximo es de 8 horas y el mínimo de 1 hora teniendo muy poca holgura de tiempo a la hora de establecer un RTO en cada uno de los procesos críticos de la institución.

ACTIVIDAD 1.8

Identificar los procedimientos alternos.

DESCRIPCIÓN DE LA ACTIVIDAD

En esta actividad con base a los procesos identificados en la actividad 1.1 y la información obtenida de la actividad 0.1 se identifican los procesos alternos de que podrían desempeñar el personal administrativo de la institución en el caso de que el proceso principal se detuviera. Teniendo como resultado una tabla que concentra el departamento, el proceso ejecutado y el proceso alternativo a este. La identificación de estos procesos alternos facilitar que más adelante se puedan identificar los sistemas de control que ejecuta la Institución para algunos de sus procesos, pues los procesos alternos en algunas ocasiones son los mismos sistemas de control.

RESULTADO DE LA ACTIVIDAD

Tabla 12. Identificación de los procesos alternos para cada uno de los procesos. [Fuente: Elaboración propia].

Departamento	Proceso Ejecutado	Proceso Alternativo
Dirección	Redacción de reportes	Creación manual de reportes en papel
	Uso de base de datos para administración de recursos	Uso de registros físicos y tablas manuales para la gestión de recursos
	Inscripciones de nuevos alumnos mediante sistemas en línea	Proceso de inscripción en papel y revisión manual
	Gestión de comunicaciones internas y externas	Comunicación a través de reuniones presenciales y correspondencia física
	Monitoreo y análisis de datos institucionales	Análisis manual de datos mediante informes impresos
Control Escolar	Realización de reportes académicos y administrativos	Compilación manual de datos y creación de reportes en papel
	Uso de plataforma institucional para gestión de cursos y calificaciones	Registro manual de calificaciones y cursos en registros físicos
	Administración de registros académicos en sistemas de información	Mantenimiento de archivos académicos en formato físico

Tabla 12. Identificación de los procesos alternos para cada uno de los procesos identificados. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso Ejecutado	Proceso Alterno
Control Escolar	Coordinación de horarios y asignaciones docentes a través de herramientas digitales	Planificación de horarios y asignaciones a través de tableros físicos
	Procesamiento de solicitudes de estudiantes y emisión de documentos oficiales	Procesamiento manual de solicitudes y documentos
Educación Dual	Gestión de convenios y programas de educación dual	Gestión manual de convenios con registros físicos
	Coordinación de prácticas profesionales y seguimiento en plataformas en línea	Seguimiento de prácticas a través de registros en papel y comunicación telefónica
	Desarrollo de alianzas con empresas e instituciones a través de herramientas digitales	Establecimiento de alianzas mediante reuniones presenciales y correspondencia física
	Monitoreo del desempeño estudiantil	Monitoreo del desempeño a través de reportes físicos y reuniones
	Comunicación y gestión de recursos para la educación dual	Gestión de recursos a través de métodos tradicionales sin soporte digital
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software	Revisión y monitoreo manual del equipamiento de cómputo
	Gestión de accesos y seguridad en sistemas de laboratorio	Uso de registros en papel para controlar accesos y seguridad
	Coordinación de prácticas de laboratorio y reservaciones en línea	Coordinación manual de prácticas y reservaciones mediante tableros físicos
	Desarrollo y mantenimiento de plataformas para prácticas virtuales	Desarrollo de prácticas y experimentos físicos tradicionales
	Soporte técnico y actualizaciones de software y hardware	Soporte técnico presencial y mantenimiento manual del hardware
Titulación	Procesamiento de solicitudes de titulación	Procesamiento manual de solicitudes de titulación y revisión documental
	Administración de expedientes académicos digitales	Mantenimiento de expedientes académicos en formato físico
	Coordinación de evaluaciones de titulación en línea	Coordinación manual de evaluaciones de titulación y revisión de trabajos

Tabla 12. Identificación de los procesos alternos para cada uno de los procesos identificados. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso Ejecutado	Proceso Alternativo
Titulación	Comunicación con egresados y seguimiento post-graduación	Seguimiento de egresados mediante llamadas telefónicas y encuentros presenciales
	Generación de certificados y documentos oficiales digitales	Creación manual de certificados y documentos oficiales
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Gestión manual de programas de idiomas con materiales físicos
	Coordinación de exámenes y certificaciones en línea	Coordinación física de exámenes y certificaciones en papel
	Administración de plataformas de aprendizaje virtual	Enseñanza de idiomas mediante métodos tradicionales sin soporte digital
	Seguimiento y evaluación del progreso estudiantil	Seguimiento del progreso estudiantil mediante reuniones y reportes físicos
	Comunicación interactiva con estudiantes y docentes	Comunicación directa con estudiantes y docentes en entorno físico
Coordinación de Ingeniería Civil	Administración de software especializado	Uso de métodos de diseño y cálculo manuales y tradicionales
	Coordinación de proyectos de investigación y desarrollo	Gestión manual de proyectos mediante tableros de planificación y reuniones regulares
	Gestión de recursos digitales y bases de datos técnicas	Mantenimiento manual de registros técnicos y archivos físicos
	Organización de talleres y seminarios virtuales	Organización de talleres y seminarios presenciales
	Evaluación y seguimiento de prácticas profesionales	Evaluación y seguimiento manual de prácticas mediante visitas y reportes
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Registro manual de procedimientos y normas de seguridad en papel
	Coordinación de experimentos y proyectos en laboratorios virtuales	Coordinación manual de experimentos y proyectos en el laboratorio
	Administración de plataformas educativas	Uso de métodos educativos tradicionales y materiales impresos

Tabla 12. Identificación de los procesos alternos para cada uno de los procesos identificados. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso Ejecutado	Proceso Alternativo
Coordinación de Ingeniería Química	Gestión de inventarios y recursos de laboratorios	Gestión manual de inventarios con registros físicos
	Evaluación de desempeño y seguimiento de estudiantes	Evaluación y seguimiento del desempeño estudiantil mediante encuentros y reportes escritos
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Gestión financiera y contable mediante registros y cálculos manuales
	Coordinación de auditorías internas y externas	Realización de auditorías mediante revisión física de documentos
	Gestión de presupuestos y pronósticos financieros	Elaboración manual de presupuestos y pronósticos en papel
	Capacitación en herramientas digitales	Capacitación presencial en habilidades y técnicas no digitales
	Seguimiento y análisis de tendencias económicas	Análisis de tendencias económicas mediante revisión de informes impresos y discusiones
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Realización de encuestas y estudios mediante métodos presenciales y en papel
	Coordinación de programas de bienestar y desarrollo personal	Coordinación de programas de bienestar mediante sesiones y talleres presenciales
	Análisis de datos para la mejora del ambiente laboral	Análisis manual del ambiente laboral a través de observaciones y entrevistas
	Implementación de sistemas de seguimiento y apoyo	Implementación de sistemas de seguimiento y apoyo a través de interacciones presenciales
	Desarrollo de programas de capacitación en entornos virtuales	Desarrollo de programas de capacitación mediante métodos tradicionales sin tecnología digital

Como se puede observar en la tabla todos los procesos críticos de la institución cuentan o pueden contar con un proceso alternativo en caso de no funcionar la TI, permitiendo la continuidad de las actividades.

OBJETIVO 2. Analizar Riesgos: Analizar las amenazas y vulnerabilidades de la institución para controlar o reducir los riesgos de un posible desastre.

ACTIVIDAD 2.1

Identificar los activos de TI de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Se lleva a cabo un conteo de los activos de TI de los que dependen los distintos procesos críticos identificados en las actividades del objetivo 1, con el motivo de identificar la TI con mayor prioridad de resguardo. Esta actividad se realiza mediante entrevistas con personal relevante, revisión de documentación existente y revisión de las mismas instalaciones. Teniendo como resultado una tabla con el departamento, proceso crítico y la TI asignada a dicho proceso. Con el añadido de un pequeño catálogo de equipos de cómputo más comunes con una ficha técnica propia.

RESULTADO DE LA ACTIVIDAD

Tabla 13. Identificación de los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia].

Departamento	Proceso critico	Ti Asignada	Ficha Técnica
Dirección	Monitoreo y análisis de datos institucionales	1 Computadora 1 Impresora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro Epson EcoThank M2120 Circuito continuo
	Gestión de comunicaciones internas y externas	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
Control Escolar	Administración de registros académicos en sistemas de información	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro

Tabla 13. Identificación de los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Ti Asignada	Ficha Técnica
Control Escolar	Uso de plataforma institucional para gestión de cursos y calificaciones	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
Educación Dual	Gestión de convenios y programas de educación dual	2 Computadoras	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Monitoreo del desempeño estudiantil		
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	1 Computadora 2 Router 4 Switches	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro Cisco 1900 Series Router 512Mb RAM Cisco Catalyst 2960 Series Switch (2) 24 Puertos Ethernet (Gigabit) 512Mb RAM
	Coordinación de prácticas de laboratorio y reservaciones en línea	23 Computadoras 20 Computadoras 40 Computadoras	HP – Sff Core i5 8va 8Gb RAM Windows 11 Pro
Titulación	Procesamiento de solicitudes de titulación	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Generación de certificados y documentos oficiales digitales		

Tabla 13. Identificación de los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Ti Asignada	Ficha Técnica
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Coordinación de exámenes y certificaciones en línea		
Coordinación de Ingeniería Civil	Administración de software especializado	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Coordinación de proyectos de investigación y desarrollo		
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Coordinación de experimentos y proyectos en laboratorios virtuales		
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Coordinación de auditorías internas y externas		

Tabla 13. Identificación de los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Ti Asignada	Ficha Técnica
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	1 Computadora	Lenovo - ThinkCentre M700 Core i7 6ta 8Gb RAM Windows 10 Pro
	Implementación de sistemas de seguimiento y apoyo		

Como se puede observar en los resultados obtenidos en la tabla, a grandes rasgos la marca de computadoras que predomina más en la Universidad es Lenovo, así mismo, la mayor concentración de activos de TI se encuentra ubicada en los laboratorios de cómputo y los procesos ejecutados dentro de ellos. Para ver el inventario completo ir al Anexo A. Inventario de los Activos de TI de la Institución.

ACTIVIDAD 2.2

Identificar las amenazas a la TI de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Para esta actividad se identifican las principales amenazas a los activos de TI asignados a los procesos críticos de la institución identificados en la actividad 2.1, dichas amenazas fueron identificadas por medio de la observación de los medios de seguridad con los que cuenta actualmente la institución, así como preguntas específicas a aquellos que desempeñan los procesos críticos de la Institución. Así mismo se resalta que la identificación de las amenazas es de gran importancia poder realizar una priorización de cada una y posteriormente idear planes de acción para poder mitigarlas, siendo esto algo que se verá en las actividades del objetivo 3. El resultado es una tabla con el departamento, proceso crítico y la amenaza a que la que se encuentran expuestos dichos procesos.

RESULTADO DE LA ACTIVIDAD

Tabla 14. Identificación de las amenazas a los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia].

Departamento	Proceso crítico	Amenaza
Dirección	Monitoreo y análisis de datos institucionales	Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos
	Gestión de comunicaciones internas y externas	Suplantación de identidad (spoofing)
Control Escolar	Administración de registros académicos en sistemas de información	Fallos del sistema como problemas de autenticación o registros no generados
	Uso de plataforma institucional para gestión de cursos y calificaciones	Interrupción del servicio por un ataque DDoS
Educación Dual	Gestión de convenios y programas de educación dual	Interrupción del servicio de internet
	Monitoreo del desempeño estudiantil	Perdida de comunicación con los estudiante y empresas que se encuentren en el programa.

Tabla 14. Identificación de las amenazas a los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Amenaza
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios	Incendio eléctrico donde se pierden los equipos de computo
	Coordinación de prácticas de laboratorio y reservaciones en línea	Interrupciones de las reservaciones en línea
Titulación	Procesamiento de solicitudes de titulación	Acceso no autorizado que provoque la manipulación de registros académicos
	Generación de certificados y documentos oficiales digitales	Perdida del equipo de cómputo donde se generan dichos documentos
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales	Infección por malware en el equipo de cómputo
	Coordinación de exámenes y certificaciones en línea	Compromiso de la integridad de los exámenes por un ataque de ingeniería social (Phishing y acceso remoto)
Coordinación de Ingeniería Civil	Administración de software especializado	Uso de software sin licencia que pueda tener malware implantado
	Coordinación de proyectos de investigación y desarrollo	Pérdida de datos críticos de investigación debido a fallas de almacenamiento
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos	Perdida de la integridad de la información de la base de datos
	Coordinación de experimentos y proyectos en laboratorios virtuales	Fallos en el servicio de internet

Tabla 14. Identificación de las amenazas a los activos de TI asignados a cada uno de los procesos críticos. [Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Amenaza
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Fallos de software de contabilidad
	Coordinación de auditorías internas y externas	Pérdida de acceso a documentos en línea durante auditorías
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional	Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas
	Implementación de sistemas de seguimiento y apoyo	Mala gestión de los sistemas de seguimiento y apoyo

Con la información sobre las amenazas identificadas con relación a los procesos críticos de la institución capturada en la tabla 14 se puede notar que, a grandes rasgos, la mayoría de las amenazas son del tipo lógico como la posible infección de equipos de cómputo por malware o un ataque de phishing.

ACTIVIDAD 2.3

Identificar las vulnerabilidades de los activos de TI de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Esta actividad parte de las amenazas identificadas en la actividad 2.2, detallando las vulnerabilidades encontradas en la TI asignada a los procesos críticos de la institución, identificadas en la actividad 2.1, que pudieran permitir que las amenazas observadas se puedan materializar. Así mismo se resalta que la identificación de las vulnerabilidades existentes es de gran importancia poder realizar una priorización de cada una y posteriormente idear planes de acción para poder mitigarlas, siendo esto algo que se verá en las actividades del objetivo 3. Como resultado se obtiene una tabla similar a la anterior, donde se observa; El departamento, proceso crítico y las vulnerabilidades.

RESULTADO DE LA ACTIVIDAD

*Tabla 15. Identificación de las vulnerabilidades de los activos de TI asignados a cada uno de los procesos críticos.
[Fuente: Elaboración propia].*

Departamento	Proceso crítico	Vulnerabilidades
Dirección	Monitoreo y análisis de datos institucionales.	Antivirus poco eficiente. Falta de conciencia sobre seguridad informática.
	Gestión de comunicaciones internas y externas.	Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican.
Control Escolar	Administración de registros académicos en sistemas de información.	Sistemas saturados de información obsoleta.
	Uso de plataforma institucional para gestión de cursos y calificaciones.	Falta de un medio de control del tráfico de red.

Tabla 15. Identificación de las vulnerabilidades de los activos de TI asignados a cada uno de los procesos críticos.
[Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Vulnerabilidades
Educación Dual	Gestión de convenios y programas de educación dual.	Infraestructura física de la red deficiente. Problemas con el proveedor del servicio.
	Monitoreo del desempeño estudiantil.	Ausencia de un respaldo de los contactos.
Laboratorios de Cómputo	Administración y monitoreo de equipamiento y software de laboratorios.	Corto circuito en las tomas de corriente de los laboratorios. Ausencia de extintores en laboratorio.
	Coordinación de prácticas de laboratorio y reservaciones en línea.	El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.
Titulación	Procesamiento de solicitudes de titulación.	Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.
	Generación de certificados y documentos oficiales digitales.	Vigilancia escasa en la oficina del departamento.
Coordinación de Inglés	Gestión de programas de idiomas y recursos digitales.	Descarga de programas de idiomas de sitios no oficiales.
	Coordinación de exámenes y certificaciones en línea.	Ausencia de software antimalware. Monitoreo inexistente de correos electrónicos no deseados. Falta de conciencia en seguridad informática.

Tabla 15. Identificación de las vulnerabilidades de los activos de TI asignados a cada uno de los procesos críticos.
[Fuente: Elaboración propia]. (Continuación).

Departamento	Proceso critico	Vulnerabilidades
Coordinación de Ingeniería Civil	Administración de software especializado.	Ausencia de software antivirus en los equipos de cómputo utilizados. Uso de software para “crackeo” de programas con licencia.
	Coordinación de proyectos de investigación y desarrollo.	Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste. Ausencia de respaldos en la nube u otra unidad de almacenamiento.
Coordinación de Ingeniería Química	Manejo de bases de datos de seguridad y procedimientos químicos.	Uso de software no especializado para bases de datos.
	Coordinación de experimentos y proyectos en laboratorios virtuales.	Infraestructura física de la red deficiente. Problemas con el proveedor del servicio.
Coordinación de Licenciatura en Contaduría	Uso de sistemas contables y de gestión financiera	Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores.
	Coordinación de auditorías internas y externas.	Proveedor del servicio de internet poco confiable. Control deficiente del servicio en la nube donde se encuentran los documentos.
Coordinación de Licenciatura en Psicología Industrial	Gestión de encuestas y estudios de clima organizacional.	Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados.
	Implementación de sistemas de seguimiento y apoyo.	El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado.

Una vez capturadas las vulnerabilidades en la tabla 15 se puede notar que varias de las vulnerabilidades identificadas se deben a la falta de conciencia por parte del personal administrativo sobre el riesgo que corren sus activos de TI. Además, como se puede observar en la actividad 2.2 y en esta (2.3) el resultado que se obtiene son dos tablas de gran extensión donde varias amenazas y vulnerabilidades se conservan muchas similitudes lo que conllevaría a que los riesgos pudieran repetirse, por ese motivo se procede a generar un catálogo de amenazas, vulnerabilidades y riesgos; donde se busca compactar los resultados obtenidos en las actividades 2.2 y 2.3.

Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos. [Fuente: Elaboración propia].

Proceso critico	Amenaza	Vulnerabilidades	Riesgos
Monitoreo y análisis de datos institucionales	Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos. Infección por malware en el equipo de cómputo. Uso de software sin licencia que pueda tener malware implantado. Compromiso de la integridad de los exámenes por un ataque de ingeniería social. (Phishing y acceso remoto).	Antivirus poco eficiente.	Perdida temporal o permanente de los equipos de cómputo afectados, así como la alta probabilidad de que se pierdan la información almacenada en ellos. Lo que provocaría que los procesos críticos que dependen de ellos se vean abruptamente detenidos.
Gestión de programas de idiomas y recursos digitales		Falta de conciencia sobre seguridad informática.	
Administración de software especializado		Descarga de programas de idiomas de sitios no oficiales.	
		Uso de software para “crackeo” de programas con licencia.	
Coordinación de exámenes y certificaciones en línea		Ausencia de software antimalware.	
		Falta de conciencia en seguridad informática.	

Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos
Gestión de comunicaciones internas y externas	Suplantación de identidad (spoofing).	Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican. Monitoreo inexistente de correos electrónicos no deseados.	Completa descoordinación en toda la institución debido a la propagación de instrucciones e información falsa por medios electrónicos (correo electrónico) debido al acceso no autorizado de una de las cuentas administrativas.
Administración de registros académicos en sistemas de información	Fallos del sistema como problemas de autenticación o registros no generados. Interrupción del servicio por un ataque DDoS. Interrupción del servicio de internet Fallos en el servicio de internet.	Sistemas saturados de información obsoleta.	Retraso indefinido de los procesos críticos, así como de las actividades dependientes, debido a que el funcionamiento de los servicios contratados a terceros no entra bajo el control de la institución.
Uso de plataforma institucional para gestión de cursos y calificaciones		Falta de un medio de control del tráfico de red.	
Gestión de convenios y programas de educación dual		Infraestructura física de la red deficiente.	
Coordinación de experimentos y proyectos en laboratorios virtuales		Problemas con el proveedor del servicio.	
		Infraestructura física de la red deficiente.	
		Problemas con el proveedor del servicio.	

Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos
Administración y monitoreo de equipamiento y software de laboratorios	Incendio eléctrico donde se pierden los equipos de cómputo.	Corto circuito en las tomas de corriente de los laboratorios. Ausencia de extintores en laboratorio.	Pérdida total o parcial de los activos de TI, principalmente equipos de cómputo, que se encuentren en el área afectada por el incendio que de no atenderse con rapidez significaría la pérdida total de laboratorio donde se generó el incendio.
Coordinación de prácticas de laboratorio y reservaciones en línea	Interrupciones de las reservaciones en línea.	El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.	Completa descoordinación entre el personal docente que solicita el uso de alguno de los laboratorios pues al no tener un registro de reservaciones y conteo de horas de uso, provocaría el abuso de tiempo en los laboratorios por parte de algunos docentes o la sobre posición de horas entre dos o más grupos.
Procesamiento de solicitudes de titulación	Acceso no autorizado que provoque la manipulación de registros académicos.	Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.	Generación de documentos para solicitud de titulación sin autorización o modificación de los datos personales las solicitudes ya realizadas.

Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos
Generación de certificados y documentos oficiales digitales	Perdida del equipo de cómputo donde se generan dichos documentos. Pérdida de datos críticos de investigación debido a fallas de almacenamiento. Perdida de la integridad de la información de la base de datos Pérdida de acceso a documentos en línea durante auditorías Perdida de comunicación con los estudiante y empresas que se encuentren en el programa.	Vigilancia escasa en la oficina del departamento.	Debido la falta de un respaldo tanto de documentos importantes almacenados para la posteridad, aquellos con los que se trabaja de forma frecuente o incluso el contacto registrado de alumnado que es participe de programas de formación dual provocarían desde la detención abrupta e indefinida de más de un proceso crítico, hasta el daño a la reputación de la Universidad.
Coordinación de proyectos de investigación y desarrollo		Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste.	
Manejo de bases de datos de seguridad y procedimientos químicos		Ausencia de respaldos en la nube u otra unidad de almacenamiento.	
Coordinación de auditorías internas y externas		Uso de software no especializado para bases de datos.	
Monitoreo del desempeño estudiantil		Control deficiente del servicio en la nube donde se encuentran los documentos.	
		Ausencia de un respaldo de los contactos.	
Uso de sistemas contables y de gestión financiera	Fallos de software de contabilidad	Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores.	Detención de las actividades previstas a trabajar con el software contable, afectando tanto al desempeño de departamento como al alumnado que hace uso de dicho software para su formación académica.

Tabla 16. Catálogo de amenazas, vulnerabilidades y riesgos. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos
Gestión de encuestas y estudios de clima organizacional	Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas	Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados.	Se generarían problemas de convivencia entre alumnado, docentes y personal administrativo que afectaría su desempeño dentro de la institución.
Implementación de sistemas de seguimiento y apoyo	Mala gestión de los sistemas de seguimiento y apoyo	El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado.	Aquellos que dependan de los sistemas de seguimiento y apoyo, se verían significativamente afectados, tanto a nivel personal como en su desempeño académico o administrativo.

Como resultado de la creación de un catálogo de amenazas, vulnerabilidades y riesgos; se puede observar una síntesis de las tablas 14 y 15, lo que permitirá en las actividades del siguiente objetivo poder abordar de una forma más eficiente la propuesta de soluciones para mitigar los riesgos encontrados.

ACTIVIDAD 2.4

Aplicar una encuesta al personal administrativo para poder calcular la exposición al riesgo.

DESCRIPCIÓN DE LA ACTIVIDAD

Para la actividad 2.6 se realiza la evaluación del riesgo al que se encuentra expuesta la Universidad, para ello de acuerdo con las recomendaciones en el trabajo de maestría titulado “Metodología para el establecimiento de objetivos de control como un medio de seguimiento en el área de Tecnologías de la Información” de la Mtra. Diana Marisol Prado Oseguera el riesgo se evaluara de forma cualitativa debido a que la institución se puede considerar de pequeño tamaño así como de recursos limitados. Para realizar dicha evaluación es imperativo la aplicación de un cuestionario con una extensa cantidad de preguntas al personal administrativo de los departamentos previamente identificados. Cabe destacar que la mayoría de los departamentos son administrados por solo una persona.

RESULTADO DE LA ACTIVIDAD

Los resultados de los cuestionarios se pueden observar a continuación.

AMENAZAS

- 1.1 ¿Con qué frecuencia considera que la Universidad Mexiquense del Bicentenario podría enfrentar un ataque de ransomware que cifre todos los datos institucionales e impida el acceso?
- 1.2 En caso de un ataque de ransomware exitoso, ¿cuál sería el impacto en la continuidad de las operaciones y en la integridad de los datos institucionales?
- 2.1.¿Cuán vulnerable cree que es la universidad a la suplantación de identidad (spoofing)?
- 2.2.¿Qué tan crítico sería un caso de suplantación de identidad para las operaciones y la seguridad de la información?
- 3.1 ¿Qué tan probable es que ocurran fallos del sistema, como problemas de autenticación o registros no generados, en la universidad?
- 3.2 ¿Cómo afectaría a las operaciones de la universidad un fallo del sistema que impide la autenticación de usuarios?

- 4.1 ¿Considera que la universidad podría ser blanco de un ataque de Denegación de Servicio (DDoS)?
- 4.2 ¿Cuál sería el impacto en la continuidad de los servicios si la universidad experimenta un ataque DDoS?
- 5.1 ¿Con qué frecuencia cree que la universidad podría enfrentar interrupciones en el servicio de internet?
- 5.2 En caso de una interrupción del servicio de internet, ¿cómo afectaría esto a las actividades académicas y administrativas?
- 3.1 ¿Cuán probable es que la universidad pierda comunicación con estudiantes y escuelas participantes en programas académicos?
- 3.2 En caso de pérdida de comunicación, ¿cómo afectaría esto a las relaciones académicas y de colaboración?
- 7.1 ¿Considera que hay riesgo de un incendio eléctrico que resulte en la pérdida de equipos de cómputo?
- 7.2 ¿Cómo impactaría un incendio eléctrico en la infraestructura de TI y en la disponibilidad de los equipos?
- 8.1 ¿Qué tan probable es que se produzcan interrupciones en las reservaciones en línea?
- 8.2 ¿Cómo afectaría a la universidad y a los usuarios la interrupción de servicios de reservas en línea?
- 9.1 ¿Cuán vulnerable es la universidad a accesos no autorizados que manipulen registros académicos?
- 9.2 ¿Cuál sería el impacto en la integridad de los registros académicos si se produjera un acceso no autorizado?
- 10.1 ¿Qué tan probable es la pérdida de equipos de cómputo donde se generan documentos importantes?
- 10.2 ¿Cómo afectaría a la universidad la pérdida de equipos con documentos críticos?
- 11.1 ¿Considera que existe riesgo de infección por malware en los equipos de cómputo de la universidad?
- 11.2 ¿Cómo afectaría a las operaciones de la universidad una infección por malware en los equipos de cómputo?

- 12.1 ¿Cuán vulnerable es la universidad a un compromiso de la integridad de exámenes mediante ingeniería social (Phishing y acceso remoto)?
- 12.2 ¿Cuál sería el impacto en la confidencialidad y autenticidad de los exámenes en caso de un compromiso por ingeniería social?
- 13.1 ¿Cuán probable es el uso de software sin licencia que pueda tener malware implantado en la universidad?
- 13.2 ¿Cómo afectaría a la universidad el uso de software sin licencia que contenga malware
- 14.1 ¿Considera que hay riesgo de pérdida de datos críticos de investigación debido a fallas de almacenamiento?
- 14.2 ¿Cómo impactaría a la universidad la pérdida de datos críticos de investigación?
- 15.1 ¿Cuán probable es la pérdida de integridad de la información en la base de datos de la universidad?
- 15.2 ¿Cómo afectaría a las operaciones y toma de decisiones la pérdida de integridad en la base de datos?
- 16.1 ¿Con qué frecuencia considera que la universidad podría experimentar fallos en el servicio de internet?
- 16.2 En caso de fallos en el servicio de internet, ¿cómo afectaría esto a las actividades académicas y administrativas?
- 17.1 ¿Cuán probable es experimentar fallos en el software de contabilidad de la universidad?
- 17.1 ¿Cómo impactaría a la universidad un fallo en el software de contabilidad en términos financieros y administrativos?
- 18.1 ¿Qué tan probable es la pérdida de acceso a documentos en línea durante procesos de auditoría?
- 18.2 ¿Cómo afectaría a la universidad la pérdida de acceso a documentos durante una auditoría?
- 19.1 ¿Considera que hay riesgos de brechas de seguridad que comprometan la confidencialidad de las respuestas de las encuestas?
- 19.2 ¿Cómo impactaría en la reputación de la universidad y la confianza de los encuestados una brecha de seguridad en encuestas?
- 20.1 ¿Cuán probable es que se produzca una mala gestión de los sistemas de seguimiento y apoyo?
- 20.2 ¿Cómo afectaría a las operaciones y servicios de apoyo una mala gestión de sistemas?

VULNERABILIDADES

- 21.1 ¿Con que frecuencia se ven afectados los equipos de cómputo con virus?
- 21.2 ¿De qué grado sería el impacto operacional si una maquina se infecta con algún tipo de virus?
- 22.1 ¿Qué tan frecuente es que los empleados incurran en prácticas inseguras debido a una falta de conciencia sobre seguridad informática?
- 22.2 ¿Cuál sería el impacto en la seguridad de la información de la escuela si continúa la falta de conciencia sobre seguridad informática?
- 23.1 ¿Con qué frecuencia son objeto de ataques de phishing los empleados administrativos en la escuela?
- 23.2 ¿Cuál sería el impacto operacional si se lograra un acceso no autorizado a las cuentas de comunicación de los empleados administrativos?
- 24.1 ¿Qué tan a menudo se enfrentan los sistemas de la escuela a problemas debido a la saturación de información obsoleta?
- 24.2 ¿Qué grado de impacto tendría en la eficiencia operativa de la escuela la saturación de los sistemas con información obsoleta?
- 25.1 ¿Qué tan a menudo surgen problemas de seguridad o de rendimiento en la red debido a la falta de un medio de control del tráfico?
- 25.2 ¿Qué tanto afectaría a la integridad y funcionamiento de la red escolar la falta de control sobre el tráfico de esta?
- 26.1 ¿Con qué frecuencia se presentan fallos o interrupciones en la red debido a una infraestructura física deficiente?
- 26.2 ¿Qué impacto tendría en las operaciones diarias de la escuela una infraestructura física de red deficiente?
- 27.1 ¿Con qué frecuencia ocurren cortocircuitos en las tomas de corriente de los laboratorios?
- 27.2 ¿Qué impacto tendría un cortocircuito en las operaciones y la seguridad de los laboratorios?
- 28.1 ¿Cuál es la probabilidad de que un incendio no pueda ser controlado a tiempo debido a la ausencia de extintores?
- 28.2 ¿Qué consecuencias tendría la ausencia de extintores en caso de un incendio en las instalaciones?

- 29.1 ¿Qué tan frecuente es que se presenten problemas o pérdidas de datos en el registro de reservaciones que se encuentra en un solo equipo?
- 29.2 ¿Cuál sería el impacto en la gestión de reservaciones si se perdiera o dañara el archivo Excel en el equipo de cómputo?
- 30.1 ¿Con qué frecuencia se presentan riesgos de seguridad debido al fácil acceso al equipo de cómputo en una oficina vacía?
- 30.2 ¿Cuál sería el impacto en la seguridad y confidencialidad de la información si alguien accediera sin autorización al equipo de cómputo?
- 31.1 ¿Qué tan a menudo ocurren incidentes de seguridad o robos en la oficina del departamento debido a la vigilancia escasa?
- 31.2 ¿Cuál sería el impacto de una vigilancia escasa en términos de seguridad y protección de activos en la oficina del departamento?
- 32.1 ¿Con qué frecuencia se descargan programas de idiomas de fuentes no oficiales, y qué riesgos implica?
- 32.2 ¿Qué impacto tendría en la seguridad informática la descarga de programas de idiomas de sitios no oficiales?
- 33.1 ¿Qué tan probable es que los equipos se vean afectados por malware debido a la falta de software antimalware?
- 33.2 ¿Cuál sería el impacto en la seguridad de la información y en el rendimiento de los sistemas debido a la ausencia de software antimalware?
- 34.1 ¿Con qué frecuencia se enfrentan a problemas relacionados con correos electrónicos no deseados debido a la falta de monitoreo?
- 34.2 ¿Qué impacto tendría en la productividad y seguridad informática el no tener un sistema de monitoreo de correos electrónicos no deseados?
- 35.1 ¿Con qué frecuencia se utiliza software de "crackeo" en la organización?
- 35.2 ¿Qué impacto tendría el uso de software de "crackeo" en la seguridad y legalidad de las operaciones de la organización?
- 36.1 ¿Qué tan a menudo se presentan fallos o pérdidas de datos debido al uso de unidades de almacenamiento desgastadas?
- 36.2 ¿Cuál sería el impacto en la continuidad de las operaciones si fallan las unidades de almacenamiento desgastadas?

- 37.1 ¿Cuál es la probabilidad de pérdida de datos críticos debido a la ausencia de respaldos adecuados?
- 37.2 ¿Qué impacto tendría en la organización la pérdida de datos importantes debido a la falta de respaldos?
- 38.1 ¿Con qué frecuencia se enfrentan a limitaciones o problemas debido al uso de software no especializado para bases de datos?
- 38.2 ¿Qué consecuencias tendría el uso de software no especializado en la gestión y seguridad de las bases de datos?
- 39.1 ¿Qué tan común es el uso de software sin soporte y cuáles son los riesgos asociados?
- 39.2 ¿Cuál sería el impacto en la seguridad y eficiencia operativa al utilizar software sin soporte ni actualizaciones?
- 40.1 ¿Qué tan frecuente es que se presenten problemas de seguridad o acceso debido a un control deficiente del servicio en la nube?
- 40.2 ¿Qué impacto tendría un control deficiente del servicio en la nube en la confidencialidad y disponibilidad de los documentos?
- 41.1 ¿Con qué frecuencia se compromete la seguridad de las encuestas en línea debido a contraseñas inseguras?
- 41.2 ¿Cuál sería el impacto si se accediera indebidamente a las cuentas de las encuestas en línea debido a contraseñas inseguras?
- 42.1 ¿Qué tan a menudo se presentan errores o ineficiencias en los procesos debido a la falta de capacitación en el software especializado?
- 42.2 ¿Qué impacto tendría en la calidad y eficiencia de los procesos el que el personal no esté adecuadamente capacitado para usar el software especializado?

ACTIVIDAD 2.5

Análisis de los resultados de las encuestas.

DESCRIPCIÓN DE LA ACTIVIDAD

Con los resultados de la actividad anterior se realiza un análisis, donde siguiendo las recomendaciones de la metodología desarrollada por la Mtra. Diana Marisol Prado Oseguera de nombre “Metodología para el establecimiento de objetivos de control como un medio de seguimiento en el área de Tecnologías de la Información” se realiza una tabla que contraste los resultados obtenidos donde se traslapen el impacto y la probabilidad de cada una de las amenazas y vulnerabilidades identificadas. Para posteriormente en la actividad 2.6 poder generar una tabla donde se ordenen las amenazas, así como las vulnerabilidades según la prioridad que tengan.

RESULTADO DE LA ACTIVIDAD

AMENAZAS

Tabla 17. Análisis preguntas 1.1 y 1.2. [Fuente: Prado (2009)].

Amenaza: Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos.			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia considera que la Universidad Mexiquense del Bicentenario podría enfrentar un ataque de ransomware que cifre todos los datos institucionales e impida el acceso?	10	0	0
En caso de un ataque de ransomware exitoso, ¿cuál sería el impacto en la continuidad de las operaciones y en la integridad de los datos institucionales?	2	2	6

La universidad muestra confianza en sus defensas ante un ataque de ransomware, reflejado en la baja percepción de ocurrencia. Sin embargo, la alta puntuación en el impacto subraya la importancia de mantener y mejorar las medidas de seguridad cibernética para minimizar cualquier riesgo potencial y garantizar la continuidad operativa y la integridad de los datos institucionales.

Tabla 18. Análisis preguntas 2.1 y 2.2. [Fuente: Prado (2009)].

Amenaza: Suplantación de identidad (spoofing)			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Cuán vulnerable cree que es la universidad a la suplantación de identidad (spoofing)?	6	4	0
¿Qué tan crítico sería un caso de suplantación de identidad para las operaciones y la seguridad de la información?	1	4	5

La Universidad Mexiquense del Bicentenario se percibe como relativamente segura frente a la suplantación de identidad (spoofing), con una ocurrencia considerada como "Casi nunca". Aunque la ocurrencia es baja, se reconoce que un caso de suplantación de identidad tendría un impacto significativo, evaluado como "Alto" en términos de crítico para las operaciones y la seguridad de la información. Es esencial mantener y fortalecer las medidas de seguridad para mitigar posibles riesgos en este aspecto.

Tabla 19. Análisis preguntas 3.1 y 3.2. [Fuente: Prado (2009)].

Amenaza: Fallos del sistema como problemas de autenticación o registros no generados			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Qué tan probable es que ocurran fallos del sistema, como problemas de autenticación o registros no generados, en la universidad?	6	4	0
¿Cómo afectaría a las operaciones de la universidad un fallo del sistema que impide la autenticación de usuarios?	0	8	2

La Universidad Mexiquense del Bicentenario se percibe como relativamente segura frente a fallos del sistema, con una ocurrencia considerada como "Casi nunca". Sin embargo, se reconoce que si ocurriera un fallo del sistema que impidiera la autenticación de usuarios, el impacto sería significativo, evaluado como "Medio". A pesar de la baja probabilidad, es crucial mantener medidas preventivas y correctivas para garantizar la estabilidad operativa y la seguridad del sistema.

Tabla 20. Análisis preguntas 4.1 y 4.2. [Fuente: Prado (2009)].

		Amenaza: Interrupción del servicio por un ataque DDoS		
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO	
	Casi nunca	Algunas veces	Siempre sucede	
¿Considera que la universidad podría ser blanco de un ataque de Denegación de Servicio (DDoS)?	9	1	0	
¿Cuál sería el impacto en la continuidad de los servicios si la universidad experimenta un ataque DDoS?	2	2	5	

La Universidad Mexiquense del Bicentenario presenta una percepción baja de ser blanco de un ataque de Denegación de Servicio (DDoS), con una ocurrencia casi nula evaluada como "Casi nunca". Aunque la probabilidad es baja, se reconoce que un eventual ataque DDoS tendría un impacto significativo en la continuidad de los servicios, calificado como "Alto". Mantener medidas de protección contra este tipo de amenaza es crucial para preservar la operatividad y la disponibilidad de los servicios universitarios.

Tabla 21. Análisis preguntas 5.1 y 5.2. [Fuente: Prado (2009)].

Amenaza: Interrupción del servicio de internet			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia cree que la universidad podría enfrentar interrupciones en el servicio de internet?	4	5	1
En caso de una interrupción del servicio de internet, ¿Cómo afectaría esto a las actividades académicas y administrativas?	2	4	4

La Universidad Mexiquense del Bicentenario tiene una percepción mixta sobre la ocurrencia de interrupciones en el servicio de internet, con una evaluación entre "Casi nunca" y "Algunas veces". En caso de una interrupción, se anticipa un impacto moderado en las actividades académicas y administrativas, calificado como "Medio". Mantener medidas de contingencia y redundancia en la conectividad es esencial para mitigar los posibles efectos adversos en las operaciones universitarias.

Tabla 22. Análisis preguntas 6.1 y 6.2. [Fuente: Prado (2009)].

Amenaza: Pérdida de comunicación con los estudiante y empresas que se encuentren en el programa.			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Cuán probable es que la universidad pierda comunicación con estudiantes y escuelas participantes en programas académicos?	5	4	1
En caso de pérdida de comunicación, ¿Cómo afectaría esto a las relaciones académicas y de colaboración?	2	6	2

La Universidad Mexiquense del Bicentenario percibe como poco probable la pérdida de comunicación con estudiantes y escuelas participantes en programas académicos, con una ocurrencia mayormente clasificada como "Casi nunca". En caso de que ocurriera, se espera un impacto de nivel medio en las relaciones académicas y de colaboración, con una puntuación de "Medio". Asegurar canales de comunicación robustos y establecer medidas de contingencia contribuiría a mantener relaciones efectivas en el ámbito académico y de colaboración.

Tabla 23. Análisis preguntas 7.1 y 7.2. [Fuente: Prado (2009)].

Amenaza: Incendio eléctrico donde se pierden los equipos de computo			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Considera que hay riesgo de un incendio eléctrico que resulte en la pérdida de equipos de cómputo?	9	1	0
¿Cómo impactaría un incendio eléctrico en la infraestructura de TI y en la disponibilidad de los equipos?	0	0	10

La Universidad Mexiquense del Bicentenario considera extremadamente baja la probabilidad de un incendio eléctrico que resulte en la pérdida de equipos de cómputo, clasificándolo como "Casi nunca". Sin embargo, se reconoce que un incendio eléctrico tendría un impacto catastrófico en la infraestructura de TI y la disponibilidad de los equipos, evaluado como "Alto". A pesar de la baja ocurrencia percibida, implementar medidas de prevención y planes de contingencia es esencial para minimizar el riesgo y preservar la integridad de la infraestructura tecnológica.

Tabla 24. Análisis preguntas 8.1 y 8.2. [Fuente: Prado (2009)].

		Amenaza: Interrupciones de las reservaciones en línea		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan probable es que se produzcan interrupciones en las reservaciones en línea?		4	6	0
¿Cómo afectaría a la universidad y a los usuarios la interrupción de servicios de reservas en línea?		3	3	4

La Universidad Mexiquense del Bicentenario reconoce la posibilidad de interrupciones en las reservaciones en línea, con una ocurrencia evaluada principalmente como "Algunas veces". En caso de interrupciones, se anticipa un impacto moderado tanto para la universidad como para los usuarios, calificado como "Medio". Implementar medidas de contingencia y monitoreo constante es esencial para minimizar los efectos adversos en los servicios de reservas en línea y garantizar una experiencia fluida para los usuarios.

Tabla 25. Análisis preguntas 9.1 y 9.2. [Fuente: Prado (2009)].

		Amenaza: Acceso no autorizado que provoque la manipulación de registros académicos		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Cuán vulnerable es la universidad a accesos no autorizados que manipulen registros académicos?		8	2	0
¿Cuál sería el impacto en la integridad de los registros académicos si se produjera un acceso no autorizado?		0	0	10

La Universidad Mexiquense del Bicentenario se percibe como relativamente segura frente a accesos no autorizados que manipulen registros académicos, con una ocurrencia considerada principalmente como "Casi nunca". Sin embargo, se reconoce que un acceso no autorizado tendría un impacto extremadamente alto en la integridad de los registros académicos, calificado como "Alto". Mantener medidas de seguridad robustas y vigilancia continua es crucial para prevenir cualquier manipulación indebida y preservar la integridad de los datos académicos.

Tabla 26. Análisis preguntas 10.1 y 10.2. [Fuente: Prado (2009)].

		Amenaza: Pérdida del equipo de cómputo donde se generan dichos documentos		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan probable es la pérdida de equipos de cómputo donde se generan documentos importantes?		0	7	3
¿Cómo afectaría a la universidad la pérdida de equipos con documentos críticos?		0	0	10

La Universidad Mexiquense del Bicentenario considera como probable la pérdida de equipos de cómputo donde se generan documentos importantes, con una ocurrencia mayormente clasificada como "Algunas veces". Se reconoce que esta pérdida tendría un impacto extremadamente alto en la universidad, evaluado como "Alto". Implementar medidas de seguridad física y respaldo de documentos es esencial para minimizar el riesgo y preservar la integridad de los documentos críticos.

Tabla 27. Análisis preguntas 11.1 y 11.2. [Fuente: Prado (2009)].

		Amenaza: Infección por malware en el equipo de cómputo		
NIVEL OCURRENCIA / IMPACTO		BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
	¿Considera que existe riesgo de infección por malware en los equipos de cómputo de la universidad?	5	3	2
	¿Cómo afectaría a las operaciones de la universidad una infección por malware en los equipos de cómputo?	3	3	4

La Universidad Mexiquense del Bicentenario reconoce un riesgo moderado de infección por malware en sus equipos de cómputo, con una ocurrencia clasificada principalmente como "Casi nunca" y "Algunas veces". En caso de una infección, se espera un impacto moderado en las operaciones de la universidad, calificado como "Medio". Implementar medidas de seguridad cibernética, como antivirus y prácticas de navegación seguras, es esencial para mitigar el riesgo y garantizar la continuidad operativa.

Tabla 28. Análisis preguntas 12.1 y 12.2. [Fuente: Prado (2009)].

		Amenaza: Compromiso de la integridad de los exámenes por un ataque de ingeniería social		
NIVEL OCURRENCIA / IMPACTO		BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
	¿Cuán vulnerable es la universidad a un compromiso de la integridad de exámenes mediante ingeniería social (Phishing y acceso remoto)?	9	2	0
	¿Cuál sería el impacto en la confidencialidad y autenticidad de los exámenes en caso de un compromiso por ingeniería social?	0	2	8

La Universidad Mexiquense del Bicentenario se percibe como altamente segura frente a un compromiso de la integridad de los exámenes mediante ingeniería social, con una ocurrencia mayormente clasificada como "Casi nunca". Sin embargo, se reconoce que un posible compromiso tendría un impacto significativo en la confidencialidad y autenticidad de los exámenes, evaluado como "Alto". A pesar de la baja probabilidad percibida, implementar medidas preventivas y de concientización sobre la ingeniería social es esencial para preservar la integridad de los procesos de evaluación académica.

Tabla 29. Análisis preguntas 13.1 y 13.2. [Fuente: Prado (2009)].

		Amenaza: Uso de software sin licencia que pueda tener malware implantado		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Cuán probable es el uso de software sin licencia que pueda tener malware implantado en la universidad?		5	5	0
¿Cómo afectaría a la universidad el uso de software sin licencia que contenga malware?		4	3	2

La Universidad Mexiquense del Bicentenario reconoce la posibilidad moderada del uso ocasional de software sin licencia que pueda contener malware, con una ocurrencia evaluada entre "Casi nunca" y "Algunas veces". En caso de tal uso, se anticipa un impacto de nivel medio en la universidad, calificado como "Medio". Es crucial implementar políticas estrictas de licenciamiento de software y fomentar prácticas seguras para minimizar el riesgo asociado con el uso de software no autorizado.

Tabla 30. Análisis preguntas 14.1 y 14.2. [Fuente: Prado (2009)].

		Amenaza: Pérdida de datos críticos de investigación debido a fallas de almacenamiento		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Considera que hay riesgo de pérdida de datos críticos de investigación debido a fallas de almacenamiento?		2	8	0
¿Cómo impactaría a la universidad la pérdida de datos críticos de investigación?		1	5	4

La Universidad Mexiquense del Bicentenario reconoce un riesgo moderado de pérdida de datos críticos de investigación debido a fallas de almacenamiento, con una ocurrencia evaluada principalmente como "Algunas veces". En caso de tal pérdida, se anticipa un impacto de nivel medio en la universidad, calificado como "Medio". Implementar medidas de respaldo regular y sistemas de almacenamiento robustos es esencial para mitigar el riesgo y preservar la integridad de los datos críticos de investigación.

Tabla 31. Análisis preguntas 15.1 y 15.2. [Fuente: Prado (2009)].

		Amenaza: Pérdida de la integridad de la información de la base de datos		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Cuán probable es la pérdida de integridad de la información en la base de datos de la universidad?		9	1	0
¿Cómo afectaría a las operaciones y toma de decisiones la pérdida de integridad en la base de datos?		0	3	7

La Universidad Mexiquense del Bicentenario percibe como altamente improbable la pérdida de integridad de la información en su base de datos, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, la pérdida tendría un impacto significativo en las operaciones y la toma de decisiones, evaluado como "Alto". Mantener medidas de seguridad de base de datos y realizar copias de respaldo periódicas son esenciales para garantizar la integridad y disponibilidad de la información crítica.

Tabla 32. Análisis preguntas 16.1 y 16.2. [Fuente: Prado (2009)].

		Amenaza: Fallos en el servicio de internet		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia considera que la universidad podría experimentar fallos en el servicio de internet?		0	6	4
En caso de fallos en el servicio de internet, ¿Cómo afectaría esto a las actividades académicas y administrativas?		0	6	4

La Universidad Mexiquense del Bicentenario reconoce la posibilidad de experimentar fallos en el servicio de internet, clasificándola mayormente como "Algunas veces". En caso de tales fallos, se espera un impacto moderado en las actividades académicas y administrativas, calificado como "Medio". Implementar medidas de contingencia y monitoreo continuo es esencial para mitigar los efectos adversos y garantizar la continuidad de las operaciones universitarias.

Tabla 33. Análisis preguntas 17.1 y 17.2. [Fuente: Prado (2009)].

Amenaza: Fallos de software de contabilidad			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Cuán probable es experimentar fallos en el software de contabilidad de la universidad?	10	0	0
¿Cómo impactaría a la universidad un fallo en el software de contabilidad en términos financieros y administrativos?	1	8	1

La Universidad Mexiquense del Bicentenario percibe como extremadamente improbable experimentar fallos en el software de contabilidad, clasificándolo mayormente como "Casi nunca". Sin embargo, se reconoce que, en caso de un fallo, el impacto financiero y administrativo sería significativo, evaluado como "Medio". Aunque la ocurrencia es baja, mantener medidas preventivas y planes de contingencia es esencial para garantizar la integridad y eficiencia de los procesos contables y administrativos.

Tabla 34. Análisis preguntas 18.1 y 18.2. [Fuente: Prado (2009)].

Amenaza: Pérdida de acceso a documentos en línea durante auditorías			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Qué tan probable es la pérdida de acceso a documentos en línea durante procesos de auditoría?	10	0	0
¿Cómo afectaría a la universidad la pérdida de acceso a documentos durante una auditoría?	1	7	2

La Universidad Mexiquense del Bicentenario percibe como altamente improbable la pérdida de acceso a documentos en línea durante procesos de auditoría, clasificándola mayormente como "Casi nunca". Aunque la probabilidad es baja, se reconoce que, en caso de ocurrir, la pérdida tendría un impacto significativo en la universidad, evaluado como "Medio". Mantener respaldos seguros y sistemas de acceso confiables es esencial para garantizar la transparencia y eficiencia durante auditorías.

Tabla 35. Análisis preguntas 19.1 y 19.2. [Fuente: Prado (2009)].

		Amenaza: Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Considera que hay riesgo de brechas de seguridad que comprometan la confidencialidad de las respuestas de las encuestas?		4	6	0
¿Cómo impactaría en la reputación de la universidad y la confianza de los encuestados una brecha de seguridad en encuestas?		2	3	5

La Universidad Mexiquense del Bicentenario reconoce la posibilidad de brechas de seguridad que comprometan la confidencialidad de las respuestas de las encuestas, evaluada principalmente como "Algunas veces". Si bien la ocurrencia es moderada, se reconoce que una brecha de seguridad tendría un impacto significativo en la reputación de la universidad y la confianza de los encuestados, calificado como "Medio-Alto". Implementar medidas de seguridad robustas y prácticas de manejo de datos confidenciales es crucial para preservar la integridad de las encuestas y la confianza de la comunidad académica.

Tabla 36. Análisis preguntas 20.1 y 20.2. [Fuente: Prado (2009)].

		Amenaza: Mala gestión de los sistemas de seguimiento y apoyo		
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO	
	Casi nunca	Algunas veces	Siempre sucede	
¿Cuán probable es que se produzca una mala gestión de los sistemas de seguimiento y apoyo?	7	3	0	
¿Cómo afectaría a las operaciones y servicios de apoyo una mala gestión de sistemas?	0	5	6	

La Universidad Mexiquense del Bicentenario percibe como moderadamente probable la ocurrencia de una mala gestión de los sistemas de seguimiento y apoyo, clasificándola mayormente como "Casi nunca" y "Algunas veces". Se reconoce que una mala gestión tendría un impacto significativo en las operaciones y servicios de apoyo, evaluado como "Medio-Alto". Implementar prácticas efectivas de gestión y supervisión continua es esencial para asegurar la eficiencia y la calidad en el soporte ofrecido por los sistemas institucionales.

VULNERABILIDADES

Tabla 37. Análisis preguntas 21.1 y 21.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Antivirus poco eficiente.		
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO	
	Casi nunca	Algunas veces	Siempre sucede	
¿Con que frecuencia se ven afectados los equipos de cómputo con virus?	7	3	0	
¿De qué grado sería el impacto operacional si una maquina se infecta con algún tipo de virus?	1	3	6	

La Universidad Mexiquense del Bicentenario reconoce una ocurrencia moderada de afectación por virus en los equipos de cómputo, clasificada mayormente como "Casi nunca". A pesar de la baja frecuencia, se reconoce que el impacto operacional de una infección sería significativo, evaluado como "Medio-Alto". Mejorar la eficiencia del software antivirus y promover prácticas de seguridad cibernética son esenciales para reducir el riesgo y mitigar los efectos de posibles infecciones en los equipos.

Tabla 38. Análisis preguntas 22.1 y 22.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Falta de conciencia sobre seguridad informática.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan frecuente es que los empleados incurran en prácticas inseguras debido a una falta de conciencia sobre seguridad informática?		2	6	2
¿Cuál sería el impacto en la seguridad de la información de la escuela si continúa la falta de conciencia sobre seguridad informática?		0	2	7

La Universidad Mexiquense del Bicentenario reconoce una ocurrencia moderada de prácticas inseguras por falta de conciencia sobre seguridad informática entre los empleados, clasificándola principalmente como "Algunas veces". Se destaca que, si persiste esta falta de conciencia, el impacto en la seguridad de la información sería significativo, evaluado como "Alto". Fortalecer programas de concientización y capacitación en seguridad informática es esencial para reducir riesgos y promover un entorno cibernético más seguro en la institución.

Tabla 39. Análisis preguntas 23.1 y 23.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia son objeto de ataques de phishing los empleados administrativos en la escuela?		10	0	0
¿Cuál sería el impacto operacional si se lograra un acceso no autorizado a las cuentas de comunicación de los empleados administrativos?		0	1	9

La Universidad Mexiquense del Bicentenario muestra una percepción muy baja de que los empleados administrativos sean objeto de ataques de phishing, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que el impacto operacional de un acceso no autorizado a las cuentas de comunicación sería significativo, evaluado como "Alto". Aunque la ocurrencia es mínima, implementar medidas de seguridad adicionales y programas de concientización continua sobre phishing es crucial para mantener la integridad de las cuentas y prevenir posibles amenazas cibernéticas.

Tabla 40. Análisis preguntas 24.1 y 24.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Sistemas saturados de información obsoleta.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
	¿Qué tan a menudo se enfrentan los sistemas de la escuela a problemas debido a la saturación de información obsoleta?	1	7	2
	¿Qué grado de impacto tendría en la eficiencia operativa de la escuela la saturación de los sistemas con información obsoleta?	1	5	4

La Universidad Mexiquense del Bicentenario reconoce que enfrenta problemas ocasionalmente debido a la saturación de información obsoleta, clasificándola principalmente como "Algunas veces". Se destaca que, si persiste esta saturación, el impacto en la eficiencia operativa sería moderado, evaluado como "Medio". Implementar políticas de gestión de información y realizar actualizaciones periódicas de sistemas son esenciales para minimizar los problemas asociados con la obsolescencia de datos y mantener la eficiencia operativa de la institución.

Tabla 41. Análisis preguntas 25.1 y 25.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Falta de un medio de control del tráfico de red.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
	¿Qué tan a menudo surgen problemas de seguridad o de rendimiento en la red debido a la falta de un medio de control del tráfico?	5	5	0
	¿Qué tanto afectaría a la integridad y funcionamiento de la red escolar la falta de control sobre el tráfico de esta?	8	2	0

La Universidad Mexiquense del Bicentenario reconoce que ocasionalmente surgen problemas de seguridad o rendimiento en la red debido a la falta de un medio de control del tráfico, clasificándola como "Algunas veces". Se destaca que, en caso de persistir esta falta de control, el impacto en la integridad y funcionamiento de la red escolar sería significativamente bajo, evaluado como "Bajo". Implementar un medio de control del tráfico es esencial para mitigar problemas potenciales y mantener la integridad y eficiencia de la red institucional.

Tabla 42. Análisis preguntas 26.1 y 26.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Infraestructura física de la red deficiente.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se presentan fallos o interrupciones en la red debido a una infraestructura física deficiente?		0	8	2
¿Qué impacto tendría en las operaciones diarias de la escuela una infraestructura física de red deficiente?		1	3	5

La Universidad Mexiquense del Bicentenario reconoce que ocasionalmente se presentan fallos o interrupciones en la red debido a una infraestructura física deficiente, clasificándola principalmente como "Algunas veces". Se destaca que, en caso de persistir esta deficiencia, el impacto en las operaciones diarias de la escuela sería moderado, evaluado como "Medio". Mejorar la infraestructura física de red es esencial para mitigar problemas potenciales y garantizar la continuidad operativa de la institución.

Tabla 43. Análisis preguntas 27.1 y 27.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Corto circuito en las tomas de corriente de los laboratorios.		
NIVEL		BAJO	MEDIO	ALTO
OCURRENCIA / IMPACTO		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia ocurren cortocircuitos en las tomas de corriente de los laboratorios?		10	0	0
¿Qué impacto tendría un cortocircuito en las operaciones y la seguridad de los laboratorios?		0	5	5

La Universidad Mexiquense del Bicentenario percibe como extremadamente rara la ocurrencia de cortocircuitos en las tomas de corriente de los laboratorios, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, un cortocircuito tendría un impacto moderado en las operaciones y la seguridad de los laboratorios, evaluado como "Medio-Alto". Mantener sistemas eléctricos seguros y realizar revisiones periódicas son esenciales para prevenir cortocircuitos y preservar la integridad de los laboratorios.

Tabla 44. Análisis preguntas 28.1 y 28.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Ausencia de extintores.		
NIVEL	OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Cuál es la probabilidad de que un incendio no pueda ser controlado a tiempo debido a la ausencia de extintores?		10	0	0
¿Qué consecuencias tendría la ausencia de extintores en caso de un incendio en las instalaciones?		0	0	10

La Universidad Mexiquense del Bicentenario percibe como extremadamente improbable que un incendio no pueda ser controlado a tiempo debido a la ausencia de extintores, clasificándola mayormente como "Casi nunca". Sin embargo, se reconoce que, en caso de esta ausencia, las consecuencias de un incendio en las instalaciones serían extremadamente altas, evaluadas como "Alto". La instalación y mantenimiento de extintores es crucial para prevenir y controlar incendios, salvaguardando la seguridad de las personas y protegiendo las instalaciones.

Tabla 45. Análisis preguntas 29.1 y 29.2. [Fuente: Prado (2009)].

		Vulnerabilidad: El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan frecuente es que se presenten problemas o pérdidas de datos en el registro de reservaciones que se encuentra en un solo equipo?		10	0	0
¿Cuál sería el impacto en la gestión de reservaciones si se perdiera o dañara el archivo Excel en el equipo de cómputo?		1	4	5

La Universidad Mexiquense del Bicentenario reconoce que es extremadamente rara la ocurrencia de problemas o pérdidas de datos en el registro de reservaciones que se encuentra en un solo equipo, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, el impacto en la gestión de reservaciones sería significativo, evaluado como "Medio-Alto". Implementar un sistema de registro más robusto y realizar copias de respaldo periódicas son medidas esenciales para prevenir posibles pérdidas de datos y garantizar la continuidad en la gestión de reservaciones.

Tabla 46. Análisis preguntas 30.1 y 30.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se presentan riesgos de seguridad debido al fácil acceso al equipo de cómputo en una oficina vacía?		8	2	0
¿Con qué frecuencia se presentan riesgos de seguridad debido al fácil acceso al equipo de cómputo en una oficina vacía?		0	2	8

La Universidad Mexiquense del Bicentenario reconoce que, aunque no es una ocurrencia constante, hay riesgos de seguridad significativos debido al fácil acceso al equipo de cómputo cuando la oficina está vacía, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que, en caso de acceso no autorizado, los riesgos de seguridad serían considerablemente altos, evaluados como "Alto". Implementar medidas de seguridad física, como cerraduras y sistemas de acceso, es esencial para mitigar estos riesgos y garantizar la protección de los equipos de cómputo.

Tabla 47. Análisis preguntas 31.1 y 31.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Vigilancia escasa en la oficina del departamento.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan a menudo ocurren incidentes de seguridad o robos en la oficina del departamento debido a la vigilancia escasa?		3	5	2
¿Cuál sería el impacto de una vigilancia escasa en términos de seguridad y protección de activos en la oficina del departamento?		0	2	8

La Universidad Mexiquense del Bicentenario reconoce que ocasionalmente ocurren incidentes de seguridad o robos en la oficina del departamento debido a la vigilancia escasa, clasificándola mayormente como "Algunas veces". Se destaca que, en caso de persistir esta escasa vigilancia, el impacto en términos de seguridad y protección de activos sería significativamente alto, evaluado como "Alto". Fortalecer las medidas de seguridad y aumentar la vigilancia en la oficina del departamento es esencial para prevenir incidentes y salvaguardar los activos institucionales.

Tabla 48. Análisis preguntas 32.1 y 32.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Descarga de programas de idiomas de sitios no oficiales.		
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO	
	Casi nunca	Algunas veces	Siempre sucede	
¿Con qué frecuencia se descargan programas de idiomas de fuentes no oficiales, y qué riesgos implica?	9	1	0	
¿Qué impacto tendría en la seguridad informática la descarga de programas de idiomas de sitios no oficiales?	1	4	5	

La Universidad Mexiquense del Bicentenario reconoce que la descarga de programas de idiomas de fuentes no oficiales es extremadamente rara, clasificándola mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, el impacto en la seguridad informática sería significativo, evaluado como "Medio-Alto". Fomentar prácticas seguras de descarga de software y concientizar a los usuarios sobre los riesgos asociados son medidas esenciales para prevenir posibles amenazas a la seguridad informática.

Tabla 49. Análisis preguntas 33.1 y 33.2. [Fuente: Prado (2009)].

Vulnerabilidad: Ausencia de software antimalware.			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Qué tan probable es que los equipos se vean afectados por malware debido a la falta de software antimalware?	1	6	3
¿Cuál sería el impacto en la seguridad de la información y en el rendimiento de los sistemas debido a la ausencia de software antimalware?	2	5	3

La Universidad Mexiquense del Bicentenario reconoce que la ausencia de software antimalware es una ocurrencia ocasional, clasificándola mayormente como "Algunas veces". Se destaca que, si persiste esta ausencia, el impacto en la seguridad de la información y en el rendimiento de los sistemas sería moderado, evaluado como "Medio". Implementar y mantener soluciones antimalware es esencial para prevenir afectaciones por malware y salvaguardar la integridad de la información y el funcionamiento de los sistemas.

Tabla 50. Análisis preguntas 34.1 y 34.2. [Fuente: Prado (2009)].

Vulnerabilidad: Monitoreo inexistente de correos electrónicos no deseados.			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se enfrentan a problemas relacionados con correos electrónicos no deseados debido a la falta de monitoreo?	8	2	0
¿Qué impacto tendría en la productividad y seguridad informática el no tener un sistema de monitoreo de correos electrónicos no deseados?	4	5	1

La Universidad Mexiquense del Bicentenario reconoce que enfrenta problemas relacionados con correos electrónicos no deseados ocasionalmente, clasificándola mayormente como "Casi nunca". Se destaca que, en caso de no tener un sistema de monitoreo, el impacto en la productividad y seguridad informática sería moderado, evaluado como "Medio". Implementar un sistema eficiente de monitoreo de correos electrónicos no deseados es esencial para reducir la incidencia de amenazas y mantener la productividad y seguridad en las comunicaciones electrónicas.

Tabla 51. Análisis preguntas 35.1 y 35.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Uso de software para "crackeo" de programas con licencia.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se utiliza software de "crackeo" en la organización?		10	0	0
¿Qué impacto tendría el uso de software de "crackeo" en la seguridad y legalidad de las operaciones de la organización?		2	6	2

La Universidad Mexiquense del Bicentenario reconoce que el uso de software de "crackeo" es extremadamente raro, clasificándolo mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, el impacto en la seguridad y legalidad de las operaciones sería moderado, evaluado como "Medio". Promover el uso legal y ético del software, así como implementar políticas claras, son medidas esenciales para prevenir la utilización indebida de software no licenciado y salvaguardar la integridad de las operaciones de la organización.

Tabla 52. Análisis preguntas 36.1 y 36.2. [Fuente: Prado (2009)].

Vulnerabilidad: Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Qué tan a menudo se presentan fallos o pérdidas de datos debido al uso de unidades de almacenamiento desgastadas?	9	1	0
¿Cuál sería el impacto en la continuidad de las operaciones si fallan las unidades de almacenamiento desgastadas?	1	7	2

La Universidad Mexiquense del Bicentenario reconoce que es extremadamente raro que se presenten fallos o pérdidas de datos debido al uso de unidades de almacenamiento desgastadas, clasificándolo mayormente como "Casi nunca". No obstante, se reconoce que, en caso de ocurrir, el impacto en la continuidad de las operaciones sería significativamente alto, evaluado como "Medio-Alto". Mantener un monitoreo constante del estado de las unidades de almacenamiento y realizar reemplazos preventivos son prácticas esenciales para evitar posibles interrupciones y garantizar la integridad de los datos.

Tabla 53. Análisis preguntas 37.1 y 37.2. [Fuente: Prado (2009)].

Vulnerabilidad: Ausencia de respaldos en la nube u otra unidad de almacenamiento			
NIVEL OCURRENCIA / IMPACTO	BAJO	MEDIO	ALTO
	Casi nunca	Algunas veces	Siempre sucede
¿Cuál es la probabilidad de pérdida de datos críticos debido a la ausencia de respaldos adecuados?	7	3	0
¿Qué impacto tendría en la organización la pérdida de datos importantes debido a la falta de respaldos?	3	1	6

La Universidad Mexiquense del Bicentenario reconoce que la ausencia de respaldos en la nube u otra unidad de almacenamiento es una ocurrencia ocasional, clasificándola mayormente como "Casi nunca". Se destaca que, en caso de persistir esta ausencia, el impacto en la organización debido a la pérdida de datos importantes sería significativamente alto, evaluado como "Alto". Implementar políticas de respaldo sólidas y almacenar copias de seguridad de manera segura son prácticas esenciales para mitigar el riesgo de pérdida de datos críticos y garantizar la continuidad operativa.

Tabla 54. Análisis preguntas 38.1 y 38.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Uso de software no especializado para bases de datos		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se enfrentan a limitaciones o problemas debido al uso de software no especializado para bases de datos?		10	0	0
¿Con qué frecuencia se enfrentan a limitaciones o problemas debido al uso de software no especializado para bases de datos?		10	0	0

La Universidad Mexiquense del Bicentenario reconoce que es extremadamente raro enfrentar limitaciones o problemas debido al uso de software no especializado para bases de datos, clasificándolo mayormente como "Casi nunca". Se destaca que, en caso de utilizar software especializado, el impacto en la eficiencia y funcionalidad de las bases de datos sería mínimo, evaluado como "Bajo". Utilizar software adecuado para la gestión de bases de datos es esencial para optimizar el rendimiento y garantizar un manejo eficiente de la información.

Tabla 55. Análisis preguntas 39.1 y 39.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan común es el uso de software sin soporte?		8	2	0
¿Cuál sería el impacto en la seguridad y eficiencia operativa al utilizar software sin soporte ni actualizaciones?		6	2	1

La Universidad Mexiquense del Bicentenario reconoce que el uso de software sin soporte es común en ciertas ocasiones, clasificándolo mayormente como "Casi nunca". Se destaca que, en caso de persistir este uso, el impacto en la seguridad y eficiencia operativa sería moderado, evaluado como "Medio-Bajo". Priorizar la actualización y sustitución de software obsoleto es esencial para mantener la seguridad de los sistemas y garantizar la eficiencia de las operaciones.

Tabla 56. Análisis preguntas 40.1 y 40.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Control deficiente del servicio en la nube donde se encuentran los documentos.		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan frecuente es que se presenten problemas de seguridad o acceso debido a un control deficiente del servicio en la nube?		10	0	0
¿Qué impacto tendría un control deficiente del servicio en la nube en la confidencialidad y disponibilidad de los documentos?		1	6	3

La Universidad Mexiquense del Bicentenario reconoce que es extremadamente raro enfrentar problemas de seguridad o acceso debido a un control deficiente del servicio en la nube, clasificándolo mayormente como "Casi nunca". No obstante, se destaca que, en caso de persistir este control deficiente, el impacto en la confidencialidad y disponibilidad de los documentos sería moderado, evaluado como "Medio". Reforzar las medidas de seguridad en el servicio en la nube es esencial para prevenir posibles amenazas y asegurar la integridad de la información almacenada.

Tabla 57. Análisis preguntas 41.1 y 41.2. [Fuente: Prado (2009)].

		Vulnerabilidad: Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Con qué frecuencia se compromete la seguridad de las encuestas en línea debido a contraseñas inseguras?		10	1	0
¿Cuál sería el impacto si se accediera indebidamente a las cuentas de las encuestas en línea debido a contraseñas inseguras?		0	4	6

La Universidad Mexiquense del Bicentenario reconoce que es extremadamente raro comprometer la seguridad de las encuestas en línea debido a contraseñas inseguras, clasificándolo mayormente como "Casi nunca". Se destaca que, en caso de persistir el uso de contraseñas inseguras, el impacto potencial al acceder indebidamente a las cuentas de las encuestas sería significativamente alto, evaluado como "Alto-Medio". Reforzar las prácticas de seguridad, como el uso de contraseñas robustas, es esencial para proteger la confidencialidad de los resultados de las encuestas y mantener la integridad de la información recopilada.

Tabla 58. Análisis preguntas 42.1 y 42.2. [Fuente: Prado (2009)].

		Vulnerabilidad: El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado		
OCURRENCIA / IMPACTO	NIVEL	BAJO	MEDIO	ALTO
		Casi nunca	Algunas veces	Siempre sucede
¿Qué tan a menudo se presentan errores o ineficiencias en los procesos debido a la falta de capacitación en el software especializado?		5	5	0
¿Qué tan a menudo se presentan errores o ineficiencias en los procesos debido a la falta de capacitación en el software especializado?		1	7	2

La Universidad Mexiquense del Bicentenario reconoce que ocasionalmente se presentan errores o ineficiencias en los procesos debido a la falta de capacitación en el software especializado, clasificándolo como "Algunas veces". Se destaca que, en caso de persistir esta falta de capacitación, el impacto en la eficiencia de los procesos sería moderado, evaluado como "Medio". Priorizar la formación continua del personal en el uso del software especializado es esencial para maximizar su eficacia y minimizar posibles errores operativos.

ACTIVIDAD 2.6

Priorizar riesgos.

DESCRIPCIÓN DE LA ACTIVIDAD

Para esta actividad de acuerdo a los valores asignados al impacto y probabilidad, se busca asignarles a las amenazas así como a las vulnerabilidades un nivel de prioridad, tomando como referencia el trabajo de maestría “Metodología para el establecimiento de objetivos de control como un medio de seguimiento en el área de Tecnologías de la Información” de la Mtra. Diana Marisol Prado Oseguera, el resultado de esta actividad son dos tablas, una para las amenazas y otra para las vulnerabilidades donde se vea: el departamento, proceso crítico, amenaza/vulnerabilidad, el impacto, la probabilidad; siendo estas dos últimas obtenidas tomando los dos números más altos de cada una de las tablas de la actividad 2.5 y la prioridad valorada de acuerdo la siguiente tabla:

VALORES DEL RIESGO ACORDE A LA PROBABILIDAD / IMPACTO				
1 Intrascendente	2 Baja	3 Media	4 Moderado	5 Alta

Figura 6. Valores del riesgo acorde a la probabilidad/impacto. [Fuente: Prado (2009)].

Así mismo para la valoración de la prioridad de acuerdo con el impacto y la probabilidad, se toma como referencia la tabla sugerida por la metodología ya mencionada, que se puede ver a continuación:

Tabla 59. Cuadro de la prioridad del riesgo acorde al impacto y probabilidad de este. [Fuente: Prado (2009)].

Impacto	Probabilidad	Valor	Prioridad
Bajo	Bajo	1	Intrascendente
Medio	Bajo	3	Media
Alto	Bajo	4	Moderada
Bajo	Medio	2	Baja
Medio	Medio	3	Media
Alto	Medio	5	Alta
Bajo	Alto	4	Moderada
Medio	Alto	5	Alta
Alto	Alto	5	Alta

Con el resultado de esta actividad se podrá obtener una visión más clara sobre cuáles deberían ser las prioridades para mitigar para la institución de tal forma que en las actividades que corresponden al objetivo 3, la institución pueda decidir con criterio cuales estrategias debería implementar lo más pronto posible.

RESULTADO DE LA ACTIVIDAD

Tabla 60. Priorización de las Amenazas de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia].

Proceso critico	Amenaza	Impacto	Probabilidad	Prioridad
Coordinación de prácticas de laboratorio y reservaciones en línea	Interrupciones de las reservaciones en línea	Alto	Medio	Alta
Generación de certificados y documentos oficiales digitales	Perdida del equipo de cómputo donde se generan dichos documentos	Alto	Medio	Alta
Gestión de encuestas y estudios de clima organizacional	Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas	Alto	Medio	Alta
Monitoreo y análisis de datos institucionales	Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos	Alto	Bajo	Moderada
Gestión de comunicaciones internas y externas	Suplantación de identidad (spoofing)	Alto	Bajo	Moderada
Uso de plataforma institucional para gestión de cursos y calificaciones	Interrupción del servicio por un ataque DDoS	Alto	Bajo	Moderada

Tabla.60. Priorización de las Amenazas de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia].
(Continuación).

Proceso critico	Amenaza	Impacto	Probabilidad	Prioridad
Administración y monitoreo de equipamiento y software de laboratorios	Incendio eléctrico donde se pierden los equipos de computo	Alto	Bajo	Moderada
Procesamiento de solicitudes de titulación	Acceso no autorizado que provoque la manipulación de registros académicos	Alto	Bajo	Moderada
Gestión de programas de idiomas y recursos digitales	Infección por malware en el equipo de cómputo	Alto	Bajo	Moderada
Coordinación de exámenes y certificaciones en línea	Compromiso de la integridad de los exámenes por un ataque de ingeniería social (Phishing y acceso remoto)	Alto	Bajo	Moderada
Manejo de bases de datos de seguridad y procedimientos químicos	Perdida de la integridad de la información de la base de datos	Alto	Bajo	Moderada
Implementación de sistemas de seguimiento y apoyo	Mala gestión de los sistemas de seguimiento y apoyo	Alto	Bajo	Moderada
Administración de registros académicos en sistemas de información	Fallos del sistema como problemas de autenticación o registros no generados	Medio	Bajo	Media
Gestión de convenios y programas de educación dual	Interrupción del servicio de internet	Medio	Medio	Media

Tabla.60. Priorización de las Amenazas de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia].
(Continuación).

Proceso critico	Amenaza	Impacto	Probabilidad	Prioridad
Monitoreo del desempeño estudiantil	Perdida de comunicación con los estudiante y empresas que se encuentren en el programa.	Medio	Bajo	Media
Coordinación de proyectos de investigación y desarrollo	Pérdida de datos críticos de investigación debido a fallas de almacenamiento	Medio	Medio	Media
Coordinación de experimentos y proyectos en laboratorios virtuales	Fallos en el servicio de internet	Medio	Medio	Media
Uso de sistemas contables y de gestión financiera	Fallos de software de contabilidad	Medio	Bajo	Media
Coordinación de auditorías internas y externas	Pérdida de acceso a documentos en línea durante auditorías	Medio	Bajo	Media
Administración de software especializado	Uso de software sin licencia que pueda tener malware implantado	Bajo	Medio	Baja

Una vez determinada la prioridad con respecto a las amenazas identificadas para los procesos críticos de la Universidad, se puede observar en la tabla 60 que existen tres amenazas de prioridad alta, nueve de prioridad moderada, siete de prioridad media y una de prioridad baja; lo que da a entender con respecto a las amenazas que afronta la institución, es que si bien son pocas cuya prioridad es alta, si existen un gran número de aquellas que requiere de una solución lo más pronto posible.

Tabla 61. Priorización de las Vulnerabilidades de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia].

Proceso critico	Vulnerabilidades	Impacto	Probabilidad	Prioridad
Monitoreo y análisis de datos institucionales.	Falta de conciencia sobre seguridad informática.	Alto	Medio	Alta
Gestión de convenios y programas de educación dual.	Infraestructura física de la red deficiente.	Alto	Medio	Alta
Generación de certificados y documentos oficiales digitales.	Vigilancia escasa en la oficina del departamento.	Alto	Medio	Alta
Coordinación de proyectos de investigación y desarrollo.	Ausencia de respaldos en la nube u otra unidad de almacenamiento.	Alto	Medio	Alta
Gestión de encuestas y estudios de clima organizacional.	Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados.	Alto	Bajo	Moderada
Gestión de comunicaciones internas y externas.	Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican.	Alto	Bajo	Moderada
Procesamiento de solicitudes de titulación.	Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.	Alto	Bajo	Moderada
Administración y monitoreo de equipamiento y software de laboratorios.	Ausencia de extintores en laboratorio.	Alto	Bajo	Moderada

Tabla 61. Priorización de las Vulnerabilidades de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Vulnerabilidades	Impacto	Probabilidad	Prioridad
Coordinación de prácticas de laboratorio y reservaciones en línea.	El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.	Alto	Bajo	Moderada
Monitoreo y análisis de datos institucionales.	Antivirus poco eficiente.	Alto	Bajo	Moderada
Administración de registros académicos en sistemas de información.	Sistemas saturados de información obsoleta.	Medio	Medio	Media
Gestión de programas de idiomas y recursos digitales.	Descarga de programas de idiomas de sitios no oficiales.	Medio	Bajo	Media
Coordinación de exámenes y certificaciones en línea.	Ausencia de software antimalware.	Medio	Medio	Media
Coordinación de exámenes y certificaciones en línea.	Monitoreo inexistente de correos electrónicos no deseados.	Medio	Bajo	Media
Administración de software especializado.	Uso de software para “crackeo” de programas con licencia.	Medio	Bajo	Media
Coordinación de proyectos de investigación y desarrollo.	Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste.	Medio	Bajo	Media

Tabla 61. Priorización de las Vulnerabilidades de acuerdo con el impacto y la probabilidad. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Vulnerabilidades	Impacto	Probabilidad	Prioridad
Implementación de sistemas de seguimiento y apoyo.	El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado.	Medio	Medio	Media
Coordinación de auditorías internas y externas.	Control deficiente del servicio en la nube donde se encuentran los documentos.	Medio	Bajo	Media
Administración y monitoreo de equipamiento y software de laboratorios.	Corto circuito en las tomas de corriente de los laboratorios.	Medio	Bajo	Media
Uso de plataforma institucional para gestión de cursos y calificaciones.	Falta de un medio de control del tráfico de red.	Bajo	Medio	Bajo
Uso de sistemas contables y de gestión financiera	Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores.	Bajo	Bajo	Intrascendente
Manejo de bases de datos de seguridad y procedimientos químicos.	Uso de software no especializado para bases de datos.	Bajo	Bajo	Intrascendente

Por su parte en la tabla 61 que corresponde a la priorización de las vulnerabilidades identificadas, se puede notar que existen cuatro de prioridad alta, seis de prioridad moderada, nueve de prioridad media, una de prioridad baja y dos de prioridad intrascendente. Lo que a entender que si bien hay una gran cantidad de vulnerabilidades que pueden no ser atendidas a corto o incluso largo plazo; la existencia de cuatro vulnerabilidades de prioridad alta puede poner en peligro la TI de la Universidad.

ACTIVIDAD 2.7

Evaluar los sistemas de control con los que cuenta la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Una vez determinada la prioridad de las amenazas y vulnerabilidades existentes en la institución se procede a identificar y evaluar los sistemas de control con los que cuenta, para posteriormente, en actividades subsecuentes, generar estrategias para corregirlos en caso de que no se estén desempeñando correctamente. El resultado son dos fichas por cada sistema de control, la primera considera el proceso crítico, descripción del riesgo, la actividad de control, descripción de la actividad de control, periodicidad de la actividad de control y clasificación de la actividad de control (manual o automática). Posteriormente la segunda contempla la descripción del plan de prueba, método y cantidad de selección de partidas (al azar, fortuito o sistemático), resultados de la prueba, conclusión sobre efectividad y la referencia de la evidencia. El formato utilizado para la creación de dichas fichas se realiza con base a las sugerencias del trabajo de maestría “Metodología para el establecimiento de objetivos de control como un medio de seguimiento en el área de Tecnologías de la Información” de la Mtra. Diana Marisol Prado Oseguera. Así mismo cabe resaltar que no se incluyen todos los procesos críticos identificados debido a que algunos dependen de servicios de terceros y cuyos sistemas de control son ajenos a la institución.

Por otra parte, para la columna sobre la efectividad del sistema de control, se decidió generar una métrica única para esta actividad, dicha métrica se basa en las métricas publicadas por Cobit y es la siguiente:

Efectividad Alta: El sistema de control funciona correctamente.

Efectividad Media: El sistema de control no cumple por completo su propósito, fallando en contadas ocasiones o no funciona como corresponde.

Efectividad Baja: El sistema de control no cumple con su propósito la gran mayoría de las veces.

Efectividad Inexistente: El sistema de control no cumple en lo absoluto con su propósito, poniendo en riesgo los activos de TI que debiera resguardar.

RESULTADO DE LA ACTIVIDAD

Tabla 62. Evaluación de los sistemas de control. Control Número 1. Parte 1. [Fuente: Prado (2009)].

Proceso critico	Descripción del riesgo	Actividad de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control Manual/Automático
Monitoreo y análisis de datos institucionales.	Perdida temporal de los equipos de cómputo afectados y pérdida total de los datos institucionales.	Análisis periódicos del antivirus instalado en el equipo de cómputo donde se realiza el proceso crítico.	En el equipo de cómputo donde se lleva el proceso crítico, el cual es el de la directora de la institución, se tiene instalado una versión desactualizada y sin licencia del sistema antivirus McAfee, el cual por su configuración por defecto realiza análisis de los archivos del equipo de cómputo cada que este es encendido.	Diario	Automático

Una vez recabada la información necesaria correspondiente al sistema de control identificado, se realiza la evaluación de este, donde en este caso se hizo uso del software WinAudit para que por medio de este obtener la información acerca del antivirus, que es la actividad de control en sí, y así determinar la efectividad de este.

Tabla 63. Evaluación de los sistemas de control. Control Número 1. Parte 2. [Fuente: Prado (2009)].

Descripción del plan de prueba	Método y Cantidad de selección de partidas (Al azar, fortuito o sistemático)	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Utilizando el software WinAudit se realiza un análisis de la computadora de la directora de la institución, tras este análisis se espera observar la información correspondiente al sistema antivirus instalado en el equipo.	Método sistemático, tamaño de la muestra 1.	Una vez el software WinAudit concluye con el análisis completo del equipo de cómputo se puede observar toda la información recabada sobre el sistema antivirus instalado, donde se confirma que no dispone con la licencia de activación para el correcto funcionamiento del producto, además de que lleva meses sin ser actualizado por la propietaria.	Efectividad Media	Por motivos de las políticas de privacidad de la Universidad no se pudieron obtener evidencias de la prueba. Revisar el Anexo B. Carta de justificación de la ausencia de evidencia de los sistemas de control. Para ver la carta de justificación expedida por la institución.

Una vez realizada la evaluación de la actividad de control, la información obtenida sobre el antivirus instalado en el equipo de cómputo de la directoria de la institución dejó en claro que si bien el control funciona no es completamente efectivo.

Tabla 64. Evaluación de los sistemas de control. Control Número 2. Parte 1. [Fuente: Prado (2009)].

Proceso critico	Descripción del riesgo	Actividad de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control Manual/Automático
Gestión de comunicaciones internas y externas.	Completa descoordinación dentro de la estructura organizacional de la institución y con rectoría por la difusión de instrucciones u ordenes falsas	Uso de contraseñas para las cuentas académicas por donde se comunican.	Las cuentas académicas utilizadas por los administrativos se encuentran protegidas por contraseñas de complejidad media, utilizando una combinación de números y letras.	No hay un cambio de contraseñas de forma regular	Manual

Una vez identificada la actividad de control y las características que la componen; como el proceso critico que resguarda o si clasificación, se procede a realizar la evaluación de esta en la tabla 65 donde utilizando una herramienta especializada se decide qué tan efectivo es el control.

Tabla 65. Evaluación de los sistemas de control. Control Número 2. Parte 2. [Fuente: Prado (2009)].

Descripción del plan de prueba	Método y Cantidad de selección de partidas (Al azar, fortuito o sistemático)	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Utilizando la herramienta Kaspersky password checker de Kaspersky lab se ponen a prueba la seguridad de las contraseñas utilizadas por el personal administrativo para sus cuentas administrativas, contra ataques de fuerza bruta o si se encuentran en una base de datos de contraseñas filtradas.	Método Al azar, tamaño de la muestra 15.	Tras haber aplicado la prueba con 15 distintas contraseñas proporcionadas por 15 de los administrativos presentes, los resultados arrojados por la herramienta indicaron en la gran mayoría de las ocasiones la contraseña era débil y dos fueron encontradas en más de una base de datos de contraseñas filtradas.	Efectividad Inexistente	Por motivos de las políticas de privacidad de la Universidad no se pudieron obtener evidencias de la prueba. Revisar el Anexo B. Carta de justificación de la ausencia de evidencia de los sistemas de control. Para ver la carta de justificación expedida por la institución.

Tras haber realizado la evaluación del control con una herramienta especializada para probar la seguridad de todo tipo de contraseñas, como se podrá observar en la tabla, las contraseñas utilizadas por el personal administrativas no son efectivas o seguras.

Tabla 66. Evaluación de los sistemas de control. Control Número 3. Parte 1. [Fuente: Prado (2009)].

Proceso critico	Descripción del riesgo	Actividad de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control Manual/Automático
Gestión de convenios y programas de educación dual.	Dado a los convenios que no puedan concluirse y los programas de educación dual detenidos, generaría una mala reputación de la escuela frente a distintas empresas.	Uso de un Access Point para extender la red existente por Wifi	Debido a que la cobertura Wifi del edificio principal no tiene el alcance suficiente para que el personal del departamento se conecte, se instaló un Access Point que se conecta por medio de un cable ethernet a uno de los puertos ethernet designados a los equipos de cómputo en el laboratorio ubicado justo atrás de la oficina del departamento, de tal forma que se extiende la red existente sin la necesidad de añadir más cableado. Dicho Access Point solo se enciende cuando el personal del departamento ingresa a la oficina.	Cada vez que el personal ingresa a la oficina	Manual

Una vez identificada la actividad de control y como esta es llevada a cabo por la institución se procede a llevar a cabo la evaluación de esta como se puede observar en la siguiente tabla.

Tabla 67. Evaluación de los sistemas de control. Control Número 3. Parte 2. [Fuente: Prado (2009)].

Descripción del plan de prueba	Método y Cantidad de selección de partidas (Al azar, fortuito o sistemático)	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Se realiza una prueba física localizando el cable ethernet que permite la conexión a la red del Access Point, para una vez encontrado determinar si su ubicación y la forma en que fue instalado es la correcta.	Método sistemático, tamaño de la muestra 1.	Tras localizar el cable ethernet que conecta al Access Point del departamento con el resto de la red de la Universidad se encontró que dicho cable entra por un agujero hecho por un taladro, cruza el pasillo de entrada al laboratorio y se conecta con una de las terminales de red del laboratorio ubicada en el suelo de este, así mismo el cable solo se encuentra fijado al suelo con cinta adhesiva. Si bien cumple su objetivo se recomienda instalarlo de una forma más adecuada.	Efectividad Media	Fotos tomadas al cableado que sale de la oficina de educación dual, entra al laboratorio y se conecta a una de las terminales Ethernet del laboratorio. Revisar las fotos tomadas en el Anexo C. Evidencia del sistema de control Número 3. Uso de un Access point para extender la red Existente por Wifi.

Una vez realizada la evaluación por medio de la revisión de cómo fue instalado el cable ethernet que permite que el Access Point se conecte al resto de la red de la institución, donde se encontró que no fue instalado correctamente, por lo que se le dio una calificación de efectividad media.

Tabla 68. Evaluación de los sistemas de control. Control Número 4. Parte 1. [Fuente: Prado (2009)].

Proceso critico	Descripción del riesgo	Actividad de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control Manual/Automático
Administración y monitoreo de equipamiento y software de laboratorios.	Pérdida total de los equipos de cómputo afectados, lo que generaría en una pérdida económica para poder remplazarlos, así como imposibilitar al alumnado realizar sus prácticas.	Uso del extintor designado.	En caso de que se suscite un incendio eléctrico en alguno de los laboratorios de cómputo, el docente asignado o el encargado del laboratorio que en este caso es el Licenciado que trabaja en conjunto con la directora de la institución deben tomar el extintor más cercano (en el edificio donde se encuentra dirección o en la planta baja del segundo edificio) y apagar el fuego lo más pronto posible, en caso de que el fuego llegue a no ser manejable se procede a llamar a las autoridades pertinentes.	En caso de que la amenaza se materialice	Manual

Tras determinar cómo se lleva a cabo la actividad de control, en caso de producirse un incendio eléctrico en alguno de los laboratorios de cómputo, se procede a realizar la evaluación del control en la tabla (tabla número).

Tabla 69. Evaluación de los sistemas de control. Control Número 4. Parte 2. [Fuente: Prado (2009)].

Descripción del plan de prueba	Método y Cantidad de selección de partidas (Al azar, fortuito o sistemático)	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Debido a que ninguno de los dos laboratorios cuenta con un extintor asignado, se localizan los extintores que si se encuentran disponibles y se determina la distancia aproximada de dichos extintores de ambos laboratorios de cómputo.	Método sistemático, tamaño de la muestra 2.	Fueron encontrados cuatro extintores en total, tres en el edificio principal en la pared frente a las escaleras de cada piso del edificio y la planta baja, así mismo el cuarto extintor fue localizado en la planta baja del segundo edificio en la parte central. La distancia entre estos y ambos laboratorios es aproximadamente de 50 metros. Revisar la tabla generada en el Anexo (Número)	Efectividad Media	Fotos tomadas a ambos laboratorios como muestra de que no hay extintores disponibles. Revisar el Anexo D. Evidencia del sistema de control número 4. Uso del extintor designado. Para visualizar las fotos. Fotos de los extintores disponibles en la institución. Revisar el Anexo D. Evidencia del sistema de control número 4. Uso del extintor designado. Tabla con un listado de los extintores encontrados, su ubicación y distancia aproximada entre estos y ambos laboratorios. Revisar el Anexo E. Tabla de ubicación de los extintores en la institución.

Una vez realizada la evaluación de la actividad de control, se encontró que Si bien el tiempo de respuesta es adecuado tratándose de un incendio eléctrico lo ideal es la respuesta más rápida posible, lo que se conseguirá si cada laboratorio dispusiera de un extintor propio, de tal forma que no se deba esperar al encargado del laboratorio.

Tabla 70. Evaluación de los sistemas de control. Control Número 5. Parte 1. [Fuente: Prado (2009)].

Proceso critico	Descripción del riesgo	Actividad de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control Manual/Automático
Procesamiento de solicitudes de titulación.	Generación de títulos sin autorización, así como la eliminación de títulos aprobados o la modificación de la información en ellos.	Uso de contraseña para el acceso al equipo de cómputo donde se realiza el proceso.	El acceso al equipo de cómputo del administrativo que desempeña el proceso critico se encuentra protegido por una contraseña de complejidad baja, utilizando únicamente una combinación de números.	La contraseña no se ha cambiado nunca	Manual

Como se puede observar en la tabla (número de tabla) la actividad de control que protege el proceso crítico “Procesamiento de solicitudes de titulación” es el uso de una contraseña de baja complejidad que restringe el acceso al equipo de cómputo donde se lleva a cabo el proceso. En la siguiente tabla se observa como esa contraseña fue evaluada por medio de una herramienta que permite evaluar contraseñas.

Tabla 71. Evaluación de los sistemas de control. Control Número 5. Parte 2. [Fuente: Prado (2009)].

Descripción del plan de prueba	Método y Cantidad de selección de partidas (Al azar, fortuito o sistemático)	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Utilizando la herramienta Kaspersky password checker de Kaspersky lab se pone a prueba la seguridad de la contraseña utilizada como medio de desbloqueo del equipo de cómputo del administrativo a cargo del proceso crítico.	Método sistemático, tamaño de la muestra 1.	Una vez analizada la contraseña utilizada para el acceso al equipo de cómputo del administrativo, la herramienta arroja como resultado que la contraseña es completamente insegura, además de encontrarse en una gran lista de bases de datos de contraseñas filtradas.	Efectividad Inexistente	Por motivos de las políticas de privacidad de la Universidad no se pudieron obtener evidencias de la prueba. Revisar el Anexo B. Carta de justificación de la ausencia de evidencia de los sistemas de control. Para ver la carta de justificación expedida por la institución.

Tras realizar la evaluación de la actividad de control con la herramienta Kaspersky password checker se determinó, tal como se muestra en la tabla, que la contraseña no es segura por lo que se recomienda cambiarla lo más pronto posible.

OBJETIVO 3. Desarrollar Estrategias de Plan de Continuidad de Negocio: Valorar los requerimientos y opciones para la recuperación de procesos críticos y sus recursos en un escenario de interrupción por un desastre.

ACTIVIDAD 3.1

Identificar las opciones de recuperación.

DESCRIPCIÓN DE LA ACTIVIDAD

Esta actividad se realizan las sugerencias en términos generales para la mitigación de las amenazas, vulnerabilidades y riesgos identificados en las actividades del objetivo 2, dichas recomendaciones se realizan con base a lo ya establecido en estándares como el ISO 17799 y otros. El resultado es el añadido de una nueva columna al catálogo de amenazas generado en la actividad 2.3 donde se redactan las recomendaciones para mitigar los riesgos, amenazas y vulnerabilidades ya concentrados en dicha tabla, abarcando tanto una solución preventiva como correctiva; para posteriormente en la siguiente actividad visualizar de forma más detallada las sugerencias planteadas en esta actividad.

RESULTADO DE LA ACTIVIDAD

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia].

Proceso crítico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Monitoreo y análisis de datos institucionales	Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos. Infección por malware en el equipo de cómputo. Uso de software sin licencia que pueda tener malware implantado. Compromiso de la integridad de los exámenes por un ataque de ingeniería social. (Phishing y acceso remoto).	Antivirus poco eficiente. Falta de conciencia sobre seguridad informática. Descarga de programas de idiomas de sitios no oficiales. Uso de software para “crackeo” de programas con licencia. Ausencia de software antimalware.	Perdida temporal o permanente de los equipos de cómputo afectados, así como la alta probabilidad de que se pierdan la información almacenada en ellos. Lo que provocaría que los procesos críticos que dependen de ellos se vean abruptamente detenidos.	Como medida preventiva de acuerdo con el estándar ISO 17799 en el 10.5 “Respaldo o Back-Up” es recomendable siempre tener un respaldo de la información importante para así evitar que el daño por un ataque de ransomware u otros malware no sea tan catastrófico. Además de acuerdo con el capítulo 10.4.1 “Controles contra códigos maliciosos” del mismo estándar, como medida preventiva y correctiva se recomienda la instalación de software antivirus con licencia para la revisión periódica de los equipos de cómputo, además también en el mismo capítulo del estándar se recomienda la implementación de una política de seguridad para proporcionar lineamientos a seguir para que el personal y el alumnado eviten poner en riesgo los equipos de cómputo.
Gestión de programas de idiomas y recursos digitales				
Administración de software especializado				
Coordinación de exámenes y certificaciones en línea				

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Gestión de comunicaciones internas y externas	Suplantación de identidad (spoofing).	Falta de conciencia en seguridad informática. Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican. Monitoreo inexistente de correos electrónicos no deseados.	Completa descoordinación en toda la institución debido a la propagación de instrucciones e información falsa por medios electrónicos (correo electrónico) debido al acceso no autorizado de una de las cuentas administrativas.	Según la recomendación del “protocolo de bloqueo de cuentas comprometidas” publicado por la Universidad Carlos III de Madrid la o las cuentas administrativas que se vean comprometidas y que permitan la suplantación de identidad debieran ser bloqueadas lo más pronto posible. Además de acuerdo con el estándar ISO 17799 en el capítulo 10.4.1 “Controles contra códigos maliciosos” es recomendable la suscripción a listas de correos y/o chequear sitios Web que dan información sobre códigos maliciosos nuevos como medida para la concientización del personal. Y como añadido se recomienda una correcta gestión de las claves y contraseñas para el acceso a las cuentas institucionales, como se menciona en el capítulo 11.3.1 “Uso de claves secretas” del ISO 17799.

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Administración de registros académicos en sistemas de información	Fallos del sistema como problemas de autenticación o registros no generados. Interrupción del servicio por un ataque DDoS. Interrupción del servicio de internet Fallos en el servicio de internet.	Sistemas saturados de información obsoleta.	Retraso indefinido de los procesos críticos, así como de las actividades dependientes, debido a que el funcionamiento de los servicios contratados a terceros no entra bajo el control de la institución.	Se recomienda establecer contacto con quienes gestionan el funcionamiento del sistema de información utilizado para que de acuerdo con las sugerencias del capítulo 10.2.2 “Monitoreo y revisión de los servicios de terceros” del estándar ISO 17799 la institución se asegure que se manejen apropiadamente los incidentes que impidan el correcto funcionamiento del sistema proporcionado a la Universidad.
Uso de plataforma institucional para gestión de cursos y calificaciones		Falta de un medio de control del tráfico de red.		
Gestión de convenios y programas de educación dual		Infraestructura física de la red deficiente.		
Coordinación de experimentos y proyectos en laboratorios virtuales		Problemas con el proveedor del servicio.		
Administración y monitoreo de equipamiento y software de laboratorios	Incendio eléctrico donde se pierden los equipos de cómputo.	Corto circuito en las tomas de corriente de los laboratorios. Ausencia de extintores en laboratorio.	Pérdida total o parcial de los activos de TI, principalmente equipos de cómputo, que se encuentren en el área afectada por el incendio que de no atenderse con rapidez significaría la pérdida total de laboratorio donde se generó el incendio.	Para la mitigación de incendios en el apartado 9.1.4 “Protección contra amenazas externas e internas” del estándar ISO 17799, es recomendable poseer equipo contra incendios ubicado adecuadamente en el área que se desea proteger, siendo este caso un extintor dentro de cada uno de los laboratorios de cómputo. Así mismo en el mismo, se recomienda la creación de un inventario de...

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Administración y monitoreo de equipamiento y software de laboratorios	Incendio eléctrico donde se pierden los equipos de cómputo.	Corto circuito en las tomas de corriente de los laboratorios. Ausencia de extintores en laboratorio.	Pérdida total o parcial de los activos de TI, principalmente equipos de cómputo, que se encuentren en el área afectada por el incendio que de no atenderse con rapidez significaría la pérdida total de laboratorio donde se generó el incendio.	... TI propio para la institución para poder tener un control sobre los activos con los que cuenta y saber si pueden remplazarlos con los que tengan en reserva o poder remplazar los que se hallan perdido, en caso de un incendio, con las mismas especificaciones técnicas; tal como se menciona en el mismo estándar en el capítulo 7.1.1 “Inventario de los activos”.
Coordinación de prácticas de laboratorio y reservaciones en línea	Interrupciones de las reservaciones en línea.	El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.	Completa descoordinación entre el personal docente que solicita el uso de alguno de los laboratorios pues al no tener un registro de reservaciones y conteo de horas de uso, provocaría el abuso de tiempo en los laboratorios por parte de algunos docentes o la sobreposición de horas entre dos o más grupos.	Se recomienda - Implementar un proceso de respaldo regular de la hoja de Excel que contiene las reservaciones, con el fin de evitar la pérdida de datos en caso de interrupciones o fallos en el sistema. - Establecer un plan de contingencia que incluya procedimientos manuales para gestionar las reservaciones en caso de interrupciones en el sistema de registro. Como se menciona en el apartado 15.5 “respaldo o Back-Up”

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Procesamiento de solicitudes de titulación	Acceso no autorizado que provoque la manipulación de registros académicos.	Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.	Generación de documentos para solicitud de titulación sin autorización o modificación de los datos personales las solicitudes ya realizadas.	Implementar controles de acceso físico y lógico para restringir el acceso no autorizado a los equipos de cómputo y a los registros académicos. Esto puede incluir la instalación de cerraduras, sistemas de alarma, controles de acceso basados en roles y autenticación de dos factores. Como se menciona en el apartado 9.1.2 “controles de ingreso físico” y 8.3.3 “Retro de derechos de acceso” de la norma ISO 17799
Generación de certificados y documentos oficiales digitales	Perdida del equipo de cómputo donde se generan dichos documentos.	Vigilancia escasa en la oficina del departamento.	Debido la falta de un respaldo tanto de documentos importantes almacenados para la posteridad, aquellos con los que se trabaja de forma frecuente o incluso el contacto registrado de alumnado que es participe de programas de formación dual provocarían desde la detención abrupta e indefinida de más de un proceso crítico, hasta el daño a la reputación de la Universidad.	Se recomienda realizar copias de forma regular de la información crítica para mantener la integridad y disponibilidad de la información, como se menciona en el punto 10.5 “Respaldo o Back-UP”, realizar mantenimiento preventivo y puntual de los equipos para su continua disponibilidad e integridad según el apartado 9.2.4 “Mantenimiento de equipo” y controlar el acceso a los dispositivos y su...
Coordinación de proyectos de investigación y desarrollo	Pérdida de datos críticos de investigación debido a fallas de almacenamiento.	Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste.		
Manejo de bases de datos de seguridad y procedimientos químicos	Perdida de la integridad de la información de la base de datos	Ausencia de respaldos en la nube u otra unidad de almacenamiento.		
Coordinación de auditorías internas y externas	Pérdida de acceso a documentos en línea durante auditorías	Uso de software no especializado para bases de datos.		

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Monitoreo del desempeño estudiantil	Perdida de comunicación con los estudiante y empresas que se encuentren en el programa.	Control deficiente del servicio en la nube donde se encuentran los documentos. Ausencia de un respaldo de los contactos.		... información para restringir el acceso a y dentro de los sistemas de aplicación como dicta el apartado “11.6 control de acceso a la aplicación y la información”
Uso de sistemas contables y de gestión financiera	Fallos de software de contabilidad	Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores.	Detención de las actividades previstas a trabajar con el software contable, afectando tanto al desempeño de departamento como al alumnado que hace uso de dicho software para su formación académica.	Se recomienda que “El software provisto por un vendedor y utilizado en el sistema operacional se debiera mantener en el nivel donde recibe soporte del proveedor” Según el punto “14.4.1” del ISO 17799
Gestión de encuestas y estudios de clima organizacional	Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas	Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados.	Se generarían problemas de convivencia entre alumnado, docentes y personal administrativo que afectaría su desempeño dentro de la institución.	Se recomienda establecer políticas de contraseñas, como que todos los usuarios deben de tener un identificador único para su uso personal como se menciona en el punto 11.5.3 “Sistema de gestión de claves secretas”),

Tabla 72. Cuadro de recomendaciones para la mitigación de riesgos con base al estándar ISO/IEC 17799. [Fuente: Elaboración propia]. (Continuación).

Proceso critico	Amenaza	Vulnerabilidades	Riesgos	Recomendaciones
Implementación de sistemas de seguimiento y apoyo	Mala gestión de los sistemas de seguimiento y apoyo	El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado.	Aquellos que dependan de los sistemas de seguimiento y apoyo, se verían significativamente afectados, tanto a nivel personal como en su desempeño académico o administrativo.	Se recomienda que “La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios” Según la ISO 17799 en su apartado 8.2.2 “conocimiento, educación y capacitación en seguridad de la información

ACTIVIDAD 3.2

Identificar los requerimientos para la recuperación.

DESCRIPCIÓN DE LA ACTIVIDAD

Esta actividad se centra en el desglose de las propuestas de la actividad 3.1, donde se identificaron las opciones para la recuperación, para ellos se realiza un nuevo formato del catálogo de riesgo, generado anteriormente, de tal forma que ahora se maneja una tabla por riesgo, propuesta, vulnerabilidades y amenazas asociados; para posteriormente de acuerdo a la propuesta abarcada en un contexto general desarrollarla en cuatro propuestas con un enfoque en específico las cuales son: preventivo, correctivo, de pago y gratuita, además de también especificar el tiempo aproximado en efectuar cada una; de tal forma que la Universidad pueda escoger que propuesta implementar. Cabe aclarar que las escogidas por la institución se ven a detalle en la actividad 3.4 posterior al análisis de viabilidad.

RESULTADO DE LA ACTIVIDAD

Tabla 73. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 1er conjunto. [Fuente: Elaboración propia].

RIESGO	
Pérdida temporal o permanente de los equipos de cómputo afectados, así como la alta probabilidad de que se pierdan la información almacenada en ellos. Lo que provocaría que los procesos críticos que dependen de ellos se vean abruptamente detenidos.	
AMENAZA	VULNERABILIDAD
• Ataque de ransomware que cifre todos los datos institucionales e impida el acceso a estos. • Infección por malware en el equipo de cómputo. • Uso de software sin licencia que pueda tener malware implantado. • Compromiso de la integridad de los exámenes por un ataque de ingeniería social. (Phishing y acceso remoto).	• Antivirus poco eficiente. • Falta de conciencia sobre seguridad informática. • Descarga de programas de idiomas de sitios no oficiales. • Uso de software para “crackeo” de programas con licencia. • Ausencia de software antimalware.

Tabla 73. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 1er conjunto. [Fuente: Elaboración propia]. (Continuación).

RECOMENDACIONES	
Como medida preventiva de acuerdo con el estándar ISO 17799 en el 10.5 “Respaldo o Back-Up” es recomendable siempre tener un respaldo de la información importante para así evitar que el daño por un ataque de ransomware u otros malware no sea tan catastrófico. Además de acuerdo con el capítulo 10.4.1 “Controles contra códigos maliciosos” del mismo estándar, como medida preventiva y correctiva se recomienda la instalación de software antivirus con licencia para la revisión periódica de los equipos de cómputo, además también en el mismo capítulo del estándar se recomienda la implementación de una política de seguridad para proporcionar lineamientos a seguir para que el personal y el alumnado eviten poner en riesgo los equipos de cómputo.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Designar unidades de almacenamiento externo (dispositivos USB de más de 32 GB o un disco duro externo) para el respaldo periódico (al menos una vez por semana) de los documentos y archivos que se desee resguardar. Siendo un dispositivo USB de al menos 32 GB ronda por los \$100.00 pesos mexicanos y un disco duro externo de 1TB en aproximadamente \$800.00 pesos mexicanos.	3 horas
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Contratar los servicios de un técnico en informática para que restaure los dispositivos de cómputo afectados a un punto en el que sean operables y en la medida de sus capacidades poder recuperar la información crítica. Teniendo en cuenta que un técnico en informática cobra aproximadamente \$80.00 pesos mexicanos la hora, pero este precio puede variar en función del tipo de solución que se necesite.	4 horas
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Compra de la licencia oficial e instalación de uso de un Software Antivirus como Norton que de acuerdo con una valoración realizada por el sitio softwarelab.org se encuentra como el mejor calificado debido a su alta tasa de efectividad contra virus y ransomware. La licencia de un año del paquete más básico de este antivirus es de \$700.00 pesos mexicanos.	2 horas
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Implementación de una política de seguridad para proporcionar al personal administrativo y alumnado de la institución los lineamientos a seguir para el correcto manejo de los equipos de cómputo y TI en general.	1 hora

Tabla 74. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 2do conjunto. [Fuente: Elaboración propia].

RIESGO	
Completa descoordinación en toda la institución debido a la propagación de instrucciones e información falsa por medios electrónicos (correo electrónico) debido al acceso no autorizado de una de las cuentas administrativas.	
AMENAZA	VULNERABILIDAD
Suplantación de identidad (spoofing).	- Falta de conciencia en seguridad informática. - Administrativos expuestos a un ataque de phishing donde se robe el acceso a las cuentas por donde se comunican. - Monitoreo inexistente de correos electrónicos no deseados.
RECOMENDACIONES	
Según la recomendación del “protocolo de bloqueo de cuentas comprometidas” publicado por la Universidad Carlos III de Madrid la o las cuentas administrativas que se vean comprometidas y que permitan la suplantación de identidad debieran ser bloqueadas lo más pronto posible. Además de acuerdo con el estándar ISO 17799 en el capítulo 10.4.1 “Controles contra códigos maliciosos” es recomendable la suscripción a listas de correos y/o chequear sitios Web que dan información sobre códigos maliciosos nuevos como medida para la concientización del personal. Y como añadido se recomienda una correcta gestión de las claves y contraseñas para el acceso a las cuentas institucionales, como se menciona en el capítulo 11.3.1 “Uso de claves secretas” del ISO 17799.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Impartir al personal administrativo de la institución un curso para la concienciación sobre la seguridad informática. Para una plática de este tipo se considera al menos una hora y media para poder impartirla correctamente, cobrando \$200.00 pesos mexicanos por persona.	1 hora y media
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Implementación del “protocolo de bloqueo de cuentas comprometidas” publicado por la Universidad Carlos III de Madrid en la institución, por medio de un informe donde se detallen los pasos a seguir de una forma fácil y clara de entender para el personal administrativo. La implementación de dicho protocolo se debe llevar a cabo por un auditor o algún experto en seguridad informática, cuyo salario mínimo aproximando es de \$150.00 pesos mexicanos la hora.	2 horas

Tabla 74. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 2do conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Contratación del servicio de Microsoft 365 Empresarial Premium para que se encargue de la gestión de todas las cuentas de la universidad, así como de la protección contra ataques de Phishing y otros. Cuyo precio es de \$1769 pesos mexicanos al año por usuario.	1 día
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Visita periódica al sitio https://cybermap.kaspersky.com/es para que el personal administrativo se mantenga constantemente actualizado sobre las amenazas en ciberseguridad más reciente. Así mismo invitar al personal a al menos una plática sobre la concientización sobre la ciberseguridad.	2 horas

Tabla 75. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 3er conjunto. [Fuente: Elaboración propia].

RIESGO	
Retraso indefinido de los procesos críticos, así como de las actividades dependientes, debido a que el funcionamiento de los servicios contratados a terceros no entra bajo el control de la institución.	
AMENAZA	VULNERABILIDAD
- Fallos del sistema como problemas de autenticación o registros no generados. - Interrupción del servicio por un ataque DDoS. - Interrupción del servicio de internet - Fallos en el servicio de internet.	- Sistemas saturados de información obsoleta. - Falta de un medio de control del tráfico de red. - Infraestructura física de la red deficiente. - Problemas con el proveedor del servicio. - Infraestructura física de la red deficiente. - Problemas con el proveedor del servicio.

Tabla 75. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 3er conjunto. [Fuente: Elaboración propia]. (Continuación).

RECOMENDACIONES	
Se recomienda establecer contacto con quienes gestionan el funcionamiento del sistema de información utilizado para que de acuerdo con las sugerencias del capítulo 10.2.2 “Monitoreo y revisión de los servicios de terceros” del estándar ISO 17799 la institución se asegure que se manejen apropiadamente los incidentes que impidan el correcto funcionamiento del sistema proporcionado a la Universidad.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Migración de los sistemas contratados por terceros a un servidor o servidores que se encuentren desplegados de forma física dentro de la institución para tener completo control sobre el funcionamiento de dichos sistemas de información. Para realizar una migración de este tipo sería necesario contratar por lo menos a tres ingenieros en sistemas cobrando aproximadamente \$500 pesos mexicanos la hora cada uno.	5 días
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
En caso de que los servicios contratados se vean interrumpidos de forma constante, se recomienda la cancelación de este y el contrato de uno distinto que cumpla con las necesidades de la institución. La cancelación del o los servicios actuales para la adquisición de otros que puedan cumplir con las necesidades de la universidad, tendría una diferencia de costo de aproximadamente un 15% de lo que se paga actualmente.	2 días
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Contratar un segundo servicio tanto del provisto para los sistemas de información como para el servicio de internet para tenerlos como medio de respaldo en caso de que uno falle poder continuar con las actividades con normalidad. El contratar servicios alternos con los que ya cuenta la institución duplicaría el dinero destinado ello.	2 días
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Generación de un protocolo propio de la institución donde se especifiquen los pasos a seguir para solucionar una posible interrupción de los servicios con los que dispone la Universidad. Abarcando desde una revisión de la infraestructura de red, hasta la comunicación con los proveedores para solicitar una solución lo más pronto posible.	1 hora

Tabla 76. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 4to conjunto. [Fuente: Elaboración propia].

RIESGO	
Pérdida total o parcial de los activos de TI, principalmente equipos de cómputo, que se encuentren en el área afectada por el incendio que de no atenderse con rapidez significaría la pérdida total de laboratorio donde se generó el incendio.	
AMENAZA	VULNERABILIDAD
Incendio eléctrico donde se pierden los equipos de cómputo.	- Corto circuito en las tomas de corriente de los laboratorios. - Ausencia de extintores en laboratorio.
RECOMENDACIONES	
Para la mitigación de incendios en el apartado 9.1.4 “Protección contra amenazas externas e internas” del estándar ISO 17799, es recomendable poseer equipo contra incendios ubicado adecuadamente en el área que se desea proteger, siendo este caso un extintor dentro de cada uno de los laboratorios de cómputo. Así mismo en el mismo, se recomienda la creación de un inventario de TI propio para la institución para poder tener un control sobre los activos con los que cuenta y saber si pueden remplazarlos con los que tengan en reserva o poder remplazar los que se hallan perdido, en caso de un incendio, con las mismas especificaciones técnicas; tal como se menciona en el mismo estándar en el capítulo 7.1.1 “Inventario de los activos”.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Adquisición de dos extintores que se destinen exclusivamente para los laboratorios de cómputo (uno para cada aula), de tal forma que en caso de suscitarse un incendio eléctrico poder apagarlo lo más pronto posible. Además, establecer un control para el remplazo de estos, debido a que con el tiempo pueden perder su efectividad. Siendo el precio de un extintor portátil para incendios eléctricos de polvo químico ABC polivalente de aproximadamente \$1300.00 pesos mexicanos por unidad.	2 horas
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Desarrollo de un protocolo donde se planteen las medidas a realizar en caso de suscitarse un incendio dentro de algunos de los laboratorios de cómputo, desde de proceder con apagarlo con el equipo adecuado, hasta el llamar a las autoridades pertinentes en caso de que el incendio pase a ser incontrolable, para posteriormente realizar un recuento tanto de los daños como de las pérdidas y proceder con las reparaciones y remplazo de los equipos dañados, así como de las instalaciones.	2 horas

Tabla 76. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 4to conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Instalación de un sistema antiincendios en ambos laboratorios que se accione de forma automática en caso de producirse uno. Dicha instalación varía dependiendo las dimensiones del edificio, sin embargo, un costo medio para dicha instalación es de \$52,800.00 pesos mexicanos, pero puede ir desde \$9,800.00 hasta \$120,000.00 pesos mexicanos.	2 semanas
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Implementación de un sistema de inventario de TI, propio de la institución, para llevar un control de los equipos de cómputo y activos de TI en general con los que cuenta la Universidad, para que, de esta forma, en caso de suceder un incendio que provoque la pérdida total de más de un activo de TI, saber si es posible remplazarlos y/o cubrir la necesidad con los que se encuentren en las instalaciones.	1 hora

Tabla 77. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 5to conjunto. [Fuente: Elaboración propia].

RIESGO	
Completa descoordinación entre el personal docente que solicita el uso de alguno de los laboratorios pues al no tener un registro de reservaciones y conteo de horas de uso, provocaría el abuso de tiempo en los laboratorios por parte de algunos docentes o la sobre posición de horas entre dos o más grupos.	
AMENAZA	VULNERABILIDAD
Interrupciones de las reservaciones en línea.	El registro de las reservaciones se encuentra únicamente en un equipo de cómputo, en un archivo Excel.
RECOMENDACIONES	
Se recomienda implementar un proceso de respaldo regular de la hoja de Excel que contiene las reservaciones, con el fin de evitar la pérdida de datos en caso de interrupciones o fallos en el sistema. Establecer un plan de contingencia que incluya procedimientos manuales para gestionar las reservaciones en caso de interrupciones en el sistema de registro. Como se menciona en el apartado 15.5 “respaldo o Back-Up”	

Tabla 77. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 5to conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Programar como tarea recursiva cada semana realizar el respaldo de la hoja de Excel donde se registran las reservaciones, así como tener a la mano una hoja de registro en caso de que el equipo de cómputo falle. Teniendo en cuenta que un técnico en informática cobra aproximadamente \$80.00 pesos mexicanos la hora, podría quedar entre 80 y 160 pesos dependiendo de la habilidad del técnico, pero este precio puede variar en función del tipo de solución que se necesite.	1 hora
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Con los datos almacenados en respaldos anteriores y hoja de registros, reorganizar los cupos y turnos para el uso de laboratorios. Esta actividad la puede realizar el administrador de las hojas de registro, no generaría un costo adicional.	30 minutos
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Crear un programa independiente con conexión a base de datos local o en línea para gestionar las reservaciones de manera segura o contratar un servicio de terceros para este fin. Tarifa por hora de desarrollo: Puede variar entre \$500 MXN y \$2,000 MXN por hora, según la experiencia del desarrollador y la complejidad del proyecto. Costo total para el desarrollo del programa: Dependiendo de la funcionalidad, podría oscilar entre \$30,000 MXN y \$45,000 MXN.	1 semana
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Implementación de los respaldos programados a lo largo del tiempo y llenado de solicitudes también de manera escrita.	1 hora

Tabla 78. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 6to conjunto. [Fuente: Elaboración propia].

RIESGO	
Generación de documentos para solicitud de titulación sin autorización o modificación de los datos personales las solicitudes ya realizadas.	
AMENAZA	VULNERABILIDAD
Acceso no autorizado que provoque la manipulación de registros académicos.	Fácil acceso al equipo de cómputo, dado a que la oficina suele estar vacía.
RECOMENDACIONES	
Implementar controles de acceso físico y lógico para restringir el acceso no autorizado a los equipos de cómputo y a los registros académicos. Esto puede incluir la instalación de cerraduras, sistemas de alarma, controles de acceso basados en roles y autenticación de dos factores. Como se menciona en el apartado 9.1.2 “controles de ingreso físico” y 8.3.3 “Retro de derechos de acceso” de la norma ISO 17799	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Implementar un sistema de autenticación de dos factores para todos los accesos al sistema de registros académicos. Este proceso debe incluir una fase de concienciación y capacitación del personal para garantizar su correcta adopción. Algunas suscripciones de autenticación en dos pasos, especialmente aquellas destinadas a empresas, pueden costar entre unos pocos dólares hasta veinte o treinta dólares por usuario al año. Por ejemplo, soluciones como Duo Security de Cisco ofrecen planes que comienzan alrededor de 3 dólares por usuario al mes para sus opciones más básicas, y pueden aumentar a 9 dólares o más por usuario al mes para planes más avanzados.	1 semana
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Conducir una auditoría exhaustiva de accesos al sistema de registros académicos para identificar cualquier actividad no autorizada. Simultáneamente, implementar mecanismos de retroalimentación de derechos de acceso para prevenir futuras manipulaciones esto podría costar en promedio entre 50,000 y 300,000 pesos mexicanos. Este rango considera la contratación de expertos en seguridad de la información para realizar la auditoría, el tiempo dedicado al análisis de los registros de acceso, la implementación de herramientas o software para la gestión de derechos de acceso, y posiblemente la capacitación del personal para gestionar y mantener estos sistemas.	1 semana

Tabla 78. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 6to conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Contratar servicios especializados de consultoría en ciberseguridad para realizar una evaluación exhaustiva de los sistemas existentes y proponer mejoras basadas en las pautas de la norma ISO 17799. Desarrollar un plan de acción detallado con hitos mensuales para implementar mejoras graduales. Tarifa por hora/día de un consultor de ciberseguridad: Puede oscilar entre \$1,500 MXN y \$5,000 MXN por hora, dependiendo de la experiencia. Costo total para una evaluación exhaustiva: Aproximadamente \$35,000 MXN.	2 semanas
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Establecer y comunicar de inmediato políticas de seguridad que requieran que todo el personal apague y asegure correctamente los equipos de cómputo al salir de la oficina.	3 días

Tabla 79. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 7mo conjunto. [Fuente: Elaboración propia].

RIESGO	
Debido la falta de un respaldo tanto de documentos importantes almacenados para la posteridad, aquellos con los que se trabaja de forma frecuente o incluso el contacto registrado de alumnado que es partícipe de programas de formación dual provocarían desde la detención abrupta e indefinida de más de un proceso crítico, hasta el daño a la reputación de la Universidad.	
AMENAZA	VULNERABILIDAD
• Pérdida del equipo de cómputo donde se generan dichos documentos. • Pérdida de datos críticos de investigación debido a fallas de almacenamiento. • Pérdida de la integridad de la información de la base de datos. • Pérdida de acceso a documentos en línea durante auditorías • Pérdida de comunicación con los estudiante y empresas que se encuentren en el programa.	• Vigilancia escasa en la oficina del departamento. • Uso de equipos de cómputo con unidades de almacenamiento con mucho desgaste. • Ausencia de respaldos en la nube u otra unidad de almacenamiento. • Uso de software no especializado para bases de datos. • Control deficiente del servicio en la nube donde se encuentran los documentos. • Ausencia de un respaldo de los contactos.

Tabla 79. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 7mo conjunto. [Fuente: Elaboración propia]. (Continuación).

RECOMENDACIONES	
Se recomienda realizar copias de forma regular de la información crítica (punto 11.7.1), realizar mantenimiento preventivo y puntual de los equipos según el apartado 9.2.4 “Mantenimiento de equipo” y controlar el acceso a los dispositivos y su información según el apartado “11.6 control de acceso a la aplicación y la información”	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Implementar un plan de copias de seguridad regulares para la información crítica, incluyendo documentos almacenados para la posteridad, datos de investigación, y contactos de alumnado, podría costar en promedio entre 10,000 y 15,000 pesos mexicanos. Este rango de costo contempla la evaluación inicial de las necesidades de la escuela, la configuración del hardware y software de respaldo (como discos duros externos, servicios en la nube, o servidores de respaldo), la implementación del plan de respaldo (incluyendo la programación de respaldos automáticos y pruebas de recuperación), y la capacitación del personal para gestionar y supervisar el sistema de respaldo.	1 semana
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Realizar mantenimiento preventivo y puntual de los equipos de cómputo, especialmente de aquellos utilizados para la generación y almacenamiento de documentos críticos. Evaluar y reemplazar unidades de almacenamiento con desgaste significativo, podría costar aproximadamente entre 10,600 y 13,800 pesos mexicanos, considerando tanto la mano de obra del técnico como el costo de los nuevos dispositivos de almacenamiento.	2 días
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Implementar un sistema especializado para bases de datos que incluya características robustas de respaldo y recuperación. Contratar servicios de gestión y control de acceso en la nube para garantizar la integridad y disponibilidad de la información crítica. Precio del software especializado: Puede variar desde \$50,000 MXN hasta \$200,000 MXN, según la marca y las características. Costos de licencia por usuario (si es aplicable): Precio por usuario puede oscilar entre \$5,000 MXN y \$20,000 MXN.	3 semanas

Tabla 79. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 7mo conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Establecer políticas y procedimientos para controlar el acceso a dispositivos y a la información almacenada. Realizar auditorías periódicas para garantizar el cumplimiento de estas políticas.	2 semanas

Tabla 80. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 8vo conjunto. [Fuente: Elaboración propia].

RIESGO	
Detención de las actividades previstas a trabajar con el software contable, afectando tanto al desempeño de departamento como al alumnado que hace uso de dicho software para su formación académica.	
AMENAZA	VULNERABILIDAD
Fallos de software de contabilidad.	Uso de un software que ya no cuenta con soporte ni resolución de errores por parte de sus desarrolladores.
RECOMENDACIONES	
Se recomienda que “El software provisto por un vendedor y utilizado en el sistema operacional se debiera mantener en el nivel donde recibe soporte del proveedor” Según el punto “14.4.1” del ISO 17799.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Actualizar el software contable a una versión que aún cuente con soporte y resolución de errores por parte de los desarrolladores. Teniendo en cuenta que un técnico en informática cobra aproximadamente \$80.00 pesos mexicanos la hora, dependería de el tiempo que tome actualizar todos los equipos, aparte del costo de la licencia del programa actualizado si es que no se posee, teniendo un precio de 80 pesos por aproximadamente cada 4 equipos a la hora de actualizar, más 3,000 – 4,500 pesos por licencia de software contable.	1 día

Tabla 80. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 8vo conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Establecer un plan de contingencia que incluya la identificación de alternativas o soluciones temporales en caso de fallos del software contable actual, podría costar alrededor de 3,000 a 5,000 pesos mexicanos, considerando el tiempo de un técnico o consultor para identificar alternativas y redactar un plan de acción sencillo.	4 días
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Adquisición de un nuevo software contable con soporte continuo y actualizaciones regulares. Algunos sistemas de software contable pueden costar tan bajo como \$9 y llegar hasta \$999 por usuario al mes. Para sistemas de contabilidad más avanzados con más usuarios, se puede esperar pagar cerca de \$375 por usuario al mes o más de \$1,000 para una licencia.	1 hora
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Establecer un proceso de revisión periódica de la disponibilidad de soporte y actualizaciones para el software contable actual. Implementar un sistema de alerta para notificar al personal sobre la necesidad de acciones preventivas.	5 días

Tabla 81. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 9no conjunto. [Fuente: Elaboración propia].

RIESGO	
Se generarían problemas de convivencia entre alumnado, docentes y personal administrativo que afectaría su desempeño dentro de la institución.	
AMENAZA	VULNERABILIDAD
Brechas de seguridad que comprometen la confidencialidad de las respuestas de las encuestas	Contraseñas inseguras de las cuentas usadas para aplicar las encuestas en línea y donde se recopilan los resultados.
RECOMENDACIONES	
Se recomienda establecer políticas de contraseñas, como que todos los usuarios deben de tener un identificador único para su uso personal como se menciona en el punto 11.5.3 “Sistema de gestión de claves secretas”).	

Tabla 81. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 9no conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Impartir al personal administrativo de la institución un curso sobre cómo crear contraseñas seguras y la importancia del uso de estas para resguardar el acceso de sus cuentas institucionales, así como personales. Para una plática de este tipo se considera al menos una hora y media para poder impartirla correctamente, cobrando \$200.00 pesos mexicanos por persona.	1 hora y media
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Elaborar de política acerca de la creación de contraseñas seguras e identificador único de uso personal, podría costar alrededor de 5,000 a 15,000 pesos mexicanos, teniendo en cuenta el tiempo de un profesional para redactar el documento, la revisión, y posiblemente la capacitación inicial al personal y estudiantes.	5 días
PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Contratar un servicio de capacitación sobre seguridad informática y contraseñas. La creación de esta política implica generalmente la realización de sesiones de capacitación y el uso de herramientas de gestión de contraseñas. Estos aspectos pueden llevar asociados ciertos costos, como el tiempo dedicado por el personal de TI y los recursos invertidos en herramientas de seguridad informática, los costos de desarrollar una política de contraseñas seguras y realizar una capacitación en seguridad informática podrían incluir alrededor de \$50 a \$100 por hora para el tiempo del personal de TI y aproximadamente \$2 a \$10 por usuario al mes para herramientas de gestión de contraseñas.	1 semana
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Utilizar un software gratuito de generación de contraseñas y obtener algún curso en línea sobre el tema.	1 semana

Tabla 82. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 10mo conjunto. [Fuente: Elaboración propia].

RIESGO	
Aquellos que dependan de los sistemas de seguimiento y apoyo, se verían significativamente afectados, tanto a nivel personal como en su desempeño académico o administrativo.	
AMENAZA	VULNERABILIDAD
Mala gestión de los sistemas de seguimiento y apoyo	El personal que lleva a cabo el proceso no está lo suficientemente capacitado para el uso del software especializado.
RECOMENDACIONES	
Se recomienda que “La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios” Según la ISO 17799 en su apartado 8.2.2 “conocimiento, educación y capacitación en seguridad de la información.	
PROPUESTA PREVENTIVA	TIEMPO DE IMPLEMENTACIÓN
Realizar un programa de capacitación formal para el personal encargado del manejo de sistemas de seguimiento y apoyo. Esto podría incluir sesiones de inducción que aborden específicamente las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios. Además, establecer un sistema continuo de actualización y capacitación para mantener al personal al tanto de las mejores prácticas de seguridad. El costo podría oscilar entre \$2,000 y \$5,000, dependiendo de la duración y la complejidad del programa. Este rango cubre tanto el desarrollo del programa como la entrega de este, ya sea en línea o presencial.	2 semanas
PROPUESTA CORRECTIVA	TIEMPO DE IMPLEMENTACIÓN
Implementar un plan de acción para mejorar la capacitación del personal que lleva a cabo el proceso de sistemas de seguimiento y apoyo. Esto podría incluir la identificación de lagunas de conocimiento específicas y la implementación de programas de capacitación específicos para abordar esas deficiencias. El costo podría oscilar entre \$2,000 y \$5,000. Este costo variaría en función del alcance del plan de acción y las áreas de conocimiento específicas a abordar, incluyendo materiales de capacitación y posiblemente el uso de plataformas de aprendizaje en línea.	1 semana

Tabla 83. Cuadro de soluciones propuestas de acuerdo con las recomendaciones. 10mo conjunto. [Fuente: Elaboración propia]. (Continuación).

PROPUESTA DE PAGO	TIEMPO DE IMPLEMENTACIÓN
Contratar servicios de consultoría especializada en gestión de sistemas de seguimiento y apoyo. Esto garantizará una implementación eficaz y una gestión continua de los sistemas. Además, podría incluir acuerdos de soporte técnico y actualizaciones periódicas de seguridad para garantizar un rendimiento óptimo y protección contra amenazas. El rango de precio sería entre \$5,000 a \$10,000. Este costo se debe a la especialización y experiencia de los consultores, e incluiría servicios como el desarrollo de estrategias, soporte técnico y actualizaciones periódicas de seguridad.	2 semanas
PROPUESTA GRATUITA	TIEMPO DE IMPLEMENTACIÓN
Explorar recursos en línea gratuitos relacionados con la capacitación en el manejo de software especializado para sistemas de seguimiento y apoyo. Utilizar plataformas de aprendizaje en línea y recursos educativos gratuitos para mejorar las habilidades del personal. Además, promover la colaboración entre los propios miembros del personal para compartir conocimientos y experiencias.	2 semanas

ACTIVIDAD 3.3

Evaluar la viabilidad de implementar las estrategias, a partir de la disponibilidad de recursos, restricciones operativas y el tiempo de implementación.

DESCRIPCIÓN DE LA ACTIVIDAD

Una vez presentadas las propuestas desarrolladas en la actividad 3.2, la institución decide cuales desea implementar para mitigar el riesgo asociado con base a una evaluación de viabilidad a partir de la disponibilidad de recursos y las restricciones operativas de la Universidad. El resultado de esta actividad es una tabla donde se abarca: La solución propuesta, la disponibilidad de recursos donde se describe los recursos (presupuesto, equipo técnico, personal, etc.) con los que cuenta la institución para implementar dicha solución, las restricciones operativas donde se abarca lo que impediría que la Universidad pudiera implementar alguna solución sea implementada, el tiempo aproximado que se requeriría para implementar las soluciones y finalmente la conclusión donde se describe si es viable o no. Las soluciones que son elegidas por la Institución se ven en la actividad 3.4 donde se describe el porqué de su elección tomando en cuenta la evaluación de viabilidad vista en esta actividad.

RESULTADO DE LA ACTIVIDAD

Tabla 84. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia].

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Designar unidades de almacenamiento externo (dispositivos USB de más de 32 GB o un disco duro externo) para el respaldo periódico (al menos una vez por semana) de los documentos y archivos que se desee resguardar.	Actualmente la institución no cuenta con unidades extraíbles disponibles para realizar respaldos de los datos importantes, sin embargo, cuenta con un presupuesto reducido únicamente para la compra de al menos tres unidades USB de 32 GB, siendo que se requeriría una por cada administrativo.	Dentro de las políticas actuales de la institución, no hay un apartado que hable sobre el uso correcto de unidades de almacenamiento portátiles, y por esa razón la universidad no quiere arriesgarse a tener una filtración de información por el uso incorrecto de dispositivos de almacenamiento extraíbles.	3 horas	La solución no es viable.
Contratar los servicios de un técnico en informática para que restaure los dispositivos de cómputo afectados a un punto en el que sean operables y en la medida de sus capacidades poder recuperar la información crítica.	Se cuenta con el presupuesto necesario para contratar los servicios de un técnico en informática cada vez que se requiera.	Requiere de la autorización de la coordinadora de la Universidad. El técnico contratado debe ajustarse a las políticas de seguridad de la Institución para realizar su trabajo.	4 horas	La solución es viable debido a que se cuentan con los recursos necesarios, sin embargo, requiere de la aprobación de la coordinadora de la institución.

Tabla 85. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Compra de la licencia oficial e instalación de un Software Antivirus como Norton que de acuerdo con una valoración realizada por el sitio softwarelab.org se encuentra como el mejor calificado debido a su alta tasa de efectividad contra virus y ransomware.	Actualmente la Universidad únicamente cuenta con el presupuesto para la adquisición de cinco licencias estándar de algún Sistema Antivirus.	Requiere de la autorización de la coordinadora de la Universidad.	2 horas	La solución sería viable si el presupuesto actual fuera suficiente para implementar la solución en su totalidad.
Implementación de una política de seguridad para proporcionar al personal administrativo y alumnado de la institución los lineamientos a seguir para el correcto manejo de los equipos de cómputo y TI en general.	La institución cuenta con lo necesario para la implementación de una nueva política de seguridad, incluyendo el colocar una versión resumida de esta en la zona más visualizada dentro de los laboratorios de la institución.	Requiere la revisión y aprobación de la coordinadora de la Universidad.	1 hora	La solución es viable debido a que se cuentan con los recursos necesarios, sin embargo, requiere de la aprobación de la coordinadora de la institución.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Impartir al personal administrativo de la institución un curso para la concienciación sobre la seguridad informática.	La Universidad cuenta con un auditorio donde impartir el curso.	Requiere la autorización de la coordinadora de la Universidad. Se necesita la disponibilidad de tiempo del personal administrativo.	1 hora y media	La solución es viable debido a que se cuentan con los recursos necesarios, sin embargo, requiere de la aprobación de la coordinadora de la institución.
Implementación del “protocolo de bloqueo de cuentas comprometidas” publicado por la Universidad Carlos III de Madrid en la institución, por medio de un informe donde se detallen los pasos a seguir de una forma fácil y clara de entender para el personal administrativo.	La Universidad cuenta con los recursos para la implementación del protocolo sugerido.	Requiere la aprobación de la coordinadora de la institución. Es necesario capacitar al personal para que pueda efectuar el protocolo correctamente.	2 horas	La solución es viable debido a que se cuentan con los recursos necesarios, sin embargo, requiere la capacitación del personal de la Universidad.
Contratación del servicio de Microsoft 365 Empresarial Premium para que se encargue de la gestión de todas las cuentas de la universidad, así como de la protección contra ataques de Phishing y otros.	La Universidad no cuenta con el presupuesto necesario para contratar el servicio para todo su personal administrativo.	Debido a la falta de conocimiento de cómo gestionar este tipo de servicio sería necesario capacitar al personal que lo utilizara.	1 día	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Visita periódica al sitio https://cybermap.kaspersky.com/es para que el personal administrativo se mantenga constantemente actualizado sobre las amenazas en ciberseguridad más reciente. Así mismo invitar al personal a al menos una plática sobre la concientización sobre la ciberseguridad.	La Universidad cuenta con los recursos necesarios para implementar la solución.	Se requiere la disponibilidad del tiempo por parte del personal administrativo.	2 horas	La solución es viable, solo requiere que el personal administrativo tenga la disposición para visitar el sitio.
Migración de los sistemas contratados por terceros a un servidor o servidores que se encuentren desplegados de forma física dentro de la institución para tener completo control sobre el funcionamiento de dichos sistemas de información.	La Universidad cuenta con dos servidores funcionales con la capacidad suficiente para migrar los sistemas que ya ha contratado.	La institución no quiere que sus servidores sean modificados o desempeñen otros procesos.	5 días	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
En caso de que los servicios contratados se vean interrumpidos de forma constante, se recomienda la cancelación de este y el contrato de uno distinto que cumpla con las necesidades de la institución.	La institución cuenta con el presupuesto necesario para cubrir la diferencia de precios al contratar un servicio distinto.	La Universidad no tiene intenciones de cambiar de proveedor de servicios.	2 días	La solución sería viable solo si la Universidad se viera en la necesidad de realizarla.
Contratar un segundo servicio tanto del provisto para los sistemas de información como para el servicio de internet para tenerlos como medio de respaldo en caso de que uno falle poder continuar con las actividades con normalidad.	No se cuenta con el presupuesto suficiente como para contratar un segundo servicio como medida de respaldo ante la interrupción del principal.	La Universidad no ve la necesidad de contratar un segundo servido. No hay forma de solicitar presupuesto adicional al que ya se tiene destinado por parte del gobierno.	2 días	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Generación de un protocolo propio de la institución donde se especifiquen los pasos a seguir para solucionar una posible interrupción de los servicios con los que dispone la Universidad. Abarcando desde una revisión de la infraestructura de red, hasta la comunicación con los proveedores para solicitar una solución lo más pronto posible.	La institución dispone de los recursos necesarios para poder redactar el protocolo e implementarlo.	La implementación de un nuevo protocolo requiere la revisión y aprobación por parte de la coordinadora de la Universidad.	1 hora	La solución es viable, solo requiere ser aprobada por la coordinadora de la universidad.
Adquisición de dos extintores que se destinen exclusivamente para los laboratorios de cómputo (uno para cada aula), de tal forma que en caso de suscitarse un incendio eléctrico poder apagarlo lo más pronto posible.	La Universidad no cuenta con el presupuesto necesario para la adquisición de dos extintores nuevo, pero si puede reubicar dos para colocarlos en los laboratorios de cómputo.	Es necesario revisar las políticas de seguridad de la institución para garantizar que no se está incumpliendo alguna al reubicar dos extintores, así mismo se requiere de la autorización de la coordinadora de la Universidad.	2 horas	La solución sería viable si la Universidad accede a reubicar dos de sus extintores.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Desarrollo de un protocolo donde se planteen las medidas a realizar en caso de suscitarse un incendio dentro de algunos de los laboratorios de cómputo, desde de proceder con apagarlo con el equipo adecuado, hasta el llamar a las autoridades pertinentes en caso de que el incendio pase a ser incontrolable, para posteriormente realizar un recuento tanto de los daños como de las pérdidas y proceder con las reparaciones y remplazo de los equipos dañados.	La Universidad cuenta con los recursos necesarios para redactar dicho protocolo.	Para la implementación del protocolo es necesario la autorización por parte de la coordinadora de la institución.	2 horas	La solución es viable, solo requiere de la aprobación de la coordinadora de la Universidad.
Instalación de un sistema antincendios en ambos laboratorios que se accione de forma automática en caso de producirse uno.	La Universidad no cuenta con el presupuesto suficiente para la instalación y el subsecuente mantenimiento que implica un sistema antiincendios automatizado.	Al tratarse de un mecanismo complejo que requeriría en gran medida modificaciones a la infraestructura de la Universidad, es necesario la autorización por parte del Gobierno del Estado.	2 semanas	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Implementación de un sistema de inventario de TI, propio de la institución, para llevar un control de los equipos de cómputo y activos de TI en general con los que cuenta la Universidad, para que, de esta forma, en caso de suceder un incendio que provoque la pérdida total de más de un activo de TI, saber si es posible cubrir la necesidad con los que se encuentren en las instalaciones.	En el área administrativa se encuentran distintos equipos de cómputo con las características necesarias para la instalación de sistema de inventario de TI.	Requiere la aprobación de la coordinadora de la institución.	1 hora	La solución es viable, solo requiere de la aprobación de la coordinadora de la Universidad.
Programar como tarea recursiva cada semana realizar el respaldo de la hoja de Excel donde se registran las reservaciones, así como tener a la mano una hoja de registro en caso de que el equipo de cómputo falle.	Programación semanal de respaldos de la hoja de Excel y disponibilidad de registros manuales.	Depende de la regularidad y disciplina del encargado de realizar la tarea. Riesgo de fallo humano.	1 hora	La solución es viable, no se requiere experiencia y se obtiene de esta solución un control.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Con los datos almacenados en respaldos anteriores y hoja de registros, reorganizar los cupos y turnos para el uso de laboratorios.	Uso de respaldos anteriores y registros físicos para reorganizar cupos y turnos.	Requiere tiempo y esfuerzo manual para reorganizar tras un incidente.	30 minutos	Viable, siempre que se manejen adecuadamente los datos y se utilicen herramientas eficientes para la planificación de cupos y turnos.
Crear un programa independiente con conexión a base de datos local o en línea para gestionar las reservaciones de manera segura o contratar un servicio de terceros para este fin.	Desarrollo o contratación de un sistema de gestión de reservaciones con base de datos.	Costo financiero y dependencia de proveedores externos o recursos de desarrollo interno.	1 semana	La solución es poco viable ya que requiere de recursos para la tarea.
Implementación de los respaldos programados a lo largo del tiempo y llenado de solicitudes también de manera escrita.	Implementar respaldos programados y llevar registros escritos de las solicitudes.	Requiere espacio físico para almacenamiento y es susceptible a daños o pérdida física.	1 hora	La solución es poco viable ya que requiere software de respaldo.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Implementar un sistema de autenticación de dos factores para todos los accesos al sistema de registros académicos. Este proceso debe incluir una fase de concienciación y capacitación del personal para garantizar su correcta adopción.	Implementación de autenticación de dos factores y capacitación del personal.	Necesidad de concienciar y entrenar al personal en el uso efectivo de la autenticación de dos factores.	1 semana	La solución no es viable.
Conducir una auditoría exhaustiva de accesos al sistema de registros académicos para identificar cualquier actividad no autorizada. Simultáneamente, implementar mecanismos de retroalimentación de derechos de acceso para prevenir futuras manipulaciones.	Realización de una auditoría de accesos y ajuste de derechos de acceso.	Requiere recursos para una auditoría detallada y puede interrumpir las operaciones regulares durante el proceso.	1 semana	Muy viable, pero requiere de personal con experiencia.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Contratar servicios especializados de consultoría en ciberseguridad para realizar una evaluación exhaustiva de los sistemas existentes y proponer mejoras basadas en las pautas de la norma ISO 17799. Desarrollar un plan de acción detallado con hitos mensuales para implementar mejoras graduales.	Contratación de servicios de consultoría en ciberseguridad para seguir ISO 17799.	Inversión financiera significativa y dependencia de la disponibilidad de consultores especializados.	2 semanas	La solución no es viable.
Establecer y comunicar de inmediato políticas de seguridad que requieran que todo el personal apague y asegure correctamente los equipos de cómputo al salir de la oficina.	Establecimiento de políticas de seguridad para el cierre de sesión y protección de equipos.	Requiere que el personal adopte nuevas rutinas y puede faltar el seguimiento para garantizar el cumplimiento.	3 días	Muy viable, la comunicación es vital en una institución para la seguridad de los equipos y sus datos.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Implementar un plan de copias de seguridad regulares para la información crítica, incluyendo documentos almacenados para la posteridad, datos de investigación, y contactos de alumnado.	Planificar copias de seguridad regulares para datos críticos.	Requiere de sistemas de almacenamiento confiables y la programación de backups automáticos.	1 semana	Viable, siempre que la institución esté comprometida a invertir en una solución de respaldo robusta y confiable.
Realizar mantenimiento preventivo y puntual de los equipos de cómputo, especialmente de aquellos utilizados para la generación y almacenamiento de documentos críticos. Evaluar y reemplazar unidades de almacenamiento con desgaste significativo.	Mantenimiento preventivo y reemplazo de unidades de almacenamiento desgastadas.	Posible inactividad durante el mantenimiento y costos asociados con la actualización de hardware.	2 días	Viable, siempre que la planificación del mantenimiento se realice de manera que minimice la interrupción de las operaciones y se disponga de un presupuesto adecuado para la adquisición de piezas de repuesto y la contratación de personal técnico competente.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Implementar un sistema especializado para bases de datos que incluya características robustas de respaldo y recuperación. Contratar servicios de gestión y control de acceso en la nube para garantizar la integridad y disponibilidad de la información crítica.	Sistema especializado de bases de datos y servicios de gestión de datos en la nube.	Inversión financiera en infraestructura tecnológica y en la contratación de servicios externos.	3 semanas	Poco viable ya que requiere una inversión financiera para la adquisición del sistema especializado de bases de datos, así como para la contratación de servicios en la nube.
Establecer políticas y procedimientos para controlar el acceso a dispositivos y a la información almacenada. Realizar auditorías periódicas para garantizar el cumplimiento de estas políticas.	Políticas de control de acceso y auditorías regulares de cumplimiento.	Necesidad de formación y concienciación del personal para el cumplimiento efectivo de políticas.	2 semanas	Viable, con la condición de que se asignen los recursos necesarios para la elaboración de políticas y la realización de auditorías.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Actualizar el software contable a una versión que aún cuente con soporte y resolución de errores por parte de los desarrolladores.	La universidad no cuenta con el recurso monetario para actualizar el software contable de cada computadora a la más reciente	Dependencia de proveedores externos; limitaciones de infraestructura tecnológica actual.	1 día	La solución no es viable.
Establecer un plan de contingencia que incluya la identificación de alternativas o soluciones temporales en caso de fallos del software contable actual.	La universidad cuenta con lo necesario para establecer un plan de contingencia con alternativas/procesos alternos en caso de fallas en el software	Requiere de la autorización de la coordinadora de la Universidad. Falta de experiencia en gestión de crisis; limitaciones de tiempo y personal.	4 días	La solución es viable, solo requiere ser aprobada por la coordinadora de la universidad.
Adquisición de un nuevo software contable con soporte continuo y actualizaciones regulares.	La universidad no cuenta con el presupuesto necesario para la adquisición de un nuevo software contable debido a la inversión inicial significativa	Falta de conocimiento técnico para evaluación y selección de software.	1 hora	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Establecer un proceso de revisión periódica de la disponibilidad de soporte y actualizaciones para el software contable actual. Implementar un sistema de alerta para notificar al personal sobre la necesidad de acciones preventivas.	La universidad no cuenta con personal de TI para realizar revisiones periódicas de la disponibilidad de soporte y actualizaciones para el software contable actual	Falta de personal de TI imposibilita las revisiones; dependencia de la respuesta y soporte de los proveedores de software.	5 días	La solución sería viable solo si la Universidad se viera en la necesidad de realizarla y si contrata personal especializado.
Impartir al personal administrativo de la institución un curso sobre cómo crear contraseñas seguras y la importancia del uso de estas para resguardar el acceso de sus cuentas institucionales, así como personales.	La Universidad cuenta con un auditorio donde impartir el curso y los medios para compartir información multimedia de manera digital.	Requiere la autorización de la coordinadora de la Universidad. Se necesita la disponibilidad de tiempo del personal administrativo.	1 hora y media	La solución es viable, solo requiere ser aprobada por la coordinadora de la universidad.
Elaborar de política acerca de la creación de contraseñas seguras e identificador único de uso personal	La universidad cuenta con los recursos para crear una policía acerca de creación de contraseñas seguras y los medios para compartirla	Requiere la autorización de la coordinadora de la Universidad y de personal especializado en el área	5 días	La solución es viable, solo requiere ser aprobada por la coordinadora de la universidad.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Contratar un servicio de capacitación sobre seguridad informática y contraseñas.	La Universidad no cuenta con el presupuesto necesario para contratar el servicio de capacitación	Requiere la autorización de la coordinadora de la Universidad y de personal especializado en el área	1 semana	La solución sería viable solo si la Universidad se viera en la necesidad de realizarla y aumentara o creara el presupuesto designado para esta actividad.
Utilizar un software gratuito de generación de contraseñas y obtener algún curso en línea sobre el tema.	La universidad cuenta con el equipo necesario para instalar el software de generación de contraseñas seguras y los medios para difundir el curso	Requiere de la autorización de la coordinadora de la Universidad y de un equipo dedicado donde todos tendrán que generar sus contraseñas, así como el recordarlas o anotarlas.	1 semana	La solución sería viable solo si la Universidad se viera en la necesidad de realizarla.
Realizar un programa de capacitación formal para el personal encargado del manejo de sistemas de seguimiento y apoyo. Esto podría incluir sesiones de inducción que aborden específicamente las políticas y expectativas de seguridad de la organización...	La universidad no cuenta con el presupuesto necesario para establecer un sistema continuo de capacitación	Requiere de la autorización de la coordinadora de la Universidad y personal especializado en el área para la creación de los programas de capacitación	2 semanas	La solución sería viable solo si la Universidad se viera en la necesidad de realizarla y requiere ser aprobada por la coordinadora de la universidad.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
... antes de otorgar acceso a la información o servicios. Además, establecer un sistema continuo de actualización y capacitación para mantener al personal al tanto de las mejores prácticas de seguridad.				
Implementar un plan de acción para mejorar la capacitación del personal que lleva a cabo el proceso de sistemas de seguimiento y apoyo. Esto podría incluir la identificación de lagunas de conocimiento específicas y la implementación de programas de capacitación específicos para abordar esas deficiencias.	La universidad no cuenta con el presupuesto necesario para establecer un sistema continuo de capacitación	Requiere de la autorización de la coordinadora de la Universidad y personal especializado en el área para la creación de los programas de capacitación	1 semana	La solución no es viable.

Tabla 83. Cuadro de evaluación de viabilidad. [Fuente: Elaboración propia]. (Continuación).

Solución Propuesta	Disponibilidad de recursos	Restricciones operativas	Tiempo de ejecución	Viabilidad
Contratar servicios de consultoría especializada en gestión de sistemas de seguimiento y apoyo. Además, incluir acuerdos de soporte técnico y actualizaciones periódicas de seguridad para garantizar un rendimiento óptimo y protección contra amenazas.	La universidad no cuenta con el presupuesto necesario para contratar servicios de consultoría especializada en gestión de sistemas de seguimiento y apoyo.	Debido al requerimiento de un servicio externo y la falta de información sobre el tema sería necesario mucho tiempo y dinero.	2 semanas	La solución no es viable.
Explorar recursos en línea gratuitos relacionados con la capacitación en el manejo de software especializado para sistemas de seguimiento y apoyo. Utilizar plataformas de aprendizaje en línea y recursos educativos gratuitos. Y promover la colaboración entre los propios miembros del personal.	La universidad cuenta con lo necesario para utilizar plataformas de aprendizaje en línea gratuitas, así como los medios de difusión digital para compartirlas.	Requiere la autorización de la coordinadora de la Universidad. Se necesita la disponibilidad de tiempo del personal administrativo.	2 semanas	La solución es viable, solo requiere ser aprobada por la coordinadora de la universidad.

ACTIVIDAD 3.4

Descripción de las propuestas seleccionadas por la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Una vez presentadas las propuestas desarrolladas en la actividad 3.2 y habiendo tomado en cuenta el análisis de viabilidad la institución decide cuales desea implementar para mitigar el riesgo asociado, de tal forma que en esta actividad se busca proporcionar una descripción detallada del porque son elegidas dichas propuestas; para más adelante desarrollar las soluciones elegidas como el plan de reanudación de operaciones.

RESULTADO DE LA ACTIVIDAD

Solución Número 1: Implementación de una Política de Seguridad para resguardar los Activos de TI de los laboratorios de la Universidad.

Debido a la falta de conciencia sobre seguridad informática y el uso inadecuado de los activos de TI tanto de los laboratorios de cómputo como del área administrativa en general, la propuesta de implementar una Política de Seguridad fue considerada una solución adecuada a las amenazas como la infección por ransomware, malware y ataques de phishing que pueden materializarse por vulnerabilidades como la falta de conciencia en seguridad o la adquisición sin cuidado de software no oficial.

Así mismo la Política se pretende focalizar para ser implementada en los laboratorios de cómputo pues la mayor cantidad de activos de TI se encuentra distribuida en ambos laboratorios, además de mencionar que existe la posibilidad de que el descuido del alumnado permita la propagación de un virus, malware o ransomware que llegue hasta los equipos de cómputo del área administrativa a través de la red o por medio de unidades de almacenamiento extraíbles. Por esa razón se redacta una Política de Seguridad con lineamientos que tanto el personal de la Institución como el alumnado debe seguir al pie de la letra o de lo contrario recibirán alguna de las sanciones redactadas en la misma Política.

Solución Número 2: Implementación de un Sistema de Inventarios para los activos de TI.

Tras la presentación de propuestas para mitigar el riesgo de la pérdida total de más de un activo de TI provocado por un incendio eléctrico, que llevaría a un caos administrativo; la institución optó por escoger la opción de la implementación de un Inventario para sus activos de TI, debido a que aparte de mitigar el impacto que significaría que la amenaza de un incendio se materialice, consideraron que el sistema de inventario les sería muy útil para otros propósitos como el tener un mejor control sobre la TI de toda la Universidad. Además, se mencionó que, si bien ya cuentan con un inventario generalizado que provee rectoría, la implementación de un inventario exclusivo para la TI les sería de gran utilidad a mediano y largo plazo permitiéndoles agilizar tareas como remplazo de equipo defectuoso u obsoleto.

Una vez acordado todos los detalles para el desarrollo del software, se procedió con el desarrollo de este utilizando las siguientes tecnologías: Para el desarrollo tanto del front end, como del back end se optó por el lenguaje de programación Java par que el producto sea un programa de escritorio y como motor de base de datos se utilizó SQL Server.

Solución Número 3: Curso para la concienciación sobre la Seguridad Informática.

Debido a la falta de conciencia generalizada en seguridad informática y las amenazas existentes en el mundo informático la Universidad vio como una buena oportunidad la capacitación de todo su personal administrativo respecto al tema, de tal forma que puedan prevenir en mayor medida cualquier incidente de seguridad informática.

Tras la selección de la solución, se procedió a desarrollar como material de apoyo una infografía que abarca el tema “Seguridad Informática”, así como un manual textual donde se expone a profundidad el tema para así poder presentarlo al personal que se busca capacitar. Además de disponer de un instrumento de aprendizaje en forma de un cuestionario en Google Forms para corroborar el conocimiento adquirido.

Solución Número 4: Curso sobre sobre cómo crear contraseñas seguras y su importancia.

Al igual que en la solución anterior, debido a la falta de conocimiento sobre como generar contraseñas seguras por parte del personal administrativo, lo que provoca más de una brecha de seguridad en el acceso de cuentas institucionales, la Universidad vio como una buena oportunidad la capacitación del personal administrativo sobre cómo es la forma correcta para generar contraseñas seguras y la importancia de ello; cabe mencionar esta solución también arregla la baja efectividad de dos sistemas de control evaluados en la actividad 2.9.

Para esta solución se procedió con el desarrollo de un manual informativo donde se expone a profundidad el tema para así poder presentárselo al personal que se busca capacitar; así mismo se genera un instrumento de aprendizaje en forma de un cuestionario en Google Forms para corroborar el conocimiento adquirido.

CAPÍTULO IV. RESULTADOS

OBJETIVO 4. Desarrollar un Plan de Reanudación de Operaciones:
Desarrollar un plan para mantener la continuidad del desempeño de la institución, específicamente en la “gestión del riesgo” y en los puntos anteriores.

ACTIVIDAD 4.1

Redactar un plan de reanudación de operaciones para los procesos críticos.

DESCRIPCIÓN DE LA ACTIVIDAD

Esta actividad consta de la redacción del plan de reanudación de operaciones acorde a las soluciones elegidas por la Universidad vistas y descritas a detalle en la actividad 3.4, donde el entregable consiste en un listado de procedimientos acorde con cada una de las soluciones escogidas por la institución iniciando con un contexto general, para posteriormente seguir con el listado como tal. La estructura inicia con el número del procedimiento, la situación que se busca realizar o resolver, el encargado de efectuarlo y finaliza con el diagrama del proceso, el cual es un diagrama de procedimientos estándar elaborado con la herramienta de diagramado Bizagi.

RESULTADO DE LA ACTIVIDAD

El resultado es el plan de reanudación de operaciones con su propia portada y formato, el cual se ve a continuación:

PLAN DE REANUDACIÓN DE OPERACIONES

UNIVERSIDAD MEXIQUENSE DEL BICENTENARIO TULTITLAN

Ubicación: Avenida Ex Hacienda los Portales SN, Colonia Villa Esmeralda.

Tultitlán, Estado de México. C.P. 54910.

Versión 1.0.0

19/04/2024

HISTORIAL DE VERSIONES				
VERSIÓN	APROBADO POR	FECHA DE REVISIÓN	DESCRIPCIÓN DEL CAMBIO	AUTOR/ES

Introducción

En el presente Plan de Reanudación de Operaciones se abarcan los procedimientos desarrollados para distintas situaciones donde los procesos críticos y la TI asociada se encuentren bajo riesgo, dichos procedimientos fueron redactados con base a las soluciones elegidas por la institución para ser aplicadas, por lo tanto, este plan solo cubre los procesos críticos relacionados a las soluciones elegidas, las cuales son: Una Política de Seguridad, un Sistema de Inventario de TI, un curso para la concienciación sobre la Seguridad Informática y Curso sobre cómo crear contraseñas seguras y su importancia.

Procedimientos para el uso de la Política de Seguridad

Una versión reducida de la política donde se abarcan los lineamientos y sanciones está disponible en la entrada de ambos laboratorios, con un código QR con el enlace a la versión completa digital, para mantener informados tanto al personal docente como al alumnado. Así mismo la versión completa de la política se entregó en formato físico en dirección.

Procedimiento No. 1

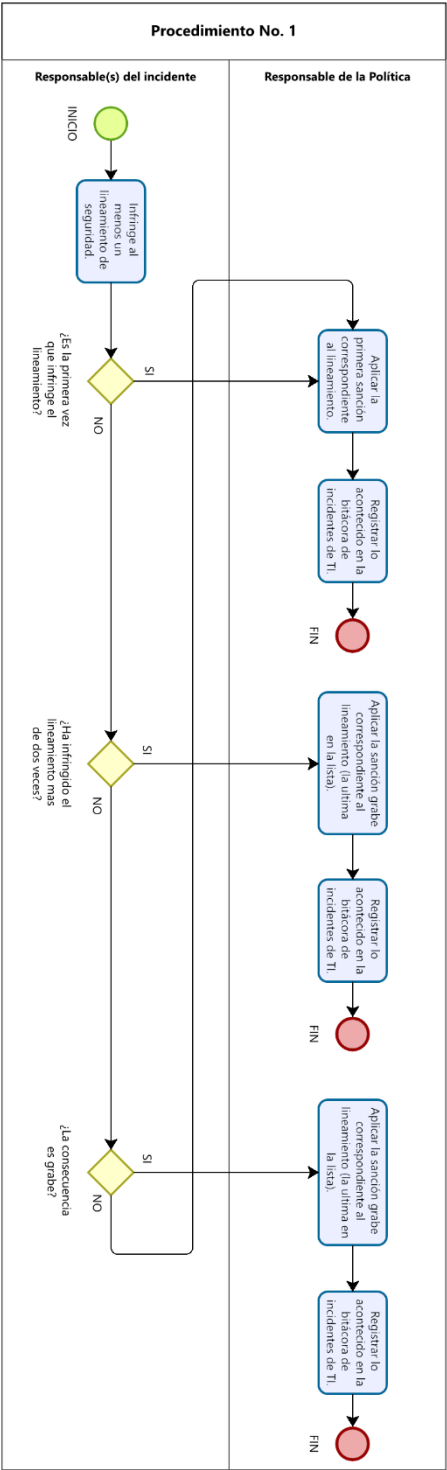
Situación: Incidente provocado intencionalmente.

Descripción: En caso de producirse un incidente que ponga en riesgo a los activos de TI de la institución dentro y fuera de los laboratorios, tales como el daño intencionado, robo, infección por malware por medios de almacenamiento extraíble o incluso inicio de una revuelta dentro de algún laboratorio de cómputo, se deberán de aplicar los lineamientos establecidos por la Política de Seguridad para resguardar los activos de TI y/o sancionar a los responsables de algún incidente ,consultar el diagrama de proceso disponible en la figura 59 para saber cómo proceder. Ir al Anexo F. Propuesta de bitácora de Incidentes de TI, para revisar la propuesta de bitácora de incidentes que se menciona en la figura 59.

Responsable de efectuar el procedimiento: Licenciado José Juan Alvarado.

Diagrama del proceso:

Figura 7. Diagrama de Procedimientos. Proceso No. 1. [Fuente: Elaboración propia].



Procedimiento No. 2

Situación: Presentación a todo el personal de la universidad, el cual consiste en: personal de limpieza, administrativo y docente, así como los prestadores de servicios sobre la implementación de la nueva política de seguridad.

Descripción: Debido a la implementación de la nueva política de seguridad, es necesario presentar a todo el personal de la Universidad y prestadores de servicios, para que sean conscientes sobre los nuevos lineamientos que deberán seguir para mantener un ambiente de seguridad informática adecuado. La capacitación será con la exposición del documento de la política de seguridad proyectada a través del proyector del auditorio o de un salón que cuente con uno. Tal como lo dice el diagrama de proceso en la figura 60, el personal que asista a la capacitación deberá registrarse en la lista de asistencia proporcionada por el responsable del procedimiento, ir al Anexo G. Propuesta de lista de asistencia para la presentación de la Política de Seguridad Informática, para ver la propuesta de lista de asistencia. Esta presentación también debe de realizarse con la llegada de nuevo personal.

Responsable de efectuar el procedimiento: Licenciado José Juan Alvarado.

Diagrama del proceso:

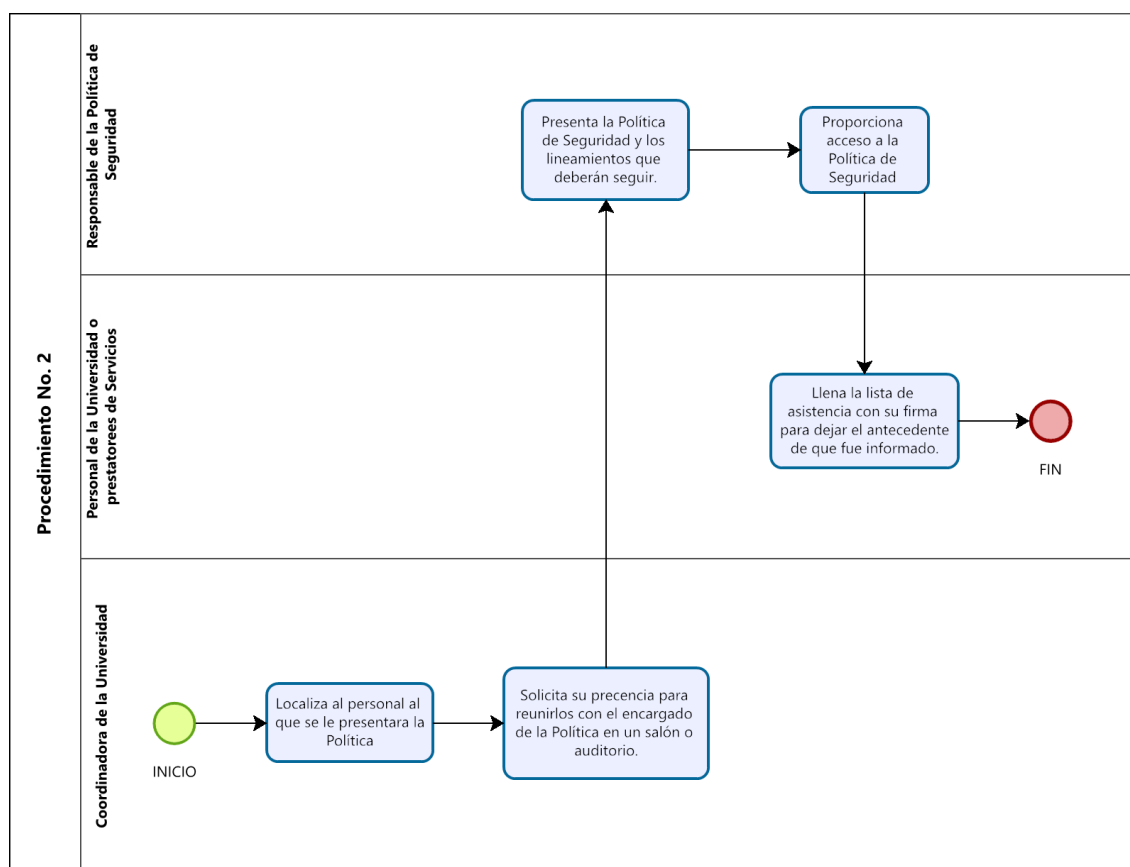


Figura 8. Diagrama de Procedimientos. Proceso No. 2. [Fuente: Elaboración propia].

Procedimientos para la aplicación del curso “Concienciación sobre la Seguridad Informática”

Procedimiento No. 3

Situación: Capacitación requerida para todo el personal administrativo y docente.

Descripción: Este curso tiene como objetivo educar al personal y a los estudiantes sobre las mejores prácticas de seguridad informática, incluyendo reconocimiento de phishing, uso seguro de Internet y protección de datos personales y de la institución. El curso se realizará al inicio de cada semestre académico y se requerirá para todos los nuevos ingresos. La asistencia al curso se registra en una lista de asistencia tal como se marca en el diagrama, ir al Anexo H. Propuesta de lista de asistencia para el curso Concienciación sobre la Seguridad Informática, para ver la propuesta de lista de asistencia.

Responsable de efectuar el procedimiento: Licenciado José Juan Alvarado.

Diagrama del proceso

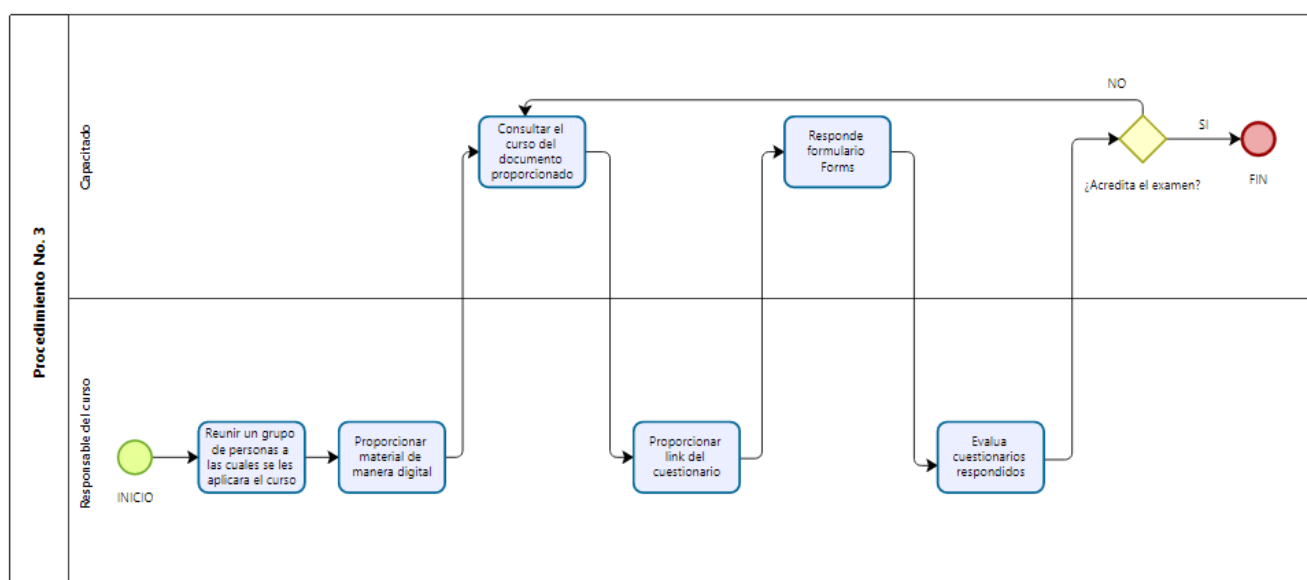


Figura 9. Diagrama de Procedimientos. Proceso No. 3. [Fuente: Elaboración propia].

Procedimientos para la aplicación del curso “Cómo crear contraseñas seguras y su importancia”

Procedimiento No. 4

Situación: Entrenamiento anual obligatorio para fortalecer la seguridad de las credenciales.

Descripción: Este procedimiento detalla la formación anual sobre contraseñas, enfocándose en cómo crear contraseñas robustas, la importancia de no reutilizar contraseñas y la implementación de gestores de contraseñas y autenticación de dos factores. El curso se impartirá a través de una presentación en el auditorio de la Universidad o en un salón que cuente con un proyector y será seguido por una evaluación para asegurar la comprensión del contenido. Se requerirá la finalización exitosa del curso para la renovación anual de acceso a los sistemas de la institución. La asistencia al curso se registra en una lista de asistencia tal como se marca en el diagrama, ir al Anexo I. Propuesta de lista de asistencia para el curso como crear contraseñas seguras y su importancia, para ver la propuesta de lista de asistencia.

Responsable de efectuar el procedimiento: Licenciado José Juan Alvarado.

Diagrama del proceso

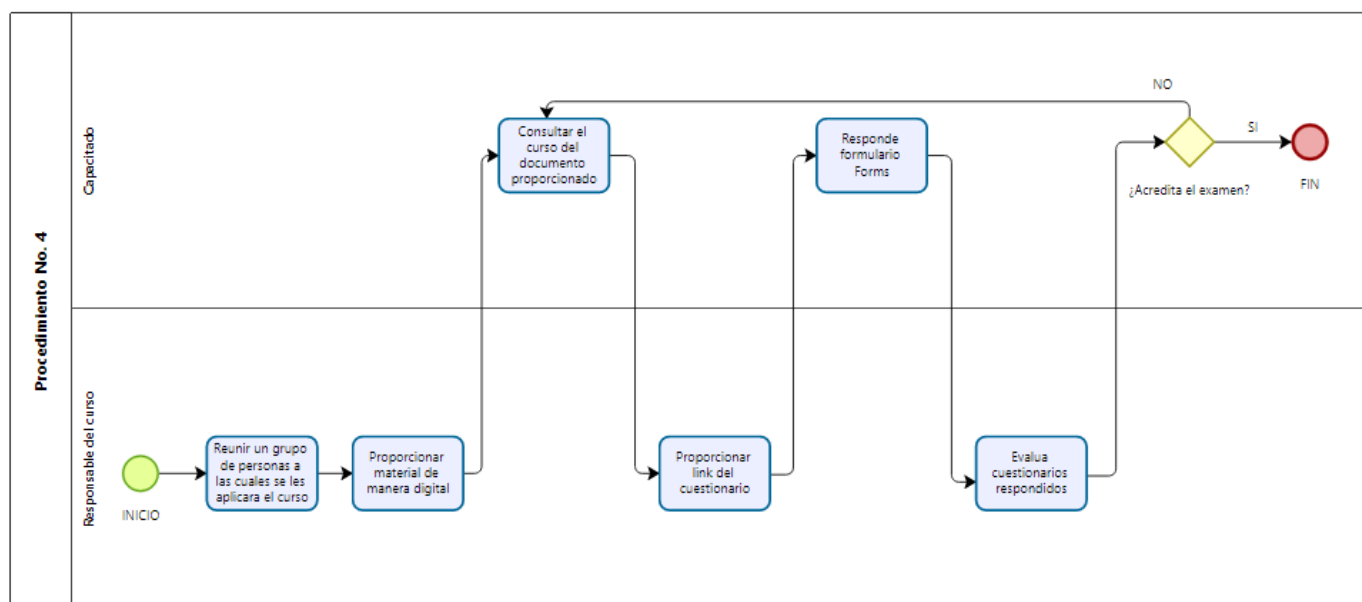


Figura 10. Diagrama de Procedimientos. Proceso No. 4. [Fuente: Elaboración propia].

Procedimientos para manejar el software SIGAIS (Sistema de inventario, gestión activos informáticos y software)

Procedimiento No. 5

Situación: Revisión periódica y supervisión de activos informáticos dentro de la institución educativa.

Descripción: Este procedimiento describe los pasos para que el Administrador del Sistema y el Personal Académico visualicen los activos informáticos asignados a través del sistema de inventario de la escuela. Comienza con el inicio de sesión en el sistema utilizando credenciales verificadas. Una vez dentro del Panel de Control, los usuarios pueden seleccionar la opción "Visualizar Activos" para acceder a una lista detallada de todos los activos informáticos, incluyendo su ubicación, estado y software asociado. El procedimiento permite a los usuarios seleccionar un activo específico para obtener información detallada, promoviendo así la transparencia y la gestión eficiente del inventario. Este proceso es esencial para el mantenimiento actualizado del registro de activos y asegura que los usuarios tengan la información necesaria para el correcto uso y asignación de recursos tecnológicos. La finalización de la visualización de activos es parte de las tareas rutinarias y se lleva a cabo conforme a las políticas de la institución para mantener la integridad y seguridad de la información del inventario.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del Proceso

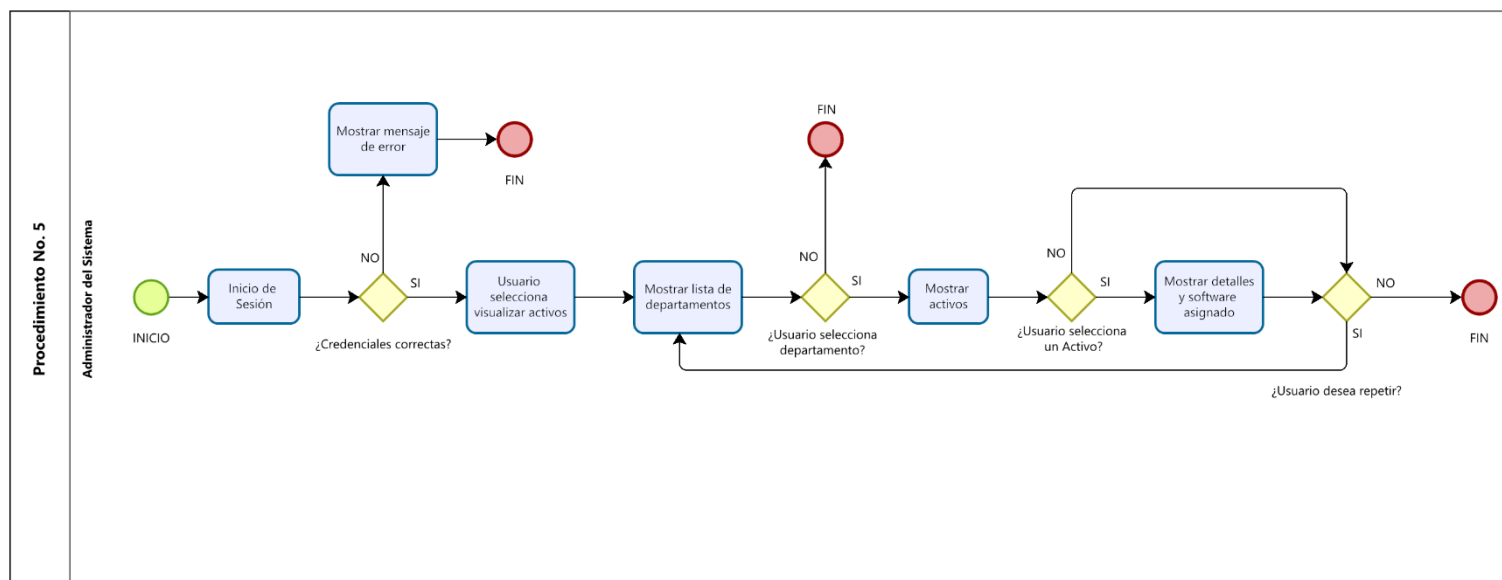


Figura 11. Diagrama de Procedimientos. Proceso No. 5. [Fuente: Elaboración propia].

Procedimiento No. 6

Situación: Incorporación de nuevos activos informáticos al inventario escolar para su administración y seguimiento.

Descripción: Este procedimiento establece la metodología para añadir nuevos activos informáticos al sistema de inventario de la escuela. Tras acceder al sistema con las credenciales adecuadas, el Administrador del Sistema selecciona la opción "Agregar Activo Informático" en el Panel de Control. Se presenta un formulario detallado que el administrador debe llenar, incluyendo toda la información relevante del activo, como marca, modelo, configuración, ubicación y cualquier otra característica pertinente.

Una vez que se completan los detalles del activo y se somete la información, el sistema proporciona una puerta de decisión para confirmar si se procederá a agregar otro activo. Si el usuario elige agregar más, se repite el proceso de llenado del formulario. Este paso puede realizarse tantas veces como sea necesario, permitiendo la adición de múltiples activos en una sola sesión. Si no se requiere agregar más activos, el procedimiento llega a su fin, y los datos del nuevo activo quedan registrados en el sistema.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del proceso

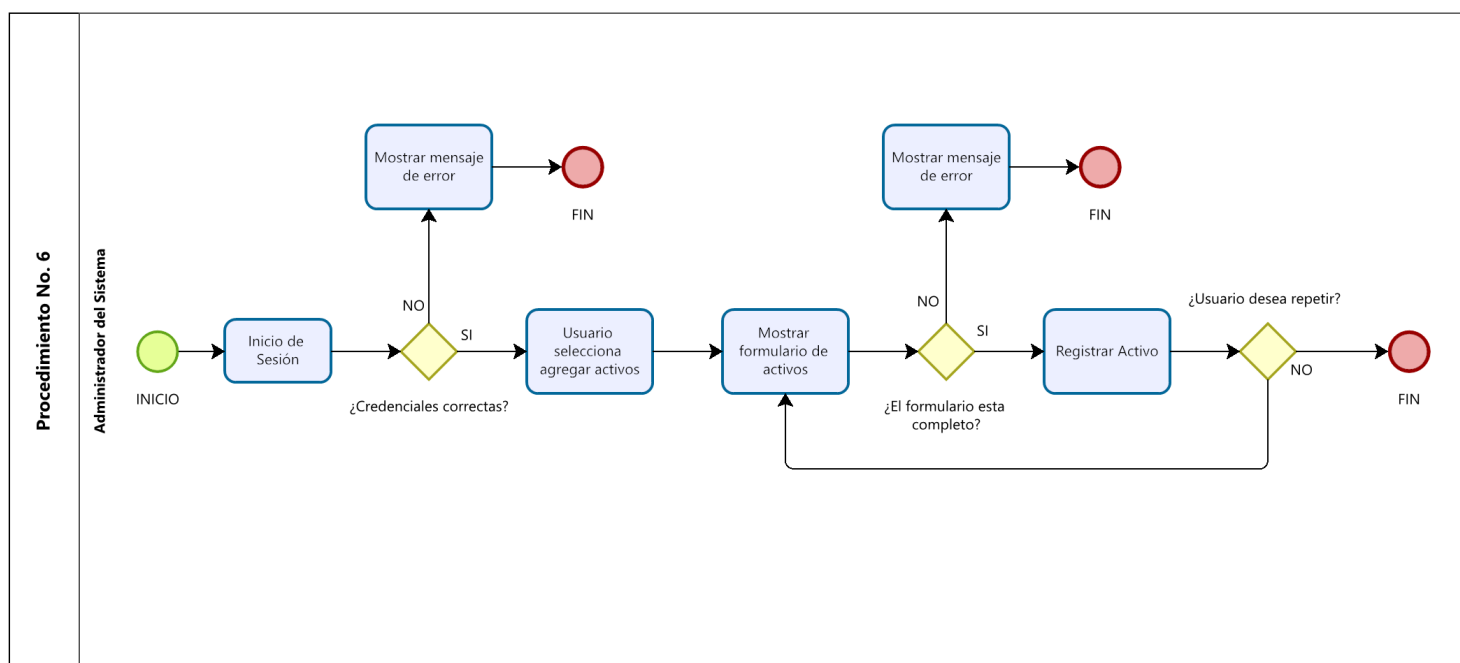


Figura 12. Diagrama de Procedimientos. Proceso No. 6. [Fuente: Elaboración propia].

Procedimiento No. 7

Situación: Eliminación de Activos Informáticos que van a descatalogar

Descripción: Este procedimiento establece la metodología para eliminar activos informáticos al sistema de inventario de la escuela. Tras acceder al sistema con las credenciales adecuadas, el Administrador del Sistema selecciona la opción "Eliminar Activo Informático" en el Panel de Control. Se presenta una tabla con todos los activos, donde deberá de seleccionar el que se desea eliminar.

Una vez que se confirmó que activo se quiere eliminar, el sistema mostrara nuevamente la tabla con todos los activos. Si el usuario elige eliminar más, se repite el proceso. Este paso puede realizarse tantas veces como sea necesario, permitiendo la eliminación de múltiples activos en una sola sesión. Si no se requiere eliminar más activos, el procedimiento llega a su fin, y los datos del nuevo activo quedan registrados en el sistema.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del proceso

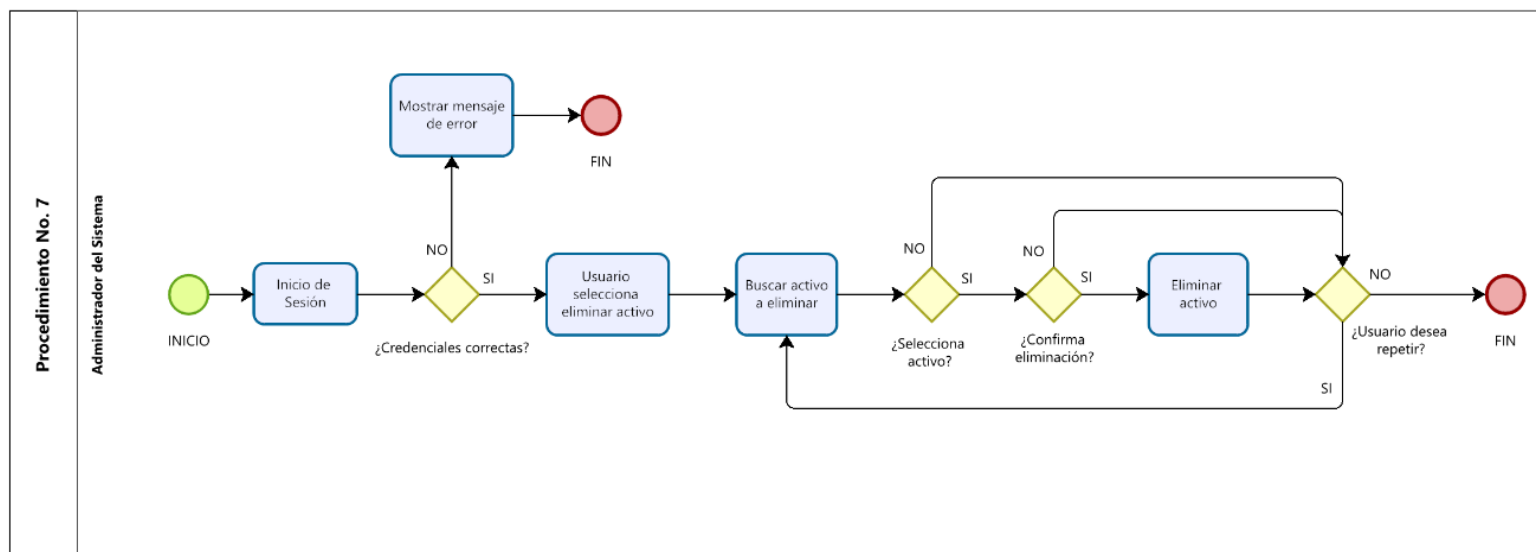


Figura 13. Diagrama de Procedimientos. Proceso No. 7. [Fuente: Elaboración propia].

Procedimiento No. 8

Situación: Incorporación de nuevos activos de Software al inventario escolar para su administración y asignación.

Descripción: Este procedimiento detalla la metodología para registrar nuevos activos de software en el sistema de inventario de la escuela. Tras iniciar sesión con las credenciales correspondientes, el Administrador del Sistema o el jefe de Laboratorios selecciona la opción "Agregar Activo de Software" en el Panel de Control. Se muestra una interfaz para introducir la información relevante del software, incluyendo nombre, versión, tipo de licencia, proveedor y costo.

Después de ingresar los datos del software y someter la información, el sistema ofrece la posibilidad de añadir otro activo de software, facilitando la inclusión de múltiples entradas en una sola sesión. Si el administrador o el jefe de laboratorios opta por continuar, se repite el proceso de ingreso de datos. El procedimiento se completa cuando todos los activos de software requeridos han sido agregados al sistema, quedando registrados para su administración y asignación posterior.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del proceso

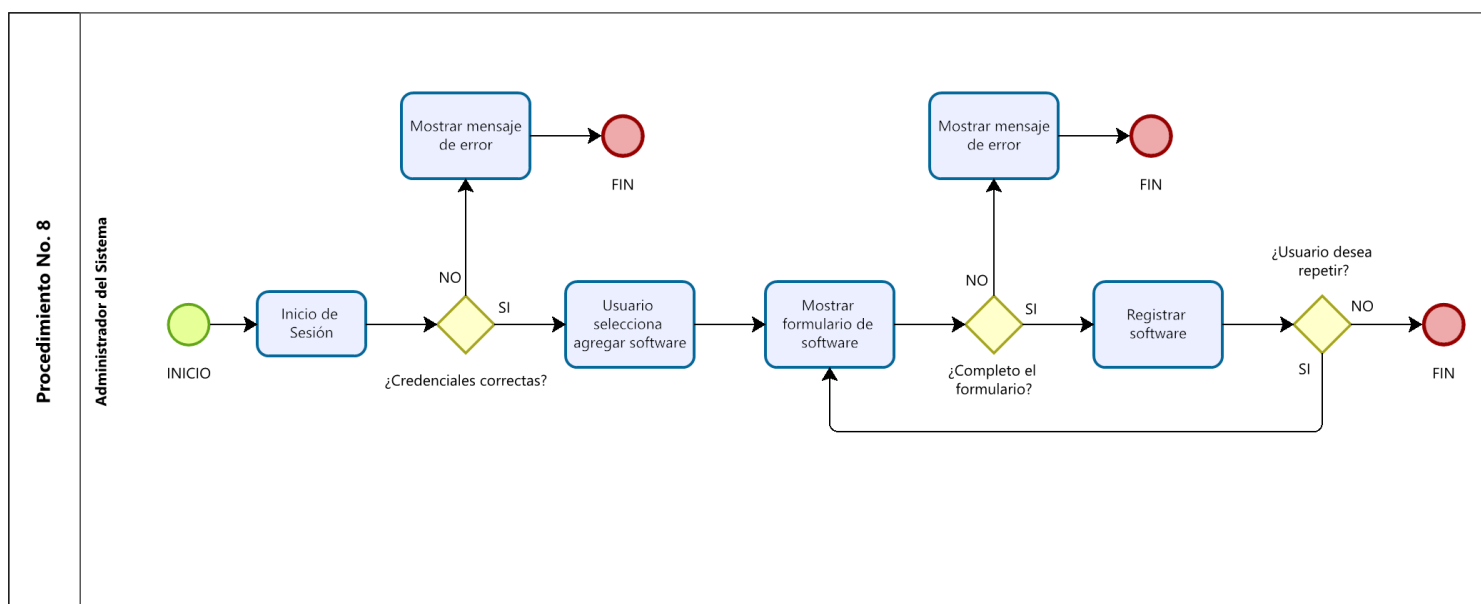


Figura 14. Diagrama de Procedimientos. Proceso No. 8. [Fuente: Elaboración propia].

Procedimiento No. 9

Situación: Mantenimiento actualizado del inventario escolar mediante la retirada de software obsoleto, no utilizado o redundante.

Descripción: Este procedimiento define los pasos para eliminar activos de software del sistema de inventario de la escuela. Tras verificar la identidad con las credenciales adecuadas, el Administrador del Sistema accede al "Panel de Control" y selecciona la opción "Eliminar Activo de Software". A continuación, se busca en el sistema el software específico a eliminar, seleccionándolo de la lista de activos registrados. El administrador procede con la operación de eliminación y el sistema solicita una confirmación para completar el proceso. Si se confirma, el activo de software se elimina del inventario. Este procedimiento puede repetirse tantas veces como sea necesario, permitiendo la eliminación de varios activos de software en una sola sesión. La operación se considera finalizada cuando no hay más activos de software para eliminar, asegurando así que solo los activos de software actuales y necesarios permanezcan en el sistema.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del proceso

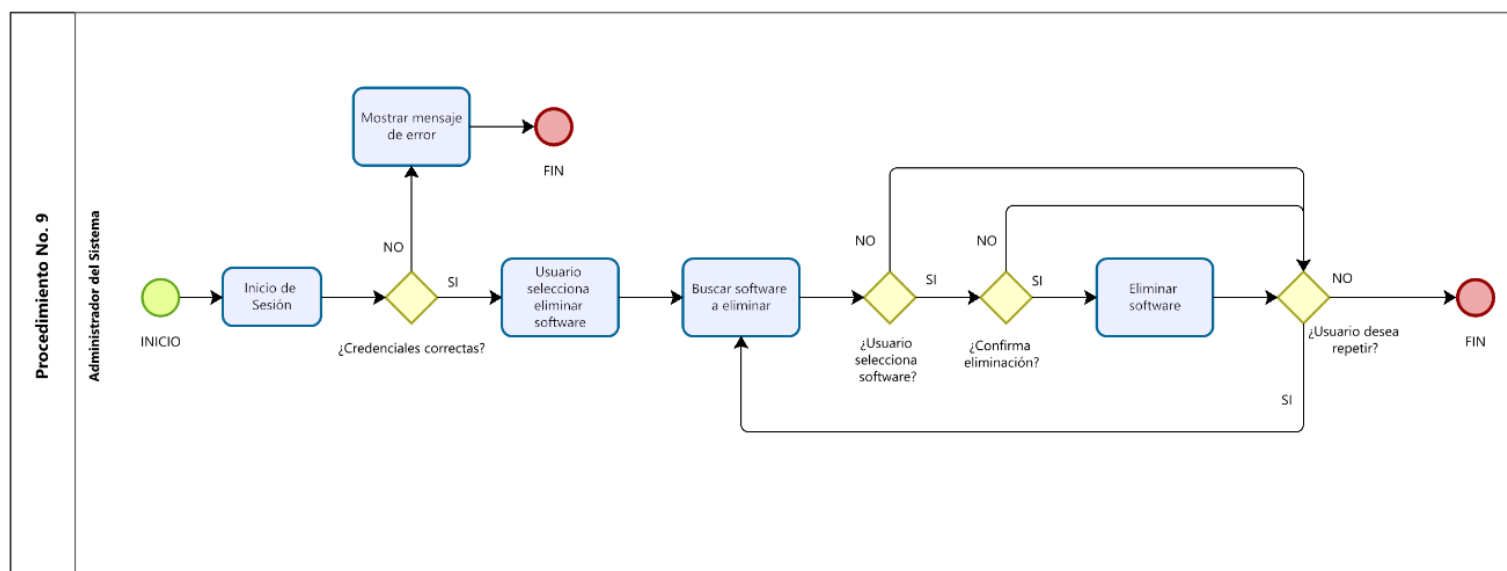


Figura 15. Diagrama de Procedimientos. Proceso No. 9. [Fuente: Elaboración propia].

Procedimiento No. 10

Situación: Gestión y Asignación de software a activos informáticos

Descripción: Este procedimiento detalla la asignación de software a los activos informáticos en el inventario escolar. Una vez dentro del sistema, el Administrador del Sistema o el jefe de Laboratorios selecciona la opción "Asignar Software" desde el Panel de Control. El sistema muestra una lista de software disponible y equipos compatibles. El responsable elige el software y el equipo correspondiente y procede a la verificación y confirmación de la asignación. El proceso permite asignaciones múltiples en una sesión, facilitando la gestión eficaz del software educativo.

Responsable de efectuar el procedimiento: Administrador del Sistema

Diagrama del proceso

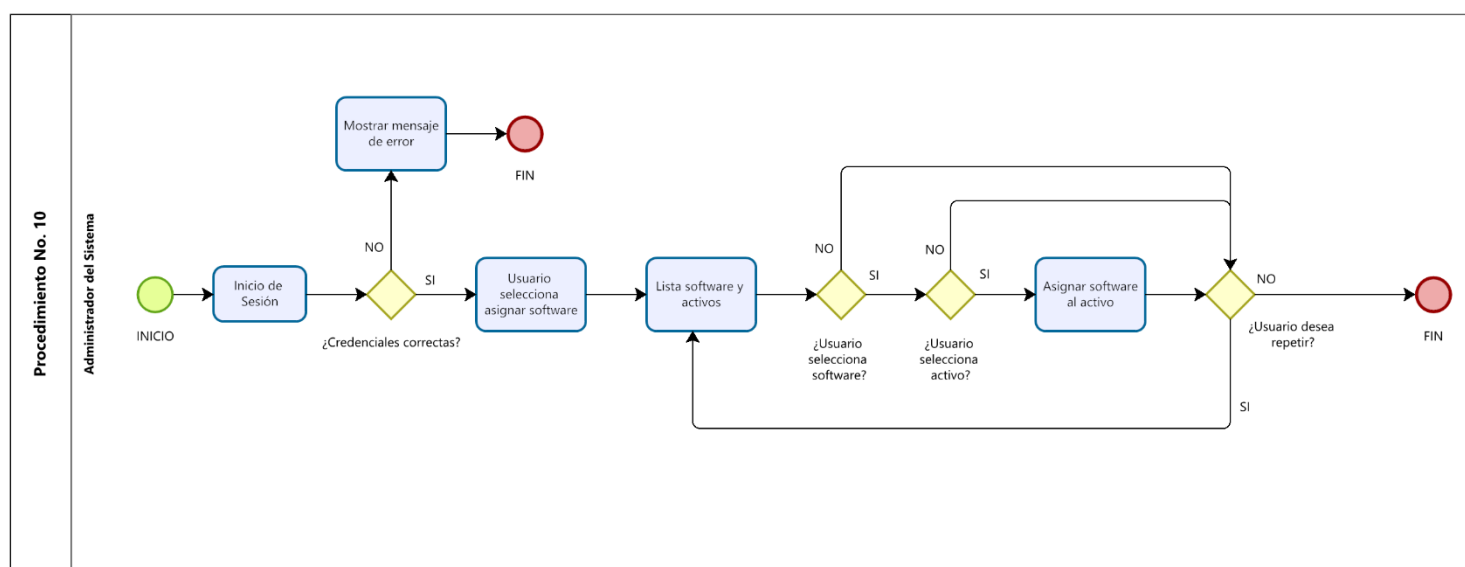


Figura 16. Diagrama de Procedimientos. Proceso No. 10. [Fuente: Elaboración propia].

ACTIVIDAD 4.2

Propuesta de División de Tecnologías de la Información (TI)

DESCRIPCIÓN DE LA ACTIVIDAD

Esta sección propone la creación de una división de TI compuesta por un equipo pequeño pero efectivo. Dicha propuesta es debido a que tras el exhaustivo análisis realizado en los Objetivos 1 y 2 así como el saber que la Universidad carece de un departamento de TI formal se determinó que sería de gran utilidad para la Institución. Su función principal será supervisar, administrar y estructurar los recursos necesarios para mantener y mejorar la gestión de TI en la universidad. Este equipo también será responsable de implementar las recomendaciones del Plan de Continuidad de Negocio, asegurar su adaptación y evolución con el tiempo. Además de mantener actualizada la política, impartir los cursos con el material entregado a la Universidad y darle un uso correcto al sistema que fue desarrollado a la medida.

RESULTADO DE LA ACTIVIDAD

Estructura Elegida: Un equipo de TI conformado por 1 a 3 personas.

Contextualización: La implementación de la división de TI en la Universidad Mexiquense del Bicentenario Tultitlán se realizaría mediante la creación de un equipo dedicado a fortalecer la infraestructura tecnológica y la seguridad de la información. Esta división, inicialmente compuesta por un Gerente de TI, un Técnico de Sistemas y opcionalmente un Analista de Seguridad de TI, se encargará de la supervisión y gestión efectiva de los recursos de TI, así como el desarrollo e implementación de políticas de seguridad.

La creación de este departamento mejorará significativamente la capacidad de la universidad para gestionar sus recursos tecnológicos, proteger datos sensibles, así como responder de manera eficiente ante incidentes de TI.

Roles del nuevo equipo de TI

1. Gerente de TI

El Gerente de TI es un líder estratégico y operativo responsable de supervisar la infraestructura tecnológica de la escuela. Esta posición juega un papel crucial en la planificación, implementación y gestión de soluciones de TI que respaldan los objetivos y operaciones de la escuela. El Gerente de TI debe garantizar que los sistemas de información sean confiables, seguros, eficientes y alineados con las necesidades educativas y administrativas de la institución.

Funciones y Supervisión en la Escuela

El Gerente de TI debe realizar y supervisar una variedad de funciones dentro de la escuela, que incluyen:

1. Gestión Estratégica:

- Desarrollar y ejecutar la estrategia de TI de la escuela en línea con los objetivos educativos y administrativos.
- Planificar y gestionar el presupuesto de TI, asegurando la asignación eficiente de recursos.

2. Supervisión de Infraestructura:

- Supervisar la infraestructura de TI de la escuela, incluyendo hardware, software, redes y sistemas de comunicación.
- Asegurar el mantenimiento regular y las actualizaciones de los sistemas para maximizar su eficiencia y seguridad.

3. Seguridad de la Información:

- Implementar políticas y procedimientos de seguridad de TI para proteger los datos sensibles de la escuela y garantizar la privacidad de los estudiantes y el personal.
- Supervisar las medidas de seguridad, como firewalls, antivirus y protocolos de respaldo y recuperación de datos.

4. Gestión de Proyectos:

- Dirigir y coordinar proyectos de TI, desde la fase de planificación hasta la implementación, asegurando que se completen a tiempo y dentro del presupuesto.
- Trabajar en colaboración con los departamentos académicos y administrativos para comprender sus necesidades y desarrollar soluciones de TI a medida.

5. Soporte y Formación:

- Garantizar que el personal y los estudiantes reciban el soporte técnico necesario.
- Organizar sesiones de formación para el personal y los estudiantes sobre el uso efectivo de las tecnologías y las prácticas de seguridad informática.

6. Innovación y Actualización:

- Mantenerse actualizado sobre las últimas tendencias y avances en tecnología educativa.
- Evaluar e implementar nuevas tecnologías y soluciones de TI para mejorar la experiencia de aprendizaje y administración en la escuela.

Responsabilidades Enumeradas

- Desarrollar y ejecutar la estrategia de TI de la escuela.
- Gestionar el presupuesto de TI y la asignación de recursos.
- Supervisar y mantener la infraestructura de TI de la escuela.
- Implementar políticas y procedimientos de seguridad de TI.
- Dirigir y coordinar proyectos de TI.
- Proporcionar soporte técnico y formación al personal y a los estudiantes.
- Evaluar e implementar nuevas tecnologías y soluciones de TI.

2. Técnico de Sistemas:

El Técnico de Sistemas es un profesional esencial dentro del equipo de TI, encargado de asegurar el correcto funcionamiento, mantenimiento y soporte de la infraestructura tecnológica de la escuela. Este rol implica una amplia gama de responsabilidades técnicas, desde la resolución de problemas de hardware y software hasta el mantenimiento de redes y sistemas. El Técnico de Sistemas trabaja en estrecha colaboración con el Gerente de TI y otros miembros del equipo para garantizar una operación fluida y eficiente de todos los componentes tecnológicos de la institución.

Funciones y Supervisión en la Escuela

Las funciones y responsabilidades del Técnico de Sistemas incluyen:

1. Mantenimiento y Reparación:

- Realizar el mantenimiento preventivo y correctivo de equipos informáticos, incluyendo computadoras, servidores y dispositivos periféricos.
- Diagnosticar y reparar problemas de hardware y software, asegurando un tiempo de inactividad mínimo.

2. Gestión de Redes:

- Mantener y supervisar la infraestructura de red de la escuela, incluyendo routers, switches y puntos de acceso inalámbrico.
- Asegurar una conectividad de red constante y segura para estudiantes, profesores y personal administrativo.

3. Soporte Técnico:

- Proporcionar soporte técnico y asistencia a usuarios con problemas de TI.
- Responder a solicitudes de servicio de manera oportuna y eficiente.

4. Implementación de Sistemas:

- Asistir en la implementación de nuevos sistemas y aplicaciones según las directrices del Gerente de TI.
- Configurar y preparar nuevos equipos y software para su uso en la escuela.

5. Seguridad de Sistemas:

- Colaborar en la implementación de medidas de seguridad, incluyendo la instalación de software antivirus y la realización de copias de seguridad de datos.
- Monitorizar los sistemas para detectar posibles problemas de seguridad y responder a incidentes de TI.

6. Documentación y Registro:

- Mantener registros detallados de problemas técnicos, reparaciones y mantenimiento.
- Documentar procedimientos y soluciones técnicas para referencia futura.

Responsabilidades Enumeradas:

- Realizar el mantenimiento y la reparación de equipos informáticos.
- Mantener y supervisar la infraestructura de red de la escuela.
- Proporcionar soporte técnico y resolver problemas de TI.
- Asistir en la implementación de nuevos sistemas y aplicaciones.
- Colaborar en la implementación y monitorización de medidas de seguridad de TI.
- Mantener una documentación detallada y registros de problemas y soluciones de TI.

3. Analista de Seguridad de TI (opcional)

Este nuevo puesto será desempeñado por un experto en tecnologías de la información y conocimientos generales en seguridad informática, así como auditoría informática; pues será el encargado de garantizar el correcto funcionamiento de los activos de TI de la institución por medio de la implementación de nuevas políticas, supervisión del funcionamiento de las ya implementadas e idealmente la aplicación del plan de continuidad del negocio. Sin embargo, pese a hacer énfasis en la recomendación de este nuevo puesto, este es opcional, pues gran parte de sus responsabilidades podrían ser llevadas a cabo por el Gerente de TI y el Técnico de Sistemas.

Funciones y Supervisión en la Escuela

Las funciones y responsabilidades del Analista de Seguridad de TI incluyen:

1. Manejo del plan de continuidad del negocio:

- Aplicación de plan de continuidad del negocio para garantizar la total operabilidad de la institución.
- Actualizar el plan de continuidad del negocio para seguir garantizando un grado razonable de seguridad.

2. Aplicación y Redacción de políticas de seguridad informática:

- Garantizar que las políticas de seguridad informática con las que cuenta la institución sean respetadas y seguidas al pie de la letra.
- Redacción de nuevas políticas de seguridad o actualización de las ya existentes en la medida en la que se requiera.

3. Supervisión de la red de la Institución:

- Supervisión continua del tráfico de red de la institución para evitar cualquier tipo de intrusión.
- Proponer mejoras de seguridad de esta.

4. Propuesta de nuevas medidas de seguridad:

- En la medida en la que sean detectadas nuevas amenazas, proponer la actualización de las medidas de seguridad existentes y la implementación de nuevas.

5. Análisis continuo de nuevas vulnerabilidades:

- Llevar a cabo un análisis periódico de todos los sistemas de la Universidad para la detección de nuevas vulnerabilidades.

Responsabilidades Enumeradas:

- Aplicar los procedimientos descritos en el plan de continuidad del negocio entregado a la institución.
- Redacción de nuevas políticas de seguridad para la institución en la medida en la que se requieran.
- Aplicación de las políticas de seguridad existentes y las que se implementen en la posterioridad.
- Gestión de los recursos de TI, en función de su usabilidad.
- Supervisión del tráfico de red para garantizar la seguridad de esta.
- Proponer nuevas medidas para la mejora continua de la seguridad de los activos de TI de acuerdo con la adquisición de nuevos activos y el surgimiento de nuevas amenazas.
- Análisis continuo sobre las vulnerabilidades existente en la institución y el surgimiento de nuevas con el pasar del tiempo.

Ubicación en el Organigrama: La división de TI se ubicará directamente bajo la dirección general para garantizar la alineación con las estrategias institucionales y una comunicación efectiva.

Mejoras esperadas:

- Gestión eficiente de recursos de TI: Con un equipo dedicado, la universidad podrá administrar mejor sus recursos tecnológicos, alineándolos con las necesidades académicas y administrativas.
- Seguridad de la información: Implementación de políticas y prácticas de seguridad que protejan datos críticos y reduzcan la vulnerabilidad ante amenazas cibernéticas.
- Soporte técnico proactivo: Mejora en la respuesta a incidentes y soporte continuo para usuarios, facilitando la continuidad de las actividades académicas y administrativas.

Proyecciones a futuro:

- Expansión de competencias: La división de TI tendrá la flexibilidad de adaptarse y expandirse según las demandas tecnológicas emergentes y las necesidades institucionales.
- Digitalización y actualización constante: El departamento será clave en la transformación digital de la universidad, manteniendo actualizaciones constantes y adoptando nuevas tecnologías.
- La visión es que este departamento no solo aborde las necesidades actuales, sino que también sea proactivo, anticipando y liderando la evolución tecnológica en la institución, asegurando su posición en el panorama educativo moderno.

OBJETIVO 5. Realizar las Estrategias Propuestas: Implementar un sistema de seguimiento y control para supervisar continuamente las estrategias de la institución y garantizar su efectividad.

ACTIVIDAD 5.1

Redactar una Política de Seguridad Informática orientada a los laboratorios de informática de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

La Política de Seguridad Informática para la Universidad Mexiquense del Bicentenario se redacta con la intención de proteger todos sus activos de TI de las amenazas y riesgos identificados durante la actividad 2.2, por medio de la mitigación algunas de las vulnerabilidades encontradas en la actividad 2.3; esto a través de la composición de una serie de lineamientos que tanto el personal de la Universidad, prestadores de servicios, así como el alumnado deben de respetar.

Así mismo los lineamientos se redactan conforme a lo que se ha ido observando en la institución que puede ser considerado como una mala práctica al momento de manipular los activos de TI, poniéndolos en riesgo; por esa razón se optó por la creación de tres capítulos de lineamientos: el primero donde se abarca el correcto uso del hardware y software dejando en claro lo que se puede y no hacer (como la manipulación inadecuada de periféricos o la instalación de software no autorizado), el segundo en el que se abarca la seguridad física donde se explica el correcto manejo del cableado o la recomendación del uso de bitácoras y por último el capítulo de servicios donde se hacen recomendaciones para el correcto control de los servicios de terceros de los que depende la institución para su correcto funcionamiento.

Sin embargo, debido a que la mayoría de los lineamientos hacen uso de términos que algunas veces pudieran ser muy técnicos para la comprensión de aquellos que no están familiarizados con el mundo de la TI, por esta razón antes del primer capítulo de opto por la implementación de un glosario donde dichos términos son definidos en un contexto general pero comprensible para los lectores.

Posterior al capítulo tres, continua el capítulo cuatro referente a personas donde se propone la asignación del personal para la ejecución de la política, además de enlistar las nuevas responsabilidades para el personal de la Universidad y para los prestadores de servicios para mantener un ambiente relativo de seguridad.

Finalmente, en el capítulo cinco se redactan las sanciones que recibirá tanto el personal como el alumnado y prestadores de servicios en caso de hacer caso omiso a los lineamientos de los

dos primeros capítulos; para dichas sanciones se toma como apoyo el reglamento actual de la institución. Así mismo para hacer más sencilla la aplicación de la política y evitar la necesidad de buscar la sanción que corresponde al lineamiento, en el último renglón del lineamiento se incluye la sanción correspondiente, sin embargo, para verla completa es necesario bajar hasta el capítulo de sanciones.

El resultado de esta actividad es una Política de Seguridad Informática de cinco capítulos y 28 páginas incluyendo la portada.

Dicha Política de Seguridad Informática ya fue aprobada por la Universidad estando a la espera de ser implementada eventualmente. Ir al Anexo J. Evidencia de la implementación de los productos seleccionados, para revisar como fueron implantados los productos elegidos y donde se encuentran dentro de la Universidad.

RESULTADO DE LA ACTIVIDAD

A continuación, se ve un lineamiento extraído de la política, el cual es el tercer lineamiento del capítulo sobre seguridad física, si se desea revisar el resto de los lineamientos, sanciones y el contenido de la política en general, ir al Anexo K. Política de Seguridad Informática.

Lineamiento:

El alumnado no deberá acceder a recursos o configuraciones a los que no se tenga autorización: Este lineamiento implica que los alumnos deben respetar los límites de acceso y no intentar acceder a recursos o configuraciones para los cuales no tienen autorización. Alumno(a) al que se le sorprenda incumpliendo el lineamiento será acreedor de la sanción 2.3 del Capítulo V. Sanciones.

Esencialmente el lineamiento se compone de tres partes: El lineamiento en si donde se acara lo que se debe o no hacer (remarcado en amarillo), la descripción completa del lineamiento donde se explican los límites y excepciones (marcado en verde) y la consecuencia por incumplir el lineamiento que es ligada a la sanción correspondiente (marcado de rojo).

Así mismo, la sanción correspondiente al lineamiento que se explicó anteriormente es la siguiente:

Sanción 2.3:

- Amonestación verbal: En caso de que se detecte a un alumno desinstalando o manipulando software sin autorización, se le dará una amonestación verbal. Esto servirá como un recordatorio inmediato de la importancia de respetar el software instalado por las autoridades correspondientes y de informar cualquier problema o duda al personal encargado.

- Restricción de acceso a los equipos: Si el incumplimiento persiste o se considera grave, se puede aplicar una restricción de acceso a los equipos del laboratorio. Durante un período determinado por el encargado en turno, que no supere los 15 días, al alumno no se le permitirá utilizar los equipos o acceder a ciertos recursos, lo que le recordará la importancia de respetar el software instalado por las autoridades.
- Acciones disciplinarias más severas: En casos graves de manipulación o desinstalación deliberada del software instalado por las autoridades, se pueden aplicar acciones disciplinarias más severas. Esto puede incluir la suspensión permanente del acceso al laboratorio, o levantamiento de un citatorio/reporte con el personal de administración.

Como se puede observar la sanción es dividida en tres apartados (en algunos casos dos), esto es debido a que se contempla la recurrencia en el incumplimiento del lineamiento, es decir, si el infractor continúa haciendo caso omiso al lineamiento la severidad de la sanción aumentara hasta la última de arriba abajo o si el daño ocasionado por no seguir el lineamiento es catastrófico será aplicada directamente la sanción de mayor gravedad.

ACTIVIDAD 5.2

Desarrollar un sistema de inventario para gestionar todos los activos de TI de la institución.

DESCRIPCIÓN DE LA ACTIVIDAD

Debido a que no existe un medio para administrar la TI en la Universidad Mexiquense del Bicentenario, se diseñó y programó un software para poder no solo gestionar la cantidad y tipo de equipos, también sus detalles específicos, ubicación, a quien se asignó y el software instalado.

El propósito de esta actividad es desarrollar un sistema integral de inventario que permita a la institución educativa gestionar eficientemente todos los activos de tecnología de la información (TI), incluyendo hardware, software y dispositivos periféricos.

Como primer paso para generar el programa, se realizó el levantamiento de requerimientos obteniendo los siguiente.

El alcance del proyecto será a únicamente almacenar activos informáticos de la escuela, no equipos personales de docentes o administrativos e incluirá todos los activos de la escuela tanto de laboratorios como de departamentos y salones.

Una vez terminado e implementado el sistema, se espera tener un control absoluto de donde se encuentran, con quien y cuáles son los activos informáticos de la Universidad Mexiquense del Bicentenario.

Requisitos funcionales:

- Registrar activos informáticos: Los activos informáticos a la hora de ser registrados deberán contener información como el tipo de activo, propósito, departamento a donde se asignó, Encargado, marca, ubicación y finalmente el poder agregar información no clasificada de manera adicional, como generalidades del equipo o etiquetado.
- Eliminar activos informáticos: El software deberá tener la capacidad de eliminar equipo descatalogado o con el que ya no se cuente en la institución para evitar datos sin uso dentro de la base de datos.
- Visualizar Activos informáticos: Al momento de entrar al software deberá de haber alguna manera de visualizar los activos informáticos, así como sus características, software asignado si es que se tiene y generalidades no catalogadas.
- Registrar Software: El sistema de inventarios deberá tener la capacidad de registrar nuevo software con el que se cuente, con información suficiente como para distinguirlo de otros similares e información de interés.

- Eliminar Software: El programa deberá de permitir eliminar software con el que ya no se cuente, o que tenga una licencia expirada.
- Asignar Software: Dada la necesidad de mostrar el software asignado en un equipo, el sistema deberá de ser capaz de asignar software a los activos informáticos que sea necesario

De manera adicional, para mantener la seguridad en el sistema y evitar fugas de información o mal uso del propio sistema, se planteó el añadir un control de acceso, para impedir la entrada de usuarios no autorizados o deseados al inventario, esta sugerencia fue aceptada, así que se agregó en el programa.

Requisitos No funcionales:

- El sistema debe de abrir de manera rápida, sin muchos tiempos de espera.
- La paleta de colores debe de ser alusiva a la escuela
- Debe de ser sencillo navegar entre las interfaces
- El sistema debe de ser fácil de entender, sin opciones redundantes.
- Tiene que poder ejecutarse en equipos con capacidad limitada
- Debe de contar escalabilidad si es que se agregan nuevos departamentos, activos o tipos de equipo.
- Deberá de asignar el ID de manera automáticamente para cada uno de los ítems

Requisitos de datos:

- El sistema deberá de utilizar una base de datos externa al programa de inventarios: Como petición de la escuela esta deberá de ser gratuita, segura, fácil de escalar, implementar y de modificar si es necesario.

La selección de tecnologías para el desarrollo de un sistema es un paso crucial que define tanto la funcionalidad como la eficiencia del software final. Para garantizar que el sistema de inventario de activos de TI cumpla con los altos estándares de rendimiento, seguridad y usabilidad requeridos, se ha optado por una pila tecnológica robusta y probada. A continuación, se presentan las tecnologías elegidas, cada una cuidadosamente seleccionada por sus características únicas, su compatibilidad con los objetivos del proyecto y su capacidad para proporcionar una experiencia de usuario excepcional.

Tabla 86. Cuadro de las tecnologías utilizadas para el desarrollo del sistema. [Fuente: Elaboración propia].

Tecnología	Razón
JAVA	Portabilidad: Sin importar el sistema operativo que se utilice el software se puede compilar y correr sin necesidad de modificar el código Rendimiento: Dada la optimización de la JVM java ofrece un rendimiento excelente en aplicaciones de este tipo. Popularidad: Debido a la popularidad de este lenguaje de programación, será más fácil para la universidad encontrar personal para actualizar o modificar el software si llegara a ser necesario más a futuro. Rendimiento: Java es el lenguaje de programación por excelencia para acceso a servicios de bases de datos por la fiabilidad y alto rendimiento que ofrece con bases de datos robustas.
SQL Server 2019	Rendimiento y escalabilidad: SQL está diseñado para manejar cargas de trabajo grandes y ofrecer una escalabilidad excepcional, lo cual es crucial para un sistema de inventario que puede crecer y evolucionar con el tiempo. Integración con herramientas de desarrollo: SQL server se integra a la perfección con distintas herramientas de desarrollo, en este caso en concreto ofrece conectividad mediante la librería JDBC Costo: La versión de SQL express 2019 es gratuita por lo que no generara un costo para la universidad. Rendimiento: Para un volumen de datos como el que se espera manejar en el inventario de activos de software de una universidad, la ejecución de los servicios de SQL en segundo plano y la búsqueda de datos se hará de manera rápida y eficiente en prácticamente cualquier equipo de cómputo con especificaciones medias/bajas.

Diseño:

Los colores para este software fueron extraídos directamente del logo y página web de UMB siendo estos:

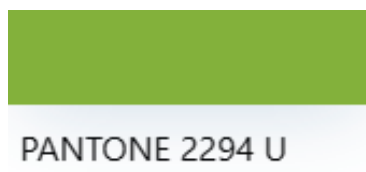


Figura 17. Color. #86B13A: Dark moderate green. [Fuente: Colorxs (2023)].

PANTONE P 15-1 C

Figura 18. Color. #EEE1C8; Light grayish orange. [Fuente: Colorxs (2023)].

Base de datos: Para la base de datos se decidió este diseño con 11 tablas, 9 conectadas entre sí y 2 sin conexión alguna que es donde se guardaran los datos para la autenticación de usuarios y los PDF de inventario.

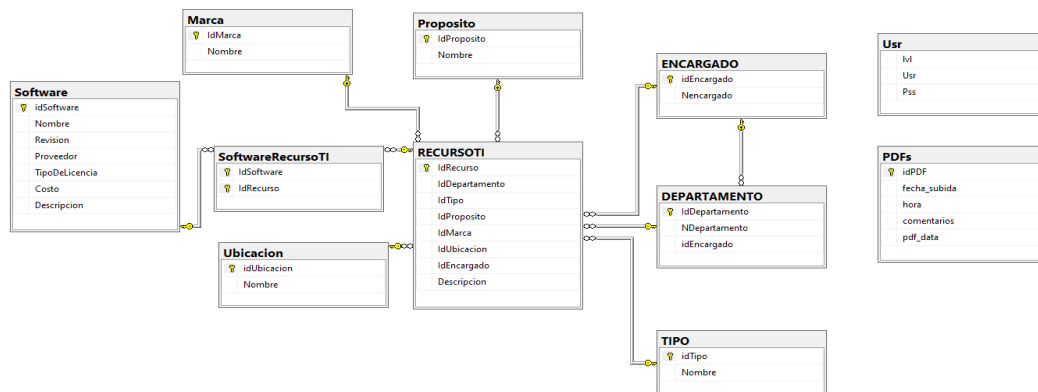


Figura 19. Diagrama de la Base de Datos en SQL Server Managment Studio. [Fuente: Elaboración propia].

El enfoque buscado en esta base de datos es tomar como principal objeto el recurso de TI que es el que almacena datos como marca, departamento, encargado, tipo, ubicación y propósito, aunque a la hora de mostrar los datos en el programa se va a mostrar por departamento, realmente el ítem principal es el recurso de TI.

Para el desarrollo de este software se empleó la metodología “Extreme Programming (XP)”:

- Planificación y Recopilación de Requerimientos: Interacción directa y continua con los usuarios para entender y documentar las necesidades del sistema de inventario.
- Diseño Iterativo y Desarrollo: Implementación iterativa con mejoras continuas, adaptándose a los cambios de requerimientos a través de la retroalimentación frecuente.
- Programación en Parejas y TDD: Uso de programación en parejas y Desarrollo Orientado a Pruebas para asegurar la calidad y precisión del software desde el inicio.
- Integración Continua y Entregas Frecuentes: Integración y pruebas regulares del sistema, con entregas periódicas para validar funcionalidades y adaptarse rápidamente a la retroalimentación.

- **Comunicación Cara a Cara y Retroalimentación del Cliente:** Fomento de la comunicación directa y regular entre desarrolladores y usuarios, priorizando la colaboración y la comprensión clara de los objetivos.

Para la fase de despliegue y mantenimiento, se esperan las indicaciones de la directora para implementar el software en la escuela, sin embargo, el sistema ya fue aprobado para ser desplegado; ir al Anexo F. Evidencia de aceptación de los productos propuestos, para ver la carta de aceptación de los productos redactada y firmada por la institución. Siguiendo los principios de XP, el sistema será mantenido y mejorado continuamente basándose en la retroalimentación y las necesidades emergentes de los usuarios y la institución.

RESULTADO DE LA ACTIVIDAD

En esta actividad, se llevará a cabo el diseño e implementación de un sistema de inventario de TI personalizado. Este sistema proporcionará funcionalidades clave, como la autenticación segura de usuarios, una interfaz de panel de control intuitiva, y la capacidad de realizar tareas críticas de gestión de inventario, tales como:

Visualización de Activos: Permitirá a los usuarios autorizados visualizar un listado completo de los activos de TI, con detalles como ubicación, estado y especificaciones técnicas.

Registro de Activos: Facilitará la inclusión de nuevos activos de TI en el sistema mediante formularios detallados, asegurando que toda la información relevante sea capturada y almacenada de manera estructurada.

Eliminación de Activos: Permitirá eliminar activos que se encuentren descatalogado o que simplemente ya no se cuente con ellos a disponibilidad del inventario escolar.

Asignación de Software: Proporcionará herramientas para asignar licencias de software a los equipos correspondientes, manteniendo un registro actualizado de las asignaciones y disponibilidad de software.

Registro de Software: Permitirá registrar software en el inventario para posteriormente asignarlo a un equipo y usuario.

Eliminación de software: Ayudará al mantenimiento actualizado del inventario escolar mediante la retirada de software obsoleto, no utilizado o redundante.

Pantallas del Software

Inicio de Sesión: En esta ventana el Administrador ingresa su Usuario y contraseña, si alguna de las dos está equivocada saltara un mensaje de error, al estar correcto saltara a la siguiente pantalla. Dependiendo el nivel administrativo que tenga el usuario, entrará ya sea al panel de control de user o de admin, primero se verá el panel de control de user.

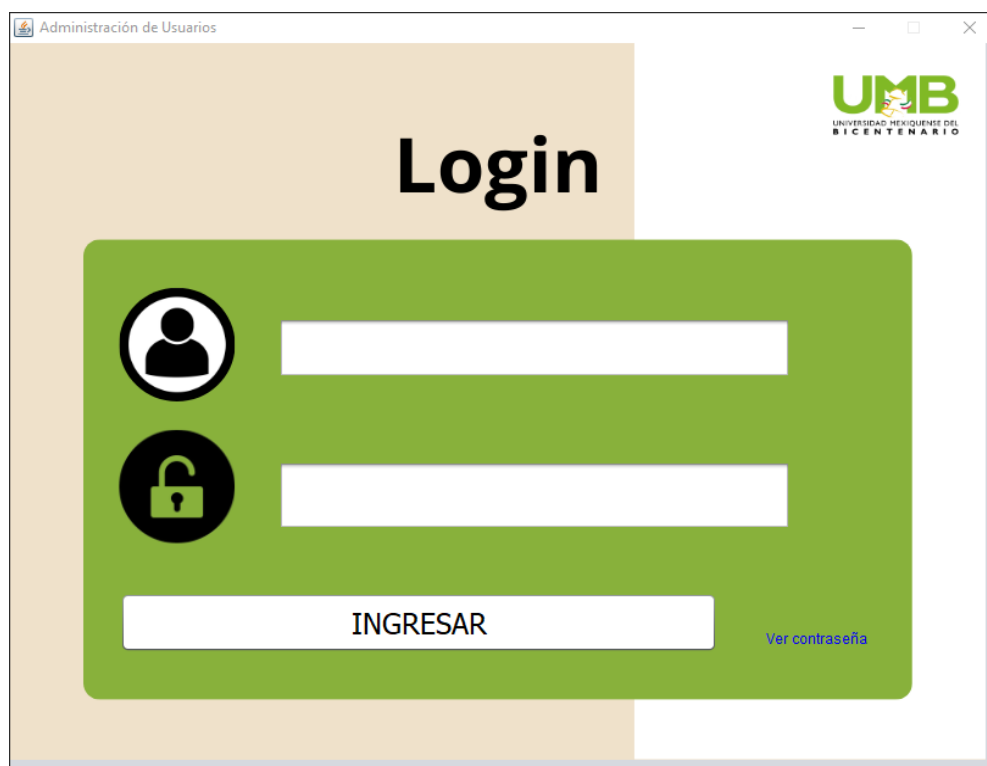


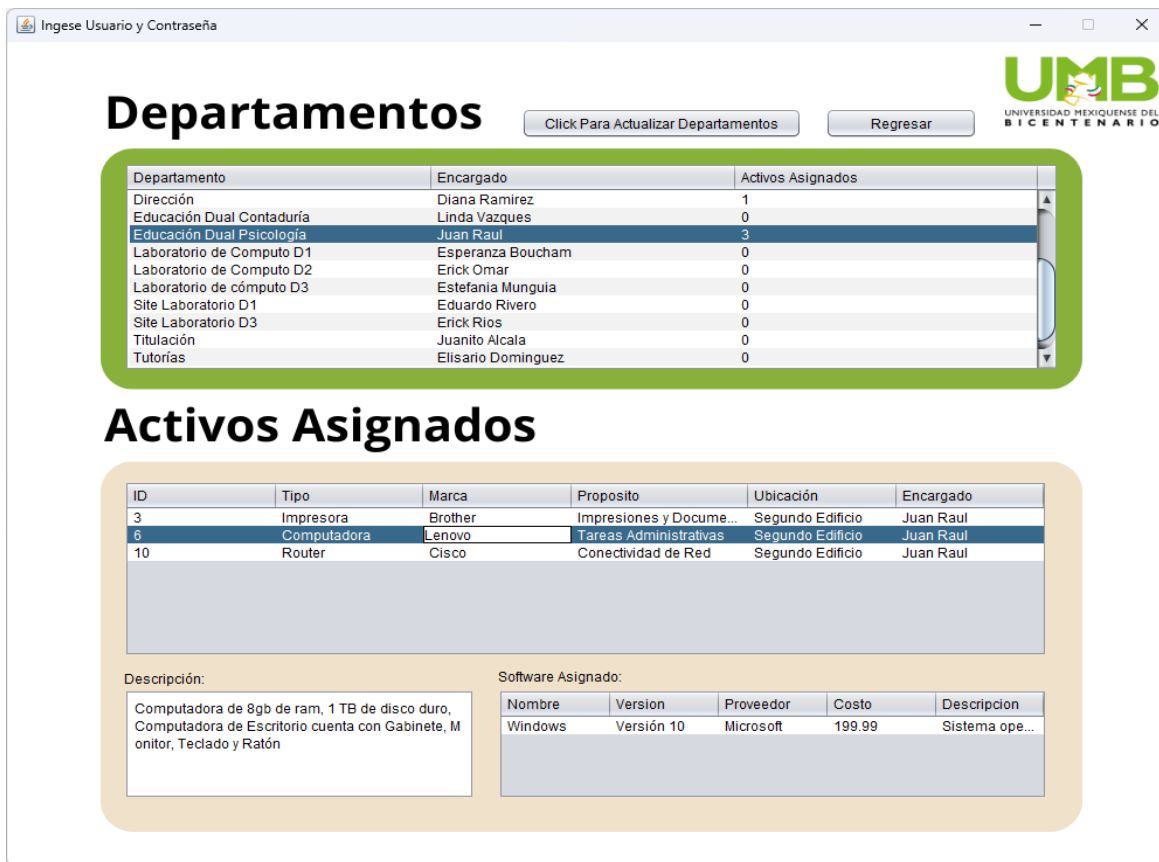
Figura 20. Ventana de Inicio de Sesión. [Fuente: Elaboración propia].

Panel de Control: Aquí se permite seleccionar la actividad a realizar en el software, con solo dar clic en el botón con el nombre de proceso deseado para ejecutar.



Figura 21. Ventana del Panel de Control. [Fuente: Elaboración propia].

Visualizar (Activos informáticos): Permite visualizar en la primer tabla todos los departamentos de la escuela, su encargado y finalmente la cantidad de activos asignados; al dar clic a un departamento mostrará la tabla de “Activos asignados” todos los activos que tiene asignados ese departamento, mencionando el tipo, marca, propósito, ubicación y encargado de cada uno; al dar clic a un activo se mostrara en descripción, generalidades que no se pudieron mencionar en la tabla de activos y en la tabla de “software Asignado” se mostrara todo software que tenga asignado el activo seleccionando, mostrando datos como nombre, versión, proveedor, costo y descripción.



The screenshot shows a web application window titled 'Ingreso Usuario y Contraseña'. The main content area is divided into two sections: 'Departamentos' and 'Activos Asignados'.

Departamentos Section:

Departamento	Encargado	Activos Asignados
Dirección	Diana Ramirez	1
Educación Dual Contaduría	Linda Vazquez	0
Educación Dual Psicología	Juan Raul	3
Laboratorio de Computo D1	Esperanza Boucham	0
Laboratorio de Computo D2	Erick Omar	0
Laboratorio de cómputo D3	Estefania Munguia	0
Site Laboratorio D1	Eduardo Rivero	0
Site Laboratorio D3	Erick Rios	0
Titulación	Juanito Alcala	0
Tutorías	Elisario Dominguez	0

Activos Asignados Section:

ID	Tipo	Marca	Proposito	Ubicación	Encargado
3	Impresora	Brother	Impresiones y Docume...	Segundo Edificio	Juan Raul
6	Computadora	Lenovo	Tareas Administrativas	Segundo Edificio	Juan Raul
10	Router	Cisco	Conectividad de Red	Segundo Edificio	Juan Raul

Below the 'Activos Asignados' table, there are two sub-sections:

Descripción:

Computadora de 8gb de ram, 1 TB de disco duro, Computadora de Escritorio cuenta con Gabinete, Monitor, Teclado y Ratón

Software Asignado:

Nombre	Version	Proveedor	Costo	Descripcion
Windows	Versión 10	Microsoft	199.99	Sistema ope...

Figura 22. Ventana de Visualización de los Activos. [Fuente: Elaboración propia].

Registrar (Activos informáticos): En esta pestaña mediante barras de opciones se llenarán los datos del activo informático y cuenta únicamente con una barra de escritura libre que es “Descripción” donde se anotan generalidades que no se pudieron abarcar con la opción múltiple anterior, se puede continuar repitiendo el proceso las veces que haga falta.

Registro Activo Informático

UMB
UNIVERSIDAD HERIQUENSE DEL
BICENTENARIO

Registro de Activo Informático

Departamento	Tipo
Encargado	Ubicación
Marca	Proposito

Registrar Activo Regresar

Figura 23. Ventana para Registrar un Activo. [Fuente: Elaboración propia].

Eliminar (Activos Informáticos): En esta pestaña se cuenta con una búsqueda inteligente, donde se ingresa el nombre del encargado y en tiempo real van apareciendo los activos que tiene asignados, para eliminar un activo se tiene que seleccionar, posteriormente dar clic en el botón “Eliminar Activo Seleccionado” y después de aceptar un aviso se eliminara el activo, se puede continuar repitiendo el proceso las veces que haga falta.



Panel de Control

Eliminación de Activo Informático Regresar Eliminar Activo Seleccionado

Busqueda inteligente por Encargado:

ID	Departamento	Tipo	Marca	Proposito	Ubicacion	Encargado	Descripción
3	Educación D...	Impresora	Brother	Impresiones ...	Segundo Edif...	Juan Raul	Impresora m...
6	Educación D...	Computadora	Lenovo	Tareas Admin...	Segundo Edif...	Juan Raul	Computadora...
10	Educación D...	Router	Cisco	Conectividad ...	Segundo Edif...	Juan Raul	Router cisco ...

Figura 24. Ventana para Eliminar un Activo. [Fuente: Elaboración propia].

Agregar (Software): En esta pestaña se llenan manualmente los campos requeridos y posteriormente se da clic en el botón “agregar”, se puede repetir este proceso las veces que haga falta para registrar los softwares necesarios.



The image shows a web application window titled "Registro De Software". Inside, there is a section titled "Agregar Software". To the right of this title are two buttons: "Regresar" and "Agregar". Further right is the logo of the "UMB" (Universidad Mexicana del Bicentenario). Below the title and buttons is a green-bordered form with six input fields arranged in two columns. The left column contains fields for "Nombre", "Revision", and "Proveedor". The right column contains fields for "Tipo de Licencia", "Costo", and "Descripción".

Nombre	Tipo de Licencia
Revision	Costo
Proveedor	Descripción

Figura 25. Ventana para Agregar un Activo. [Fuente: Elaboración propia].

Asignar Software: En esta pestaña con búsqueda inteligente en tiempo real en ambos lados se tiene que seleccionar el software a asignar, después el equipo al que se quiere asignar, posteriormente dar clic en el botón “asignar”, el proceso se puede repetir las veces que haga falta con cada software.

The screenshot shows a web application window titled "Asignar". In the top right corner, there is a "Regresar" button and the UMB logo (Universidad Michoacana del Bicentenario). The main area is divided into two sections: "Software Busqueda Inteligente" and "Equipo Busqueda Inteligente".

Software Busqueda Inteligente Table:

ID	Nombre	Version	Costo
1	Windows	Versión 10	199.99
3	Cisco IOS	Versión 15.7	299.99
4	Cisco IOS	Versión 16.8	349.99

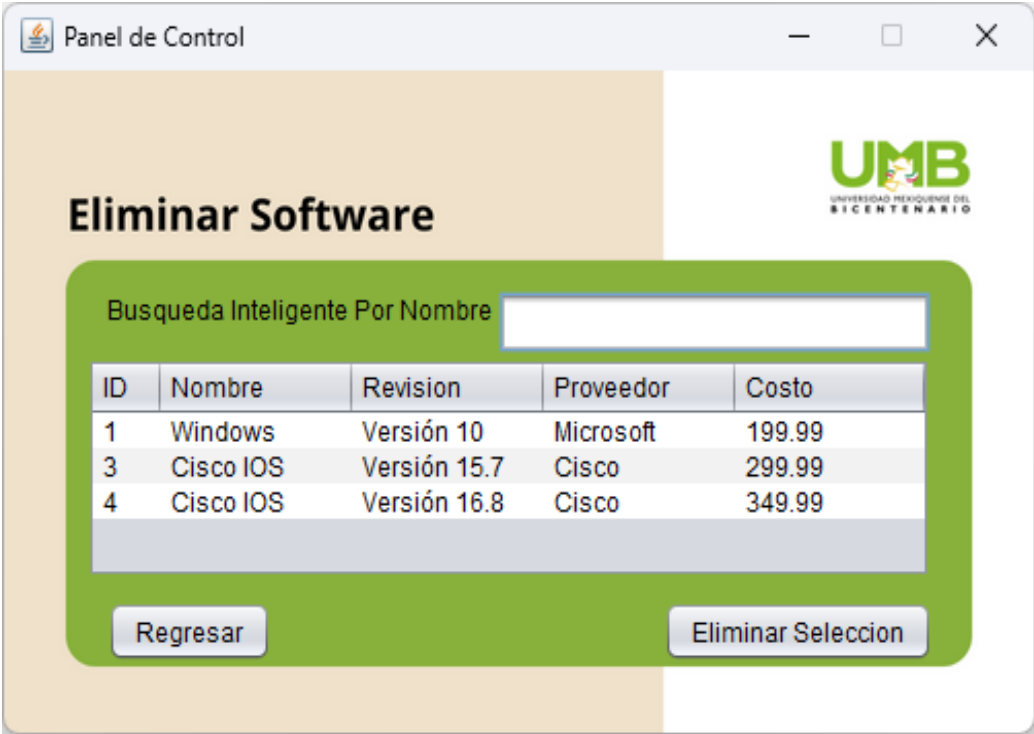
Equipo Busqueda Inteligente Table:

ID	Encargado	Departamento	Tipo	Descripción
2	Esmeralda Dias	Dirección	Router	Router
3	Juan Raul	Educación Dual...	Impresora	Impresora multi...
7	Darius Garcia	Control Escolar	Computadora	Computadora c...
8	Esmeralda Dias	Coordinación A...	Computadora	Compu esmer...
10	Juan Raul	Educación Dual...	Router	Router cisco co...

Between the two tables is an "Asignar" button. Arrows indicate the flow from the software table to the equipment table and back. At the bottom, a instruction box says: "Seleccione un Software, posteriormente el equipo a asignar y finalmente pulse 'Asignar'".

Figura 26. Ventana para Asignar un Software a un Activo. [Fuente: Elaboración propia].

Eliminar (Software): En esta pestaña se cuenta con una búsqueda inteligente, donde se ingresa el nombre del software, para eliminar uno se tiene que seleccionar, posteriormente dar clic en el botón “Eliminar Software” y después de aceptar un aviso se eliminara el activo, se puede continuar repitiendo el proceso las veces que haga falta.



Panel de Control

Eliminar Software

Busqueda Inteligente Por Nombre

ID	Nombre	Revision	Proveedor	Costo
1	Windows	Versión 10	Microsoft	199.99
3	Cisco IOS	Versión 15.7	Cisco	299.99
4	Cisco IOS	Versión 16.8	Cisco	349.99

Figura 27. Ventana para Eliminar un Software de un Activo. [Fuente: Elaboración propia].

Panel de Control de Admin: Aquí se permite seleccionar la actividad a realizar en el software, con solo dar clic en el botón con el nombre de proceso deseado para ejecutar.



Figura 28. Ventana Panel de Control de Admin. [Fuente: Elaboración propia].

Registro múltiple: En esta pestaña mediante una lista seleccionable, se escogerá el tipo de registro que se quiere llenar, posteriormente se escribirá en el único campo disponible el nombre a asignar, para finalizar, se dará click en registrar.



Figura 29. Ventana para Registro Múltiples de Activos. [Fuente: Elaboración propia].

Eliminar múltiple: En esta pestaña mediante una lista seleccionable, se escogerá el tipo de registro que se quiere quitar, posteriormente en una tabla se mostraran los registros disponibles para ese tipo de dato y se dará click al que se desea eliminar, para finalizar, se dará click en Eliminar Selección.

Eliminar Multiple

¿Qué Desea Eliminar? Proposito De Activo

ID	Nombre

Eliminar Selección **Regresar**

Figura 30. Ventana para Eliminar Múltiples de Activos. [Fuente: Elaboración propia].

Asignar Departamento: En esta pestaña con búsqueda inteligente en tiempo real en ambos lados se tiene que seleccionar el departamento a asignar, después el encargado al que se quiere asignar, posteriormente dar clic en el botón “asignar”, el proceso se puede repetir las veces que haga falta con cada departamento.

Asignar Departamento

Regresar

Departamentos

ID	Departamento

Encargados

ID	Nombre De Encargado

Asignar

Figura 31. Ventana para Asignar Departamento. [Fuente: Elaboración propia].

Al finalizar esta actividad, la institución contará con una herramienta centralizada para la gestión de activos de TI que mejorará la eficiencia operativa, reducirá los riesgos asociados con la gestión de activos y proporcionará una visión clara de los recursos tecnológicos disponibles. Esto se traduce en una mejor planificación de recursos, optimización de las inversiones en TI y un soporte más eficaz a las funciones educativas y administrativas de la institución. Ir a el Anexo (Letra) para revisar la carta de aceptación del Sistema por parte de la Universidad.

Plazo de Ejecución:

El desarrollo del sistema de inventario está programado para completarse en el transcurso de 3 semanas, con fases periódicas de revisión y pruebas para asegurar la calidad y la funcionalidad del sistema antes de su lanzamiento oficial.

ACTIVIDAD 5.3

Desarrollar un curso para la concienciación sobre la Seguridad Informática.

DESCRIPCIÓN DE LA ACTIVIDAD:

Este curso está diseñado para ofrecer una visión completa y accesible de los fundamentos de la seguridad informática. A lo largo de la sesión, los participantes se familiarizarán con conceptos clave como la protección de datos sensibles, la identificación y prevención de amenazas comunes como el malware y el phishing, así como la importancia de adoptar prácticas de navegación y gestión de la información seguras y responsables.

El contenido del curso se ha estructurado para ser claro y comprensible, asegurando que todos, independientemente de su nivel de conocimiento previo en informática, puedan comprender y poner en práctica las medidas de seguridad recomendadas. El curso no solo proporcionará una base teórica sólida, sino que también incluirá ejemplos prácticos, demostraciones y ejercicios interactivos para reforzar el aprendizaje y la aplicación práctica de los conceptos discutidos.

Objetivo del Curso:

El objetivo principal de este curso es fortalecer la conciencia sobre la seguridad informática dentro de la Universidad, equipando al personal encargado de TI con conocimientos y herramientas esenciales. A su vez, estos conocimientos se transmitirán al resto del personal y al alumnado, fomentando una cultura de seguridad y precaución en el manejo de la información y los recursos tecnológicos de la institución.

El curso abarcará los siguientes temas clave:

- **Importancia de la Seguridad Informática:** Entender por qué la protección de la información es crucial en nuestro contexto actual.
- **Protección de Datos Sensibles:** Aprender a identificar datos sensibles y aplicar medidas para protegerlos.
- **Prevención de Malware y Phishing:** Reconocer las amenazas comunes y aprender estrategias para evitarlas.
- **Prácticas Seguras de Navegación y Gestión de la Información:** Adoptar hábitos que minimicen los riesgos de seguridad en la navegación web y el manejo de la información.

Al finalizar el curso, los participantes estarán mejor preparados para reconocer y enfrentar los riesgos de seguridad informática, proteger sus datos y contribuir a un entorno educativo más seguro y protegido.

Revisar el Anexo F. Evidencia de la implementación de los productos seleccionados, donde se pudo visualizar la lista de asistencia propuesta con los nombres del personal administrativo que tomo el curso.

RESULTADO DE LA ACTIVIDAD

5 tips para la seguridad informática

- 1 Proteger los datos
- 2 Evitar el Malware
- 3 Ser consciente de las amenazas
- 4 Hacer copias de seguridad de los datos
- 5 Mantener los sistemas actualizados



*Figura 32. Material del Curso. Imagen de apoyo para el curso de Concienciación sobre la Seguridad informática.
[Fuente: Elaboración propia].*

Seguridad informática



La seguridad informática es la protección de los sistemas informáticos, la información y los datos: de accesos no autorizados, uso indebido, alteraciones, destrucción o pérdida.



1 Proteger los datos

Los datos son la base de cualquier negocio, por lo que es importante protegerlos de cualquier acceso no autorizado. Esto se puede hacer mediante el uso de contraseñas seguras, firewalls y otros métodos de seguridad.

2 Evitar el malware

El malware es un software malicioso que puede dañar o destruir los datos de un sistema informático. Es importante tener un software antivirus actualizado para proteger el sistema contra el malware.





3 Ser consciente de las amenazas

Es importante estar al tanto de las últimas amenazas de seguridad informática para poder protegerse de ellas. Esto se puede hacer leyendo las noticias sobre seguridad informática y siguiendo las recomendaciones de expertos en informática.

4 Hacer copias de seguridad de los datos

Es importante hacer copias de seguridad de los datos regularmente en caso de que se pierdan o se corrompan. Esto se puede hacer mediante el uso de un servicio de almacenamiento en la nube o una unidad de almacenamiento portátil.





5 Mantener los sistemas actualizados

Es importante mantener los sistemas actualizados con las últimas actualizaciones de seguridad para protegerse de las nuevas amenazas. Como puede ser mantener el sistema operativo en uso siempre actualizado.

¿Porque es importante?

Es importante conocer acerca de la seguridad informática pues esta permite proteger la privacidad y la confidencialidad de nuestra información en un entorno cada vez más conectado.



Figura 33. Material del Curso. Infografía sobre Seguridad Informática. [Fuente: Elaboración propia].



Cuestionario Seguridad "Informatica"

Aplicar los conocimientos adquiridos gracias al curso de **Seguridad Informatica** impartido en UMB Plantel Tultitlan.

saullazoplata@gmail.com [Cambiar de cuenta](#)



No compartido

* Indica que la pregunta es obligatoria

¿Qué es la seguridad informática? *

1 punto

- ☐ Proteger la información de ataques maliciosos.
- ☐ Instalar programas de edición de texto.
- ☐ Optimizar el rendimiento de la computadora.
- ☐ Ninguna de las anteriores.

¿Qué es un virus informático? *

1 punto

- ☐ Un programa que mejora el rendimiento de la computadora.
- ☐ Un tipo de ataque que roba información personal.
- ☐ Un programa diseñado para replicarse y dañar archivos.
- ☐ Un componente de hardware de una computadora.

Figura 34. Material del Curso. Prueba de Aprendizaje sobre el curso para la Concienciación sobre la Seguridad Informática. Parte 1. [Fuente: Elaboración propia].

¿Qué es la autenticación de dos factores (2FA)? *

1 punto

- ☐ Un método para acceder a cuentas en línea con una sola contraseña.
- ☐ Un método para verificar la identidad mediante dos pasos distintos.
- ☐ Un tipo de ataque informático.
- ☐ Un programa de edición de imágenes.

¿Qué es el ransomware? *

1 punto

- ☐ Un tipo de software antivirus.
- ☐ Un programa para mejorar el rendimiento de la computadora.
- ☐ Un tipo de malware que bloquea el acceso a archivos o sistemas y exige un rescate.
- ☐ Una herramienta de edición de videos en línea.

¿Por qué es importante estar al tanto de las actualizaciones de seguridad? *

1 punto

- ☐ Porque hacen que la computadora funcione más lento.
- ☐ Porque pueden corregir vulnerabilidades que podrían ser explotadas por los hackers.
- ☐ Porque aumentan el riesgo de ataques cibernéticos.
- ☐ Porque no tienen impacto en la seguridad de la computadora.

Enviar **Borrar formulario**

Este contenido no ha sido creado ni aprobado por Google. [Denunciar abuso](#) - [Términos del Servicio](#) - [Política de Privacidad](#)

Google Formularios

Figura 35. Material del Curso. Prueba de Aprendizaje sobre el curso para la Concienciación sobre la Seguridad Informática. Parte 2. [Fuente: Elaboración propia].

Para revisar el material completo, ir al Anexo L. Curso de Concienciación sobre Seguridad Informática.

ACTIVIDAD 5.4

Desarrollar un curso para la creación de contraseñas seguras y su importancia.

DESCRIPCIÓN DE LA ACTIVIDAD:

Este curso proporciona una comprensión integral de cómo las contraseñas seguras actúan como una línea de defensa esencial contra el acceso no autorizado y las brechas de datos. A través de una combinación de teoría y práctica, los participantes aprenderán la importancia de crear contraseñas robustas, los métodos para generarlas y las estrategias para gestionarlas de manera segura.

El contenido del curso se presenta de manera clara y accesible, asegurando que todos los participantes, independientemente de su experiencia previa en informática, puedan comprender y adoptar las prácticas recomendadas. Además de proporcionar una base teórica, el curso incluirá ejemplos prácticos, simulaciones y ejercicios interactivos para reforzar el aprendizaje.

Objetivo del Curso:

El propósito de este curso es destacar la importancia crítica de las contraseñas seguras en la protección de la infraestructura tecnológica de la universidad y concienciar al personal y al alumnado sobre cómo sus acciones individuales pueden influir en la seguridad informática general. La sesión está diseñada para equipar a la persona encargada de TI con los conocimientos y herramientas necesarios para fomentar prácticas robustas de creación y manejo de contraseñas en toda la institución.

Los temas clave del curso incluirán:

- **Importancia de las Contraseñas Seguras:** Comprender por qué una contraseña segura es fundamental en la protección de la información y los sistemas de la universidad.
- **Principios de Creación de Contraseñas Seguras:** Aprender los componentes de una contraseña segura, incluyendo longitud, complejidad y unicidad.
- **Herramientas y Técnicas para Contraseñas Seguras:** Explorar el uso de gestores de contraseñas y otras herramientas para crear y gestionar contraseñas de manera eficiente y segura.
- **Prácticas de Manejo de Contraseñas:** Discutir estrategias para mantener la seguridad de las contraseñas, como la regularidad en el cambio de contraseñas y la precaución en su compartición.

Al concluir el curso, los participantes estarán capacitados para implementar y promover prácticas de contraseñas seguras, contribuyendo significativamente a la seguridad informática de la universidad. La meta es cultivar una comprensión profunda de la importancia de las contraseñas seguras y asegurar que esta comprensión se traduzca en acciones que fortalezcan la postura de seguridad de toda la institución.

Revisar el Anexo F. Evidencia de la implementación de los productos seleccionados, donde se puede visualizar la lista de asistencia propuesta con los nombres del personal administrativo que tomó el curso.

RESULTADO DE LA ACTIVIDAD

5 tips para crear contraseñas seguras

- 1 Evitemos usar la misma contraseña para todas nuestras cuentas
- 2 No usemos contraseñas predecibles
- 3 Evitemos usar vocales
- 4 Usemos iniciales de frases para nuestras contraseñas
- 5 Procuremos implementar la autenticación en dos factores



Figura 36. Material del Curso. Imagen de apoyo para el curso de creación de contraseñas seguras y su importancia.
[Fuente: Elaboración propia].



UNIVERSIDAD MEXIQUENSE DEL
BICENTENARIO



UMB Tultitlán

Cuestionario "Contraseñas Seguras"

Aplicar los conocimientos adquiridos gracias al curso de **Contraseñas Seguras** impartido en UMB Plantel Tultitlán.

sauillazoplata@gmail.com [Cambiar de cuenta](#) 

 No compartido

* Indica que la pregunta es obligatoria

¿Por qué es importante tener contraseñas seguras? *

1 punto

- ☐ Para hacer que sea más fácil recordarlas.
- ☐ Para evitar que otras personas accedan a tus cuentas.
- ☐ Para aumentar la velocidad de la conexión a Internet.
- ☐ Ninguna de las anteriores.

¿Cuál de las siguientes contraseñas es más segura? *

1 punto

- ☐ "123456".
- ☐ "contraseña".
- ☐ "P@ssw0rd!".
- ☐ "miNombre123".

Figura 37. Material del Curso. Prueba de Aprendizaje sobre el curso para la Creación de Contraseñas Seguras y su Importancia. Parte 1. [Fuente: Elaboración propia].

☐ Una herramienta para crear contraseñas simples.

☐ Un programa diseñado para recordar tus contraseñas por ti.

☐ Una medida de seguridad que protege tus contraseñas.

☐ Un tipo de ataque informático.

¿Por qué es importante evitar el uso de información personal en tus contraseñas? ★ 1 punto

☐ Porque la información personal es fácilmente accesible para los hackers.

☐ Porque la información personal no tiene relación con la seguridad de las contraseñas.

☐ Porque es más fácil recordar contraseñas que contienen información personal.

☐ Porque el uso de información personal hace que las contraseñas sean más seguras.

¿Cuál de las siguientes afirmaciones es cierta sobre las contraseñas temporales o desechables? 1 punto

☐ Son contraseñas que nunca expiran.

☐ Son contraseñas que solo se pueden usar una vez.

☐ Son contraseñas que no necesitan ser seguras.

☐ Son contraseñas que se comparten públicamente en línea.

Enviar Borrar formulario

Este contenido no ha sido creado ni aprobado por Google. [Denunciar abuso](#) - [Términos del Servicio](#) - [Política de Privacidad](#)

Google Formularios

Figura 38. Material del Curso. Prueba de Aprendizaje sobre el curso para la Creación de Contraseñas Seguras y su Importancia. Parte 2. [Fuente: Elaboración propia].

Para más detalles sobre el curso ir al Anexo M. Curso para la Creación de Contraseñas Seguras y su Importancia.

CONCLUSIONES

Tras la finalización de este proyecto los objetivos establecidos al inicio del documento fueron alcanzados satisfactoriamente; empezando por la adquisición de información para conocer la estructura de TI así como los procesos ejecutados por la institución, seguido del análisis de impacto donde se determinaron los procesos críticos, para continuar con el análisis de riesgo que sirvió para identificar los activos de TI más vulnerables de los que dependen muchos procesos críticos, posteriormente la generación de propuestas de soluciones de las cuales la Universidad procedió con la elección de cuatro soluciones las cuales fueron desarrolladas e implementadas junto con un plan de reanudación de operaciones y una propuesta para la creación de un departamento de TI para que este mismo se encargue de efectuar el plan de reanudación de operaciones además de manejar correctamente los productos entregados.

Cabe resaltar que durante el desarrollo de este proyecto aquellos que lo llevaron a cabo pudieron poner en práctica una amplia variedad de competencias desarrolladas durante la carrera, principalmente aquellas correspondientes con la especialidad de auditoría en seguridad informática, junto con habilidades blandas como la comunicación clara y el trabajo en equipo. Lo que permitió poder desempeñar un papel ético, así como profesional durante ejecución del proyecto.

Finalmente la elaboración íntegra del proyecto también permitió a los aspirantes al título de “Ingeniero en Sistemas Computacionales” la adquisición de nuevos aprendizajes desde la profundización en el área de la seguridad informática con el desarrollo de un análisis de impacto y de riesgo tomando datos reales, así como la construcción del plan de continuidad del negocio en sí; pues aunque fue parte del temario de una de las materia de la carrera no se compara en lo absoluto cuando se lleva a la práctica en un ambiente real donde las amenazas, vulnerabilidades así como riesgos son innegables. Evidentemente lo aprendido junto con la experiencia obtenida se convierte en una adquisición valiosa en su formación académica y por sobre todo profesional.

COMPETENCIAS DESARROLLADAS

Materia: Administración de la Función Informática.

Competencias Específicas:

1. Manejo de los fundamentos teóricos de seguridad informática para su aplicación en casos prácticos.

Explicación: Fue desarrollada debido a que para el progreso del proyecto fue necesario la aplicación de los conocimientos teóricos de seguridad informática adquiridos de libros como la “Metodología para el desarrollo de un plan de continuidad del negocio con enfoque al 27001” de Alberto G. Alexander.

2. Uso e interpretación de los lineamientos, estándares y marcos referenciales que complementen el conocimiento de la asignatura.

Explicación: La competencia fue desarrollada debido a que para las soluciones propuestas a la institución fue necesario la interpretación del estándar ISO/IEC 17799.

3. Estructuración de un plan de continuidad del negocio.

Explicación: La competencia de desarrollo debido a que el proyecto fue esencialmente la estructuración de un plan de continuidad del negocio.

4. Proponer medidas de seguridad basadas en lineamientos y estándares actuales.

Explicación: Fue desarrollada debido a que durante el desarrollo de las actividades del objetivo 3 del proyecto fueron propuestas una gran variedad de medidas de seguridad basadas en el estándar ISO/IEC 17799.

Competencias Genéricas

1. Comprende y manipula ideas y pensamientos respecto a la seguridad informática.

Explicación: Fue desarrollada debido a que para la creación de las sugerencias para solucionar los problemas de seguridad de la institución fue necesaria la comprensión de ideas y pensamientos respecto a seguridad informática tanto propios como de distintos autores.

2. Comprende las necesidades del medio ambiente y toma decisiones para resolver la problemática que se le presenta.

Explicación: La competencia se desarrolló debido a que fue necesario comprender las necesidades de la institución con la que se trabajó para poder tomar las decisiones correctas y ayudarlos a crear un ambiente relativo de seguridad.

Materia: Administración de la Seguridad en Comunicaciones

Competencias Específicas:

1. Localiza los principales elementos críticos de la red de una organización y evalúa los principales riesgos de seguridad.

Explicación: Esta competencia fue desarrollada debido a la identificación de más de una amenaza, vulnerabilidad y riesgos; donde algunas fueron respecto a la infraestructura de red de la Universidad.

2. Toma decisiones para elegir las medidas de seguridad más apropiadas ante un determinado escenario de riesgos.

Explicación: La competencia fue desarrollada debido a la creación de sugerencias para solventar los escenarios de riesgo de la red de la Universidad.

FUENTES DE INFORMACIÓN

[Fuente: Alexander (2007)] Alexander, A. G. (2007). *Diseño de un Sistema de Gestion de Seguridad de Información*. Alfaomega.

[Asana, 2023] Asana, Inc. (1 de Febrero de 2023). *Qué es la gestión de riesgos y cómo aplicarla a tu proyecto en 6 pasos*. Asana: <https://asana.com/es/resources/project-risk-management-process>

[Disaster Recovery, 2018] Disaster Recovery. (25 de Abril de 2018). *El Plan de Manejo de Crisis PMC y el Plan de Continuidad de Negocio BCP, puntos clave para una recuperación exitosa*. - SDR México. SDR México: <https://sdr.com.mx/index.php/el-plan-de-manejo-de-crisis-pmc-y-el-plan-de-continuidad-de-negocio-bcp-puntos-clave-para-una-recuperacion-exitosa/>

[IFCR, 2023] IFCR. (2023). *¿Qué es la planificación de contingencias?* Planificación de contingencias: <https://www.ifrc.org/es/nuestro-trabajo/desastres-clima-y-crisis/preparacion-para-desastres/planificacion-contingencias#:~:text=La%20planificaci%C3%B3n%20de%20contingencias%20significa,preparaci%C3%B3n%20de%20las%20Sociedades%20Nacionales>.

[ISO/IEC JTC 1/SC 27, 2005] ISO/IEC JTC 1/SC 27. (2005). *Técnicas de seguridad. Código de prácticas para la gestión de la seguridad de la información*. ISO.

[LISA Institute, 2023] LISA Institute. (2023). *¿Qué es la continuidad de negocio y por qué es importante?* LISA Institute: <https://www.lisainstitute.com/blogs/blog/que-es-continuidad-negocio-importante>

[Martin, 2021] Martin, C. (3 de Septiembre de 2021). *Estándares y normas ISO para mejorar la ciberseguridad*. GlobalSuite Solutions: <https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/>

[Mendoza, 2015] Mendoza, M. Á. (29 de Diciembre de 2015). *Cómo aplicar la resiliencia operativa en infraestructura crítica*. welivesecurity: <https://www.welivesecurity.com/la-es/2015/12/29/resiliencia-operativa-infraestructura-critica/>

[Ortega, 2023] Ortega, C. (18 de Junio de 2023). *Análisis de riesgos: Qué es y cómo realizarlo*. QuestionPro: <https://www.questionpro.com/blog/es/analisis-de-riesgos/>

[Ponce, 2023] Ponce, J. L. (10 de Febrero de 2023). *Auditoría informática: ¿Qué es y cómo hacer una con éxito?* Ikusi: <https://www.ikusi.com/mx/blog/auditoria-informatica/>

[Fuente: Prado (2009)] Prado, D. M. (Junio de 2009). *METODOLOGIA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE*

SEGUIMIENTO EN EL AREA DE TECNOLOGIAS DE LA INOFORMACION.
Ciudad de Mexico, Mexico: Instituto Politecnico Nacional.

- [Prosegur, 2022] Prosegur. (06 de Julio de 2022). *zonapyme.prosegur.es*.
zonapyme.prosegur.es: <https://zonapyme.prosegur.es/seguridad-logica>
- [Redacción KeepCoding, 2022] Redacción KeepCoding. (26 de Septiembre de 2022).
keepcoding.io. *keepcoding.io*: <https://keepcoding.io/blog/que-es-una-vulnerabilidad-informatica/>
- [Riveros, 2020] Riveros, A. (02 de Junio de 2020). *www.ealde.es*. *www.ealde.es*:
<https://www.ealde.es/ataque-amenaza-vulnerabilidad-ciberseguridad/>
- [Riveros, 2023] Riveros, A. (11 de Septiembre de 2023). *Pasos para implementar un plan de continuidad de negocio*. EALDE Business School: <https://www.ealde.es/plan-de-continuidad-de-negocio/>
- [Rojas, 2017] Rojas, J. D. (2017). *Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador*. Ecuador: Quito: Universidad de las Américas.
- [Serafin, 2020] Serafin, M. O. (18 de Junio de 2020). *¿Qué características son clave en un plan de continuidad del negocio?* ITMasters:
<https://www.itmastersmag.com/noticias-analisis/que-caracteristicas-son-clave-en-un-plan-de-continuidad-del-negocio/>
- [Universidad Carlemany, s.f.] Universidad Carlemany. (s.f.).
www.universitatcarlemany.com. *www.universitatcarlemany.com*:
<https://www.universitatcarlemany.com/actualidad/blog/seguridad-informatica-que-es/>
- [Veritas, 2023] Veritas. (2023). *Sobre el RTO: Cómo calcular el RTO y aprovechar los planes de copia de seguridad y recuperación después de un desastre*. Veritas:
<https://www.veritas.com/es/mx/information-center/rto>

ANEXOS

ANEXO A. INVENTARIO DE LOS ACTIVOS DE TI DE LA INSTITUCIÓN.

Tabla 87. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia].

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Dirección	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Tareas Administrativas	Administración
	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Tareas Administrativas	Administración
	Impresora	Impresora	Impresora de circuito de tinta	Impresiones y Documentación	Administración
Control Escolar	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Gestión de Alumnos	Administración
Titulación	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Digitalización de Documentos	Administración
Coordinación Académica	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Coordinación Académica	Administración

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Vinculación, Becas y Servicio Social	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Gestión de Vinculación	Administración
	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Gestión de Servicio Social y Becas	Administración
Laboratorio de Computo D1	Computadora 1	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 2	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 3	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 4	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 5	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D1	Computadora 6	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 7	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 8	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 9	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 10	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 11	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 12	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D1	Computadora 13	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 14	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 15	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 16	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 17	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 18	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
	Computadora 19	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D1	Computadora 20	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D1
Site Laboratorio D1	Computadora (Sistema de Cámaras)	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Monitoreo de Cámaras y Red	Site D1
	Router	Cisco	Dispositivo de abastecimiento de red	Gestión de Red y Conectividad	Site D1
	Switch 1	Cisco	Dispositivo de distribución de red	Conectividad de Red	Site D1
	Switch 2	Cisco	Dispositivo de distribución de red	Conectividad de Red	Site D1
Laboratorio de Computo D2	Computadora 1	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 2	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 3	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 4	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D2	Computadora 5	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 6	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 7	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 8	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 9	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 10	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 11	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D2	Computadora 12	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 13	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 14	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 15	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 16	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 17	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 18	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de Computo D2	Computadora 19	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 20	HP	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 21	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 22	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
	Computadora 23	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Laboratorio de Computo	D2
Site Laboratorio D3	Router	Cisco	Dispositivo de abastecimiento de red	Gestión de Red y Conectividad	Site D3
	Switch 1	Cisco	Dispositivo de distribución de red	Conectividad de Red	Site D3
	Switch 2	Cisco	Dispositivo de distribución de red	Conectividad de Red	Site D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 1	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 2	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 3	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 4	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 5	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 6	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 7	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 8	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 9	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 10	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 11	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 12	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 13	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 14	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 15	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 16	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 17	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 18	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 19	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 20	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 21	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 22	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 23	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 24	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 25	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 26	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 27	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 28	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 29	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 30	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 31	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 32	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 33	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 34	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 35	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 36	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Laboratorio de cómputo D3	Computadora 37	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 38	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 39	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
	Computadora 40	HP	Computadora Todo en 1 (Pantalla y Computadora juntas, Teclado y Ratón)	Laboratorio de Computo	D3
Coordinación Inglés	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Apoyo a la Enseñanza	Primer Edificio
Coordinación Civil	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Documentación de Proyectos	Primer Edificio
Coordinación Química	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Análisis de Muestras	Primer Edificio

Tabla 85. Inventario completo de todos los Activos de TI de la Institución. [Fuente: Elaboración propia]. (Continuación).

Departamento	Recurso de TI	Marca	Descripción	Propósito	Ubicación
Coordinación de Licenciatura en Contaduría	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Registro y Análisis Contable	Primer Edificio
Coordinación de Licenciatura en Psicología Industrial	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Análisis de Datos Psicológicos	Primer Edificio
Educación Dual Psicología	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Soporte a Programas de Educación Dual	Segundo Edificio
Educación Dual Contaduría	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Soporte a Programas de Educación Dual	Segundo Edificio
Tutorías	Computadora	Lenovo	Computadora de Escritorio (Gabinete, Monitor, Teclado y Ratón)	Apoyo a Programas de Tutorías	Segundo Edificio

ANEXO B. CARTA DE JUSTIFICACION DE LA AUSENCIA DE EVIDENCIA DE LOS SISTEMAS DE CONTROL.



Figura 39. Carta de justificación de la ausencia de evidencia de los sistemas de control. [Fuente: Elaboración propia].

ANEXO C. EVIDENCIAS DEL SISTEMA DE CONTROL NÚMERO 3. USO DE UN ACCESS POINT PARA EXTENDER LA RED EXISTENTE POR WIFI.



Figura 40. Sistema de Control Número 3. Evidencia 1. Salida del cable ethernet del Access Point por la pared. [Fuente: Elaboración propia].



Figura 41. Sistema de Control Número 3. Evidencia 2. Cruce del cable ethernet por el pacillo. [Fuente: Elaboración propia].



Figura 42. Sistema de Control Número 3. Evidencia 3. Conexión del cable ethernet a la terminal de red del laboratorio de cómputo. [Fuente: Elaboración propia].



Figura 43. Sistema de Control Número 3. Evidencia 4. Foto completa del cable ethernet. [Fuente: Elaboración propia].

ANEXO D. EVIDENCIAS DEL SISTEMA DE CONTROL NÚMERO 4. USO DEL EXTINTOR DEGINADO.



Figura 44. Sistema de Control Número 4. Evidencia 1. Foto de ausencia de extintor en el laboratorio D1. [Fuente: Elaboración propia].



Figura 45. Sistema de Control Número 4. Evidencia 2. Foto de ausencia de extintor en el laboratorio C6. [Fuente: Elaboración propia].



Figura 46. Sistema de Control Número 4. Evidencia 3. Foto del extintor número 1. [Fuente: Elaboración propia].



Figura 47. Sistema de Control Número 4. Evidencia 4. Foto del extintor número 2. [Fuente: Elaboración propia].



Figura 48. Sistema de Control Número 4. Evidencia 5. Foto del extintor número 3. [Fuente: Elaboración propia].

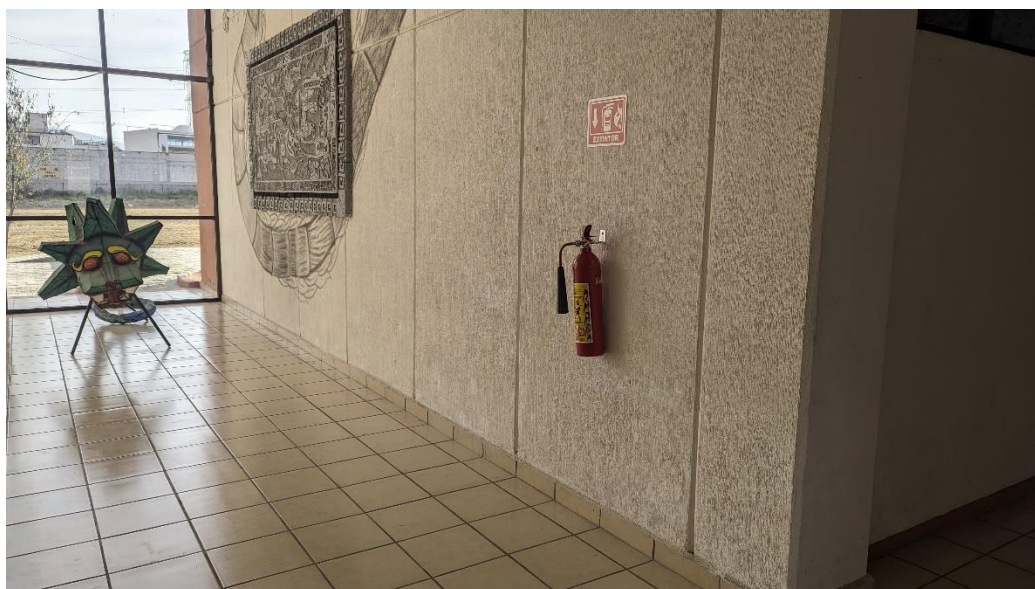


Figura 49. Sistema de Control Número 4. Evidencia 6. Foto del extintor número 4. [Fuente: Elaboración propia].

ANEXO E. TABLA DE UBICACIÓN DE LOS EXTINTORES EN LA INSTITUCIÓN.

*Tabla 88. Ubicación de los extintoras en la Institución. Resultado de la evaluación del sistema de control Número 4.
[Fuente: Elaboración propia].*

	Ubicación	Distancia del laboratorio C6	Distancia del laboratorio D1
Extintor 1	Planta baja del primer edificio, frente a las escaleras.	30 metros	10 metros
Extintor 2	Primer piso del primer edificio frente a las escaleras.	35 metros	15 metros
Extintor 3	Segundo piso del primer edificio frente a las escaleras.	40 metros	20 metros
Extintor 4	Planta baja del segundo edificio frente a las escaleras.	10 metros	30 metros

ANEXO F. PROPUESTA DE BITÁCORA DE INCIDENTES DE TI.



Bitácora de Incidentes de TI

Incidente	Fecha	Lugar	Causante/es	Provocado o Fortuito	Activos de TI afectados	Lineamiento de la política implementado	Solución aplicada

Figura 50. Propuesta de Bitácora de Incidentes de TI. [Fuente: Elaboración propia].

Fecha: _____ Impartido por: _____

[illegible]

279

UMB
UNIVERSIDAD MEXIQUENSE DEL
BICENTENARIO

Fecha: _____ Impartido por: _____

[illegible]

280

Fecha: _____ Impartido por: _____

[illegible]

281

ANEXO J. EVIDENCIA DE LA IMPLEMENTACIÓN DE LOS PRODUCTOS SELECCIONA

Elaboró	Revisó	Autorizó
Ceja Lopez Mikael, Lazo Plata Saúl y Moreno Rivero Michael Alexis estudiantes de Ingeniería en Sistemas Computacionales	Mtra. Diana Marisol Prado Oseguera	M.A.D.N Juan José Olin Fabela
Firmas: 	Firma: 	Firma:  Revisó Jose Juan Alvarado Rosales 
07 de Abril, 2024	28 de Mayo, 2024	28 de Mayo, 2024

CAMBIOS A ESTA VERSIÓN		
No. de Revisión	Fecha de Actualización	Descripción del Cambio
1	02/03/2024	Implementación de nuevos lineamientos enfocados en el personal administrativo.
2	23/03/2024	Modificación de lineamientos y sanciones.

Figura 54. Aprobación por parte de todos los involucrados de la Política de Seguridad Informática. [Fuente: Elaboración propia].

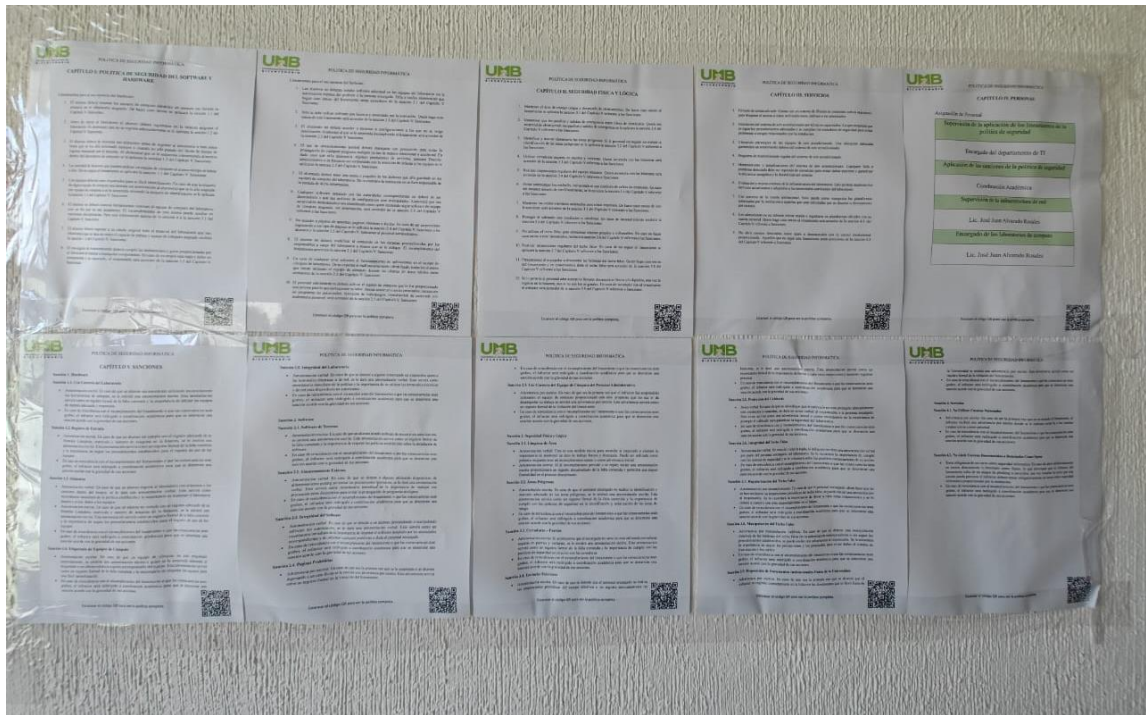


Figura 55. Aplicación de la versión recortada de la Política de Seguridad Informática en el Laboratorio C6. [Fuente: Elaboración propia].

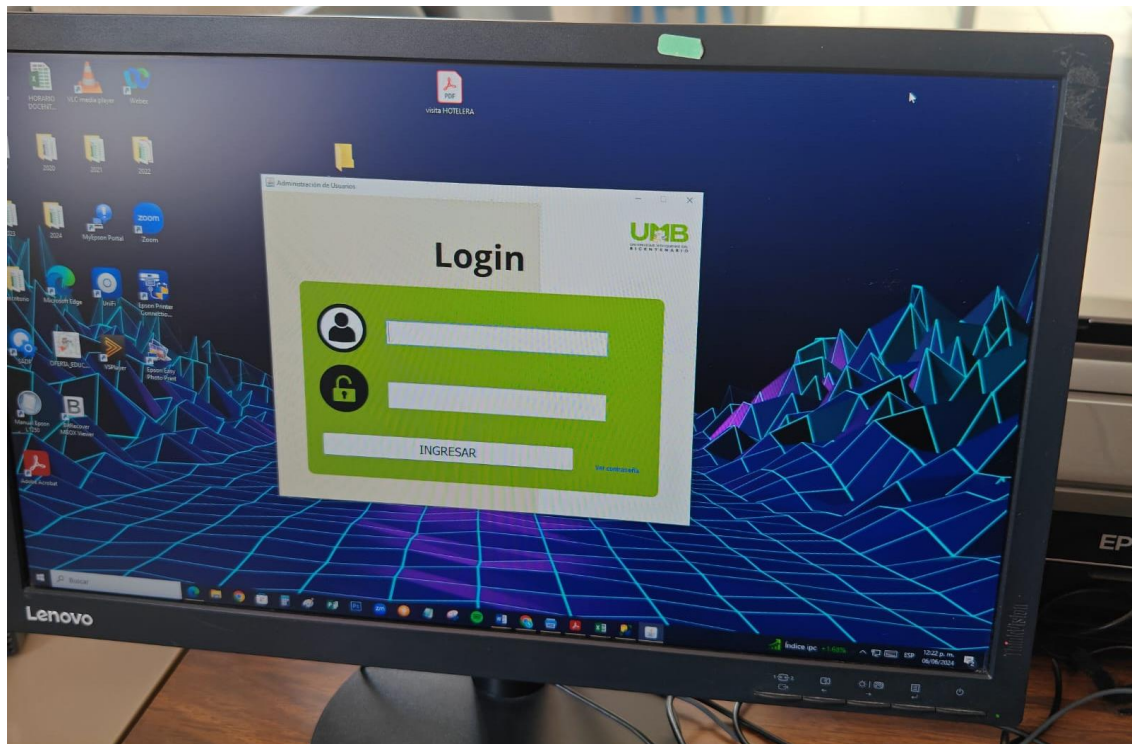


Figura 56. Ejecución del Sistema de Inventario de TI. Parte 1. [Fuente: Elaboración propia].



Figura 57. Ejecución del Sistema de Inventario de TI. Parte 2. [Fuente: Elaboración propia].

Cuestionario Seguridad "Informatica"

Preguntas

Respuestas

6

ConfiguraciPuntos totales: 20

Nombre completo

6 respuestas

Edgar Ulises Pavon Zamarripa

Diana Mireya Ramirez Ramirez

Karla Esmeralda Arredondo

José Alonso Pérez Ramírez

Alvarado Rosales José Juan

Juan Raúl Vargas Hernández

Figura 59. Captura de pantalla del aquellos que respondieron el cuestionario del curso de "Concienciación sobre seguridad informática". [Fuente: Elaboración propia].

Cuestionario "Contraseñas Seguras"

Preguntas

Respuestas

6

Configuración Puntos totales: 10

Nombre completo

6 respuestas

Edgar Ulises Pavon Zamarripa

Diana Mireya Ramirez Ramirez

Karla Esmeralda Arredondo

José Alonso Pérez Ramírez

Alvarado Rosales José Juan

Juan Raúl Vargas Hernández

Figura 61. Captura de pantalla de aquellos que respondieron el cuestionario del curso de "Creación de contraseñas seguras y su importancia". [Fuente: Elaboración propia].



Figura 62. Distribución de las puntuaciones totales del curso de “Concienciación sobre seguridad informática”.
[Fuente: Elaboración propia].



Figura 63. Distribución de las puntuaciones totales del curso de “Creación de contraseñas seguras y su importancia”.
[Fuente: Elaboración propia].

ANEXO K. POLÍTICA DE SEGURIDAD INFORMÁTICA.

**UNIVERSIDAD MEXIQUENSE DEL
BICENTENARIO PLANTEL TULTITLÁN**

POLÍTICA DE SEGURIDAD INFORMÁTICA

Enero 2024

Elaboró	Revisó	Autorizó
Ceja Lopez Mikael, Lazo Plata Saúl y Moreno Rivero Michael Alexis estudiantes de Ingeniería en Sistemas Computacionales	Mtra. Diana Marisol Prado Oseguera	Lic. Alma Angélica Torres Contreras
Firmas:	Firma:	Firma:
07 de Enero, 2024	28 de Mayo, 2024	28 de Mayo, 2024

CAMBIOS A ESTA VERSIÓN		
No. de Revisión	Fecha de Actualización	Descripción del Cambio
1	02/03/2024	Implementación de nuevos lineamientos enfocados en el personal administrativo.
2	23/03/2024	Modificación de lineamientos y sanciones.

INTRODUCCIÓN

En el presente documento se tiene como objetivo establecer una política de seguridad para resguardar los activos de TI ubicados en los laboratorios de cómputo de la Universidad, tales como los equipos de cómputo, proyectores, el software utilizado, la información almacenada, etc. A través de cinco capítulos los cuales abarcaran los lineamientos, responsabilidades del personal y sanciones en caso de incumplimiento; dichos capítulos son: política de seguridad del hardware y software, seguridad física, servicios, personas y sanciones.

INTENCIÓN DE LA INSTITUCIÓN

Contar con un documento que permita generar un ambiente de seguridad, proveyendo guías de pensamiento para la protección de todos los activos de TI localizados en los laboratorios de cómputo de la Universidad a través de los lineamientos y sanciones que se dictan en esta es de vital importancia ya que hablando de una institución de nivel superior los laboratorios de cómputo debieran de ser protegidos adecuadamente, tanto de potenciales amenazas, así como de un uso indebido de estos.

A QUIEN VA DIRIGIDA

La presente política va dirigida a todo aquel que tenga acceso a los dos laboratorios de cómputo ubicados dentro de las instalaciones de la Universidad, siendo principalmente al alumnado, personal docente y administrativo.

REFERENCIAS

Estándar ISO/IEC 17799, 2005

GLOSARIO

Seguridad informática: Es una especialidad de dicha disciplina centrada en proteger la estructura relacionada con ordenadores y dispositivos portátiles, como tablets y smartphones. Es decir, se ocupa de proteger cualquier dispositivo que cuenta con conexión a internet, pero esta misión es solo una parte de su trabajo. Y es que también existe la seguridad in situ, para evitar que otras personas puedan acceder a ciertos contenidos. (Universitat Carlemany, s.f.).

Vulnerabilidad: Es un punto de quiebre o un vacío donde se identifican todos los errores o problemas relacionados con seguridad que puede existir en un programa de código y de una estructura de seguridad. Todos estos errores son el motivo por el que cualquier hacker puede entrar y realizar un ataque cibernético en el programa. Hay muchos tipos de vulnerabilidad informática que afectan a elementos característicos del pensamiento computacional, tales como el hardware, software, de proceso de código, de errores humanos. (Redacción KeepCoding, 2022).

Amenaza: Las amenazas de seguridad de la información o ciberamenazas son definidas por el Instituto Nacional de Estándares y Tecnologías (NIST) norteamericano. Este entiende la amenaza como un evento con potencial de afectar negativamente a las operaciones de una organización o a sus activos, “a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio”. (Riveros, 2020).

Seguridad Lógica: La seguridad lógica se trata de un conjunto de medidas implementadas para garantizar el resguardo de la información que se maneja en una empresa. Se sustenta en tres principios básicos que determinan la eficacia de dichas medidas:

- **Integridad:** Los datos deben estar protegidos frente a ataques informáticos o terceras personas que intenten modificarlos, dañarlos o borrarlos de forma permanente.
- **Disponibilidad:** La información debe estar disponible en todo momento, sin retrasos ni trabas.
- **Confidencialidad:** Solo las personas autorizadas pueden tener acceso a los datos. Además, se debe impedir su divulgación para fines distintos de aquellos por los que fueron almacenados. Esto supone prevenir también las brechas causadas por errores humanos o fallos en los sistemas.

Estos tres pilares son cruciales para la seguridad y el buen funcionamiento de una empresa. La información no siempre se limita a los asuntos relacionados con sus actividades u operaciones, sino que puede incluir datos financieros o de los clientes, con la confidencialidad que eso exige. Su exposición podría ocasionar problemas legales y sanciones económicas, además de afectar la credibilidad y reputación de la compañía. (prosegur, 2022).

Ataque de Phishing: Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing

que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o “suplanta su identidad”) a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro. (Malwarebytes, 2024).

CAPÍTULO I: POLITICA DE SEGURIDAD DEL SOFTWARE Y HARDWARE

Lineamientos para el uso correcto del Hardware:

1. El alumno deberá respetar los equipos de cómputo dándoles un correcto uso durante su estancia en el laboratorio asignado: Esto significa que el alumno debe utilizar adecuadamente las herramientas de cómputo disponibles en el laboratorio. Debe tratar los equipos con cuidado y utilizarlos según su propósito previsto. No debe maltratar físicamente los dispositivos, así como los periféricos conectados; además de abstenerse desconectar los periféricos ya conectados o conectar alguno que no corresponda al equipo de cómputo. De hacer caso omiso se aplicará la sanción 1.1 del Capítulo V. Sanciones.
2. Antes de entrar al laboratorio el alumno deberá registrarse en la bitácora asignada al laboratorio: Para llevar un registro adecuado de la utilización de los equipos del laboratorio, se solicita al alumno que anote su Nombre Completo, matrícula (lo cual es su identificación estudiantil) y el número de la máquina en la que se encuentra. Esto ayuda a identificar quién está utilizando cada equipo y permite realizar un seguimiento en caso de algún inconveniente con el equipo de cómputo, contactar al alumno que lo utilizo. El alumno(a) que no se registre adecuadamente se le aplicara la sanción 1.2 del Capítulo V. Sanciones.
3. El alumno deberá de terminar sus alimentos antes de ingresar al laboratorio o bien entrar hasta que se los allá terminado siempre y cuando no allá pasado del límite de tiempo de ingreso manejado por el docente. Esto ayuda a prevenir derrames, restos de comida o malos olores en el área de trabajo. Al alumno(a) que se le sorprenda consumiendo alimentos dentro del laboratorio de cómputo se le aplicara la sanción 1.3 del Capítulo V. Sanciones.
4. La cantidad de alumnos que pueden utilizar un equipo de cómputo al mismo tiempo se limita a dos: Esto permite que cada usuario tenga suficiente espacio y recursos para llevar a cabo sus tareas sin interferencias. Limitar el número de usuarios también ayuda a evitar daños accidentales a los equipos y a mantener un ambiente de trabajo ordenado. De no seguir el lineamiento se aplicará la sanción 1.1 del Capítulo V. Sanciones.
5. Los equipos deberán estar etiquetados para su fácil identificación: Cada equipo de cómputo en el laboratorio debe tener una etiqueta claramente visible que permita su identificación rápida y precisa. Esto facilita el proceso de registro, ayuda a los usuarios a encontrar el equipo asignado y permite una mejor gestión de los recursos del laboratorio. En caso de que la etiqueta de algún equipo de cómputo sea retirada sin autorización al alumno(a) que se le allá asignado ese equipo de cómputo o se le sorprenda retirando la etiqueta de identificación se le aplicara la sanción 1.4 del Capítulo V. Sanciones.

6. El alumno no deberá conectar herramientas externas al equipo de cómputo del laboratorio con un fin que no sea académico: Esto con el fin de cuidar el estado integro de los equipos. En caso de necesitar utilizar herramientas externas con fines académicos, se deberá solicitar autorización previa al encargado del laboratorio, quien evaluará la pertinencia y seguridad de su uso. El incumplimiento de esta norma puede resultar en sanciones disciplinarias. Para más información acerca de la sanción ir a la sanción 1.1 del Capítulo V. Sanciones.
7. El alumno deberá regresar a su estado original todo el material del laboratorio que use: Se debe mantener el orden en el área de trabajo asignada, además de que en caso de detectar cualquier desperfecto que tenga algún material (ratón, teclados, monitores, Gabinetes, Cables) se deberá registrar en las observaciones de la bitácora para que el departamento de mantenimiento haga proceso pertinente con el material reportado, esto ayudando a que el material del laboratorio de cómputo se preserve de la mejor manera. Alumno(a) que no deje en orden el espacio de trabajo y equipo de cómputo asignado recibirá la sanción 1.5 del Capítulo V. Sanciones.
8. El encargado de mantenimiento deberá cumplir las instrucciones y guías proporcionadas por el fabricante al instalar o manipular componentes: Seguir las instrucciones y guías del fabricante es crucial para evitar daños costosos en los componentes o en el equipo en su conjunto. Además, el incumplimiento de las instrucciones puede invalidar la garantía del producto. En caso de incumplir esta regla y dañar un componente y no reportarlo, el responsable será acreedor de la sanción 1.5 del Capítulo V. Sanciones.

Lineamientos para el uso correcto del Software:

1. Los alumnos no deberán instalar software adicional en los equipos del laboratorio sin la autorización expresa del profesor o la persona encargada: Esto se debe a que la instalación de software adicional, no autorizado puede afectar el funcionamiento de los equipos, introduciendo algún tipo de malware o virus. Los alumnos deben respetar esta regla y solicitar permiso antes de realizar cualquier instalación. El/la o los/las alumnos(as) que hagan caso omiso del lineamiento serán acreedores de la sanción 2.1 del Capítulo V Sanciones.
2. Solo se debe utilizar software con licencia y autorizado por la institución: Está prohibido instalar o ejecutar software pirata, ilegal o no autorizado por la institución, El software autorizado es aquel que cuenta con una licencia válida emitida por el fabricante o distribuidor legítimo. Esta licencia establece los términos y condiciones bajo los cuales el software puede ser utilizado, incluyendo restricciones. Quien haga caso omiso de este lineamiento será acreedor de la sanción 2.1 del Capítulo V. Sanciones.
3. El alumnado no deberá acceder a recursos o configuraciones a los que no se tenga autorización: Este lineamiento implica que los alumnos deben respetar los límites de acceso y no intentar acceder a recursos o configuraciones para los cuales no tienen autorización. Alumno(a) al que se le sorprenda incumpliendo el lineamiento será acreedor de la sanción 2.3 del Capítulo V. Sanciones.
4. El uso de almacenamiento portátil deberá manejarse con precaución para evitar la propagación de cualquier programa maligno ya sea de manera intencional o accidental: Si los alumnos desean utilizar dispositivos de almacenamiento portátil, como unidades USB, discos duros externos o tarjetas de memoria, deben tener cuidado para evitar la propagación de programas malignos o malware. Esto implica escanear los dispositivos de almacenamiento en busca de virus antes de conectarlos a los equipos del laboratorio y asegurarse de no copiar o ejecutar archivos sospechosos. La precaución es importante para proteger la seguridad y la integridad de los sistemas informáticos del laboratorio. En dado caso que el/la alumno(a), algún(a) prestador(a) de servicios, personal Docente, administrativo o de limpieza sea sorprendido con la intención de infectar a los equipos se le aplicaran la sanción 2.2 del Capítulo V. Sanciones.
5. El alumnado deberá tener una copia o respaldo de los archivos que allá guardado en los equipos de cómputo del laboratorio: Lo que incluye archivos de proyectos, documentos, datos o cualquier otro tipo de información relevante. Tener copias de seguridad ayuda a prevenir la pérdida de datos en caso de fallas técnicas, errores humanos o cualquier otro incidente inesperado. Los alumnos deben tomar esta precaución para asegurarse de no perder información valiosa. De lo contrario la institución no se hará responsable de la perdida de dicha información.

6. Cualquier software instalado por las autoridades correspondientes no deberá de ser desinstalado o que sus archivos de configuración sean manipulados: Esto se debe a que el software puede ser necesario para fines educativos, de seguridad o de gestión. Cualquier manipulación no autorizada puede afectar negativamente el funcionamiento de los equipos o violar las políticas establecidas. Los/las alumnos(as) deben respetar esta regla y, en caso de dudas o problemas con el software instalado, informar al personal encargado. Alumno(a) que sea sorprendido desinstalado o sea identificado como quien desinstalo algún software del equipo de cómputo asignado, sin autorización, será acreedor de la sanción 2.3 del Capítulo V referente a las Sanciones.
7. No acceder a páginas de apuestas, paginas obscenas e ilícitas: Tanto el personal administrativo como el alumnado deben abstenerse de acceder a sitios web que promuevan apuestas, contengan contenido obsceno o sean ilegales. Esto es importante para mantener un ambiente académico y respetuoso en la institución, así como para cumplir con las regulaciones y políticas establecidas por la institución educativa. El acceso a este tipo de páginas puede ser considerado inapropiado. En caso de ser sorprendidos ingresando a ese tipo de páginas se le aplicara la sanción 2.4 del Capítulo V. Sanciones a los alumnos y la sanción 2.5 del Capítulo V. Sanciones al personal administrativo.
8. El alumno no deberá, modificar el contenido de las carpetas preestablecidas por los responsables a cargo del laboratorio a menos que se le indique: Este lineamiento contempla que la información de dichas carpetas debe conservar la integridad para las aplicaciones que fueron instaladas. El incumplimiento del lineamiento ameritara la sanción 2.3 del Capítulo V. Sanciones.
9. En caso de cualquier error referente al funcionamiento de aplicaciones en el equipo de cómputo de laboratorio. El alumno debe reportarlo y especificar si el error estaba antes del uso del equipo o si el alumno en turno lo provoco, con el encargado en turno para que este lo registre y se tomen las medidas pertinentes para su pronta solución. De no reportar el malfuncionamiento identificado, todos los alumnos que hayan utilizado el equipo de cómputo durante las últimas 24 horas hábiles serán acreedores de la sanción 2.3 del Capítulo V. Sanciones.
10. El personal administrativo deberá utilizar el equipo de cómputo que le fue proporcionado únicamente para lo que corresponde su labor: Al personal administrativo se le es asignado un equipo de cómputo (ya sea de escritorio o portátil) desde el cual únicamente deberá realizar las actividades que corresponden a su trabajo, utilizando además la cuenta institucional que también le fue proporcionada para ingresar a las plataformas oficiales utilizadas por la institución. Todo aquel que sea sorprendido utilizando el equipo de cómputo para otro propósito que no sea el

desempeñar su labor como: Iniciar sesión en cuentas personales, instalación de programas no autorizados, ejecución de videojuegos, reproducción de contenido y/o multimedia personal, será acreedor de la sanción 2.5 del Capítulo V. Sanciones.

CAPÍTULO II. SEGURIDAD FÍSICA Y LÓGICA

1. Mantener el área de trabajo limpia y despejada de obstrucciones: Este punto implica mantener el espacio de trabajo libre de objetos que puedan causar tropiezos o caídas. Cajas, mochilas u otros elementos deben ser almacenados adecuadamente en áreas designadas para evitar obstruir los pasillos o zonas de circulación. De hacer caso omiso al lineamiento se aplicará la sanción 3.1 del Capítulo V referente a las Sanciones.
2. Garantizar que los pasillos y salidas de emergencia estén libres de obstáculos: Es importante garantizar que los pasillos y las salidas de emergencia estén despejados y sean fácilmente accesibles en caso de una evacuación rápida. No deben existir objetos, muebles o cualquier otro elemento que obstruya el camino hacia las salidas. Quien sea sorprendido obstruyendo los pasillos y salidas de emergencia se le aplicara la sanción 3.1 del Capítulo V referente a las Sanciones.
3. Identificar y marcar claramente las áreas peligrosas: Algunas áreas de trabajo pueden representar riesgos específicos, como zonas de alta tensión eléctrica o áreas de almacenamiento de materiales peligrosos. Estas áreas deben ser identificadas claramente y señalizadas apropiadamente para advertir a las personas sobre los posibles peligros y tomar las precauciones necesarias. Si el personal encargado no realiza la identificación de las áreas peligrosas se le aplicara la sanción 3.2 del Capítulo V referente a las Sanciones.
4. Utilizar cerraduras seguras en puertas y ventanas: Para mantener la seguridad de la instalación, es importante utilizar cerraduras seguras en puertas y ventanas. Además, estas cerraduras deben ser revisadas y mantenidas regularmente para asegurarse de que funcionen correctamente y no sean vulnerables a una intrusión por la fuerza. Esto debe de ser revisado periódicamente por el encargado en turno del laboratorio y realizar bitácoras del estado. Quien incumpla con las bitácoras será acreedor de la sanción 3.3 del Capítulo V referente a las Sanciones.
5. Realizar inspecciones regulares del equipo eléctrico: Es responsabilidad del personal encargado llevar a cabo inspecciones periódicas de los enchufes, interruptores y cables eléctricos para identificar posibles signos de desgaste, daños o funcionamiento defectuoso. Cualquier equipo defectuoso debe ser reparado o reemplazado de inmediato para evitar riesgos de incendio o descargas eléctricas. Así mismo se debiera llevar una bitácora del estado de dicho equipo. Quien incumpla con las bitácoras será acreedor de la sanción 3.4 del Capítulo V referente a Sanciones.
6. Evitar sobrecargar los enchufes, incluyendo el uso indebido de cables de extensión: Es importante respetar las capacidades de carga de los enchufes y no conectar múltiples dispositivos que excedan su capacidad. Además, el uso indebido de cables de extensión, como conectar múltiples extensiones en serie o utilizar cables dañados, puede representar un riesgo de incendio o descarga eléctrica. En caso del

incumplimiento de este lineamiento, se le aplicara la sanción 3.4 del Capítulo V referente a las Sanciones.

7. Mantener los cables eléctricos ordenados para evitar tropiezos: Los cables sueltos o colgantes pueden ser un peligro potencial, ya que las personas pueden tropezar o enredarse con ellos. Utilizar organizadores de cables o mantenerlos sujetos adecuadamente a lo largo de las paredes o debajo de los escritorios puede ayudar a mantenerlos ordenados y reducir el riesgo de accidentes. De hacer caso omiso de este lineamiento será acreedor de la sanción 3.1 del Capítulo V referente a las Sanciones.
8. Proteger el cableado con conductos o canaletas: Para evitar daños físicos o manipulaciones no autorizadas, se recomienda utilizar conductos o canaletas para proteger el cableado eléctrico y de red. Estas cubiertas brindan una capa adicional de seguridad y evitan que los cables sean expuestos a condiciones adversas o interferencias no deseadas. En caso de incumplimiento recibirá la sanción 3.5 del Capítulo V referente a las Sanciones.
9. No utilizar el techo falso para almacenar objetos pesados o inflamables: El techo falso tiene una función específica y no debe utilizarse como área de almacenamiento para objetos pesados o materiales inflamables. Esto puede comprometer la integridad del techo falso y, en casos extremos, representar un riesgo para la seguridad de las personas en el edificio. En caso de hacer caso omiso a este lineamiento, recibirá la sanción 3.6 del Capítulo V referente a las Sanciones.
10. Realizar inspecciones regulares del techo falso: Es responsabilidad del personal encargado llevar a cabo inspecciones periódicas del techo falso para asegurarse de que esté en buen estado. Esto implica verificar si hay signos de deterioro, filtraciones de agua u otros problemas que puedan comprometer la estructura o la seguridad del techo falso. En caso de no seguir el lineamiento se aplicará la sanción 3.7 del Capítulo V referente a las Sanciones.
11. Precauciones al manipular o desmontar las baldosas del techo falso: En caso de ser necesario manipular o desmontar las baldosas del techo falso, es importante obtener la autorización correspondiente y tomar precauciones para evitar dañar el sistema de iluminación o los cables que puedan estar ocultos detrás del techo falso. Cualquier manipulación debe realizarse de manera segura y siguiendo las pautas y protocolos establecidos. Quien haga caso omiso del lineamiento y en consecuencia dañe el techo falso será acreedor de la sanción 3.8 del Capítulo V referente a las Sanciones.
12. Se le permite al personal administrativo llevarse documentos físicos y/o digitales, una vez lo registre en la bitácora, aun si no son los originales. En caso de que su trabajo así lo requiera, se le permitirá al personal administrativo llevarse documentos físicos y/o digitales ya sea de carácter público o privado, bajo la condición de que lo registre

en la bitácora correspondiente. En caso de incumplir con el lineamiento el infractor será acreedor de la sanción 3.9 del Capítulo V referente a Sanciones.

CAPÍTULO III. SERVICIOS

1. Filtrado de contenido web: Contar con un sistema de filtrado de contenido web es importante para bloquear el acceso a sitios web maliciosos, dañinos o no autorizados. Este sistema puede ayudar a prevenir ataques cibernéticos y proteger a los usuarios de amenazas en línea. Es crucial mantenerlo actualizado para asegurarse de que esté al tanto de las últimas amenazas y pueda bloquear eficazmente el acceso a sitios no deseados.
2. Instalación del sistema de aire acondicionado por técnicos capacitados: Para garantizar un funcionamiento seguro y eficiente del sistema de aire acondicionado, es importante que la instalación sea realizada por técnicos capacitados y calificados. Esto asegurará que se sigan los procedimientos adecuados y se cumplan los estándares de seguridad para evitar problemas o riesgos relacionados con la instalación.
3. Ubicación estratégica de los equipos de aire acondicionado: Es recomendable colocar los equipos de aire acondicionado en áreas estratégicas para lograr una distribución óptima del aire en el espacio. Esto implica considerar factores como el flujo de aire, la obstrucción de los conductos y la eficiencia energética. Una ubicación adecuada garantizará un rendimiento óptimo del sistema de aire acondicionado.
4. Programa de mantenimiento regular del sistema de aire acondicionado: Para mantener el sistema de aire acondicionado en buen estado de funcionamiento, es necesario establecer un programa de mantenimiento regular. Esto incluye la limpieza periódica de los filtros para garantizar un flujo de aire adecuado, verificar los niveles de refrigerante, revisar las conexiones eléctricas y realizar cualquier otra tarea de mantenimiento recomendada por el fabricante.
5. Mantenimiento y actualizaciones del sistema de aire acondicionado: Es importante mantener el sistema de aire acondicionado actualizado con las últimas revisiones y mejoras proporcionadas por el fabricante. Esto implica estar al tanto de las actualizaciones de software o firmware, y programar su instalación de manera oportuna. Además, cualquier falla o problema detectado debe ser reparado de inmediato para evitar daños mayores y garantizar la eficiencia energética y la durabilidad del sistema.
6. Evaluación y mejora continua de la infraestructura del laboratorio: Se deben realizar evaluaciones periódicas de los servicios para identificar posibles mejoras en términos de seguridad, rendimiento y cumplimiento de las políticas. Esto permite mantener los servicios actualizados y adaptados a las necesidades cambiantes del laboratorio.
7. Uso correcto de la cuenta institucional: Al ser la cuenta institucional un servicio adquirido con terceros y de uso exclusivamente académico, no debe de ser utilizada para enlazarla con servicios web, servicios de entretenimiento, cuentas de redes

sociales o parecidos. Solo queda como excepción las plataformas autorizadas por la institución o aquellas que sean solicitadas por un docente o directamente por rectoría.

8. Los administrativos no deberán iniciar sesión o registrarse en plataformas oficiales con su cuenta personal: Debido a que la institución provee una cuenta institucional lo correcto es utilizar la misma para todo lo que corresponda al desempeño de su labor dentro de la Universidad. Quien haga caso omiso al lineamiento será acreedor de la sanción 4.1. del Capítulo V referente a Sanciones.
9. No abrir correos detectados como spam o desconocidos con la cuenta institucional proporcionada: Debido a la creciente actividad en ataques de phishing, de forma generalizada, para no exponer a miembros de la institución ya sea personal administrativo, docentes o alumnado; a un posible robo de datos, pérdida de la cuenta institucional, etc. Se recomienda de forma insistente no abrir correos desconocidos o detectados como spam. Aquellos que no sigan este lineamiento serán acreedores de la sanción 4.2 del Capítulo V referente a Sanciones.

CAPÍTULO IV. PERSONAS

Asignación de Personal

Tabla 89. Cuadro de asignación de personal para ejecutar la Política. Elemento 3 de la Política. [Fuente: Elaboración propia].

Supervisión de la aplicación de los lineamientos de la política de seguridad
Encargado del departamento de TI
Aplicación de las sanciones de la política de seguridad
Coordinación Académica
Supervisión de la infraestructura de red
Lic. José Juan Alvarado Rosales
Encargado de los laboratorios de computo
Lic. José Juan Alvarado Rosales

Responsabilidades del Personal

1. Responsabilidades de los encargados en turno del laboratorio:
 - Supervisión del Uso de Equipos de Laboratorio: Supervisar y asegurar el uso adecuado y seguro de los equipos de laboratorio por parte del personal y los estudiantes, incluyendo el cumplimiento de los protocolos y normas establecidas.
 - Mantenimiento del Inventario: Realizar un seguimiento y mantener actualizado el inventario de los activos de TI del laboratorio, asegurando su disponibilidad y solicitando reposiciones cuando sea necesario.
 - Cumplimiento de Procedimientos: Asegurarse de que se sigan los procedimientos y protocolos establecidos en el laboratorio, incluyendo los lineamientos de seguridad, manipulación de sustancias, así como la eliminación de residuos, y tomar medidas correctivas en caso de incumplimiento.
 - Informe y Documentación: Registrar y documentar adecuadamente las actividades, resultados y cualquier incidente relevante ocurrido durante el turno, proporcionando información precisa y completa para el seguimiento y la toma de decisiones.

2. Responsabilidades de los prestadores de servicio:

- Cumplimiento de Instrucciones: Cumplir con las instrucciones y tareas asignadas por el personal administrativo, siguiendo las pautas y procedimientos establecidos.
- Comunicación Efectiva: Comunicar cualquier problema, duda o situación relevante al personal administrativo de manera oportuna y clara, manteniendo una comunicación efectiva y abierta.
- Cumplimiento de Normas y Regulaciones: Cumplir con las normas y regulaciones establecidas en el entorno de trabajo, incluyendo los lineamientos establecidos en esta política.

3. Responsabilidades del personal de limpieza:

- Mantenimiento de la Higiene: Mantener limpias las áreas asignadas, incluyendo la limpieza regular de superficies y equipo, siguiendo los estándares de limpieza establecidos.
- Manipulación Segura de Productos Químicos: Utilizar y manipular adecuadamente los productos químicos de limpieza, siguiendo las instrucciones de seguridad y utilizando el equipo de protección personal necesario.
- Comunicación de Incidentes: Informar de inmediato cualquier incidente de seguridad o riesgo identificado durante las tareas de limpieza al personal autorizado, siguiendo los procedimientos establecidos.

CAPÍTULO V. SANCIONES

Sanción 1. Hardware

Sanción 1.1. Uso Correcto del Laboratorio

- Amonestación escrita: En caso de que un alumno sea encontrado utilizando incorrectamente las herramientas de cómputo, se le emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de utilizar los equipos de manera adecuada y respetuosa.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 1.2. Registro de Entrada

- Amonestación escrita: En caso de que un alumno no cumpla con el registro adecuado de su Nombre Completo, matrícula y número de máquina en la bitácora, se le emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de seguir los procedimientos establecidos para el registro de uso de los equipos.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 1.3. Alimentos

- Amonestación verbal: En caso de que un alumno ingrese al laboratorio con alimentos o los consuma dentro del mismo, se le dará una amonestación verbal. Esto servirá como recordatorio inmediato de la política establecida y la importancia de mantener el laboratorio limpio y evitar daños a los equipos.
- Amonestación escrita: En caso de que un alumno no cumpla con el registro adecuado de su Nombre Completo, matrícula y número de máquina en la bitácora, se le emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de seguir los procedimientos establecidos para el registro de uso de los equipos.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 1.4. Etiquetado de Equipos de Cómputo

- Amonestación escrita: En caso de que un equipo de cómputo no esté etiquetado correctamente, se emitirá una amonestación escrita a quien se le sorprenda retirando el etiquetado o en última estancia a quien sea responsable del equipo. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de etiquetar los equipos para una fácil identificación.

- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 1.5. Integridad del Laboratorio

- Amonestación verbal: En caso de que se detecte a alguien conectando un dispositivo ajeno a las terminales eléctricas o de red, se le dará una amonestación verbal. Esto servirá como recordatorio inmediato de la política y la importancia de no utilizar las terminales eléctricas y de red para dispositivos no autorizados.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 2. Software

Sanción 2.1. Software de Terceros

- Amonestación escrita: En caso de que un alumno instale software de terceros sin autorización, se emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de respetar las políticas establecidas sobre la instalación de software.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 2.2. Almacenamiento Externo.

- Amonestación verbal: En caso de que se detecte a alguien utilizando dispositivos de almacenamiento portátil sin tomar las precauciones necesarias, se le dará una amonestación verbal. Esto servirá como recordatorio inmediato de la importancia de manejar con precaución estos dispositivos para evitar la propagación de programas malignos.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 2.3. Integridad del Software

- Amonestación verbal: En caso de que se detecte a un alumno desinstalando o manipulando software sin autorización, se le dará una amonestación verbal. Esto servirá como un recordatorio inmediato de la importancia de respetar el software instalado por las autoridades correspondientes y de informar cualquier problema o duda al personal encargado.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 2.4. Páginas Prohibidas

- Advertencia por escrito: En caso de que sea la primera vez que se le sorprenda a un alumno ingresando a un sitio ilícito se le emitirá una advertencia por escrito: Esta advertencia servirá como un registro formal de la violación del lineamiento.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 2.5. Uso Correcto del Equipo de Cómputo del Personal Administrativo.

- Advertencia por escrito: En caso de que sea la primera vez que el infractor fue sorprendido utilizando el equipo de cómputo proporcionado con otro propósito que

no sea el de desempeñar su trabajo se emitirá una advertencia por escrito. Esta advertencia servirá como un registro formal de la violación del lineamiento.

- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3. Seguridad Física y Lógica

Sanción 3.1. Limpieza de Área

- Amonestación verbal: Esta es una medida inicial para recordar al empleado o alumno la importancia de mantener un área de trabajo limpia y despejada. Puede ser utilizada como primera respuesta ante un incumplimiento menor o como advertencia inicial.
- Amonestación escrita: Si el incumplimiento persiste o se repite, emitir una amonestación escrita proporcionará un registro documentado de la falta cometida y permitirá una mayor formalidad en el proceso disciplinario.

Sanción 3.2. Áreas Peligrosas

- Amonestación escrita: En caso de que el personal encargado no realice la identificación y marcado adecuado de las áreas peligrosas, se le emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de cumplir con las políticas de seguridad en la identificación y señalización de las áreas de riesgo.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.3. Cerraduras – Puertas

- Amonestación escrita: Si se encuentra que el encargado en turno no está utilizando cerraduras seguras en puertas y ventanas, se le emitirá una amonestación escrita. Esta amonestación servirá como un registro formal de la falta cometida y la importancia de cumplir con las políticas de seguridad en relación con las cerraduras.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.4. Enchufes Eléctricos

- Amonestación escrita: En caso de que se detecte que el personal encargado no realiza las inspecciones periódicas del equipo eléctrico o no registra adecuadamente las bitácoras, se le dará una amonestación escrita. Esta amonestación servirá como un recordatorio formal de la importancia de llevar a cabo estas inspecciones y mantener registros precisos.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.5. Protección del Cableado

- Aviso verbal: En caso de que se identifique que el cableado no está protegido adecuadamente con conductos o canaletas, se dará un aviso verbal al responsable o al

personal encargado. Este aviso servirá como una advertencia inicial y como recordatorio de la importancia de proteger el cableado para garantizar la seguridad del laboratorio.

- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.6. Integridad del Techo Falso

- Amonestación verbal: En caso de violar la regla, el infractor recibirá una amonestación verbal por parte del personal encargado del laboratorio. Se le recordará la importancia de cumplir con las normas de seguridad y se le informará sobre las posibles consecuencias de su acción.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.7. Regularización del Techo Falso

- Amonestación por incumplimiento: En caso de que el personal encargado identifique que no se han realizado las inspecciones periódicas del techo falso, se puede emitir una amonestación al responsable. Se le recordará la importancia de llevar a cabo estas inspecciones y se le instará a cumplir con esta responsabilidad en el futuro.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.8. Manipulación del Techo Falso

- Advertencia por manipulación indebida: En caso de que se detecte una manipulación indebida de las baldosas del techo falso sin la autorización correspondiente o sin seguir los procedimientos establecidos, se puede emitir una advertencia al responsable. Se le recordará la importancia de seguir las precauciones y los protocolos para evitar daños al sistema de iluminación y los cables.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 3.9. Disposición de Documentos Institucionales Fuera de la Universidad

- Advertencia por escrito: En caso de que sea la primera vez que se detectó que el infractor no registro correctamente en la bitácora los documentos que se llevó fuera de la Universidad se emitirá una advertencia por escrito. Esta advertencia servirá como un registro formal de la violación del lineamiento.

- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 4. Servicios

Sanción 4.1. No Utilizar Cuentas Personales

- Advertencia por escrito: En caso de ser la primera vez que no es acatado el lineamiento, el infractor recibirá una advertencia por escrito donde se le indicará cerrar la o las cuentas creadas con su correo personal.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

Sanción 4.2. No Abrir Correos Desconocidos o Detectados Como Spam

- Toma obligatoria de un curso sobre seguridad informática: En caso de abrir deliberadamente un correo desconocido o detectado como Spam, lo que provoque que el infractor del lineamiento sufra de un ataque de phishing o parecidos, una vez resuelta la crisis que este suceso pueda provocar el infractor deberá tomar obligatoriamente un curso sobre seguridad informática proporcionado por la institución.
- En caso de reincidencia con el incumplimiento del lineamiento o que las consecuencias sean graves, el infractor será redirigido a coordinación académica para que se determine una sanción acorde con la gravedad de sus acciones.

ANEXO L. CURSO DE CONCIENCIACIÓN SOBRE SEGURIDAD INFORMÁTICA.

Manual: Seguridad informática

Introducción

En el mundo interconectado de hoy, la información es uno de nuestros activos más valiosos. Desde datos personales hasta secretos corporativos, la información impulsa nuestras vidas, negocios y decisiones. Sin embargo, con el aumento exponencial en el volumen de datos que compartimos y almacenamos digitalmente, surge un desafío significativo: garantizar la seguridad de esa información.

La importancia de la Seguridad informática

La importancia de la seguridad informática no puede subestimarse. En el mundo digital de hoy, casi todas nuestras actividades involucran alguna forma de tecnología o intercambio de datos. Desde realizar transacciones bancarias en línea hasta enviar correos electrónicos laborales, cada acción tiene una huella digital que, si no se protege adecuadamente, puede ser vulnerable a la intromisión.

Los ciberataques pueden tener una variedad de objetivos, como el robo de identidad, el acceso a información financiera, la interrupción de operaciones comerciales o incluso el compromiso de la seguridad nacional. Además, la naturaleza de las amenazas está en constante evolución, con ciberdelincuentes que desarrollan continuamente nuevas formas de explotar vulnerabilidades.

La seguridad informática, también conocida como ciberseguridad, se refiere a las prácticas, tecnologías y políticas diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados. En esencia, es la práctica de defender nuestros sistemas y nuestra información de la ciberdelincuencia.

Tips y Recomendaciones para la Seguridad Informática

No Subestimar las Contraseñas Sencillas:

Evite contraseñas obvias o fáciles de adivinar.

Utilice combinaciones de letras, números y símbolos.

Ser Escéptico y Alerta:

No haga clic en enlaces o descargue archivos de fuentes desconocidas.

Verifique la autenticidad de los correos electrónicos antes de proporcionar información sensible.

Actualizar Regularmente:

Mantenga su software, antivirus y sistemas operativos actualizados.

Utilice la opción de actualizaciones automáticas cuando sea posible.

Realizar Copias de Seguridad:

Realice copias de seguridad regulares de su información importante.

Utilice soluciones de almacenamiento en la nube y dispositivos externos para diversificar sus backups.

Educar y Capacitar:

Participe en programas de capacitación sobre seguridad informática.

Manténgase informado sobre las últimas amenazas y tendencias en ciberseguridad.

Siguiendo estos consejos y manteniendo una actitud proactiva, puede fortalecer significativamente su postura de seguridad informática y protegerse mejor a sí mismo y a su organización contra las crecientes amenazas cibernéticas. La seguridad informática no es solo una responsabilidad individual, sino también colectiva. Al estar informados, preparados y vigilantes, podemos construir un entorno digital más seguro para todos.

Protección contra Malware:

El malware, incluidos virus, troyanos y ransomware, puede infiltrarse en su sistema y causar daños significativos. Para protegerse, es vital instalar un software antivirus confiable y mantenerlo actualizado. Sea cauteloso al descargar archivos o abrir adjuntos de correo electrónico, especialmente si provienen de fuentes desconocidas. Realice escaneos regulares de su sistema para detectar y eliminar software malicioso.

Seguridad en Redes y Wi-Fi:

Las redes y conexiones Wi-Fi son puntos comunes de vulnerabilidad. Utilice redes seguras y configure su router con una contraseña fuerte y cifrado. Evite realizar actividades sensibles, como transacciones bancarias, en redes Wi-Fi públicas.

Actualización y Mantenimiento de Sistemas:

Los ciberdelincuentes a menudo explotan vulnerabilidades en software desactualizado para acceder a sistemas y robar datos. Asegúrese de que su sistema operativo, software y aplicaciones estén actualizados con los últimos parches y actualizaciones de seguridad. Active las actualizaciones automáticas cuando sea posible para garantizar que su sistema esté protegido contra amenazas recientes.

Copias de Seguridad y Recuperación de Datos:

Las copias de seguridad regulares son esenciales para proteger sus datos contra pérdidas causadas por fallas de hardware, ataques de malware o desastres naturales. Realice copias de seguridad de sus datos críticos en soluciones de almacenamiento en la nube y en dispositivos de almacenamiento externos. Configure copias de seguridad automáticas y pruebe regularmente sus procedimientos de recuperación para asegurarse de que funcionen correctamente.

Conclusión

En conclusión, la seguridad informática es un aspecto fundamental de nuestra vida digital que no puede ser subestimado ni ignorado. A medida que avanzamos en este mundo interconectado, la protección de nuestra información personal y corporativa se convierte en una necesidad imperativa. Las amenazas cibernéticas son cada vez más sofisticadas y omnipresentes, lo que nos obliga a ser vigilantes, informados y proactivos en la adopción de medidas de seguridad. La gestión efectiva de contraseñas, la protección contra el malware, la conciencia sobre el phishing y los ataques de ingeniería social, la seguridad en redes, la actualización regular de sistemas, las copias de seguridad de datos y, sobre todo, la educación y la creación de una cultura de seguridad, son pilares fundamentales para salvaguardar

nuestra integridad digital. Cada uno de estos elementos desempeña un rol crucial en la creación de una barrera robusta contra los ciberdelincuentes.

ANEXO M. CURSO PARA LA CREACIÓN DE CONTRASEÑAS SEGURAS Y SU IMPORTANCIA.

Manual: Contraseñas Seguras

Introducción

La seguridad de nuestra información personal y laboral es vital en la era digital. Una de las herramientas más importantes para proteger nuestros datos son las contraseñas. A través de este manual, buscamos proporcionar al personal de la escuela las pautas para crear contraseñas fuertes y mantener la seguridad de la información.

La Importancia de las Contraseñas

Una contraseña es como una llave digital; protege el acceso a su información personal y laboral en la escuela, como registros académicos y datos financieros. Una contraseña segura es la primera línea de defensa contra el acceso no autorizado.

Es fundamental comprender los riesgos que conlleva el uso de contraseñas débiles o predecibles. Contraseñas como "123456", "password" o fechas de nacimiento son extremadamente vulnerables a ataques de fuerza bruta o adivinación. Las consecuencias de una contraseña comprometida pueden variar desde el acceso no autorizado a información personal hasta brechas de seguridad en toda la organización.

Estructura Recomendada para Contraseñas

Una contraseña fuerte debe ser difícil de adivinar y debería incluir:

1. Al menos 8 caracteres de longitud.
2. Una combinación de letras mayúsculas y minúsculas.
3. Números.
4. Símbolos especiales (como @, #, \$, %).

Cómo Elaborar una Contraseña Segura

-  Para crear una contraseña segura, siga estos pasos:
-  Empiece con una frase o línea de una canción que sea fácil de recordar.
-  Transforme la frase en una abreviatura usando la primera letra de cada palabra.
-  Intercambie algunas letras por números o símbolos.

 Asegúrese de que su contraseña sea única y no la use para varias cuentas.

#ProTip para Contraseñas seguras y Fáciles de recordar puedes crear una contraseña alternando entre los caracteres de dos contraseñas simples para formar una fuerte y sencilla de aprender

Ejemplo

Contraseña 1: MORALES12 Contraseña2: A1TAM4R#

Resultado Mezclado: MAO1RTA4LME4SR1#2

Si decide no usar un gestor de contraseñas, aquí hay algunas estrategias para recordar sus contraseñas seguras:

Utilice una técnica de memoria como la creación de una historia alrededor de su contraseña, lo que puede facilitar el recuerdo de combinaciones complejas.

Asocie la contraseña con una visualización

mental específica o un conjunto de imágenes que le ayuden a recordar los caracteres y su orden.

Mantenimiento de la Seguridad de las Contraseñas

Cambie sus contraseñas regularmente y nunca las comparta con nadie. No las escriba en lugares accesibles o visibles. Considere el uso de un gestor de contraseñas para mantenerlas seguras y accesibles solo para usted.

Uso de Autenticación de Dos Factores

Siempre que sea posible, active la autenticación de dos factores para añadir una capa adicional de seguridad. Esto usualmente implica ingresar un código enviado a su teléfono después de introducir su contraseña.

Conclusión

Las contraseñas son una parte esencial de la seguridad informática. Al seguir estas pautas, ayudará a proteger tanto su información personal como la de la escuela. La seguridad es

responsabilidad de todos, y una contraseña fuerte es un paso fundamental. En la era digital, una contraseña segura actúa como la primera y más crucial línea de defensa contra el acceso no autorizado a información personal y datos importantes. Adoptar y mantener prácticas robustas de seguridad de contraseñas es esencial, no solo para su protección individual sino también para la seguridad de la organización en su conjunto. Al comprometerse con la creación, gestión y actualización regular de contraseñas, cada individuo contribuye a un entorno digital más seguro y protegido.