



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Auditoria con ISO 17799 para gestión
de la seguridad de Activos de TI de la
empresa embotelladora mexicana
jarritos S.A de C.V

Informe Técnico de Residencias
Profesionales para obtener el título en:

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Especialidad
Auditoria en seguridad informática

Presenta:

Katia Elizabeth Aguirre Olmos

Karla Celeste Pantoja Hernández

Coacalco de Berriozábal, Octubre del 2024

RESUMEN

La gestión de la seguridad de Activos de TI es crucial para garantizar la protección, confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos de una organización.

El desarrollo de esta auditoria se enfoca en la revisión de hardware y software, así como los aspectos relacionados con la seguridad de información, cumplimiento normativo y gestión de riesgos en donde se buscará evaluar la eficacia, seguridad y eficiencia en el manejo de los recursos tecnológicos de la empresa Embotelladora Mexicana S.A de C.V, identificando áreas de mejora, asegurando que la infraestructura tecnológica sea gestionada de manera óptima, emergiendo como un instrumento valioso para garantizar la competitividad de la empresa. El trabajo se desenvuelve siguiendo métodos de investigación, así como técnicas y pruebas para la recopilación de la información relevante y necesaria.

El capítulo I, consta de las generalidades del proyecto, donde se describe la empresa a auditar, su nombre, razón social, misión, visión, valores y una breve historia, así como el planteamiento del problema, la justificación y los objetivos a alcanzar.

El capítulo II, presenta el marco teórico donde vienen definidos algunos conceptos que se ocuparan a lo largo del proyecto, de igual forma de describen los tipos y métodos de investigación y las técnicas a utilizar para la recopilación de información.

El capítulo III, refiere al desarrollo del proyecto, donde se definen las actividades a realizarse por cada objetivo establecido al inicio del plan de auditoría, en este apartado se encontrará la implementación de las técnicas y tipos de investigación que se menciona en el capítulo anterior.

El capítulo IV, se mostrarán los resultados obtenidos a lo largo de la auditoria, así como los objetivos y beneficios logrados.

ÍNDICE DE CONTENIDOS

GENERALIDADES DEL PROYECTO	6
Introducción	7
Descripción de la empresa	8
Problema a resolver	11
Objetivos	12
MARCO TEÓRICO	15
Seguridad de la información	16
Tipo de investigación	17
Técnicas de investigación	17
Metodología de auditoria informática	21
DESARROLLO	25
3.1 Plan de trabajo	26
3.2 Análisis	43
Inspección y pruebas de seguridad física	48
Inspección a los activos hardware del departamento	60
Inspección y pruebas de seguridad lógica	98
Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 1	98
Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 2	113
Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 3	127
RESULTADOS	142
Hallazgos de seguridad física	145
Hallazgos de seguridad lógica	151
EVIDENCIAS	155
COMPETENCIAS DESARROLLADAS	159
FUENTES DE INFORMACIÓN	161
ANEXOS	163
Anexo 1. Cuestionario	163

ÍNDICE DE FIGURAS

<i>Figura 1. Organigrama general de la empresa Embotelladora Mexicana S.A de C.</i>	8
<i>Figura 2. Organigrama del departamento de Sistemas. Fuente: Michelle Araceli Flores</i>	8
<i>Figura 3. Evidencia de inventario desactualizado.</i>	155
<i>Figura 4. Inventario actualizado.</i>	155
<i>Figura 5. Nobreak</i>	156
<i>Figura 6. Nobreak nuevos.</i>	156

ÍNDICE DE TABLAS

<i>Tabla 1. Plan de trabajo de la auditoría con ISO 17799. Elaboración propia</i>	26
<i>Tabla 2. Planificación de la auditoría. Elaboración propia</i>	29
<i>Tabla 3. Evaluar y actualizar el plan de auditoría. Elaboración propia</i>	30
<i>Tabla 4. Redactar cuestionario. Elaboración propia.</i>	32
<i>Tabla 5. Aplicar cuestionario. Elaboración propia</i>	34
<i>Tabla 6. Inspección física al departamento. Elaboración propia</i>	36
<i>Tabla 7. Inspección de los activos hardware. Elaboración propia</i>	38
<i>Tabla 8. Inspección de software y activos de red. Elaboración propia</i>	40
<i>Tabla 9. Identificar hallazgos. Elaboración propia</i>	42
<i>Tabla 10. FODA seguridad física y lógica. Elaboración propia</i>	45
<i>Tabla 11. Análisis de riesgo. Elaboración propia</i>	46
<i>Tabla 12. Desarrollo de prueba de estructura física del departamento (paredes, ventanas, puerta).</i>	49
<i>Tabla 13. Desarrollo prueba de estructura física del departamento (mesas, sillas).</i>	51
<i>Tabla 14. Desarrollo de prueba de señalamiento.</i>	53
<i>Tabla 15. Desarrollo de prueba de uso de aire acondicionado.</i>	55
<i>Tabla 16. Desarrollo de prueba de cableado.</i>	57
<i>Tabla 17. Desarrollo de prueba laptop encargado de FROG</i>	60
<i>Tabla 18. Desarrollo de prueba de monitor de encargado de soporte y mantenimiento 1</i>	63
<i>Tabla 19. Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1</i>	65
<i>Tabla 20. Desarrollo de prueba de monitor de Becarios</i>	67
<i>Tabla 21. Desarrollo prueba de CPU de becarios.</i>	69
<i>Tabla 22. Desarrollo de prueba de laptop de encargada de departamento</i>	71
<i>Tabla 23. Desarrollo de prueba de monitor de la encargada de soporte y mantenimiento 2.</i>	74
<i>Tabla 24. Desarrollo de prueba de CPU de encargada de soporte y mantenimiento 2.</i>	76
<i>Tabla 25. Desarrollo de prueba de laptop de encargada de soporte y mantenimiento 3.</i>	79
<i>Tabla 26. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4</i>	81
<i>Tabla 27. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5</i>	84
<i>Tabla 28. Desarrollo de prueba de monitor de analista de datos de SAP.</i>	86
<i>Tabla 29. Desarrollo de prueba de CPU de analista de datos SAP.</i>	88
<i>Tabla 30. Desarrollo de prueba de mouses</i>	90
<i>Tabla 31. Desarrollo de prueba de teclados</i>	92
<i>Tabla 32. Desarrollo de prueba de telefonía</i>	94
<i>Tabla 33. Desarrollo de prueba de impresoras.</i>	97
<i>Tabla 34. Desarrollo de Prueba de Conectividad de la Red (Auxiliar de mantenimiento 1).</i>	99
<i>Tabla 35. Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 1).</i>	100
<i>Tabla 36. Desarrollo de prueba de instalación de software (Auxiliar de soporte 1)</i>	103
<i>Tabla 37. Desarrollo de prueba de licencia de software (Auxiliar de soporte 1)</i>	107

<i>Tabla 38. Desarrollo de prueba de seguridad del software (Auxiliar de soporte 1)</i>	<i>109</i>
<i>Tabla 39. Desarrollo de prueba de autenticación (Auxiliar de soporte 1)</i>	<i>111</i>
<i>Tabla 40. Prueba de conectividad de red. (Auxiliar de soporte 2).....</i>	<i>113</i>
<i>Tabla 41. Prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 2).</i>	<i>115</i>
<i>Tabla 42. Desarrollo de prueba de instalación de software (Auxiliar de soporte 2).....</i>	<i>118</i>
<i>Tabla 43. Desarrollo de prueba de licencias de software (Auxiliar de soporte 2).....</i>	<i>121</i>
<i>Tabla 44. Prueba de seguridad del software (Auxiliar de soporte 2).....</i>	<i>123</i>
<i>Tabla 45. Desarrollo de prueba de autenticación (Auxiliar de soporte 2)</i>	<i>125</i>
<i>Tabla 46. Desarrollo de prueba de conectividad de la red (Auxiliar de soporte 3).</i>	<i>127</i>
<i>Tabla 47. Desarrollo de prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 3).</i>	<i>129</i>
<i>Tabla 48. Desarrollo de prueba de instalación de software (Auxiliar de soporte 3).....</i>	<i>132</i>
<i>Tabla 49. Prueba de licencias de software. Auxiliar 3.</i>	<i>135</i>
<i>Tabla 50. Desarrollo de prueba de seguridad del software (Auxiliar de soporte 3)</i>	<i>138</i>
<i>Tabla 51. Desarrollo de prueba de autenticación (Auxiliar de soporte 3)</i>	<i>140</i>
<i>Tabla 52. Lista de recomendaciones/contramedidas de acuerdo con la norma ISO 17799</i>	<i>153</i>

CAPÍTULO I

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

Actualmente en las empresas y organizaciones la información y la tecnología son pilares esenciales para el desarrollo y la continuidad operativa, la seguridad de los activos de Tecnologías de la Información (TI) emerge como un aspecto fundamental y dependen cada vez más de sistemas, redes y datos electrónicos para llevar a cabo sus operaciones diarias, lo que convierte a los activos de TI en un elemento principal para el logro de sus objetivos estratégicos.

Las amenazas, los riesgos lógicos y físicos produce daños significativos a la integridad y confidencialidad de la información en empresas. En este contexto, existen marcos internacionalmente reconocidos para el desarrollo de una auditoria de seguridad de activos de TI, como la norma ISO 17799, también conocida como ISO 27001 la cual se considera una herramienta esencial para evaluar y fortalecer los controles internos para identificar vulnerabilidades y aminorar los riesgos potenciales.

Este proyecto tiene como punto principal la realización de una auditoria de seguridad de los activos de TI en la empresa Embotelladora Mexicana S.A de C.V, con el propósito de analizar las medidas de seguridad implementadas y proponer recomendaciones para fortalecer la protección de la información y de los activos en base a la ISO 17799

DESCRIPCIÓN DE LA EMPRESA

Nombre, razón social

EMBOTELLADORA MEXICANA S.A DE C.V SUC. TULTITLAN

Ubicación

Blvd. Tultitlán No. 183, Barrio los Reyes, Tultitlán, Estado de México

Organigrama

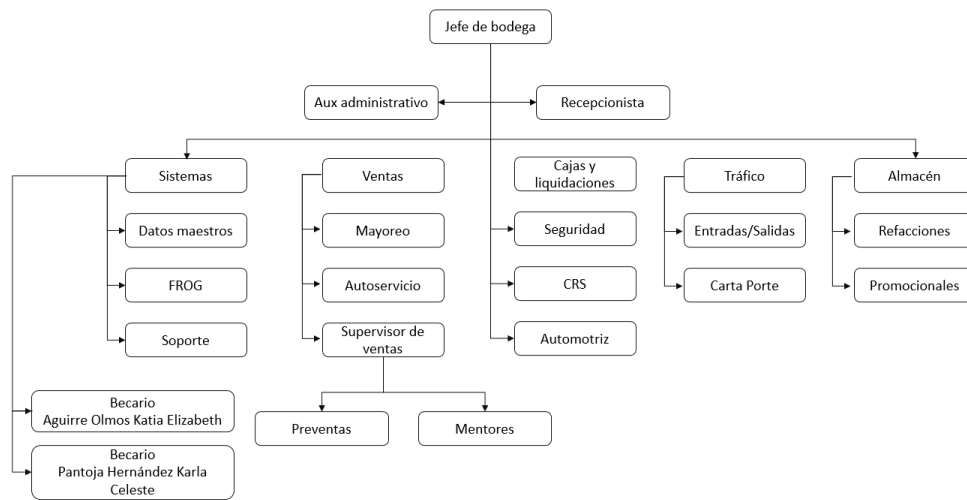


Figura 1. Organigrama general de la empresa Embotelladora Mexicana S.A de C. Fuente: Michelle Araceli Flores

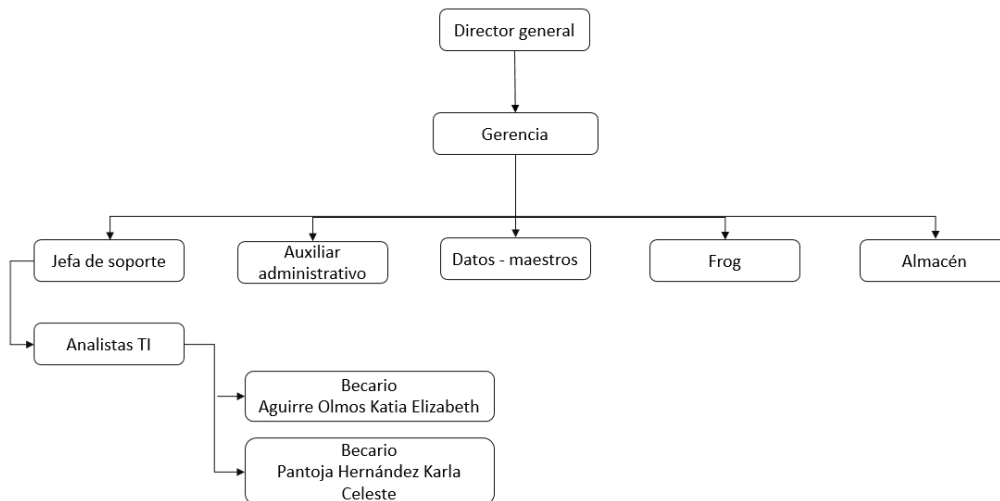


Figura 2. Organigrama del departamento de Sistemas. Fuente: Michelle Araceli Flores

Sector productivo de la empresa

Terciario

MISIÓN

“Ser líderes en la venta de refrescos satisfaciendo las necesidades de nuestros clientes mediante la producción, adquisición y distribución de productos con la más alta calidad, proporcionando un servicio. excelente. Lograr altos niveles de productividad para cumplir nuestro compromiso de bienestar con los trabajadores, de responsabilidad social con la comunidad y de rentabilidad con los accionistas, manteniendo la permanencia de la empresa, siendo congruentes con nuestra declaración de principios.

VISIÓN

Estando siempre cerca de nuestros consumidores, en todas partes y en todas las ocasiones. Actuando de acuerdo con principios éticos, proveyendo claridad en su interpretación, viviéndolos y asegurándonos de su aplicación a través de toda la organización. Proporcionando información al personal sobre su trabajo, lo que se espera de ellos y de su desempeño, así como de sus metas y objetivos.

Promoviendo la Integración y el trabajo de equipo. Proporcionando a los accionistas información correcta y suficiente. Actuando con honestidad y eficiencia en el manejo de sus recursos. Respetando las leyes y reglamentos y colaborando en la solución de los problemas de la comunidad

VALORES

- El fomento a la mexicanidad.
- La total satisfacción de nuestros clientes.
- El desarrollo integral de nuestros empleados.
- El respeto a la naturaleza y a los valores éticos.
- Honestidad y confianza
- Alta calidad en productos y servicios
- Responsabilidad social y con las familias

Reseña Histórica de la Embotelladora Mexicana S.A de C.V

Embotelladora Mexicana, S.A. de C.V. opera desde 1983 y forma parte de Consorcio AGA, el cual, nace en la ciudad de Guadalajara, Jalisco, a principios del siglo pasado, ubicándose como una empresa pionera en los mercados del agua purificada y refrescos gaseosos.

El capital accionario es 100% mexicano y está dirigido por empresarios mexicanos lo que la ha convertido en la primera empresa en el país con un verdadero espíritu nacional.

Su filosofía es marcada por poseer ejecutivos 100% mexicanos. Todos los sabores de los refrescos son elaborados y procesados en la planta de concentrados de la misma empresa, empleando materias primas naturales mexicanas, tales como el tamarindo, la manzana, la mandarina, etc....

Embotelladora Mexicana, S.A. de C.V. es una empresa completamente integrada, desde la fabricación de sus envases pet, las tapa roscas, hasta el llenado y distribución de sus refrescos.

Embotelladora Mexicana, S.A. de C.V. contribuye al desarrollo económico del país, generando muchos empleos a las familias mexicanas, que orgullosamente laboran en una empresa de éxito y reconocimiento a nivel nacional e internacional.” (Jarritos, s.f)

PROBLEMA A RESOLVER

Embotelladora Mexicana S.A de C.V es una empresa especializada en producir y distribuir refrescos gaseosos de alta calidad que opera desde 1983 y forma parte del Consorcio AGA naciente en la Ciudad de Guadalajara, Jalisco. Actualmente cuenta con 11 centros de distribución; 8 en el área metropolitana y 3 en el interior de la república. Su planta principal está ubicada en Tultitlán, Estado de México, en la cual a lo largo de los años se ha tenido un considerable crecimiento en las áreas y el personal que conforma dicha planta.

Debido a esta situación se han tenido que reubicar distintas áreas en la planta, afectando la ubicación del mobiliario y activos de TI, dificultando el control, la efectividad y eficiencia de operaciones, así como el cumplimiento de reglas y lineamientos en la seguridad de información y activos, que el personal de las áreas debe cumplir.

Por otra parte, no se tiene el registro de una auditoria de seguridad de información de activos de TI antes realizada en la planta y el no realizar el proyecto de auditoría planteado, podría traer consecuencias a la empresa, como las amenazas cibernéticas, pérdida de datos y acceso no autorizado, lo que conlleva a una incapacidad por parte de la empresa para mantener la continuidad del negocio en caso de fallos del sistema o desastres cibernéticos.

OBJETIVOS

OBJETIVO GENERAL

Diagnosticar el funcionamiento general y control interno de la seguridad de TI de la empresa Embotelladora Mexicana S.A de C.V

OBJETIVOS ESPECÍFICOS

- 1) Planificación de auditoria
 - a) Establecer objetivos y alcances
 - b) Estipular procesos y procedimientos a utilizar
- 2) Evaluar y actualizar el plan establecido para asegurar la efectividad
 - a) Recopilar y revisar la información relevante del plan de auditoría
 - b) Identificar las áreas de mejora y determinar si requieren ajustes o cambios
 - c) Realizar una evaluación de los riesgos actuales que podrían afectar la realización de la auditoría
 - d) Analizar y ajustar el alcance de la auditoría para asegurarse de que sea apropiado y completo
- 3) Redactar cuestionario
 - a) Definir objetivo de la encuesta
 - b) Identificar los puntos a tratar sobre el departamento
 - c) Seleccionar la muestra
 - d) Formular las preguntas
- 4) Aplicar cuestionario al personal
 - a) Programar reuniones para los usuarios a entrevistar
 - b) Dar a conocer la encuesta y las partes que la componen
 - c) Aplicar la encuesta al personal involucrado
 - d) Evaluar los resultados obtenidos
- 5) Realizar inspección física del departamento de sistemas
 - a) Inspeccionar la integridad estructural del departamento de sistemas
 - b) Revisar el funcionamiento de servicios como aire acondicionado, calefacción, etc
 - c) Inspeccionar la instalación del cableado de red y eléctrico
 - d) Conocer las medidas de seguridad
 - e) Poner a prueba las medidas de seguridad
- 6) Realizar inspección de los activos hardware del departamento de sistemas

- a) Obtener las características de hardware de los activos
 - b) Revisar el estado en el que se encuentran los activos (computadoras, routers, switches)
 - c) Revisar en qué estado se encuentran los periféricos (monitores, teclados, mouses)
- 7) Realizar inspección del software y servicios de red del departamento de sistemas
- a) Revisar el software que se encuentra instalado en los equipos de cómputo
 - b) Realizar un análisis en busca de software malicioso
 - c) Realizar análisis en los servicios de red
- 8) Identificar hallazgos
- a) Identificar las fortalezas y debilidades del departamento

JUSTIFICACIÓN

Dado el crecimiento de áreas y personal de la planta principal de la Embotelladora Mexicana S.A de C.V ubicada en Tultitlan, realizar una auditoria bajo la norma ISO 17799 tiene como finalidad contribuir a la toma de medidas preventivas y correctivas pertinentes a cada uno de los casos encontrados durante el proceso además de disminuir la vulnerabilidad a la que las TI de la empresa podría estar expuesta de manera interna y externa, protegiendo y mejorando así la gestión de la seguridad de TI, su control, efectividad y eficiencia de operaciones principalmente del departamento de sistemas.

La seguridad de las TI, sus activos y la comunicación es vital para el funcionamiento adecuado de servicios y operaciones de las distintas áreas que conforman la planta debido a que, si esta fallara, el personal estaría en una situación ineficiente retrasando así la realización de las diversas actividades del día en la planta y los procesos externos.

Es por esto, que la Embotelladora Mexicana S.A de C.V, ha considerado pertinente llevar a cabo la auditoría, dado que esta proporcionará información crítica sobre la infraestructura de tecnologías de la información. Se percibe como un ámbito propicio para identificar oportunidades de optimización y para implementar estrategias destinadas a la mitigación de riesgos.

CAPÍTULO II

MARCO TEÓRICO

2.1 Seguridad de la información

“Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Implica la implementación de herramientas y tecnologías que mejoran la visibilidad de la organización sobre dónde residen sus datos críticos y cómo se utilizan. Idealmente, estas herramientas deberían poder aplicar protecciones como el cifrado, el enmascaramiento de datos y la redacción de archivos confidenciales, y deberían automatizar los informes para agilizar las auditorías y cumplir con los requisitos regulatorios” (IBM, s.f).

La seguridad de la información se alcanza mediante la implementación de un conjunto adecuado de controles. Esto incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Es necesario establecer, implementar, monitorear, revisar y mejorar estos controles según sea necesario para garantizar el cumplimiento de los objetivos específicos de seguridad y negocios.

En 1995 el British Standard Institute publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información. En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.

Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Aplicable por toda organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la tecnología. En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (no existe equivalente ISO).”

“La estructura de la normatividad de gestión en seguridad de sistemas de información, norma ISO 17799, queda especificada en diez componentes, que incluyen política de seguridad, organización de la seguridad, control y clasificación de los recursos de información, seguridad de personal, seguridad física y ambiental, manejo de las comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, manejo de la continuidad de la empresa, así como el cumplimiento” (Castillo, s.f).

Para realizar la auditoría sobre la seguridad de los activos de TI mediante la ISO 17799, se definió que el enfoque de la investigación se hará de forma cualitativa y cuantitativa, ya que se obtendrá información directa por medio de una técnica de investigación y prueba (encuesta) y se determinarán cuantos hallazgos se encuentran a lo largo de la auditoría.

Tipo de investigación

- **Descriptivo:** Se aplicarán elementos claves de este tipo de investigación, como la descripción detallada, los datos cuantitativos y cualitativos, diseño de estudio, como lo son las encuestas, observaciones y análisis de contenido.
- **Explicativo:** Se usarán aspectos de este tipo de investigación, como la identificación de causas efecto, donde se buscará identificar variables independientes (causas) y variables dependientes (efectos) en una relación.

Técnicas de investigación

- **Análisis Documental:** Se examinarán las documentaciones relevantes, como las políticas de seguridad, procedimientos operativos, el inventario que posee el departamento respecto a sus recursos tecnológicos.
- **Encuesta:** Se le aplicarán al personal que utiliza las instalaciones y activos del departamento de Sistemas.
- **Análisis de vulnerabilidades:** Se ocuparán herramientas de software para identificar posibles vulnerabilidades en los equipos de cómputo
- **Revisión física:** Se evaluará la seguridad física de los sistemas, como la protección de servidores y equipos de red

Según Coppola (s.f) menciona la existencia de siete características importantes de la seguridad informática:

- **Confidencialidad:** Las acciones de seguridad informativas están orientadas a proteger la confidencialidad, es decir, la información de acceso no autorizado y garantizar que solo las personas adecuadas tengan acceso a ella.
- **Integridad:** Esta característica es la capacidad de mantener la precisión y la integridad de los datos, garantizando que no se alteren o manipulen sin autorización. Algo fundamental en esta época en la que se maneja una enorme cantidad de datos.
- **Disponibilidad:** Las medidas de seguridad informática deben garantizar que los sistemas y la información estén disponibles para su uso en todo momento, y que cualquier interrupción en la disponibilidad sea mitigada y resuelta rápidamente.
- **Autenticidad:** Parte fundamental de la labor de la seguridad informática es corroborar la identidad de un usuario o recurso, así que protegerá que dicha identidad no se falsifique.
- **Resiliencia:** A través de la seguridad informática una organización tendrá la capacidad de recuperarse rápidamente de cualquier interrupción o ataque de seguridad, ya que es crucial para las empresas ser resilientes informáticos.

- **Seguridad en capas:** Se refiere a la implementación de múltiples medidas de seguridad en diferentes niveles, para garantizar una mayor protección contra posibles amenazas.
- **Actualización constante:** La seguridad informática es un campo en constante evolución, por lo que es necesario actualizar y mejorar regularmente las medidas de seguridad a fin de estar protegidos adecuadamente contra nuevas amenazas.

Tipos de seguridad informática según (Coppola, HUBSPOT, s.f):

1. Seguridad de red

La seguridad en la red se enfoca en la protección de la red de una empresa u organización, mediante medidas de protección que identifiquen y repelen amenazas externas, hackers, malware y virus. Proteger la red es igual de importante que proteger los equipos propiamente dichos. La seguridad de la red está formada por todas las acciones dirigidas a proteger el acceso, uso, integridad y seguridad de la red y los datos que fluyen a través de ella. Dentro de las herramientas de protección con las que se cuenta tenemos: antivirus, cortafuegos o firewalls, utilización de redes privadas (VPN) para garantizar un acceso seguro y sistemas de prevención de intrusos (IPS).

2. Seguridad de datos

Este tipo de seguridad es fundamental, ya que sus acciones se centran en proteger los datos durante el proceso de recopilación y gestión de estos. Así se protege la información de la compañía, como los datos de los clientes, informes financieros y registros de empleados; por supuesto, uno de los pilares de la seguridad informática es la prevención de pérdida de datos.

3. Seguridad de aplicaciones

La seguridad informática de las aplicaciones empresariales es sumamente importante para que una organización opere de la mejor manera. Sus acciones se encargan de proteger las aplicaciones que usa una empresa, como el correo electrónico, la mensajería instantánea y los programas personalizados.

4. Seguridad de la nube

Este tipo de seguridad es más concreto, pero sus acciones abarcan muchas plataformas y software que operan en la nube. Busca la protección de los datos y aplicaciones alojados en la nube, incluyendo la seguridad de su infraestructura y los datos almacenados en ella.

5. Seguridad de la identidad

Esta tiene que ver con la protección de la identidad digital de los empleados y los clientes, incluyendo el control de acceso y la autenticación de usuarios, incluyendo el SSO.

6. Seguridad de software

El software está formado por las aplicaciones y programas instalados en los dispositivos, y estos sistemas son vulnerables a diferentes tipos de ataques que pueden causar daños desde funcionamiento hasta robo de información.

Un software puede tener defectos que involucren desde el diseño, hasta fallas en el manejo de errores y desbordamientos de buffer. La alta frecuencia con la que los intrusos acceden sin autorización es lo que motiva al constante desarrollo de actualizaciones con el fin de ir corrigiendo errores sobre la marcha.

7. Seguridad de hardware

Los sistemas de seguridad para hardware son los que aportan el mayor nivel de protección contra ciberataques. Para tener noción de la seguridad de un dispositivo y cómo reforzarla, se puede evaluar los puntos débiles que tienen los dispositivos desde su fabricación y cómo podrían ser víctimas de algún ataque.

Dentro de las herramientas de protección de hardware tenemos los firewalls o cortafuegos de hardware y servidores proxy, utilizados para controlar el tráfico en la red. Además, tenemos los módulos de seguridad de hardware (HSM) que se encargan del suministro de claves encriptadas para diferentes sistemas.

“Una gran parte de los datos que resguarda una empresa es información confidencial, como propiedad intelectual, datos financieros, información personal u otros tipos de datos, para los que el acceso o la exposición no están autorizados. Pese a esto, la transmisión de datos confidenciales se da a través de redes y otros dispositivos día a día. Por eso la seguridad informática es necesaria, pues se encarga de proteger esa información y los sistemas utilizados para procesarla y almacenarla. Cada tecnología en la que se alojen entornos digitales de una organización debe tener alguna forma o medida de seguridad informática.” (Coppola, HUBSPOT, s.f)

Según Coppola (s.f), dentro de la auditoría informática destacan los siguientes tipos (entre otros dependiendo los objetivos específicos y el alcance:

1. Auditoría de cumplimiento normativo

El propósito de esta auditoría es examinar si una entidad cumple con las normas legales y reglamentarias relacionadas con la seguridad de la información. Este análisis puede incluir la conformidad con leyes de privacidad de datos, normativas específicas de la industria, como el PCI-DSS para el ámbito de pagos con tarjeta, o estándares a nivel internacional, como la ISO 27001.

2. Auditoría de políticas y procedimientos

Se enfoca en examinar y valorar las políticas, estándares y procesos de seguridad implementados dentro de una entidad. El propósito es verificar si estas políticas y procedimientos son apropiados, se mantienen al día y se aplican efectivamente en la realidad operativa.

3. Auditoría de controles de acceso

Se enfoca en analizar los sistemas y enfoques empleados para supervisar el acceso a los sistemas y datos de la entidad. Esto implica examinar la administración de contraseñas, los privilegios de los usuarios, la autenticación multifactorial, y otros mecanismos de control.

4. Auditoría de seguridad de redes

Se centra en analizar la estructura de red de una entidad para descubrir posibles vulnerabilidades y amenazas de seguridad. Esto puede incluir la realización de pruebas de penetración, el análisis de la configuración de los cortafuegos, la detección de intrusiones y la evaluación de la efectividad de la protección de la red contra posibles ataques.

5. Auditoría de seguridad de aplicaciones

Se enfoca en analizar la seguridad de las aplicaciones y sistemas creados o empleados por la entidad. Esto incluye la revisión del código fuente, la configuración de seguridad de las aplicaciones, la autenticación y autorización de usuarios, además de la protección contra amenazas comunes, como inyecciones SQL o scripts entre sitios (cross-site scripting, XSS).

6. Auditoría de gestión de incidentes

Se encarga de valorar las prácticas y la capacidad de reacción de una entidad frente a eventos de seguridad. Esto abarca la revisión de la preparación y planificación para afrontar incidentes, la detección y comunicación de estos eventos, la gestión de la respuesta y recuperación, así como el análisis de lecciones aprendidas de incidentes previos.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

1. Pruebas sustantivas:

“Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información” (ALTP, 2018).

2. Pruebas de cumplimiento:

“Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente” (ALTP, 2018).

Principales herramientas de las que dispone un auditor informático:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico (Trazas y/o huellas)
- Flujogramas
- Listas de chequeo (checklist)
- Mapas conceptuales
- Inventario

2.1.1 Metodología de auditoria informática

Según el autor Altp (2018), La obtención de datos, el examen, la implementación de distintas pautas según el tipo de auditoría, la identificación de descubrimientos y la realización de pruebas que respalden estos resultados son fundamentales en la ejecución de una auditoría. Para alcanzar el desenlace deseado, es necesario seguir una secuencia de pasos que proporcione claridad y organización en la aplicación de la auditoría.

“El alcance de la auditoria expresa los límites de esta. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoria, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del informe final” (ALTP, 2018).

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

- **Organización:** para el auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizarlo el auditor deberá fijarse en:
- **Organigrama:** el organigrama expresa la estructura oficial de la organización a auditar. Permite identificar las jerarquías, dependencias y direcciones entre las áreas existentes.
- **Departamentos:** se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

- **Relaciones Jerárquicas y funcionales entre órganos de la Organización:** el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.
- **Flujos de información:** además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales.
- **Número de puestos de trabajo:** el equipo auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales distintas.
- **Número de personas por puesto de trabajo:** es un parámetro que los auditores informáticos deben tener en cuenta ya que la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.
- **Entorno operacional:** el auditor informático debe tener una referencia del entorno en el que va a desenvolverse y se obtiene determinando lo siguiente:
- **Situación geográfica de los sistemas:** se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa, continuando con la verificación de la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- **Arquitectura y configuración de hardware y software:** cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, para esto es importante que los auditores, en su estudio inicial, tengan en su poder la distribución e interconexión de los equipos.
- **Inventario de hardware y software:** el auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto al hardware figurarán las CPU's, unidades de control local y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
- **Redes de comunicación:** al realizar el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, igualmente, poseerán información de las redes locales de la Empresa y todo lo que tenga que ver con la red de comunicaciones.

De acuerdo con el autor Altp (2018), mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoria.

1. **Recursos humanos:** La cantidad de recursos necesarios varía según la extensión de lo que se va a auditar. Las cualidades y perfiles del personal elegido se determinan en función del área sujeta a auditoría. También es importante destacar que la práctica de auditoría suele llevarse a cabo tanto por profesionales universitarios como por individuos con experiencia comprobada en diversas disciplinas.
2. **Recursos materiales:** los recursos materiales del auditor son de dos tipos:
 - **Recursos software** como son, cantidad y complejidad de BD y ficheros, que son programas propios de la auditoria, son muy potentes y flexibles.
 - **Recursos materiales hardware:** los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Por lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, scanner, etc.

Según (ALTP, 2018), existen técnicas que hacen que el auditor el aplique de acuerdo con su juicio y al tipo de auditoría a ejecutar son:

- Técnicas de Trabajo.
- Análisis de la información obtenida del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.
- Inspección.
- Confirmación.
- Investigación.
- Certificación.
- Observación.
- Herramientas:
- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoria (Generadores de programas)
- Matrices de riesgo.

El informe comienza con la fecha de comienzo de la auditoria y la fecha de redacción de este. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Siguiendo los siguientes pasos:

- Definición de objetivos y alcance de la auditoria.
- Enumeración de temas considerados.
- Cuerpos expositivos.

Modelo conceptual de la exposición del informe final, según (ALPT, 2018):

- El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El informe debe consolidar los hechos que se describen en el mismo.
- El término de «hechos consolidados» adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:
 1. El hecho debe poder ser sometido a cambios.
 2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
 3. No deben existir alternativas viables que superen al cambio propuesto.
 4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

CAPÍTULO III

DESARROLLO

3.1 Plan de trabajo

Un plan de trabajo para una auditoría es esencial ya que proporciona organización y estructura, estableciendo los objetivos, definiendo el alcance, facilita la asignación eficiente de recursos, como el personal. Tiempo, tecnologías, herramientas y técnicas a utilizar, así como anticipar posibles obstáculos, lo cual permite desarrollar estrategias para abordar los problemas que puedan surgir a lo largo de la auditoría. De igual forma, establece un marco de seguimiento y control de progreso de la auditoría, asegurando que se cumplan los objetivos, estándares y regulaciones aplicables (véase tabla 1. Plan de trabajo de la auditoría)

Tabla 1. Plan de trabajo de la auditoría con ISO 17799. Elaboración propia

Plan de trabajo de la auditoría con ISO 17799 para gestión de la seguridad de activos de TI de la empresa Embotelladora Mexicana jarritos S.A de C.V		
	FECHAS ESTIMADAS	
	Inicio: 11 de Octubre del 2023	Termino:19 de Febrero del 2024
OBJETIVO GENERAL	Diagnosticar el funcionamiento general y control interno de la seguridad de TI de la empresa Embotelladora Mexicana S.A de C.V	
OBJETIVOS ESPEÍFICOS	- Objetivo: Planificar auditoria Actividades: - Establecer los objetivos y alcances - Estipular procesos y procedimientos a utilizar - Objetivo: Evaluar el plan establecido para asegurar la efectividad Actividades: - Recopilar toda la información relevante del plan de auditoría - Identificar las áreas de mejora y determinar si se requieren ajustes o cambios - Realizar una evaluación de los riesgos actuales y emergentes que podrían afectar la realización de la auditoría - Analizar el alcance de la auditoría para asegurarse de que sea apropiado y completo - Objetivo: Redactar cuestionario como tipo de evidencia Actividades: - Definir objetivo de la encuesta	

Tabla 1 (continuación). Plan de trabajo de la auditoría con ISO 17799. Elaboración propia

Plan de trabajo de la auditoría con ISO 17799 para gestión de la seguridad de activos de TI de la empresa Embotelladora Mexicana jarritos S.A de C.V	
OBJETIVOS ESPEÍFICOS	3.2. Identificar los puntos a tratar sobre el departamento 3.3. Seleccionar la muestra 3.4. Formular las preguntas 4. Objetivo: Aplicar cuestionario al personal Actividades: 4.1. Programar reuniones para los usuarios a entrevistar 4.2. Aplicar la encuesta al personal involucrado 4.3. Evaluar los resultados obtenidos 5. Objetivo: Realizar inspección física del departamento de sistemas Actividades: 5.1. Inspeccionar la integridad del departamento de sistemas 5.2. Revisar el funcionamiento de servicios como aire acondicionado, calefacción, etc 5.3. Inspeccionar la instalación del cableado de red y eléctrico 5.4. Conocer las medidas de seguridad 5.5. Probar las medidas de seguridad 6. Objetivo: Realizar inspección de los activos hardware del departamento de sistemas Actividades: 6.1. Obtener las características de hardware de los activos 6.2. Revisar el estado en el que se encuentran los activos (computadoras, routers, switches) 6.3. Revisar en qué estado se encuentran los periféricos (monitores, teclados, mouses) 7. Objetivo: Realizar inspección del software y servicios de red del departamento de sistemas Actividades: 7.1. Revisar el software que se encuentra instalado en los equipos de cómputo 7.2. Realizar un análisis en busca de software malicioso 7.3. Realizar un análisis en los servicios de red

	8. Objetivo: Identificar hallazgos Actividades: 8.1. Identificar las fortalezas y debilidades del departamento
--	---

Tabla 1 (continuación). Plan de trabajo de la auditoría con ISO 17799. Elaboración propia

Plan de trabajo de la auditoría con ISO 17799 para gestión de la seguridad de activos de TI de la empresa Embotelladora Mexicana jarritos S.A de C.V	
ALCANCE	Evaluar el estado de las instalaciones físicas del departamento de sistemas de la empresa Embotelladora Mexicana S.A de C.V, incluyendo la disponibilidad y calidad de los equipos de cómputo, la conectividad de red y la disposición de mobiliario, así como las medidas de seguridad implementadas, como sistemas de control de acceso, protección contra virus y malware.
MIEMBROS DEL EQUIPO AUDITOR Y PERSONAS INVOLUCRADAS	Michelle Araceli Flores Florido (Encargada del Departamento) Aguirre Olmos Katia (Auditor) Pantoja Hernández Karla (Auditor)
DISTRIBUCIÓN DEL INFORME DE AUDITORIA Y FECHA DE EMISIÓN	19 de Febrero 2024

La planificación de la auditoría (véase tabla 2. Planificación de la auditoría) es una herramienta crucial en el ámbito de la auditoría, diseñada para organizar y estructurar el proceso de evaluación de una entidad financiera, organización o sistema. Esta tabla incluye información clave para guiar a los auditores a lo largo de cada fase del proceso de planificación.

Tabla 2. Planificación de la auditoría. Elaboración propia

Plan de Trabajo de la Auditoría con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: 1. Planificación de la Auditoria	FECHAS ESTIMADAS				
	INICIO: 16 de Octubre 2023			TÉRMINO: 20 de Octubre 2023	
DESCRIPCIÓN DEL OBJETIVO:	Redactar el plan de auditoria para el lugar a evaluar (Departamento de Sistemas) para llevar un control de actividades.				
PERSONAS INVOLUCRADAS	Encargada del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
1.1 Establecer objetivos y alcances	Investigación, análisis de información	Equipo de cómputo, procesador de texto, internet	Analizar a simple vista el lugar a auditar, para hacer una redacción de los objetivos y alcances que se tienen para la auditoria	- Aguirre Olmos KatiaElizabeth - Pantoja Hernández Karla Celeste	3 días
1.2 Estipular los procesosy procedimientos a utilizar	Observación, análisis de información, investigación	Equipo cómputo, procesador de texto, documentos proporcionados por la encargada del departamento, internet	A partir de los objetivos y alcances, estipular los procesos y procedimientos que se van a utilizar a lo largo de la auditoría.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	3 días

Evaluar y actualizar el plan de auditoría (véase tabla 3. Evaluar y actualizar el plan de auditoría), es una herramienta dinámica que permite revisar y mejorar continuamente el plan previamente establecido. Su función principal es garantizar que el plan de auditoría sea relevante, efectivo y capaz de adaptarse a cambios en el entorno empresarial.

Tabla 3. Evaluar y actualizar el plan de auditoría. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: <u>2. Evaluar y actualizar el plan previamente establecido para asegurarse que sea relevante y efectivo</u>	FECHAS ESTIMADAS				
	INICIO: 23 de Octubre 2023		TÉRMINO: 7 de Noviembre 2023		
DESCRIPCIÓN DEL OBJETIVO:	Revisar todos los elementos del plan de auditoría y realiza los ajustes necesarios.				
PERSONAS INVOLUCRADAS	Encargada del departamento de sistemas: Michelle Araceli Flores Florido Audidores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
2.1 Recopilar y revisar la información relevante del plan de auditoría.	Observación	Equipo de Cómputo, internet	Obtener una comprensión completa y precisa del alcance, los objetivos, los procedimientos y los recursos asignados a la auditoría.	- Flores Florido Michelle Araceli - Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	2 días
2.2 Identificar las áreas de mejora y determinar si se requieren ajustes o cambios.	Observación, análisis de información	Equipo de Cómputo, internet	Asegurar que la auditoría se realice de manera eficiente y efectiva, y que se logren los resultados deseados	- Flores Florido Michelle Araceli - Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	3 días

2.3 Realizar una evaluación de los riesgos actuales que podrían afectar la realización de la auditoría.	Observación	Equipo de Cómputo, internet	Identificar y comprender los posibles riesgos que podrían impactar negativamente en el proceso de auditoría y en la obtención de resultados confiables.	• Flores Florido Michelle Araceli • Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	5 días
2.4 Analizar y ajustar el alcance de la auditoría para asegurarse de que sea apropiado y completo	Análisis de información, observación	Equipo de cómputo	Cubrir todos los elementos y áreas relevantes que deben ser evaluados.	• Flores Florido Michelle Araceli • Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	2 días

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

La redacción de cuestionarios (véase tabla 4. Redactar cuestionario) es una herramienta diseñada para estructurar preguntas específicas que permitan recopilar información relevante y confiable como evidencia durante el proceso de auditoría.

Tabla 4. Redactar cuestionario. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: <u>3.Redactar cuestionario como tipo de evidencia</u>	FECHAS ESTIMADAS				
	INICIO: 8 de Noviembre 2023			TÉRMINO: 17 de Noviembre del 2023	
DESCRIPCIÓN DEL OBJETIVO:	Redactar una serie de preguntas en general sobre el departamento de sistemas para el personal involucrado.				
PERSONAS INVOLUCRADAS	Encargado del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
3.1. Definir Objetivo de la encuesta	Análisis de información	Procesador y Editor de Texto, Equipo de cómputo, Memoria USB, Impresora	Proporcionar una dirección clara para guiar la toma de decisiones durante el seguimiento del proyecto.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	2 días
3.2. Identificar los puntos a tratar sobre el departamento	Investigación Análisis de información	Procesador y Editor de Texto, Equipo de cómputo, Memoria USB.	Determinar los temas o aspectos específicos que se abordarán en el cuestionario con el fin de obtener información relevante y significativa.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	2 días
3.3. Seleccionar la muestra	Investigación, Análisis de información	Procesador y Editor de Texto, Equipo de cómputo,	Obtener una representación adecuada y precisa de la población objetivo que se desea	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	2 días

		Memoria USB, organigrama del departamento.	estudiar		
3.4. Formular las preguntas	Análisis de información	Procesador y Editor de Texto, Equipo de cómputo, Memoria USB.	Garantizar la calidad de los datosrecopilados y la validez de los resultados obtenidos.	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	2 días

(Véase tabla 5. Aplicar cuestionario), la tabla se enfoca en la implementación de preguntas estructuradas a los miembros del personal de una entidad o empresa y programar las reuniones para dar a conocer las preguntas que componen la encuesta.

Tabla 5. Aplicar cuestionario. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: 4. <u>Aplicar cuestionario al personal.</u>	FECHAS ESTIMADAS				
	INICIO: 20 de Noviembre 2023			TÉRMINO: 7 de Diciembre 2023	
DESCRIPCIÓN DEL OBJETIVO:	Aplicar la encuesta al personal que utiliza la instalación y al encargado del departamento, a través de una reunión previamente programada.				
PERSONAS INVOLUCRADAS	Encargado del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
4.1. Programar reuniones para al personal a entrevistar	Organización	Equipo de cómputo, dispositivo móvil.	Establecer un horario conveniente para el personal y encargado del departamento de sistemas en el cual no afecte sus múltiples y distintas actividades.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	1 día
4.2. Dar a conocer la encuesta y las partes que la componen	Comunicación	Procesador y Editor de Texto, Equipo de cómputo, Memoria USB, dispositivo móvil.	Informar al encargado las partes que componen la encuesta, así como el propósito de su aplicación.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	1 día

4.3. Aplicar encuesta al personal involucrado	Recopilación de datos	Equipo de cómputo, Memoria USB, internet y dispositivo móvil	Obtener los datos necesarios del personal y el encargado para realizar un análisis sobre la operatividad del departamento de sistemas.	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	6 días
4.4. Evaluar los resultados obtenidos	Análisis y recopilación de datos	Equipo de cómputo, Memoria USB, internet y dispositivo móvil.	Realizar un análisis en base a la aplicación y obtener resultados de la percepción del personal y encargado del departamento.	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	6 días

Planear la inspección física (véase tabla 6. inspección física del departamento) es una herramienta diseñada para guiar y documentar el proceso de examen físico de las instalaciones y equipos relacionados con el departamento de sistemas.

Tabla 6. Inspección física al departamento. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: <u>5. Realizar inspección física del departamento de Sistemas</u>	FECHAS ESTIMADAS				
	INICIO: 8 de Diciembre 2023			TÉRMINO: 4 de Enero 2024	
DESCRIPCIÓN DEL OBJETIVO:	Una vez que se realizado el análisis del plan de auditoría, se procederá a inspeccionar de forma física las instalaciones del departamento de Sistemas, evaluando el estado en el que se encuentra la instalación misma.				
PERSONAS INVOLUCRADAS	Encargada del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
5.1 Inspeccionar la integridad estructural del departamento de sistemas	Recopilación de datos y observación	Dispositivo móvil o laptop y procesador de texto	Conocer la integridad estructural del departamento, denotando grietas en paredes, el estado de las ventanas y puertas. Así como el estado de las mesas y sillas	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	3 días
5.2 Revisar el funcionamiento de servicios como aire acondicionado o calefacción	Recopilación de datos y observación	Dispositivo móvil o laptop y procesador de texto	Conocer si el departamento cuenta con servicios de calefacción y/aire acondicionado y saber si se encuentran en buen estado y operando	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	5 días

5.3 Inspeccionar la instalación del cableado de red y eléctrico	Recopilación de datos y observación	Dispositivo móvil o laptop y procesador de texto	Conocer si el cableado fue instalado correctamente siguiendo las medidas de seguridad adecuadas, así como el estado de este	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	5 días
5.4 Conocer las medidas de seguridad	Recopilación de datos y observación	Dispositivo móvil o laptop y procesador de texto	Saber con qué medidas de seguridad cuenta el departamento ante incidentes y/o situaciones de riesgo	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	2 días
5.5 Poner a prueba las medidas de seguridad	Recopilación de datos, observación y ejecución de pruebas	Dispositivo móvil	Saber que las medidas de seguridad implementadas en el departamento son efectivas	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	5 días

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

La tabla 7. Inspección de los activos hardware, del departamento es una herramienta específica diseñada para realizar una evaluación detallada y documentada de los activos de hardware, como parte de las prácticas de gestión de activos y mantenimiento.

Tabla 7. Inspección de los activos hardware. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: <u>6. Inspección de los activos hardware del departamento</u>	FECHAS ESTIMADAS				
	INICIO: 5 de Enero 2024			TÉRMINO: 25 de Enero 2024	
DESCRIPCIÓN DEL OBJETIVO:	Se realiza la inspección de los activos hardware del departamento de sistemas				
PERSONAS INVOLUCRADAS	Encargada del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
<i>ACTIVIDADES</i>	<i>TÉCNICAS</i>	<i>HERRAMIENTAS</i>	<i>OBJETIVO / META</i>	<i>REALIZADOR</i>	<i>TIEMPO HRS/ DÍAS</i>
6.1 Obtener las características de hardware de los activos	Recopilación de datos	Procesador de texto y software	Conocer toda la información de los componentes de hardware de los activos	- Aguirre Olmos KatiaElizabeth - Pantoja Hernández Karla Celeste	5 días
6.2 Revisar el estado en el que se encuentra activos de cómputo (computadoras, routers y switches).	Recopilación de datos, observación y prueba física	Dispositivo móvil o laptop y procesador de texto	Conocer el estado físico de los activos de hardware, destacandosu integridad física (golpes, rayones, manchas, etc) y si el dispositivo sigue en funcionamiento	- Aguirre Olmos KatiaElizabeth - Pantoja Hernández Karla Celeste	5 días

6.3 Revisar en qué estado se encuentran los periféricos (monitores, teclados, ratones)	Recopilación de datos, observación y prueba física	Dispositivo móvil o laptop y procesador de texto	Conocer la integridad física de los periféricos de entrada y salida que se encuentren en el laboratorio.	• Aguirre Olmos KatiaElizabeth • Pantoja Hernández Karla Celeste	5 días
--	--	--	--	--	--------

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

La tabla 8. Inspección de software y activos de red, del departamento es una herramienta específica diseñada para realizar una evaluación detallada y documentada sobre los softwares que se encuentran instalados en los equipos de cómputo y los análisis del servicio de red.

Tabla 8. Inspección de software y activos de red. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: <u>7. Realizar inspección del software y servicios de red del departamento de sistemas</u>	FECHAS ESTIMADAS				
	INICIO: 26 de Enero 2024			TÉRMINO: 13 de Febrero 2024	
DESCRIPCIÓN DEL OBJETIVO:	Revisar el estado del software de los activos de TI y la red de datos del departamento.				
PERSONAS INVOLUCRADAS	Encargada del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
<i>ACTIVIDADES</i>	<i>TÉCNICAS</i>	<i>HERRAMIENTAS</i>	<i>OBJETIVO / META</i>	<i>REALIZADOR</i>	<i>TIEMPO HRS/ DÍAS</i>
7.1. Revisar el software que se encuentra instalado en los equipos de computo	Investigación Observación	Software (WinAudit) Software (MyPC) Editor de Texto Memoria USB	Conocer el estado en que se encuentran los activos de cómputo sobre el software y si cuenta con las licencias activas y protección contra malware.	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández Karla Celeste	4 días

7.2. Realizar un análisis en busca de software malicioso.	Investigación Análisis de información Observación	Software (Nessus) Software (ClamWin) Editor de Texto Memoria USB	Conocer si los equipos de cómputo se encuentran infectados con algún virus o malware	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	5 días
7.3. Realizar análisis en los servicios de red	Investigación, Análisis de información	Software (Nmap) Editor de Texto Memoria USB	Conocer el estado en que se encuentran los servicios de red para identificar las posibles vulnerabilidades que podría tener.	• Aguirre Olmos Katia Elizabeth • Pantoja Hernández Karla Celeste	4 días

La tabla 8. Identificar hallazgos, es una herramienta para llevar un orden y facilitar el desarrollo del análisis de las fortalezas y debilidades del departamento.

Tabla 9. Identificar hallazgos. Elaboración propia

Plan de Trabajo de la Auditoria con ISO 17799 para gestión de seguridad de activos de TI de la empresa Embotelladora Mexicana S.A de C.V					
OBJETIVO: 8. Identificar Hallazgos	FECHAS ESTIMADAS				
	INICIO: 14 de Febrero			TÉRMINO: 20 de Febrero 2024	
DESCRIPCIÓN DEL OBJETIVO:	Realizar un análisis de información recabada y obtener resultados de la percepción del personal y el encargado del departamento de sistemas.				
PERSONAS INVOLUCRADAS	Encargado del departamento de sistemas: Michelle Araceli Flores Florido Auditores: Aguirre Olmos Katia Elizabeth Pantoja Hernández Karla Celeste				
ACTIVIDADES	TÉCNICAS	HERRAMIENTAS	OBJETIVO / META	REALIZADOR	TIEMPO HRS/ DÍAS
8.1. Identificar las fortalezas y debilidades del departamento	Investigación y Análisis de información.	Equipo de cómputo, dispositivo móvil.	Obtener una evaluación completa del desempeño del departamento para identificar las áreas de mejora y establecer un plan de acción	- Aguirre Olmos Katia Elizabeth - Pantoja Hernández KarlaCeleste	5 días

3.2 ANÁLISIS

La realización de encuestas en auditorías (véase tabla 4. Redactar cuestionario y tabla 5. Aplicar cuestionario), sirve como un medio eficaz para evaluar la satisfacción de los empleados, usuarios u otras partes involucradas en la operación de una organización. Al capturar de manera cuantitativa y cualitativa las percepciones de aquellos directamente afectados por los procesos auditados, se obtiene información crítica sobre la efectividad de los controles internos, la calidad de los productos o servicios, y la conformidad con estándares y regulaciones.

Estas encuestas no solo sirven como una herramienta de evaluación retrospectiva, sino también como un mecanismo proactivo para identificar posibles riesgos y áreas de mejora. Las respuestas recopiladas proporcionan una base de datos documentada y una evidencia tangible que respalda hallazgos y recomendaciones.

Para la realización de la encuesta en el departamento de sistemas de la Embotelladora Mexicana S.A de C.V, se tomó en cuenta a los 8 ingenieros que utilizan las instalaciones y el equipo del departamento, la encuesta consta de 29 preguntas, las cuales se dividen en preguntas acerca de la infraestructura, inventario, seguridad física, seguridad lógica y los servicios.

La encuesta realizada busca recopilar información para identificar los riesgos y áreas de mejora que se puede tener, esto se obtiene después de hacer un análisis con las respuestas obtenidas de cada personal del departamento.

El cuestionario comienza con la parte de la infraestructura, donde se puede concluir que dentro del departamento no cuentan con suficientes racks para tener bien organizado los cables, router y switches, sin embargo, el rack que poseen está bien ubicado en un lugar sin humedad ni altas temperaturas. Una desventaja que se encontró al realizar esta parte de la encuesta es que no se realizan revisiones periódicamente al departamento para confirmar que la infraestructura esté en óptimas condiciones.

La segunda parte del cuestionario trata sobre el inventario que se lleva dentro del departamento, aquí se pudo visualizar que cuentan con un registro detallado de los dispositivos y periféricos (cables, pantallas, teclados, mouses) que poseen los cuales se identifican con masking tape colocándole la marca, modelo y el área de donde viene el equipo y de la misma forma se marcan los dispositivos obsoletos que se dan de baja, esto se realiza junto con una relación de los equipos, donde se coloca información como la marca, modelo, serie, que problema o fallo tuvo el equipo, cual es el cedis y el área de donde viene.

La tercera parte de la encuesta es de la seguridad física, donde se realizan preguntas para saber cómo se supervisa y controla el acceso a los componentes del departamento, cuáles son las medidas de seguridad implementadas para prevenir el robo de equipos, aquí los trabajadores mencionan que existen registros donde se colocan los equipos que van ingresando al departamento, de qué bodega y área son y el día que fueron entregados.

Para realizar una salida de equipos se cuenta con un formato que contiene la fecha de salida, el nombre de la persona que recibe el equipo, la compañía, bodega y área donde será enviado el equipo, la descripción, marca, modelo, número de serie, número de registro y observaciones, este formato es firmado por 3 personas, la persona que entrega, la que recibe y la que autoriza la salida del equipo, estos documentos se realizan para evitar el robo o que los equipos se pierdan al ser enviados.

Con esta parte del cuestionario se confirmó la nula existencia de cámaras de seguridad dentro del departamento, sin embargo, para la supervisión y control de los visitantes que ingresan al departamento se cuenta con un registro que se debe realizar por la persona que visita el área, donde ingresa la fecha, nombre completo, de donde viene, la hora de entrada, hora de salida y su firma.

La cuarta parte trata de la seguridad lógica, donde se indica que todos los trabajadores tienen diferentes roles en los sistemas que se utilizan dentro de la embotelladora, esto con ayuda de los permisos que fueron otorgados al crear las cuentas que cada persona usará dependiendo las actividades que necesite realizar, cada cuenta tiene contraseñas seguras para evitar que personas no autorizadas accedan a ellas.

La quinta y última parte de la encuesta es sobre los servicios, aquí se describe que es lo que realizan cada vez que existe un fallo en alguno de los servicios como el aire acondicionado, el internet, la electricidad, etc y a quienes se debe acudir para darle solución a las fallas presentadas (Anexo 1. Cuestionario).

El objetivo de la encuesta realizada es recopilar la información clave de manera estructurada y así, obtener datos relevantes (incluyendo percepciones, opiniones y experiencias de las partes involucradas) para la auditoria, así como, identificar los riesgos o debilidad en los sistemas, procesos o infraestructura permitiendo abordar los problemas antes de que crezcan. De igual forma, se obtiene una documentación y evidencia con las respuestas que brindan los trabajadores y se logren respaldar las conclusiones obtenidas al final de la auditoria.

Con el análisis del cuestionario se sacaron posibles riesgos y fortalezas (véase tabla 10. FODA) con las que cuenta el departamento de sistemas y fueron almacenadas en un FODA.

Tabla 10. FODA seguridad física y lógica. Elaboración propia

Fortalezas	Oportunidades
1. Cuenta con equipos funcionales 2. Buena iluminación para la realización de soporte y mantenimiento 3. El departamento cuenta con señalamiento de emergencia 4. Cuenta con equipo contra accidentes 5. Cuenta con políticas de uso	1. Los servicios de red pueden perfeccionarse más 2. Mejoramiento de las instalaciones 3. Actualización de equipo físico 4. Actualización lógica de los equipos de cómputo 5. Mejoramiento en el mobiliario para la organización de activos
Debilidades	Amenazas
1. El desorden existente tanto en el cableado y organización de los equipos 2. Inequitativa distribución del trabajo en el departamento 3. Poco personal para atender las necesidades de la planta 4. Se carece de un espacio adecuado para la realización de mantenimiento. 5. Los equipos de cómputo del departamento no cuentan con seguridad de acceso	1. El acceso al departamento cuenta con un bajo grado de control de seguridad 2. Eventos externos, como desastres naturales, pueden afectar la continuidad de los servicios del departamento 3. Limitaciones presupuestarias de la empresa pueden afectar los recursos del departamento

ANÁLISIS DE RIESGO

Tabla 11. Análisis de riesgo. Elaboración propia

VULNERABILIDADES	RECOMENDACIONES
V1. Sistemas Operativos y aplicaciones no actualizados	R1. De acuerdo con la sección 11.5.1 de ISO/IEC 17799, el acceso a los sistemas operativos deberá ser controlado mediante un procedimiento de registro seguro.
V2. Falta de software antivirus actualizado en los dispositivos	R2. De acuerdo con la sección 11.2.3 de ISO/IEC 17799, se deberá implementar soluciones de seguridad actualizadas y realizar análisis periódicos de virus y actualizaciones automáticas
V4. No realizar evaluaciones periódicas de riesgos	R4. De acuerdo con la sección 4.2 de ISO/IEC 17799, para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión tomando en cuenta los requerimientos y restricciones de la legislación, los objetivos organizacionales, el costo de implementación y operación.
V5. Uso de software pirata o no licenciado	R5. De acuerdo con sección 8.2.2 de ISO/IEC 17799 se deberá dar una capacitación constante que debe incluir los requerimientos de seguridad, así como el uso de procesamiento de información, por ejemplo, el procedimiento de un registro o el uso de paquetes de software con licencia.
V6. Filtrado de información	R6. De acuerdo con la sección 12.5.4 de ISO/IEC 17799 se deberán evitar las oportunidades para la filtración de información y se debe considerar lo siguiente: hacer uso de los sistemas y software de alta integridad, monitorear la utilización del recurso en los sistemas de cómputo y realizar un monitoreo regular de las actividades.
V7. Ausencia de políticas y procedimientos de respaldo y recuperación de datos	R7. De acuerdo con la sección 10.5 de ISO/IEC 17799 se debe mantener la integridad y disponibilidad de la información, por lo que se deberán producir registros exactos de las copias de respaldo, estas se deberán almacenar en un lugar apartado y se le debe dar el nivel de protección física.
V8. Insuficiente control de acceso a dispositivos y sistemas	R8. De acuerdo con la sección 9.2 de ISO/IEC 17799, se deberá controlar el acceso del usuario a la información y a las funciones del sistema de aplicación, para esto se deberán utilizar medios de seguridad para restringir el acceso afuera y dentro del sistema.
V9. Falta de control y monitoreo de los registros de eventos de seguridad	R9. De acuerdo con la sección 10.10.1 de ISO/IEC 17799, se deben monitorear los sistemas y reportar los eventos de seguridad, para esto se deberán usar bitácoras de operador y se deben registrar las fallas.

V10. Falta de procedimientos de gestión de incidentes de seguridad	R10. De acuerdo con la sección 13.1.1 de ISO/IEC 17799 se deberán establecer procedimientos formales de reporte para la gestión de un incidente de seguridad. El reporte deberá contener: procesos de retroalimentación para asegurar que se trató con el problema, formatos para respaldar la acción del reporte, anotar los detalles del mal funcionamiento.
--	--

Tabla 11 (continuación). Análisis de riesgos

AMENAZAS	RECOMENDACIONES
A1. Descarga de archivos infectados desde Internet	R11. De acuerdo con la sección de ISO/IEC 17799 se debe establecer una política formal prohibiendo el uso de software no autorizado, así como una política para proteger contra riesgos asociados con la obtención de archivos , se deben realizar revisiones regulares del software y contenido data de los sistemas.
A2. Dispositivos USB infectados conectados a los sistemas del departamento	R12. De acuerdo con la sección 7.1.3 de ISO/IEC 17799, se deberán identificar, documentar e implementar reglas para el uso de los activos asociados con los medios del procesamiento de la información. Los empleados y terceros deberán ser responsables por el uso que le den a cualquier recurso de procesamiento de información.
A3. Descarga de software no autorizado o pirata	R13. De acuerdo con la sección 12.1.1 de ISO/IEC 17799, si los productos son comprados, se deberá realizar un proceso de prueba y adquisición formal. Cuando la funcionalidad de seguridad de un producto propuesto no satisface el requerimiento especificado entonces se debieran reconsiderar el riesgo introducido y los controles asociados antes de comprar el producto.
A4. Uso de software desactualizado y sin soporte	R14. De acuerdo con la sección 12.6.1 de ISO/IEC 17799, se deberán identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener conciencia sobre ellas para el software, estos recursos deberán actualizarse en base a los cambios
A5. Descuidos en la configuración de sistemas y aplicaciones	R15. De acuerdo con la sección 11.4.1 de ISO/IEC 17799, se deberá formular una política relacionada con el uso de los servicios, la cual debe abarcar los servicios a los cuales tiene acceso, los controles, procedimientos y configuraciones para proteger el acceso a las conexiones, etc.

INSPECCIÓN Y PRUEBAS DE SEGURIDAD FÍSICA

La seguridad física es un aspecto fundamental en la auditoría de un departamento de TI, ya que busca evaluar y garantizar la protección de las instalaciones físicas como el estado de las paredes, ventanas, puertas, los equipos de cómputo y los datos sensibles que se manejan en el entorno.

En el caso específico de la auditoría del departamento de Sistemas de la Embotelladora Mexicana S.A de C.V Suc, Tultitlán, el objetivo es evaluar el estado de las instalaciones físicas y verificar el cumplimiento de las medidas de seguridad implementadas. Esto incluye la disponibilidad y calidad de los equipos de cómputo, la conectividad de red, la disposición de mobiliario y las medidas de control de acceso para identificar posibles deficiencias y áreas de mejora en términos de seguridad física, garantizando un entorno adecuado y seguro para el desarrollo de las actividades del departamento.

Para este apartado se realizan diferentes pruebas acerca de las instalaciones y los activos del departamento, primero se ingresa al área que será evaluada, se utilizan diferentes técnicas y herramientas para su análisis, como lo son la observación, investigación, pruebas físicas, con la ayuda de los dispositivos móviles y procesador de textos para ir recopilando la información y las fotografías obtenidas durante las evaluaciones.

Los resultados de estas pruebas se muestran en tablas, donde se necesita ingresar información como los objetivos de la prueba, descripción, técnicas y herramientas a utilizar, así como un proceso de medición el cual se divide en 4; Funciona excelente, Funciona muy bien, Funciona regular y Funciona mal, en otro apartado se anota la calificación obtenida después de analizar los resultados, se añaden consideraciones especiales, así como la interpretación de resultados, que es donde se incluyen las fotografías tomadas durante el análisis y para finalizar con la tabla, se escriben recomendaciones de acuerdo a la norma ISO 17799.

Este apartado comienza con la inspección física del departamento, analizando la estructura, si esta cuenta con grietas en las paredes, si el techo está bien colocado y observando el estado de las puertas y ventanas (véase tabla 12. Desarrollo de prueba de estructura física del departamento).

Tabla 12. Desarrollo de prueba de estructura física del departamento (paredes, ventanas, puerta)

Desarrollo prueba de estructura física del departamento (paredes, ventanas, puerta)	
Objetivo de la prueba	La estructura debe estar en buen estado para evitar accidentes y garantizar la seguridad de los trabajadores, así como proteger los activos de TI que se encuentran dentro del departamento
Descripción de la prueba y Valor esperado	La prueba de estructura física se realiza para verificar que el estado de las paredes, ventanas, puertas y techos sea adecuado
Técnica	1. Ingresar al departamento de sistemas. 2. Observar si existen grietas en las paredes, si las ventanas y puertas se encuentran en buen estado y si el techo está bien colocado.
Herramientas Requeridas	Teléfono celular para toma de fotografías de la estructura
Proceso de medición	Funciona excelente: Si las paredes no cuentan con grietas, las ventanas y puertas están en buen estado y si el techo está colocado de manera correcta. Funciona muy bien: Si las paredes y el techo se encuentran en buen estado y las puertas y ventanas cuentan con detalles estéticos sin afectar su funcionamiento Funciona Regular: Si las paredes, techo, puertas y ventanas cuentan con pequeños detalles estéticos que no afectan el funcionamiento Funciona Mal: Si la pared tiene grietas muy visibles, el techo no está colocado de manera correcta o incluso está roto, si las ventanas y puertas no funcionan correctamente.
Criterios de Terminación / Valor obtenido	Funciona regular: Se observa que las paredes no cuentan con ninguna grieta, el techo está colocado de manera correcta y las puertas y ventanas funcionan con normalidad y no existe ningún detalle estético, sin embargo, las puertas no cuentan con un sistema de seguridad.
Interpretación de resultados	Observar y anotar cualquier anomalía encontrada en la estructura física del departamento de sistemas

Tabla 12 (continuación). Desarrollo de prueba de estructura física del departamento (paredes, ventanas, puerta)

Desarrollo prueba de estructura física del departamento (paredes, ventanas, puerta)	
Interpretación de resultados	
Recomendaciones	1. De acuerdo con la sección 9.1.1 de la norma ISO 17799, perímetro de seguridad física, inciso F: “se debieran instalar adecuados sistemas de detección de intrusos y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; también se debiera proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones” 2. Realizar mantenimiento en manillas y herrajes. Utilizando limpiador específico para metales, aplicar lubricantes en las bisagras y cerraduras para asegurar su buen funcionamiento.

Se continua con la inspección física, esta vez analizando la estructura de las mesas y sillas (véase tabla 13. Desarrollo de prueba de estructura física del departamento) y si estas cuentan con algún defecto o se encuentran en buen estado.

Tabla 13. Desarrollo prueba de estructura física del departamento (mesas, sillas)

Desarrollo prueba de estructura física del departamento (mesas, sillas)	
Objetivo de la prueba	La estructura debe estar en buen estado para evitar accidentes y garantizar la seguridad de los trabajadores, así como proteger los activos de TI que se encuentran dentro del departamento
Descripción de la prueba y Valor esperado	La prueba de estructura física se realiza para verificar que el estado de las mesas y sillas sea adecuado
Técnica	1. Ingresar al departamento de sistemas. 2. Observar si existe algún detalle en las mesas y sillas que utilizan las personas que trabajan en el departamento
Herramientas Requeridas	Teléfono celular para toma de fotografías de las mesas y sillas
Proceso de medición	Funciona excelente: Si las mesas están bien reforzadas, sin detalles estéticos y si las sillas se encuentran en buen estado Funciona muy bien: Si las mesas están reforzadas y las sillas funcionan correctamente Funciona Regular: Si las mesas no están reforzadas y se mueven al tocarlas Funciona Mal: Si las mesas se mueven con cualquier contacto, las sillas no están en buen estado y ambas cuentan con detalles estéticos muy notorios.
Criterios de Terminación / Valor obtenido	Funciona muy bien: Se observa que algunas mesas y sillas cuentan con detalles estéticos, sin embargo, estos no interfieren con su funcionamiento
Interpretación de resultados	Se cuentan con detalles estéticos, como desgaste en la pintura, tela rasgada o pata de la mesa chueca, pero esto no interfieren con el funcionamiento.

Tabla 13 (continuación). Desarrollo prueba de estructura física del departamento (mesas, sillas)

Desarrollo prueba de estructura física del departamento (mesas, sillas)	
Interpretación de resultados	
Recomendaciones	1. De acuerdo con la sección 9.1.3. Asegurar las oficinas, habitaciones y medios, “se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios.”, ya que el mobiliario en malas condiciones, como las mesas y sillas, podría ocasionar un accidente con los activos y al personal involucrado. 2. No subir equipos pesados a las mesas, ya que con el tiempo pueden debilitarse.

Para la siguiente prueba se observaron los señalamientos que existen dentro del laboratorio (véase tabla 14. Desarrollo de prueba de señalamiento), donde se busca verificar la efectividad, visibilidad con el fin de prevenir o evitar accidentes.

Tabla 14. Desarrollo de prueba de señalamiento

Desarrollo de prueba de señalamiento	
Objetivo de la prueba	Los señalamientos deben ayudar a prevenir accidentes y garantizar la seguridad de las personas que trabajan en el departamento.
Descripción de la prueba y Valor esperado	La prueba de señalamientos se realiza para verificar la efectividad y la visibilidad de los señalamientos utilizados en un entorno determinado, como un laboratorio, un área de trabajo o un edificio.
Técnica	1. Ingresar al departamento de sistemas. 2. Observar los señalamientos de seguridad.
Herramientas Requeridas	Señalamientos de seguridad
Proceso de medición	Funciona Excelente: Si los señalamientos están colocados de manera correcta, son visibles y su tamaño es correcto. Funciona Muy bien: Si los señalamientos están colocados de manera correcta, con visibles. Funciona Regular: Si los señalamientos son visibles Funciona Mal: Si no existen señalamientos
Criterios de Terminación / Valor obtenido	Funciona excelente: Se observa que los señalamientos están en un lugar visible, su tamaño es adecuado y las personas que ingresan al departamento notan y ubican cual es la salida de emergencia
Interpretación de resultados	Analizar y comprender la información y los mensajes transmitidos por los señalamientos, así como tomar acciones en función de esa información.  

Recomendaciones	1. De acuerdo con la sección 9.1.1. Perímetro de seguridad física de la norma ISO 17799: “los perímetros de seguridad debieran estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro” y la sección 9.1.4. Protección contra amenazas externas e internas “se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre”. Inciso C: “se debiera proporcionar equipo contraincendios ubicado adecuadamente.” 2. Los señalamientos de seguridad deben seguir un estilo y diseño consistentes en todo el entorno. 3. Los pictogramas y símbolos pueden ser más rápidos de entender que el texto, especialmente en situaciones de emergencia. Utilice pictogramas y símbolos reconocibles internacionalmente para indicar diferentes tipos de riesgos.
-------------------------------	---

Otra parte importante que se debe revisar es el aire acondicionado (Véase tabla 15. Desarrollo de prueba de aire acondicionado) para verificar está realizando su funcionamiento sin ninguna falla, aportando el flujo de aire limpio a los equipos de cómputo.

Tabla 15. Desarrollo de prueba de uso de aire acondicionado

Desarrollo de prueba de uso de aire acondicionado	
Objetivo de la prueba	Analizar la eficiencia de los diferentes servicios con los que cuenta el departamento en cuanto a la calefacción/ventilación dentro de las instalaciones.
Descripción de la prueba y Valor esperado	1. Ingresar al departamento 2. Encender aire acondicionado
Técnica	Análisis y Observación
Herramientas Requeridas	Cámara fotográfica Aire acondicionado
Proceso de medición	Funciona Excelente: El departamento cuenta con al menos de 2 a 4 aires acondicionados, los cuales son grandes y el rango de aire abarca gran parte de las oficinas del departamento enfocándose a los equipos de cómputo, estos aparatos permiten el flujo de aire limpio y se encuentran en buen estado generalmente (cables de conexión). Funciona Muy bien: El departamento cuenta con al menos de 2 a 4 aires acondicionados, los cuales son grandes y el rango de aire abarca gran parte de las oficinas del departamento, pero no se enfoca a los equipos de cómputo, estos aparatos permiten el flujo de aire limpio y se encuentran en buen estado generalmente (cables de conexión). Funciona Regular: El departamento cuenta con al menos de 2 a 4 aires acondicionados, los cuales son grandes y el rango de aire abarca gran parte de las oficinas del departamento, pero no se enfoca a los equipos de cómputo, estos aparatos están semi limpios y no permite el flujo de aire limpio en su totalidad y se encuentran en buen estado generalmente (cables de conexión). Funciona Mal: El departamento cuenta con menos de 2 aires acondicionados, los cuales son pequeños y el rango de aire no abarca gran parte de las oficinas del departamento, no se enfoca a los equipos de cómputo y no permite el flujo de aire limpio en su totalidad, los aparatos se encuentran en pésimas condiciones (cables de conexión).

Tabla 15 (continuación). Desarrollo de prueba de uso de aire acondicionado

Desarrollo de prueba de uso de aire acondicionado	
Criterios de Terminación / Valor obtenido	Funciona muy bien: El departamento cuenta con 3 aires acondicionados que abarcan la mayor parte del departamento exceptuando una oficina donde se encuentran 4 equipos de cómputo y más dispositivos a los cuales les debería llegar el flujo de aire limpio.
Interpretación de resultados	El aire abarcan gran cantidad del departamento pero no se enfoca en algunos equipos de computo, tambien se pudo observar el buen estado de los aparatos. 
Recomendaciones	De acuerdo con la sección 9.2.2. Servicios Públicos de Soporte de la norma ISO 17799. “Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; debieran ser adecuados e inspeccionados regularmente y, conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla para los sistemas que soportan” Siendo así, se debería contemplar lo siguiente: 1. Los aires acondicionados deben estar limpios, libres de polvo o pelusa que pueda dañar cualquier equipo dentro del laboratorio. 2. Los aires acondicionados deben estar en excelentes condiciones y enfocarse más a los equipos de cómputo para mantener un equilibrio de temperaturas dentro de las instalaciones causadas por dichos equipos.

Para finalizar con la inspección física se analizó el cableado de red y eléctrico (Véase tabla 16. Desarrollo de prueba de cableado), se observa detenidamente cómo se encuentran acomodados y divididos los cables de acuerdo con su funcionamiento y si estos están etiquetados para evitar la confusión.

Tabla 16. Desarrollo de prueba de cableado

Desarrollo de prueba de cableado	
Objetivo de la prueba	Analizar la seguridad del cableado y observar la organización de acuerdo su funcionamiento.
Descripción de la prueba y Valor esperado	La observación y análisis de esta prueba se realiza para verificar que las conexiones y el cableado se encuentren organizadas de manera correcta para evitar cualquier daño o accidente de estos.
Técnica	1. Ingresar al departamento. 2. Observar conexiones y el cableado de toda la instalación, incluyendo cableado del equipo de cómputo, iluminación, equipo de redes, energía, etc.
Herramientas Requeridas	Cableado y conexiones
Proceso de medición	Funciona Excelente: El cableado de los equipos de cómputo y equipo de redes está organizado de manera impecable. Se siguen las mejores prácticas de cableado, como el uso de canaletas para mantener los cables ordenados y separados. Los cables están etiquetados adecuadamente, lo que facilita su identificación y seguimiento. Además, se toman medidas para prevenir el enredo o cruzamiento de cables. Funciona muy bien: En general, el cableado de los equipos de cómputo y equipo de redes está bien organizado. Se siguen las prácticas estándar de cableado y se utilizan herramientas apropiadas para mantener los cables ordenados. Los cables están etiquetados, aunque puede haber algunas áreas de mejora en cuanto a la legibilidad de las etiquetas. Se evitan enredos y cruzamientos de cables en la medida de lo posible. Funciona Regular: El cableado de los equipos de cómputo y equipo de redes cumple con los requisitos mínimos de organización. Se utilizan métodos básicos de cableado, pero puede haber cables sueltos o desordenados en ciertas áreas. Las etiquetas pueden estar ausentes o ser poco claras, dificultando la identificación de los cables. Puede haber algunos enredos o

Tabla 16 (continuación). Desarrollo de prueba de cableado

Desarrollo de prueba de cableado	
	cruzamientos de cables que afectan la apariencia y la facilidad de mantenimiento. Funciona mal: El cableado de los equipos de cómputo y equipo de redes no cumple con los requisitos mínimos de organización. No utilizan métodos básicos de cableado. No existen etiquetas de identificación de los cables. Hay enredos o cruzamientos de cables que afectan la apariencia y la facilidad de mantenimiento.
Criterios de Terminación / Valor obtenido	Funciona Regular: Los cables del equipo de redes y del equipo de cómputo están organizados y separados de acuerdo su función, sin embargo, faltan etiquetas en cada cableado y existen cables sueltos o enredados que dificultan su identificación.
Interpretación de resultados	Se verifica que los sistemas de cableado del equipo de redes se encuentran separado correctamente de acuerdo su función.   Se observa que el cableado del equipo de cómputo está separado de acuerdo con cada dispositivo, sin embargo, existen cables sueltos.

	
Recomendaciones	De acuerdo con la sección 9.2.3. Seguridad del cableado de la norma ISO/IEC 17799, se proporcionan las siguientes recomendaciones: 1. “El cableado de la red debiera estar protegido contra interceptaciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas” 2. “Los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia” 3. “Se debieran utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados”

Inspección a los activos hardware del departamento

El equipo (Laptop 1) (véase tabla 17. Desarrollo de prueba de laptop de encargado de FROG) se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El equipo debería encontrarse en perfecto estado.
- **Muy bien:** El equipo debería encontrarse en buen estado, puede tener ligeros detalles estéticos, pero sin afectar en su uso como rayones, manchas o suciedad,
- **Bien:** El equipo podría contar con detalles estéticos visibles e identificables como suciedad, falta de 1 o 2 teclas o daños en la pantalla.
- **Regular:** El equipo podría contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado y suciedad.
- **Mal:** El equipo se podría encontrar en pésimas condiciones como pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad o carcasa rota. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 17. Desarrollo de prueba laptop encargado de FROG

Desarrollo de prueba de laptop de encargado de FROG	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el equipo de cómputo.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los equipos de cómputo se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal.
Técnica	1. Ingresar al departamento de sistemas y evaluar el equipo de cómputo. 2. Lograr identificar los posibles desperfectos que podría tener el equipo.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad) Bien: El equipo cuenta con detalles estéticos visibles e identificables (suciedad, falta de 1 o 2 teclas, daño en la pantalla).

Tabla 17 (continuación). Desarrollo de prueba laptop encargado de FROG

Desarrollo de prueba de laptop de encargado de FROG	
	Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, etc). Mal: El equipo se encuentra en pésimas condiciones (Pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, carcasa rota, etc)
Criterios de Terminación / Valor obtenido	Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad).
Interpretación de resultados	Se puede observar que el equipo de marca Lenovo, modelo T 460s, se encuentra en buen estado, cuenta con ligeras manchas en la pantalla y touchpad, no cuenta con carcasa rota o algún imperfecto pronunciado. 

	
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

El monitor 1 (véase tabla 18. Desarrollo de prueba de monitor del encargado de soporte y mantenimiento 1), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El monitor debe encontrarse en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El monitor se debe encontrar en buen estado, con algunos ligeros detalles estéticos, pero sin afectar su función como rayones, manchas o suciedad.
- **Bien:** El monitor puede contar con detalles estéticos visibles e identificables como suciedad, daño en la pantalla, rayones o manchas.
- **Regular:** El monitor puede contar con detalles estéticos muy pronunciados y visibles como la carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado.
- **Mal:** El monitor se puede encontrar en pésimas condiciones como pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 18. Desarrollo de prueba de monitor de encargado de soporte y mantenimiento 1

Desarrollo de prueba de monitor del encargado de soporte y mantenimiento 1	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el monitor.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los monitores se encuentren en buenas condiciones permiten visualizar la información relevante al puesto del personal.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el monitor se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El monitor se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El monitor cuenta con detalles estéticos visibles e identificables (suciedad, daño en la pantalla, rayones o manchas). Regular: El monitor cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado etc). Mal: El monitor se encuentra en pésimas condiciones (Pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones, etc).
Criterios de Terminación / Valor obtenido	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.

Tabla 18 (continuación). . Desarrollo de prueba de monitor de encargado de soporte y mantenimiento 1

Desarrollo de prueba de laptop de encargado de FROG	
Interpretación de resultados	Se puede observar que el monitor marca Ghia modelo MG2423, no cuenta con ninguna anomalía o imperfecto, está en excelentes condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

El CPU 1 (Véase tabla 19. Desarrollo de prueba de CPU de encargado de soporte y mantenimiento 1), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El CPU se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El CPU se debe encontrar en buen estado, puede contar con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.
- **Bien:** El CPU puede contar con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.
- **Regular:** El CPU puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso.
- **Mal:** El CPU se encuentra en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones o golpes. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 19. Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1

Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1.	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el CPU.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los CPU se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento de sistemas.
Técnica	3. Ingresar al departamento de Sistemas 4. Observar que el CPU se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El CPU se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El CPU se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El CPU cuenta con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: El CPU cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso). Mal: El CPU se encuentra en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, etc).

Tabla 19 (continuación). Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1

Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1.	
Criterios de Terminación / Valor obtenido	Muy bien: El CPU Marca DELL, modelo Vostro, se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad)
Interpretación de resultados	Se puede observar que el CPU cuenta con ligeros detalles de desgastamiento por uso, se encuentra en buenas condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza. 3. Evitar colocar el CPU en lugares donde se pueda raspar o pronunciar más el desgaste. 4. Limpiar el exterior del CPU con productos especiales para equipo de cómputo por lo menos una vez a la semana, para mantener el buen estado del monitor y prolongar su vida.

El monitor 2 (véase tabla 20. Desarrollo de prueba de monitor de becarios), se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía, se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El monitor se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El monitor se debe encontrar en buen estado, puede contar con ligeros detalles estéticos, pero sin afectar en su función. como rayones, manchas o suciedad.
- **Bien:** El monitor puede contar con detalles estéticos visibles e identificables como suciedad, daño en la pantalla, rayones o manchas.
- **Regular:** El monitor puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado.
- **Mal:** El monitor se puede encontrar en pésimas condiciones como pantalla imposible de ver, como suciedad, carcasa rota, soporte dañado o sin funcionar o rayones. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 20. Desarrollo de prueba de monitor de Becarios

Desarrollo de prueba de monitor de becario del departamento de sistemas.	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el monitor.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los monitores se encuentren en buenas condiciones permiten visualizar la información relevante al puesto del personal.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el monitor se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El monitor se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El monitor cuenta con detalles estéticos visibles e identificables (suciedad, daño en la pantalla, rayones o manchas). Regular: El monitor cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado etc). Mal: El monitor se encuentra en pésimas condiciones (Pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones, etc).

Tabla 20 (continuación). Desarrollo de prueba de monitor de Becarios

Desarrollo de prueba de monitor de becario del departamento de sistemas.	
Criterios de Terminación / Valor obtenido	Excelente: El monitor marca DELL, modelo E1911f, se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que el monitor no cuenta con ninguna anomalía o imperfecto, está en excelentes condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

El CPU 2 (véase tabla 21. Desarrollo de prueba de CPU de becarios), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El CPU se debe encontrar en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.
- **Muy bien:** El CPU se debe encontrar en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.
- **Bien:** El CPU puede contar con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.
- **Regular:** El CPU puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso.
- **Mal:** El CPU se puede encontrar en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones o golpes. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 21. Desarrollo prueba de CPU de becarios

Desarrollo de prueba de CPU del Becario del departamento de sistemas	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el CPU.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los CPU se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento de sistemas.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el CPU se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El CPU se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El CPU se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El CPU cuenta con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: El CPU cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso).

Tabla 21 (continuación). Desarrollo prueba de CPU de becarios

Desarrollo de prueba de CPU del Becario del departamento de sistemas	
	Mal: El CPU se encuentra en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, etc).
Criterios de Terminación / Valor obtenido	Bien: El CPU cuenta con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas).
Interpretación de resultados	Se puede observar que el CPU marca HP, modelo Hewlett Packard, cuenta con ligeros detalles de desgastamiento por uso, se encuentra en buenas condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para cómputo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza. 3. Evitar colocar el CPU en lugares donde se pueda raspar o pronunciar más el desgaste.

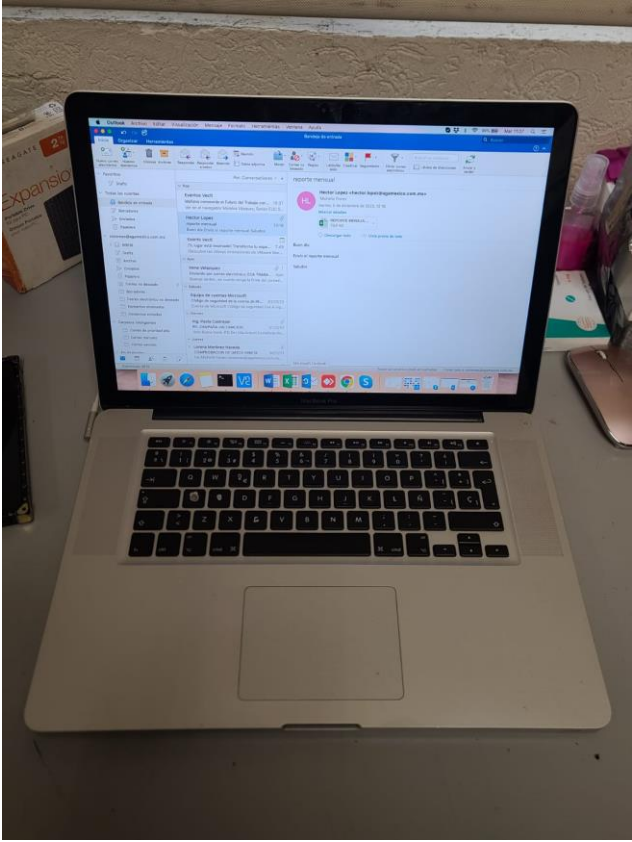
El equipo (Laptop 2) (véase tabla 22. Desarrollo de prueba de laptop de encargada del departamento), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El equipo se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El equipo se debe encontrar en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso como rayones, manchas o suciedad o desgaste por uso.
- **Bien:** El equipo puede contar con detalles estéticos visibles e identificables como suciedad, falta de 1 o 2 teclas, daño en la pantalla, desgaste por uso.
- **Regular:** El equipo puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad o desgaste por uso.
- **Mal:** El equipo se puede encontrar en pésimas condiciones como pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad y carcasa rota. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 22. Desarrollo de prueba de laptop de encargada de departamento

Desarrollo de prueba de laptop de encargada de departamento	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el equipo de cómputo.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los equipos de cómputo se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento.
Técnica	1. Ingresar al departamento de sistemas y evaluar el equipo de cómputo. 2. Lograr identificar los posibles desperfectos que podría tener el equipo.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad, desgaste por uso) Bien: El equipo cuenta con detalles estéticos visibles e identificables (suciedad, falta de 1 o 2 teclas, daño en la pantalla, desgaste por uso).

Tabla 22 (continuación). Desarrollo de prueba de laptop de encargada de departamento

Desarrollo de prueba de laptop de encargada de departamento	
	Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc). Mal: El equipo se encuentra en pésimas condiciones (Pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, carcasa rota, etc)
Criterios de Terminación / Valor obtenido	Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad, desgaste por uso)
Interpretación de resultados	Se puede observar que el equipo Marca Apple, Modelo Mackbook Pro-2012 se encuentra en buen estado, cuenta con ligero desgaste por uso, no cuenta con carcasa rota o algún imperfecto pronunciado. 

	
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

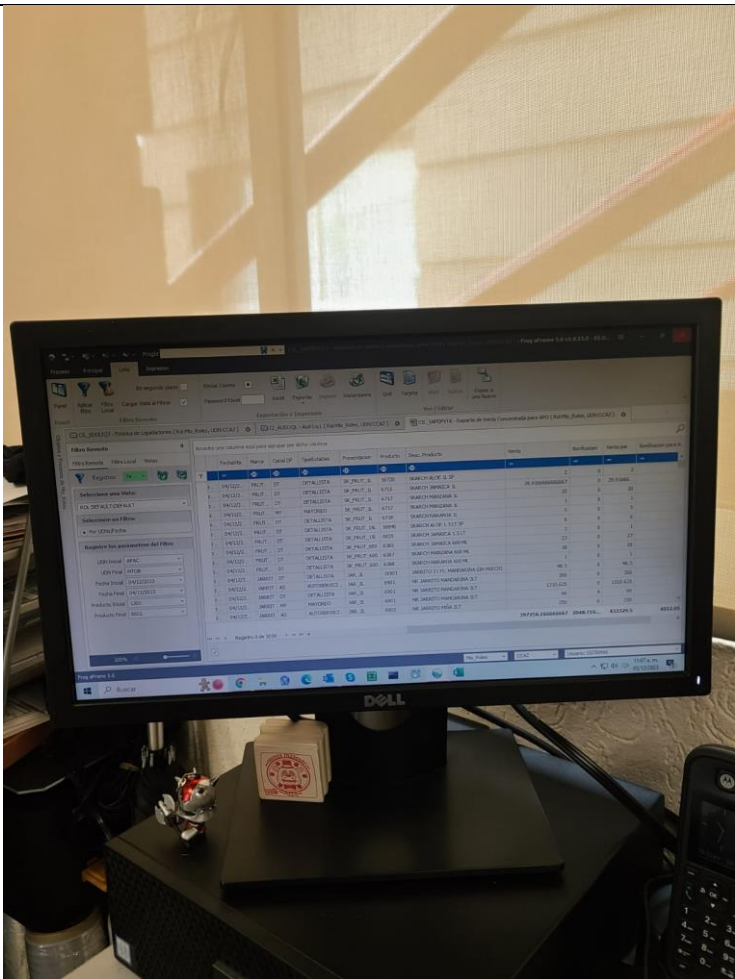
El monitor 3 (véase tabla 23. Desarrollo de prueba de monitor de la encargada de soporte y mantenimiento 2) se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El monitor se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.

- **Muy bien:** El monitor se debe encontrar en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. como rayones, manchas o suciedad.
- **Bien:** El monitor puede contar con detalles estéticos visibles e identificables como suciedad, daño en la pantalla, rayones o manchas.
- **Regular:** El monitor puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado.
- **Mal:** El monitor se encuentra en pésimas condiciones como pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar o rayones. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 23. Desarrollo de prueba de monitor de la encargada de soporte y mantenimiento 2.

Desarrollo de prueba de monitor de la encargada de soporte y mantenimiento 2	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el monitor.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los monitores se encuentren en buenas condiciones permiten visualizar la información relevante al puesto del personal.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el monitor se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El monitor se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El monitor cuenta con detalles estéticos visibles e identificables (suciedad, daño en la pantalla, rayones o manchas). Regular: El monitor cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado etc). Mal: El monitor se encuentra en pésimas condiciones (Pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones, etc).
Criterios de Terminación / Valor obtenido	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que el monitor marca DELL, modelo E1911f, no cuenta con ninguna anomalía o imperfecto, está en excelentes condiciones.

	
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

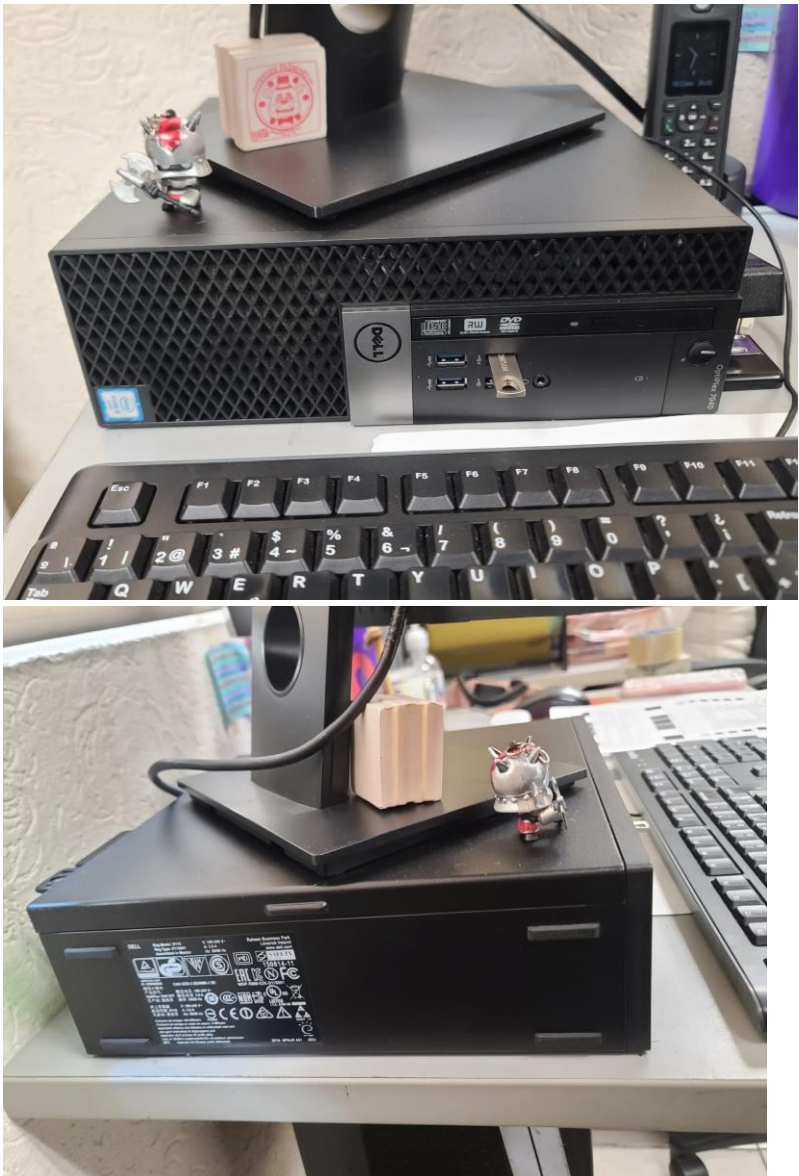
El CPU 3 (véase tabla 24. Desarrollo de prueba de CPU de la encargada de soporte y mantenimiento 2), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El CPU se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El CPU se debe encontrar en buen estado, puede contar con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.
- **Bien:** El CPU puede contar con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.
- **Regular:** El CPU puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes o desgaste por uso.
- **Mal:** El CPU se puede encontrar en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones o golpes. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 24. Desarrollo de prueba de CPU de encargada de soporte y mantenimiento 2.

Desarrollo de prueba de CPU de la encargada de soporte y mantenimiento 2	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el CPU.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los CPU se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento de sistemas.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el CPU se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El CPU se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El CPU se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El CPU cuenta con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: El CPU cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso).

Tabla 24 (continuación). Desarrollo de prueba de CPU de encargada de soporte y mantenimiento 2.

Desarrollo de prueba de CPU de la encargada de soporte y mantenimiento 2	
	Mal: El CPU se encuentra en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, etc).
Criterios de Terminación / Valor obtenido	Excelente: El CPU se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía
Interpretación de resultados	Se puede observar que el CPU marca DELL, modelo Optiplex 7040, se encuentra en perfectas condiciones, no cuenta con desperfectos o algún tipo de anomalía. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento

	autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza. 3. Evitar colocar el CPU en lugares donde se pueda raspar o pronunciar más el desgaste. 4. Limpiar el exterior del CPU con productos especiales para equipo de cómputo por lo menos una vez a la semana, para mantener el buen estado del monitor y prolongar su vida.
--	---

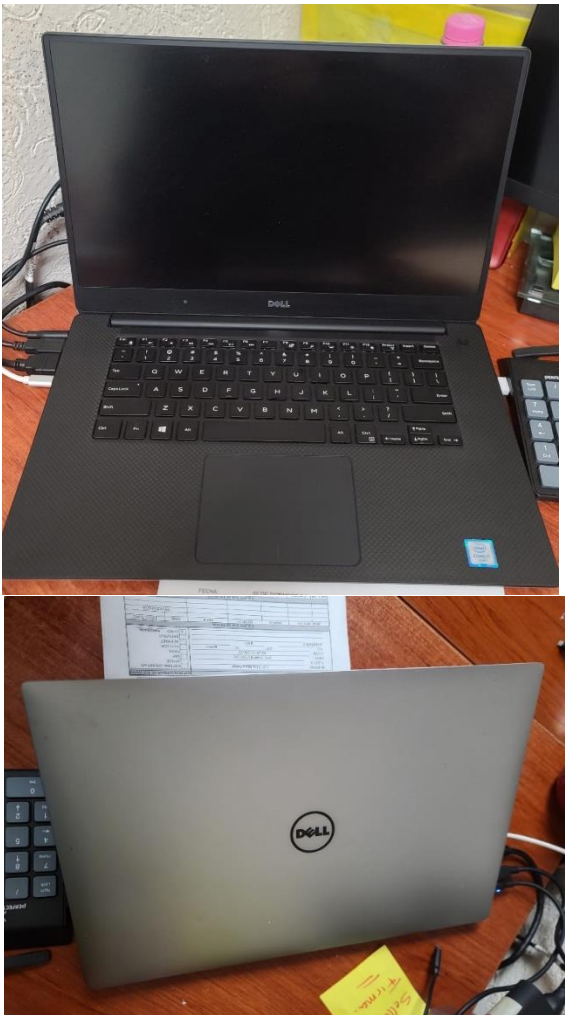
El equipo (Laptop 3) (véase tabla 25. Desarrollo de prueba de laptop de encargada de soporte y mantenimiento 3), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El equipo se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El equipo se debe encontrarse en buen estado, con ligeros detalles estéticos, pero sin afectar en su uso como rayones, manchas o suciedad, desgaste por uso.
- **Bien:** El equipo puede contar con detalles estéticos visibles e identificables como suciedad, falta de 1 o 2 teclas, daño en la pantalla o desgaste por uso.
- **Regular:** El equipo puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad o desgaste por uso.
- **Mal:** El equipo se encuentra en pésimas condiciones como pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, o carcasa rota. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 25. Desarrollo de prueba de laptop de encargada de soporte y mantenimiento 3.

Desarrollo de prueba de laptop de encargado de soporte y mantenimiento 3	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el equipo de cómputo.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los equipos de cómputo se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento.
Técnica	1. Ingresar al departamento de sistemas y evaluar el equipo de cómputo. 2. Lograr identificar los posibles desperfectos que podría tener el equipo.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad, desgaste por uso) Bien: El equipo cuenta con detalles estéticos visibles e identificables (suciedad, falta de 1 o 2 teclas, daño en la pantalla, desgaste por uso). Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc). Mal: El equipo se encuentra en pésimas condiciones (Pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, carcasa rota, etc)
Criterios de Terminación / Valor obtenido	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.

Tabla 25 (continuación). Desarrollo de prueba de laptop de encargada de soporte y mantenimiento 3.

Desarrollo de prueba de laptop de encargado de soporte y mantenimiento 3	
Interpretación de resultados	
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

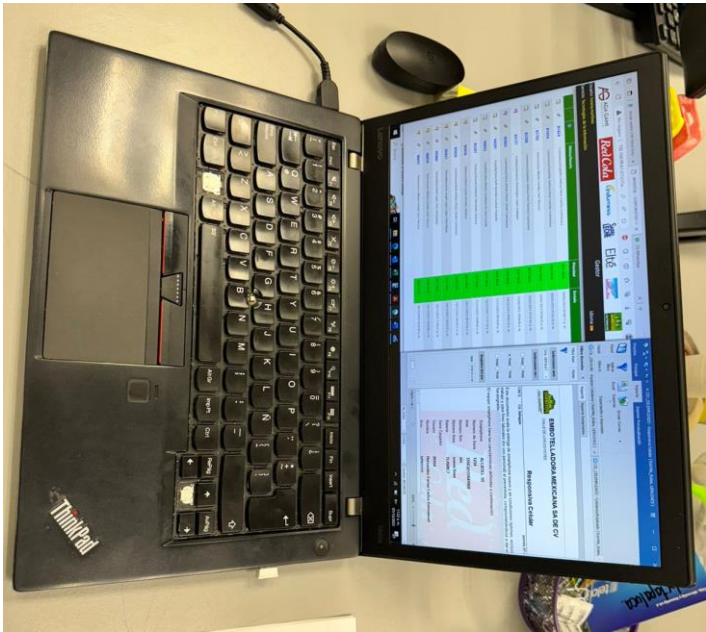
El equipo 4 (laptop) (véase tabla 26. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4), se evaluó utilizando la técnica de observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El equipo se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El equipo se debe encontrar en buen estado, con ligeros detalles estéticos, pero sin afectar en su uso como rayones, manchas o suciedad o desgaste por uso.
- **Bien:** El equipo no debe contar con detalles estéticos visibles e identificables como suciedad, falta de 1 o 2 teclas, daño en la pantalla o desgaste por uso.
- **Regular:** El equipo puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad o desgaste por uso.
- **Mal:** El equipo se encuentra en pésimas condiciones pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad o carcasa rota. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 26. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4

Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el equipo de cómputo.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los equipos de cómputo se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento.
Técnica	1. Ingresar al departamento de sistemas y evaluar el equipo de cómputo. 2. Lograr identificar los posibles desperfectos que podría tener el equipo.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad, desgaste por uso) Bien: El equipo cuenta con detalles estéticos visibles e identificables (suciedad, falta de 1 o 2 teclas, daño en la pantalla, desgaste por uso).

Tabla 26 (continuación). Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4

Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4	
	Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc). Mal: El equipo se encuentra en pésimas condiciones (Pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, carcasa rota, etc)
Criterios de Terminación / Valor obtenido	Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc).
Interpretación de resultados	Se puede observar que el equipo Marca Lenovo, Modelo thinkpad T460s, se encuentra con detalles estéticos muy visibles y faltante de teclas. 

	
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

El equipo 5 (Laptop) (Véase tabla 27. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El equipo se debe encontrar en perfecto estado; el equipo no debe contar con ningún tipo de anomalía.
- **Muy bien:** El equipo se debe encontrar en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso como rayones, manchas o suciedad o desgaste por uso.

- **Bien:** El equipo cuenta con detalles estéticos visibles e identificables como suciedad, falta de 1 o 2 teclas, daño en la pantalla o desgaste por uso.
- **Regular:** El equipo puede contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad o desgaste por uso.
- **Mal:** El equipo se encuentra en pésimas condiciones como la pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad y carcasa rota. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 27. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5

Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el equipo de cómputo.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los equipos de cómputo se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento.
Técnica	3. Ingresar al departamento de sistemas y evaluar el equipo de cómputo. 4. Lograr identificar los posibles desperfectos que podría tener el equipo.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El equipo se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El equipo se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su uso. (rayones, manchas o suciedad, desgaste por uso) Bien: El equipo cuenta con detalles estéticos visibles e identificables (suciedad, falta de 1 o 2 teclas, daño en la pantalla, desgaste por uso). Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc). Mal: El equipo se encuentra en pésimas condiciones (Pantalla imposible de ver, teclado sin muchas teclas, el touchpad no funciona, suciedad, carcasa rota, etc)
Criterios de Terminación / Valor obtenido	Regular: El equipo cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, en

Tabla 27 (continuación) Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5

Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5	
	el teclado faltan teclas, el touchpad esta dañado, suciedad, desgaste por uso, etc).
Interpretación de resultados	Se puede observar que el equipo Marca Lenovo, Modelo thinkpad L460, se encuentra con detalles estéticos muy visibles como el desgaste del touchpad y algunas partes del teclado. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

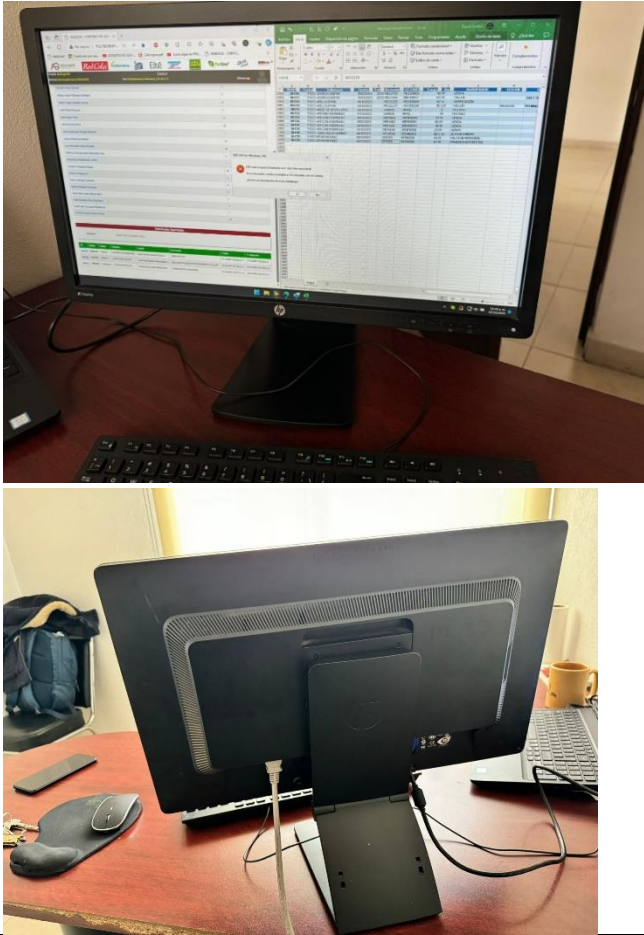
El monitor 4 (véase tabla 28. Desarrollo de prueba de monitor de analista de datos SAP), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El monitor se debe encontrar en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.
- **Muy bien:** El monitor se debe encontrar en buen estado, con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.
- **Bien:** El monitor puede contar con detalles estéticos visibles e identificables como suciedad, daño en la pantalla, rayones o manchas.
- **Regular:** El monitor cuenta con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado.
- **Mal:** El monito se encuentra en pésimas condiciones como pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 28. Desarrollo de prueba de monitor de analista de datos de SAP

Desarrollo de prueba de monitor del analista de datos de SAP	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el monitor.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los monitores se encuentren en buenas condiciones permiten visualizar la información relevante al puesto del personal.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el monitor se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El monitor se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El monitor cuenta con detalles estéticos visibles e identificables (suciedad, daño en la pantalla, rayones o manchas). Regular: El monitor cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas de pantalla, suciedad, soporte/ base dañado etc). Mal: El monitor se encuentra en pésimas condiciones (Pantalla imposible de ver, suciedad, carcasa rota, soporte dañado o sin funcionar, rayones, etc).
Criterios de Terminación / Valor obtenido	Excelente: El monitor se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.

Tabla 28 (continuación). Desarrollo de prueba de monitor de analista de datos de SAP

Desarrollo de prueba de monitor del analista de datos de SAP	
Interpretación de resultados	Se puede observar que el monitor marca HP modelo ZDisplay, no cuenta con ninguna anomalía o imperfecto, está en excelentes condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza.

El CPU 4 (véase tabla 29. Desarrollo de prueba de CPU del analista de datos de SAP), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** El CPU se debe encontrar en perfecto estado; el equipo no cuenta con ningún tipo de anomalía.
- **Muy bien:** El CPU debe encontrar en buen estado, con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.
- **Bien:** El CPU puede contar con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.
- **Regular:** El CPU cuenta con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes o desgaste por uso.
- **Mal:** El CPU se encuentra en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones, golpes, etc. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 29. Desarrollo de prueba de CPU de analista de datos SAP

Desarrollo de prueba de CPU del analista de datos de SAP	
Objetivo de la prueba	Analizar el estado físico en que se encuentra el CPU.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que los CPU se encuentren en buenas condiciones ya que en ella se encuentra almacenada información relevante al puesto del personal y del departamento de sistemas.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que el CPU se encuentre en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: El CPU se encuentra en perfecto estado; el equipo no cuenta con ningún tipo de anomalía. Muy bien: El CPU se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: El CPU cuenta con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: El CPU cuenta con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, marcas de golpes, desgaste por uso).

Tabla 29 (continuación). Desarrollo de prueba de CPU de analista de datos SAP

Desarrollo de prueba de CPU del analista de datos de SAP	
	Mal: El CPU se encuentra en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, etc).
Criterios de Terminación / Valor obtenido	Muy bien: El CPU Marca DELL, modelo Vostro, se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad)
Interpretación de resultados	Se puede observar que el CPU cuenta con ligeros detalles de desgastamiento por uso, se encuentra en buenas condiciones.
Recomendaciones	De acuerdo con la sección 9.2.4. Mantenimiento del equipo de la norma ISO 17799; “sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo”, por lo que se recomienda: 1. Limpiar externamente el equipo con productos especiales para computo (espuma limpiadora, aire comprimido, limpia pantallas, etc) por lo menos una vez por semana, para evitar manchas o desvanecimiento de color. 2. Evitar consumir alimentos en el espacio donde se encuentre el equipo o mientras se utiliza. 3. Evitar colocar el CPU en lugares donde se pueda raspar o pronunciar más el desgaste. 4. Limpiar el exterior del CPU con productos especiales para equipo de cómputo por lo menos una vez a la semana, para mantener el buen estado del monitor y prolongar su vida.

Los mouses del departamento de sistemas (véase tabla 30. Desarrollo de prueba de mouses), se evaluaron utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el activo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Excelente:** Los mouses se deben encontrar en perfecto estado; los mouses no cuentan con ningún tipo de anomalía.
- **Muy bien:** Los mouses se encuentran en buen estado, con ligeros detalles estéticos, pero sin afectar en su función. como rayones, manchas o suciedad.
- **Bien:** Los mouses pueden contar con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.
- **Regular:** Los mouses cuentan con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso.

- **Mal:** Los mouses se encuentran en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 30. Desarrollo de prueba de mouses

Desarrollo de prueba de mouses	
Objetivo de la prueba	Analizar el estado físico en que se encuentran los mouses de los equipos del departamento.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que todo el equipo de cómputo se encuentre en buenas condiciones ya que facilita la realización de tareas y funciones.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que todos los mouses se encuentren en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: Los mouses se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía. Muy bien: Los mouses se encuentran en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: Los mouses cuentan con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: Los mouses cuentan con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso). Mal: Los mouses se encuentran en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado, etc).
Criterios de Terminación / Valor obtenido	Excelente: Los mouses se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que los mouses no cuentan con desperfectos o alguna anomalía, se encuentran en perfectas condiciones.

Tabla 30 (continuación). Desarrollo de prueba de mouses

Desarrollo de prueba de mouses	
Interpretación de resultados	
Recomendaciones	1. Utilizar un paño suave y ligeramente humedecido con agua o un líquido especial para limpiar la superficie del mouse. Evita que el líquido entre en el interior del mouse. 2. Usar un bastoncillo de algodón humedecido para limpiar alrededor de los botones y la rueda de desplazamiento. Esto ayuda a eliminar el polvo y la suciedad acumulada.

Los teclados del departamento de sistemas (véase tabla 31. Desarrollo de prueba de teclados), se evaluaron utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

Excelente: Los teclados se deben encontrar en perfecto estado; los mouses no cuentan con ningún tipo de anomalía.

Muy bien: Los teclados se deben encontrar en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.

Bien: Los teclados cuentan con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.

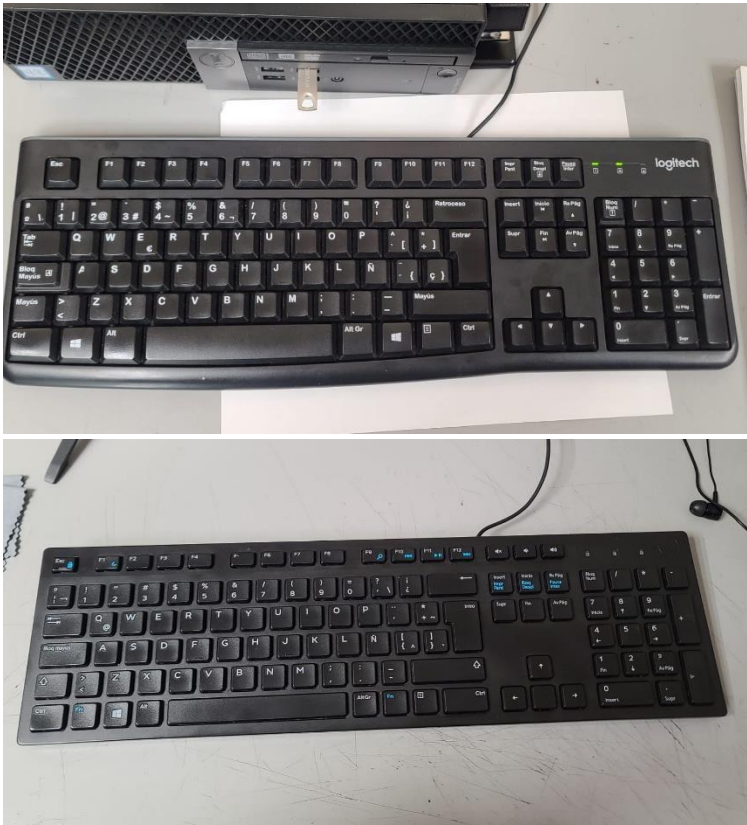
Regular: Los teclados cuentan con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso.

Mal: Los teclados se encuentran en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 31. Desarrollo de prueba de teclados

Tabla 11. Desarrollo de prueba de teclados	
Objetivo de la prueba	Analizar el estado físico en que se encuentran los teclados de los equipos del departamento.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que todo el equipo de cómputo se encuentre en buenas condiciones ya que facilita la realización de tareas y funciones.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que todos los teclados se encuentren en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: Los teclados se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía. Muy bien: Los teclados se encuentran en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: Los teclados cuentan con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas).

Tabla 31 (continuación). Desarrollo de pruebas de mouses

Desarrollo de prueba de mouses	
	Regular: Los teclados cuentan con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso). Mal: Los teclados se encuentran en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado, etc).
Criterios de Terminación / Valor obtenido	Excelente: Los teclados se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que los teclados no cuentan con desperfectos o alguna anomalía, se encuentran en perfectas condiciones. 
Recomendaciones	De acuerdo con la sección 9.2.1. Ubicación y protección del equipo de la norma ISO 17799: 1. “se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo”

	2. Se recomienda dar mantenimiento con productos adecuados para la limpieza como alcohol isopropílico o espuma limpiadora.
--	--

Los teléfonos del departamento de sistemas (véase tabla 32. Desarrollo de prueba de telefonía), se evaluaron utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

Excelente: Los teléfonos se deben encontrar en perfecto estado; los teléfonos no cuentan con ningún tipo de anomalía.

Muy bien: Los teléfonos se deben encontrar en buen estado, con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.

Bien: Los teléfonos cuentan con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.

Regular: Los teléfonos pueden contar con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso.

Mal: Los teléfonos se encuentran en pésimas condiciones con suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 32. Desarrollo de prueba de telefonía

Desarrollo de prueba de telefonía	
Objetivo de la prueba	Analizar el estado físico en que se encuentran los teléfonos de los equipos del departamento.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que todo el equipo de cómputo y telefonía se encuentre en buenas condiciones ya que facilita la comunicación y realización de actividades.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que todos los teléfonos se encuentren en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.

Tabla 32. (Continuación). Desarrollo de prueba de telefonía. Elaboración propia.

Desarrollo de prueba de telefonía	
Proceso de medición	Excelente: Los teléfonos se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía. Muy bien: Los teléfonos se encuentran en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: Los teléfonos cuentan con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: Los teléfonos cuentan con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso). Mal: Los teléfonos se encuentran en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado, etc).
Criterios de Terminación / Valor obtenido	Excelente: Los teléfonos se encuentran en perfecto estado; los teléfonos no cuentan con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que los teléfonos no cuentan con desperfectos o alguna anomalía, se encuentran en perfectas condiciones. 

Recomendaciones	De acuerdo con la sección 9.2.2. Servicios públicos de soporte de la norma ISO 17799: “los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia” Los servicios de voz, como las líneas telefónicas, son fundamentales para poder brindar soporte técnico de manera rápida y personalizada. 1. Se recomienda limpiar el exterior del teléfono con productos especiales para equipo de cómputo por lo menos una vez a la semana, para mantener el buen estado y prolongar su vida.
------------------------	---

La impresora 1 (véase tabla 33. Desarrollo de prueba de impresoras), se evaluó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

Excelente: La impresora se debe encontrar en perfecto estado; la impresora no cuenta con ningún tipo de anomalía.

Muy bien: La impresora se encuentra en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función como rayones, manchas o suciedad.

Bien: La impresora cuenta con detalles estéticos visibles e identificables como suciedad, daño en la carcasa, rayones o manchas.

Regular: La impresora cuentan con detalles estéticos muy pronunciados y visibles como carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso.

Mal: La impresora se encuentra en pésimas condiciones como suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado 8u. Esto con el objetivo de evaluar la calidad del estado en que se encuentra el activo.

Tabla 33. Desarrollo de prueba de impresoras

Desarrollo de prueba de impresoras	
Objetivo de la prueba	Analizar el estado físico en que se encuentran las impresoras de los equipos del departamento.
Descripción de la prueba y Valor esperado	En el departamento de sistemas es esencial que todo el equipo de cómputo se encuentre en buenas condiciones ya que facilita la realización de tareas y funciones.
Técnica	1. Ingresar al departamento de Sistemas 2. Observar que todos los mouses se encuentren en buen estado.
Herramientas Requeridas	Dispositivo móvil con cámara.
Proceso de medición	Excelente: Las impresoras se encuentran en perfecto estado; los mouses no cuentan con ningún tipo de anomalía. Muy bien: Las impresoras se encuentran en buen estado, cuenta con ligeros detalles estéticos, pero sin afectar en su función. (rayones, manchas o suciedad) Bien: Las impresoras cuentan con detalles estéticos visibles e identificables (suciedad, daño en la carcasa, rayones o manchas). Regular: Las impresoras cuentan con detalles estéticos muy pronunciados y visibles (carcasa rota, manchas, suciedad, puertos dañados, desgaste por uso). Mal: Las impresoras se encuentran en pésimas condiciones (suciedad, carcasa rota, desgaste por uso, rayones, golpes, puertos y cable dañado, etc).
Criterios de Terminación / Valor obtenido	Excelente: Las impresoras se encuentran en perfecto estado, no cuentan con ningún tipo de anomalía.
Interpretación de resultados	Se puede observar que las impresoras no cuentan con desperfectos o alguna anomalía, se encuentran en perfectas condiciones.
Recomendaciones	1. Limpiar el exterior de la impresora con productos especiales para este tipo de equipos, por lo menos una vez a la semana, para mantener el buen estado y prolongar su vida.

INSPECCIÓN Y PRUEBAS DE SEGURIDAD LÓGICA

La seguridad lógica es un aspecto fundamental de la auditoría de seguridad en un entorno de departamentos de TI. Se refiere a las medidas y controles implementados para proteger los sistemas de información, redes y datos contra amenazas y riesgos cibernéticos que podrían comprometer su confidencialidad, integridad y disponibilidad. En el contexto de esta auditoría, se evaluará el estado de las medidas de seguridad lógica implementadas en el departamento de sistemas, centrándose en la disponibilidad y calidad de los equipos de cómputo, la conectividad de red y las medidas de protección contra virus y malware.

Durante la auditoría, se realizarán pruebas técnicas, revisiones de configuración, análisis de vulnerabilidades y revisiones documentales para evaluar el estado de las medidas de seguridad lógica implementadas. Se identificarán posibles brechas de seguridad y se ofrecerán recomendaciones para mejorar la protección lógica de los sistemas, redes y datos. El objetivo final es asegurar la confidencialidad, integridad y disponibilidad de la información del departamento de sistemas, mitigando los riesgos cibernéticos y promoviendo un entorno seguro para las actividades de TI.

Los resultados de estas pruebas se muestran en tablas, donde se ingresa información como los objetivos de la prueba, descripción, técnicas y herramientas a utilizar, así como un proceso de medición, se añaden consideraciones especiales, así como la interpretación de resultados, que es donde se incluyen las fotografías tomadas durante el análisis y para finalizar con la tabla, se escriben recomendaciones de acuerdo con la norma ISO 17799.

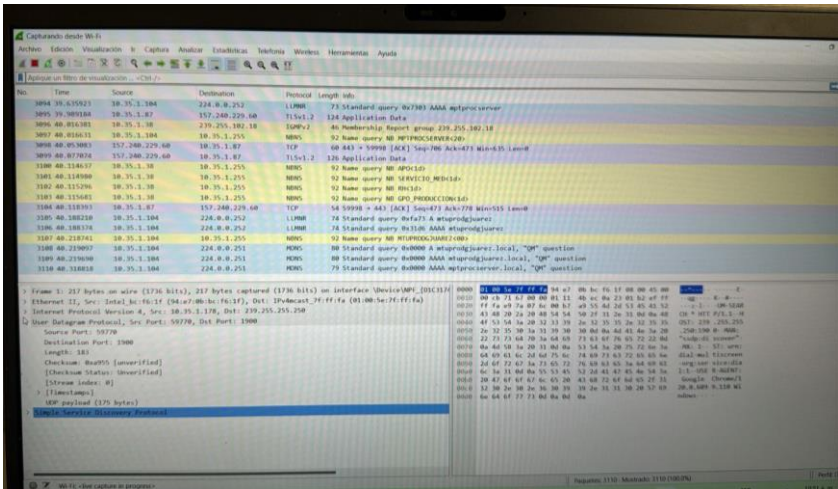
Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 1

El equipo del auxiliar de soporte y mantenimiento 1 (véase tabla 34. Desarrollo e prueba de conectividad de la red), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Conexión buena:** la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad,
- **Conexión estable:** la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo,
- **Conexión intermitente:** la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella,
- **Mala conexión:** el servicio de Internet tiene muchas fallas y funciona en pocos equipos, Sin conexión: no existe servicio de Internet.

Esto con el objetivo de evaluar la **conectividad de la Red** que se encuentra en el activo.

Tabla 34. Desarrollo de Prueba de Conectividad de la Red (Auxiliar de mantenimiento 1).

Desarrollo de Prueba de Conectividad de la Red (Auxiliar de mantenimiento 1)	
Objetivo de la prueba	Evaluar la capacidad de los dispositivos de red para establecer y mantener conexiones confiables y seguras dentro del entorno
Descripción de la prueba y Valor esperado	1. Instalar y ejecutar Wireshark en los equipos de cómputo 2. Obtener un escaneo de la señal de WiFi / ETHERNET del equipo del personal del departamento de sistemas.
Técnica	Análisis de resultados de los datos en Wireshark
Herramientas Requeridas	Equipo de computo Wireshark
Proceso de medición	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad Conexión estable: la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo Conexión intermitente: la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella Mala conexión: el servicio de Internet tiene muchas fallas y funciona en pocos equipos Sin conexión: no existe servicio de Internet
Criterios de Terminación / Valor obtenido	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad
Interpretación de resultados	Se observa que la conectividad del cable ethernet es buena y estable. 
Recomendaciones	1. Revisar el cable ethernet por lo menos cada 15 días para asegurar que se encuentre en óptimas condiciones y no haya intermitencia o desconexión.

El equipo del auxiliar de soporte y mantenimiento 1 (véase tabla 35. Desarrollo de prueba de seguridad de los puertos con NMAP), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

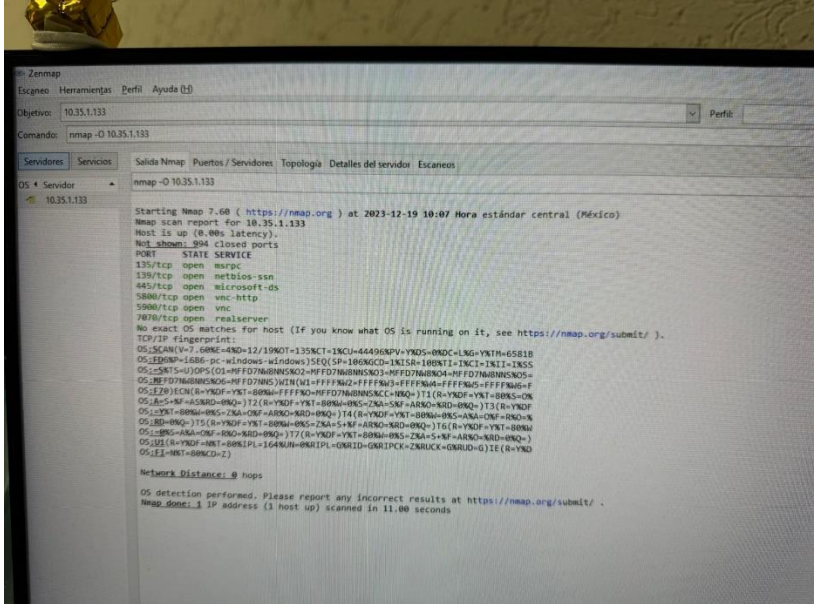
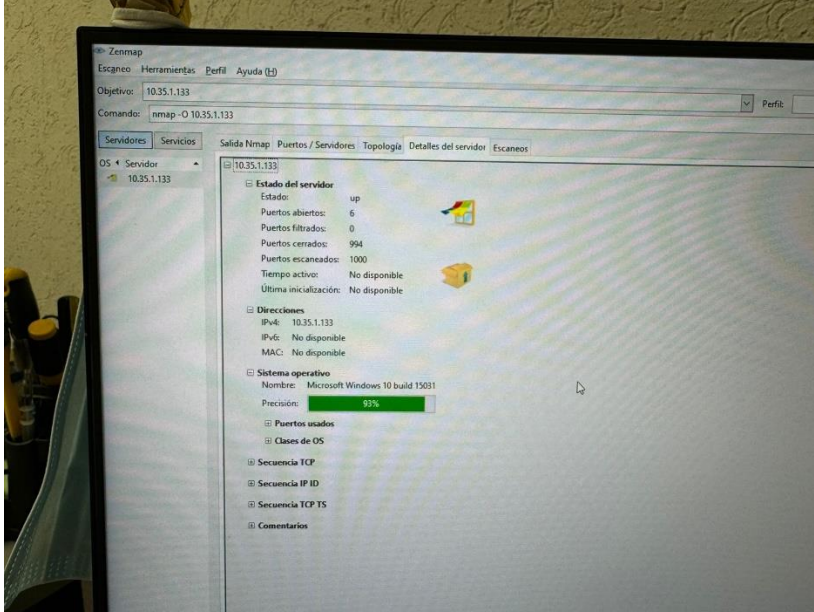
- **Puertos seguros:** se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados,
- **Puertos cerrados:** se mantienen cerrados los puertos inactivos,
- **Puertos inseguros:** no cuenta con seguridad y se encuentran los puertos activos por default.

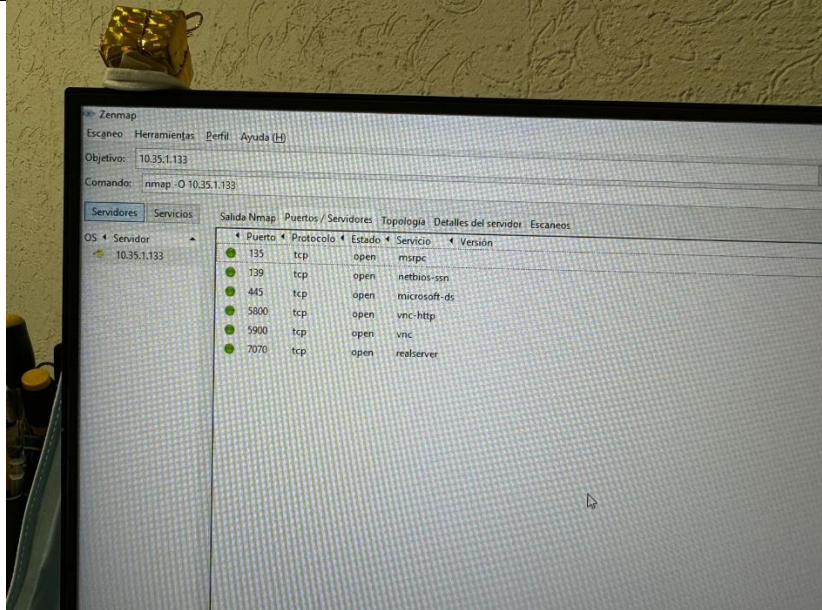
Esto con el objetivo de evaluar la **Seguridad de los Puertos** que se encuentra en el activo.

Tabla 35. Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 1).

Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 1).	
Objetivo de la prueba	Evaluar la seguridad de los sistemas y redes identificando los puertos abiertos y servicios expuestos
Descripción de la prueba y Valor esperado	1. Instalar y ejecutar Nmap en los equipos de cómputo 2. Obtener un escaneo de los puertos del equipo de computo
Técnica	Análisis de la información sobre los puertos
Herramientas Requeridas	Nmap Equipo de computo Dispositivo móvil con cámara
Proceso de medición	Puertos seguros: se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados Puertos cerrados: se mantienen cerrados los puertos inactivos Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Criterios de Terminación / Valor obtenido	Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Interpretación de resultados	Con el escaneo nos muestra información sobre los puertos que están habilitados en el pc, son los puertos que vienen por default. De igual manera nos muestra los dispositivos que se encuentran conectados en dicha red dándonos una idea de cómo detectar actividad sospechosa.

Tabla 35 (continuación). Desarrollo de prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 1)

Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 1).	
Interpretación de resultados	 

	 <table><thead><tr><th>Puerto</th><th>Protocolo</th><th>Estado</th><th>Servicio</th><th>Versión</th></tr></thead><tbody><tr><td>135</td><td>tcp</td><td>open</td><td>msrpc</td><td></td></tr><tr><td>139</td><td>tcp</td><td>open</td><td>netbios-ssn</td><td></td></tr><tr><td>445</td><td>tcp</td><td>open</td><td>microsoft-ds</td><td></td></tr><tr><td>5800</td><td>tcp</td><td>open</td><td>vnc-http</td><td></td></tr><tr><td>5900</td><td>tcp</td><td>open</td><td>vnc</td><td></td></tr><tr><td>7070</td><td>tcp</td><td>open</td><td>realserver</td><td></td></tr></tbody></table>	Puerto	Protocolo	Estado	Servicio	Versión	135	tcp	open	msrpc		139	tcp	open	netbios-ssn		445	tcp	open	microsoft-ds		5800	tcp	open	vnc-http		5900	tcp	open	vnc		7070	tcp	open	realserver	
Puerto	Protocolo	Estado	Servicio	Versión																																
135	tcp	open	msrpc																																	
139	tcp	open	netbios-ssn																																	
445	tcp	open	microsoft-ds																																	
5800	tcp	open	vnc-http																																	
5900	tcp	open	vnc																																	
7070	tcp	open	realserver																																	
Recomendaciones	De acuerdo con la sección 11.4. Protección del puerto de diagnóstico y configuración remoto: “Los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad comercial, debieran ser desactivados o removidos”. Se recomienda: 1. Realizar un procedimiento de soporte para asegurar que los puertos de diagnóstico y configuración sólo sean accesibles entre el gerente del servicio de cómputo y el personal de soporte de hardware/software que requiere acceso 2. Considerando el punto 10.8.1 de la ISO 17799, se recomienda mantener inhabilitados los puertos cuando no estén en uso.																																			

El equipo del auxiliar de soporte y mantenimiento 1 (véase tabla 36. Desarrollo de prueba de instalación de software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.

- **Funciona muy bien:** En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados.
- **Funciona bien:** La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas.
- **Funciona suficiente:** La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto. Se requiere una mayor atención para garantizar que solo se instalen softwares autorizados y que estén plenamente funcionales.
- **Deficiente:** La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino.

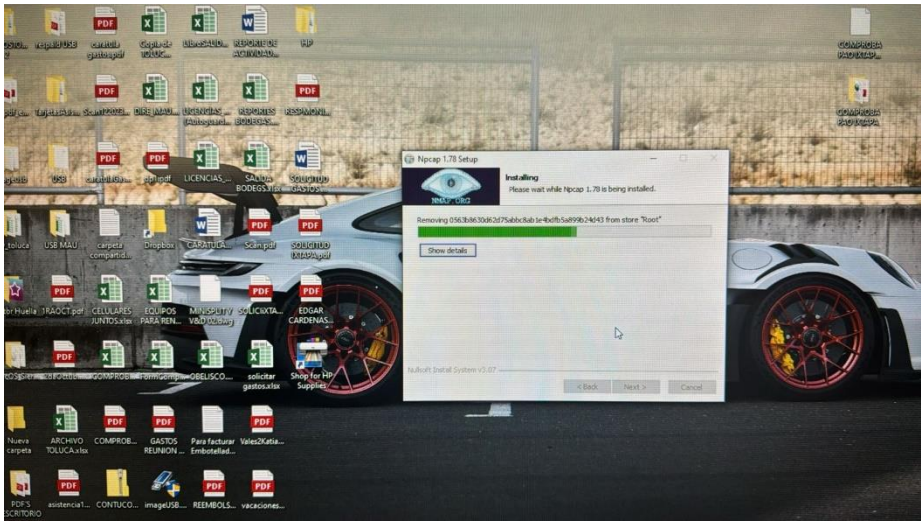
Esto con el objetivo de evaluar la **Instalación de Software** en el activo.

Tabla 36. Desarrollo de prueba de instalación de software (Auxiliar de soporte 1)

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 1)	
Objetivo de la prueba	Observar y analizar el proceso de instalación de cualquier software en los equipos de cómputo del laboratorio de cisco para verificar su seguridad y facilidad en la instalación.
Descripción de la prueba y Valor esperado	La realización de esta prueba se ejecuta para comprobar y analizar el procedimiento de instalación de softwares en los equipos de cómputo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la Instalación de algún software en cualquier equipo de cómputo
Herramientas Requeridas	Memoria USB, laptop y dispositivo móvil con cámara.

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 1)	
Proceso de medición	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino. Funciona muy bien: En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados. Funciona bien: La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas. Funciona suficiente: La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto. Se requiere una mayor atención para garantizar que solo se instalen softwares autorizados y que estén plenamente funcionales. Deficiente: La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino.
Criterios de Terminación / Valor obtenido	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.

Tabla 36 (continuación). Desarrollo de prueba de instalación de software (Auxiliar de soporte 1)

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 1)	
Interpretación de resultados	El proceso de instalación se muestra de manera correcta siguiendo el procedimiento adecuado sin interrupciones ni complicaciones.  
Recomendaciones	1. Antes de proceder con la instalación, revisar los requisitos del sistema especificados por el fabricante del software y verificar que el equipo cumpla con los requisitos mínimos de hardware, sistema operativo y otros componentes necesarios. 2. Descargar el software únicamente de fuentes confiables y oficiales. Evitar sitios web no verificados o descargas de dudosa procedencia, ya que pueden contener versiones modificadas, malware u otros problemas de seguridad. 3. Leer atentamente las instrucciones de instalación proporcionadas por el desarrollador del software y seguir los pasos de instalación recomendados,

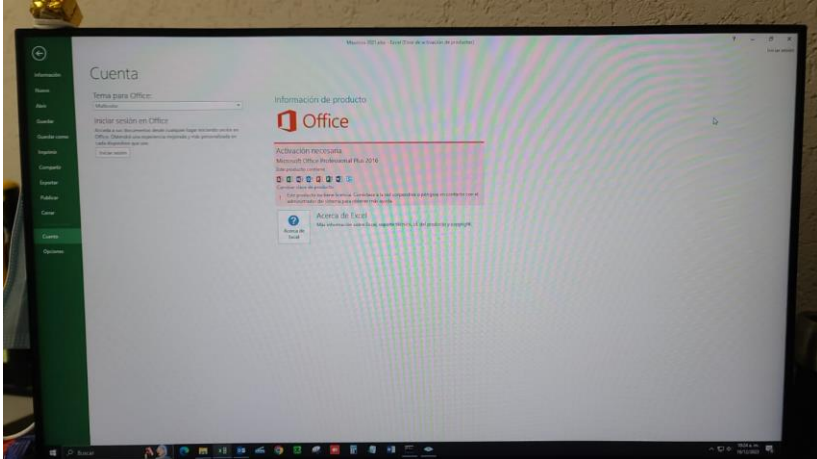
El equipo del auxiliar de soporte y mantenimiento 1, (véase tabla 37. Desarrollo de prueba de licencia de software) se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna.
- **Funciona muy bien:** En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas.
- **Funciona bien:** Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias.
- **Funciona suficiente:** Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas.
- **Deficiente:** El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Esto con el objetivo de evaluar el estado de las **Licencias de Software** que se encuentra en el activo.

Tabla 37. Desarrollo de prueba de licencia de software (Auxiliar de soporte 1)

Desarrollo de Prueba de Licencias de Software (Auxiliar de soporte 1)	
Objetivo de la prueba	Observar que la instalación de los softwares en el equipo de cómputo y los softwares ya instalados cuenten con la licencia correspondiente para su uso adecuado.
Descripción de la prueba y Valor esperado	La prueba se realiza para verificar que cada uno de los softwares instalados en el equipo de cómputo cuenten con sus respectivas licencias de uso.
Técnica	1. Ingresar al departamento de sistemas 2. Buscar en la configuración de los softwares la licencia de estos y verificar que dichas licencias se encuentren activas.
Herramientas Requeridas	Equipo de cómputo y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna. Funciona muy bien: En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas. Funciona bien: Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias. Funciona suficiente: Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas. Deficiente: El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Criterios de Terminación / Valor obtenido	Funciona bien: Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias.
Interpretación de resultados	Se observa que el software más utilizado por el personal (Microsoft Word, Excel y Power Point) no cuenta con la licencia activa y el usuario la utiliza de esta manera, sin contar con todas las funciones que este proporciona. 
Recomendaciones	De acuerdo con la sección 15.1.2. Derechos de propiedad intelectual (IPR) de la norma ISO 17799, se recomienda: 1. “Mantener prueba y evidencia de la propiedad de las licencias” 2. “Llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia” 3. Evitar el uso de software pirata o copias no autorizadas, ya que esto puede violar los derechos de autor y generar consecuencias legales.

El equipo del auxiliar de soporte y mantenimiento 1, (véase tabla 38. Desarrollo de prueba de seguridad del software) se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura.
- **Funciona muy bien:** En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones.
- **Funciona bien:** El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general.
- **Funciona suficiente:** El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente.
- **Deficiente:** El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.

Esto con el objetivo de evaluar la **Seguridad de Software** que se encuentra en el activo.

Tabla 38. Desarrollo de prueba de seguridad del software (Auxiliar de soporte 1)

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 1)	
Objetivo de la prueba	Analizar y comprobar la seguridad del software en los equipos de cómputo para verificar que se cuente con autenticación y protección de datos.
Descripción de la prueba y Valor esperado	La realización de esta prueba es para verificar que todos los equipos de cómputo de laboratorio cisco cuenten con la seguridad de los softwares deseada y así evitar daños al equipo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la seguridad del software en los equipos de cómputo

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 1)	
Herramientas Requeridas	Equipos de cómputo, memoria USB y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura. Funciona muy bien: En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones. Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general. Funciona suficiente: El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente. Deficiente: El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.
Criterios de Terminación / Valor obtenido	Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general

Tabla 38 (continuación). Prueba de seguridad del software (Auxiliar de soporte 1)

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 1)	
Interpretación de resultados	Se observó que cuenta con la protección de windows defender, básica protección contra amenazas.
Recomendaciones	1. Implementar mecanismos de autenticación y autorización robustos para controlar el acceso al software y a los datos sensibles. 2. Asignar los permisos de acceso adecuados para cada usuario y evita el uso de privilegios excesivos. 3. Adquirir un medio de protección adicional.

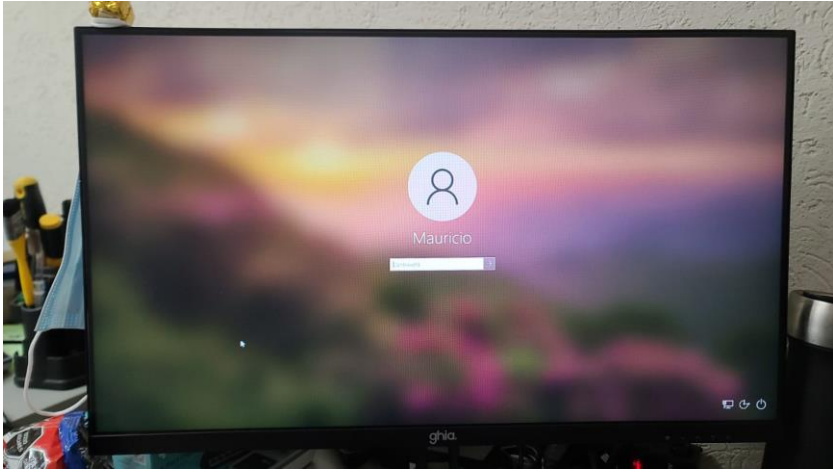
El equipo del auxiliar de soporte y mantenimiento 1, (véase tabla 39. Desarrollo de prueba de autenticación) se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
- **Funciona muy bien:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico
- **Funciona Regular:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.

Esto con el objetivo de evaluar el tipo de **Autenticación** que se encuentra en el activo.

Tabla 39. Desarrollo de prueba de autenticación (Auxiliar de soporte 1)

Desarrollo de Prueba de Autenticación (Auxiliar de soporte 1)	
Objetivo de la prueba	El objetivo de la prueba de autenticación es verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso en particular. Esta prueba tiene como objetivo principal garantizar la seguridad y protección de los datos y recursos al asegurarse de que solo usuarios autorizados puedan acceder a ellos. Algunos objetivos específicos de la prueba de autenticación incluyen:
Descripción de la prueba y Valor esperado	La prueba de autenticación es un proceso mediante el cual se evalúa la efectividad de los mecanismos utilizados para verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso. Esta prueba busca detectar posibles debilidades en los métodos de autenticación utilizados y garantizar que solo los usuarios autorizados puedan acceder a la información y los recursos protegidos.

Técnica	Es utilizada y consiste en que el usuario proporcione una contraseña secreta que solo él o ella debe conocer. La contraseña se compara con la almacenada previamente en el sistema para verificar la identidad del usuario.
Herramientas Requeridas	Equipo de cómputo, memoria USB, dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus. Funciona muy bien: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico Funciona Regular: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.
Criterios de Terminación / Valor obtenido	Funciona muy bien: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
Interpretación de resultados	Se puede observar que al intentar ingresar al equipo del usuario pide una contraseña para verificar la identidad del personal. 
Recomendaciones	En la sección 11.5.3. Sistema de gestión de claves secreta, de la norma ISO 17799, “Las claves secretas son uno de los principales medios para validar la autoridad del usuario para tener acceso a un servicio de cómputo.” Por lo que se recomienda: 1. Utilizar contraseñas de al menos 8 caracteres alfanuméricos y caracteres especiales (\$#%&) 2. No compartir la contraseña con ninguna persona fuera de la autorización.

Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 2

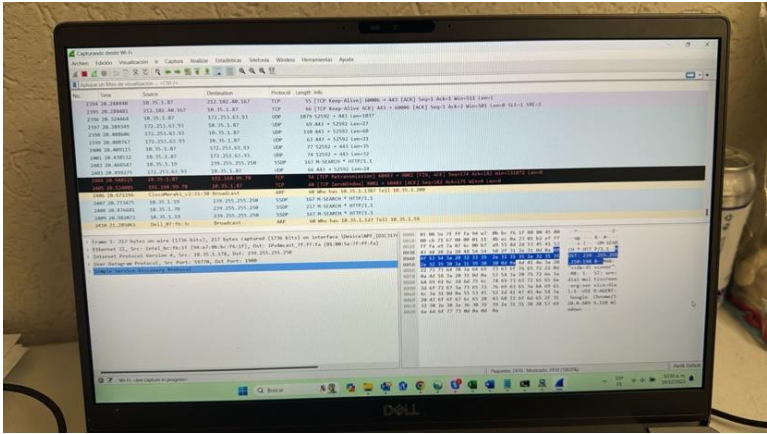
El equipo del auxiliar de soporte y mantenimiento 2, (véase tabla 40. Prueba de conectividad de red) se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Conexión buena:** la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad,
- **Conexión estable:** la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo,
- **Conexión intermitente:** la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella,
- **Mala conexión:** el servicio de Internet tiene muchas fallas y funciona en pocos equipos, Sin conexión: no existe servicio de Internet.

Esto con el objetivo de evaluar la **conectividad de la Red** que se encuentra en el activo.

Tabla 40. Prueba de conectividad de red. (Auxiliar de soporte 2).

Desarrollo de Prueba de Conectividad de la Red. (Auxiliar de soporte 2)	
Objetivo de la prueba	Evaluar la capacidad de los dispositivos de red para establecer y mantener conexiones confiables y seguras dentro del entorno
Descripción de la prueba y Valor esperado	1. Instalar y ejecutar Wireshark en los equipos de cómputo 2. Obtener un escaneo de la señal de WiFi / ETHERNET del equipo del personal del departamento de sistemas.
Técnica	Análisis de resultados de los datos en Wireshark
Herramientas Requeridas	Equipo de computo Wireshark Dispositivo móvil con cámara
Proceso de medición	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad Conexión estable: la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo Conexión intermitente: la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella Mala conexión: el servicio de Internet tiene muchas fallas y funciona en pocos equipos

	Sin conexión: no existe servicio de Internet
Criterios de Terminación / Valor obtenido	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad.
Interpretación de resultados	Se observa que la conectividad Wifi del equipo es buena, es estable y sin variaciones. 
Recomendaciones	1. Cambiar la contraseña de Wifi por lo menos cada 15 días para evitar la lentitud y saturación de dispositivos conectados.

El equipo del auxiliar de soporte y mantenimiento 2, (véase tabla 41. Prueba de seguridad de puertos. Auxiliar 2), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Puertos seguros:** se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados,
- **Puertos cerrados:** se mantienen cerrados los puertos inactivos,
- **Puertos inseguros:** no cuenta con seguridad y se encuentran los puertos activos por default.

Esto con el objetivo de evaluar la **Seguridad de los Puertos** que se encuentra en el activo.

Tabla 41. Prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 2).

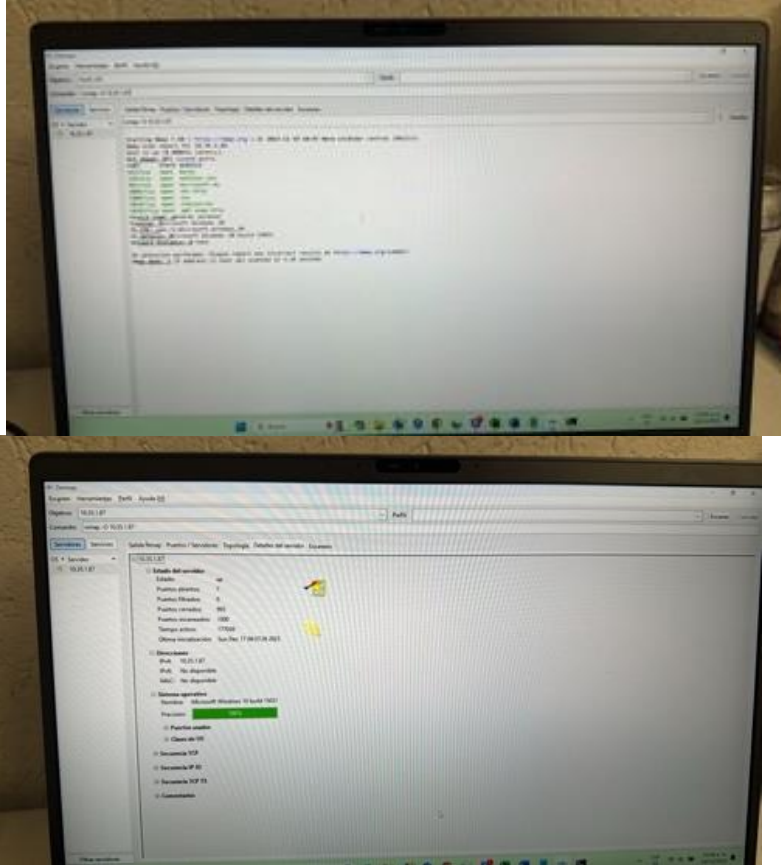
Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 2).	
Objetivo de la prueba	Evaluar la seguridad de los sistemas y redes identificando los puertos abiertos y servicios expuestos
Descripción de la prueba y Valor esperado	3. Instalar y ejecutar Nmap en los equipos de cómputo 4. Obtener un escaneo de los puertos del equipo de computo
Técnica	Análisis de la información sobre los puertos
Herramientas Requeridas	Nmap Equipo de computo Dispositivo móvil con cámara
Proceso de medición	Puertos seguros: se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados Puertos cerrados: se mantienen cerrados los puertos inactivos Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Criterios de Terminación / Valor obtenido	Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Interpretación de resultados	

Tabla 41 (continuación). Desarrollo de prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 2)

Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 2).	
Interpretación de resultados	 Con el escaneo nos muestra información sobre los puertos que están habilitados en el pc, son los puertos que vienen por default. De igual manera nos muestra los dispositivos que se encuentran conectados en dicha red dándonos una idea de cómo detectar actividad sospechosa.
Recomendaciones	De acuerdo con la sección 11.4. Protección del puerto de diagnóstico y configuración remoto: “Los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad comercial, debieran ser desactivados o removidos”. Se recomienda: 1. Realizar un procedimiento de soporte para asegurar que los puertos de diagnóstico y configuración sólo sean accesibles entre el gerente del servicio de cómputo y el personal de soporte de hardware/software que requiere acceso 2. Considerando el punto 10.8.1 de la ISO 17799, se recomienda mantener inhabilitados los puertos cuando no estén en uso.

El equipo del auxiliar de soporte y mantenimiento 2 (véase tabla 42. Prueba de instalación de software) se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

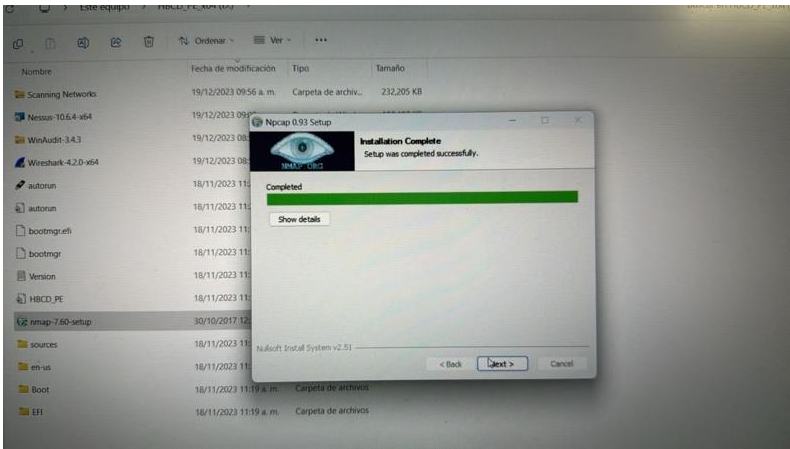
- **Funciona excelente:** La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.
- **Funciona muy bien:** En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados.
- **Funciona bien:** La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas.
- **Funciona suficiente:** La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto. Se requiere una mayor atención para garantizar que solo se instalen softwares autorizados y que estén plenamente funcionales.
- **Deficiente:** La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino.

Esto con el objetivo de evaluar la **Instalación de Software** en el activo.

Tabla 42. Desarrollo de prueba de instalación de software (Auxiliar de soporte 2)

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 2)	
Objetivo de la prueba	Observar y analizar el proceso de instalación de cualquier software en los equipos de cómputo del laboratorio de cisco para verificar su seguridad y facilidad en la instalación.
Descripción de la prueba y Valor esperado	La realización de esta prueba se ejecuta para comprobar y analizar el procedimiento de instalación de softwares en los equipos de cómputo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la Instalación de algún software en cualquier equipo de cómputo
Herramientas Requeridas	Memoria USB, laptop y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino. Funciona muy bien: En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados. Funciona bien: La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas. Funciona suficiente: La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto. Se requiere una mayor atención para

Tabla 42. (continuación). Prueba de instalación de software (Auxiliar de soporte 2).

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 2)	
	garantizar que solo se instalen softwares autorizados y que estén plenamente funcionales. Deficiente: La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino.
Criterios de Terminación / Valor obtenido	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.
Interpretación de resultados	Se puede observar que en el equipo que el proceso de instalación se muestra de manera correcta siguiendo el procedimiento adecuado. 
Recomendaciones	1. Antes de proceder con la instalación, revisar los requisitos del sistema especificados por el fabricante del software y verificar que el equipo cumpla con los requisitos mínimos de hardware, sistema operativo y otros componentes necesarios. 2. Descargar el software únicamente de fuentes confiables y oficiales. Evitar sitios web no verificados

	o descargas de dudosa procedencia, ya que pueden contener versiones modificadas, malware u otros problemas de seguridad. 3. Leer atentamente las instrucciones de instalación proporcionadas por el desarrollador del software y seguir los pasos de instalación recomendados,
--	--

El equipo del auxiliar de soporte y mantenimiento 2, (véase tabla 43. Prueba de licencias de software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

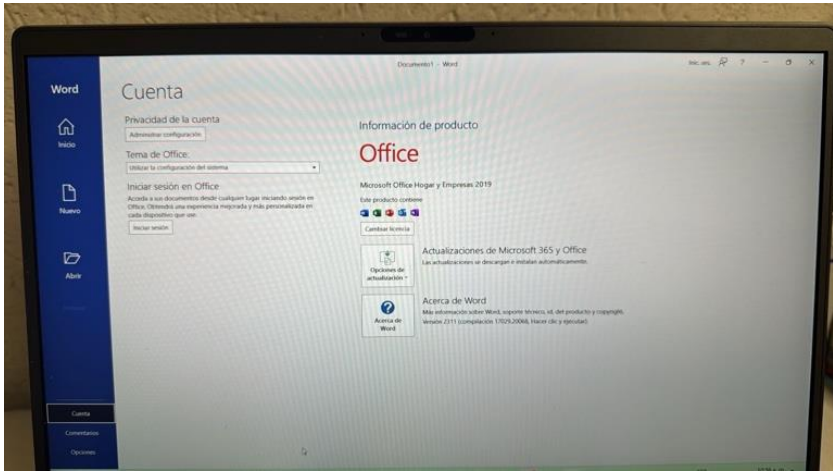
- **Funciona excelente:** Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna.
- **Funciona muy bien:** En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas.
- **Funciona bien:** Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias.
- **Funciona suficiente:** Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas.
- **Deficiente:** El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Esto con el objetivo de evaluar el estado de las **Licencias de Software** que se encuentra en el activo.

Tabla 43. Desarrollo de prueba de licencias de software (Auxiliar de soporte 2)

Desarrollo de Prueba de Licencias de Software (Auxiliar de soporte 2)	
Objetivo de la prueba	Observar que la instalación de los softwares en el equipo de cómputo y los softwares ya instalados cuenten con la licencia correspondiente para su uso adecuado.
Descripción de la prueba y Valor esperado	La prueba se realiza para verificar que cada uno de los softwares instalados en el equipo de cómputo cuenten con sus respectivas licencias de uso.
Técnica	1. Ingresar al departamento de sistemas 2. Buscar en la configuración de los softwares la licencia de estos y verificar que dichas licencias se encuentren activas.
Herramientas Requeridas	Equipo de cómputo y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna. Funciona muy bien: En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas. Funciona bien: Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias. Funciona suficiente: Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas. Deficiente: El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Tabla 42 (continuación). Prueba de licencias de software (Auxiliar de soporte 2).

Desarrollo de Prueba de Licencias de Software (Auxiliar de soporte 2)	
Criterios de Terminación / Valor obtenido	Funciona excelente: Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna
Interpretación de resultados	Se observa en el equipo que el software más utilizado por el personal (Microsoft Word, Excel y Power Point) cuenta con la licencia activa. 
Recomendaciones	De acuerdo con la sección 15.1.2. Derechos de propiedad intelectual (IPR) de la norma ISO 17799, se recomienda: 1. “Mantener prueba y evidencia de la propiedad de las licencias” 2. “Llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia” 3. Evitar el uso de software pirata o copias no autorizadas, ya que esto puede violar los derechos de autor y generar consecuencias legales.

El equipo del auxiliar de soporte y mantenimiento 2, (véase tabla 44. Prueba de seguridad del software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura.
- **Funciona muy bien:** En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones.
- **Funciona bien:** El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general.
- **Funciona suficiente:** El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente.
- **Deficiente:** El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.

Esto con el objetivo de evaluar la **Seguridad de Software** que se encuentra en el activo.

Tabla 44. Prueba de seguridad del software (Auxiliar de soporte 2).

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 2)	
Objetivo de la prueba	Analizar y comprobar la seguridad del software en los equipos de cómputo para verificar que se cuente con autenticación y protección de datos.
Descripción de la prueba y Valor esperado	La realización de esta prueba es para verificar que todos los equipos de cómputo de laboratorio cisco cuenten con la seguridad de los softwares deseada y así evitar daños al equipo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la seguridad del software en los equipos de cómputo

Tabla 44 (continuación). Desarrollo de prueba de seguridad del software (Auxiliar de soporte 2).

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 2)	
Herramientas Requeridas	Equipos de cómputo, memoria USB y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura. Funciona muy bien: En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones. Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general. Funciona suficiente: El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente. Deficiente: El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.
Criterios de Terminación / Valor obtenido	Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general

Tabla 44 (continuación). Prueba de seguridad del software (Auxiliar de soporte 2).

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 2)	
Interpretación de resultados	Se observó que el equipo cuenta con la protección de windows defender, básica protección contra amenazas y aparte un antivirus SYMANTEC.
Recomendaciones	1. Implementar mecanismos de autenticación y autorización robustos para controlar el acceso al software y a los datos sensibles. 2. Asignar los permisos de acceso adecuados para cada usuario y evita el uso de privilegios excesivos. 3. Adquirir un medio de protección adicional.

El equipo del auxiliar de soporte y mantenimiento 2 (véase tabla 45. Prueba de autenticación), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
- **Funciona muy bien:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico
- **Funciona Regular:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.

Esto con el objetivo de evaluar el tipo de **Autenticación** que se encuentra en el activo.

Tabla 45. Desarrollo de prueba de autenticación (Auxiliar de soporte 2)

Desarrollo de Prueba de Autenticación (Auxiliar de soporte 2)	
Objetivo de la prueba	El objetivo de la prueba de autenticación es verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso en particular y garantizar la seguridad y protección de los datos y recursos al asegurarse de que solo usuarios autorizados puedan acceder a ellos.
Descripción de la prueba y Valor esperado	La prueba de autenticación es un proceso mediante el cual se evalúa la efectividad de los mecanismos utilizados para verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso. Esta prueba busca detectar posibles debilidades en los métodos de autenticación utilizados y garantizar que solo los usuarios autorizados puedan acceder a la información y los recursos protegidos.

Técnica	1. Ingresar al departamento de sistemas 2. Observar el inicio de sesión del equipo.
Herramientas Requeridas	Equipo de cómputo, memoria USB, dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus. Funciona muy bien: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico Funciona Regular: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.
Criterios de Terminación / Valor obtenido	Funciona excelente: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
Interpretación de resultados	Se puede observar que en el equipo, al intentar ingresar al equipo del usuario pide una contraseña para verificar la identidad del personal. 
Recomendaciones	En la sección 11.5.3. Sistema de gestión de claves secreta, de la norma ISO 17799, “Las claves secretas son uno de los principales medios para validar la autoridad del usuario para tener acceso a un servicio de cómputo.” Por lo que se recomienda: 1. Utilizar contraseñas de al menos 8 caracteres alfanuméricos y caracteres especiales (\$#%&) 2. No compartir la contraseña con ninguna persona fuera de la autorización.

Pruebas de seguridad lógica al equipo de cómputo del auxiliar en soporte y mantenimiento 3

El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 46. Prueba de conectividad de red), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

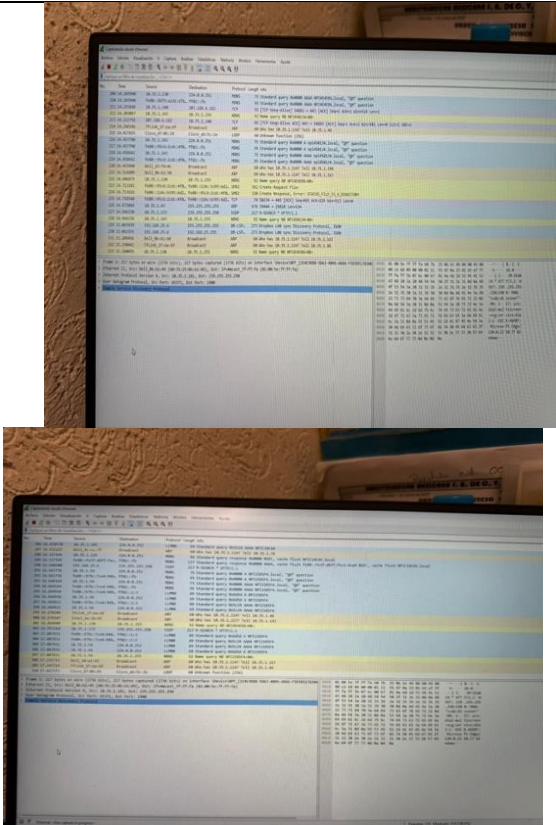
- **Conexión buena:** la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad,
- **Conexión estable:** la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo,
- **Conexión intermitente:** la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella, **Mala conexión:** el servicio de Internet tiene muchas fallas y funciona en pocos equipos, Sin conexión: no existe servicio de Internet.

Esto con el objetivo de evaluar la **conectividad de la Red** que se encuentra en el activo.

Tabla 46. Desarrollo de prueba de conectividad de la red (Auxiliar de soporte 3).

Desarrollo de Prueba de Conectividad de la Red (Auxiliar de soporte 3)	
Objetivo de la prueba	Evaluar la capacidad de los dispositivos de red para establecer y mantener conexiones confiables y seguras dentro del entorno
Descripción de la prueba y Valor esperado	1. Instalar y ejecutar Wireshark en los equipos de cómputo 2. Obtener un escaneo de la señal de WiFi / ETHERNET del equipo del personal del departamento de sistemas.
Técnica	Análisis de resultados de los datos en Wireshark
Herramientas Requeridas	Equipo de computo Wireshark Dispositivo móvil con acamara
Proceso de medición	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad Conexión estable: la señal del Internet es estable y da cobertura a la mayoría los equipos de cómputo Conexión intermitente: la señal de Internet no es estable, solo algunos equipos de cómputo cuentan con ella Mala conexión: el servicio de Internet tiene muchas fallas y funciona en pocos equipos Sin conexión: no existe servicio de Internet

Tabla 46 (continuación). Desarrollo de prueba de conectividad de la red (Auxiliar de soporte 3)

Desarrollo de Prueba de Conectividad de la Red (Auxiliar de soporte 3)	
Criterios de Terminación / Valor obtenido	Conexión buena: la señal del Internet es estable y da cobertura a todos los equipos de cómputo sin variación en su velocidad
Interpretación de resultados	
Recomendaciones	1. Revisar el cable ethernet por lo menos cada 15 días para el asegurar que se encuentre en óptimas condiciones y no haya intermitencia o desconexión.

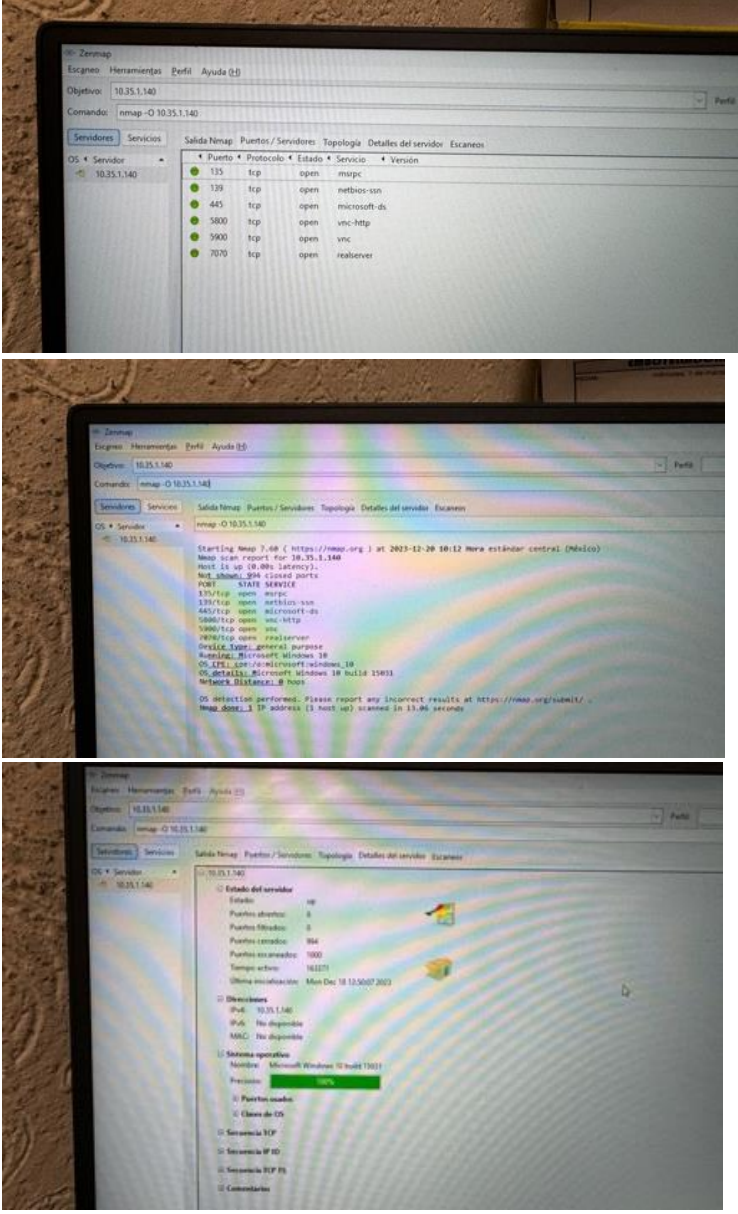
El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 47. Prueba de seguridad de los puertos), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Puertos seguros:** se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados,
- **Puertos cerrados:** se mantienen cerrados los puertos inactivos,
- **Puertos inseguros:** no cuenta con seguridad y se encuentran los puertos activos por default.

Esto con el objetivo de evaluar la **Seguridad de los Puertos** que se encuentra en el activo.

Tabla 47. Desarrollo de prueba de seguridad de los puertos con NMAP (Auxiliar de soporte 3).

Desarrollo de Prueba de Seguridad de los Puertos con NMAP (Auxiliar de soporte 3).	
Objetivo de la prueba	Evaluar la seguridad de los sistemas y redes identificando los puertos abiertos y servicios expuestos
Descripción de la prueba y Valor esperado	1. Instalar y ejecutar Nmap en los equipos de cómputo 2. Obtener un escaneo de los puertos del equipo de computo
Técnica	Análisis de la información sobre los puertos
Herramientas Requeridas	Nmap Equipo de computo Dispositivo móvil con cámara
Proceso de medición	Puertos seguros: se tiene un control y seguridad de los puertos que se utilizan y los que no se encuentran cerrados Puertos cerrados: se mantienen cerrados los puertos inactivos Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Criterios de Terminación / Valor obtenido	Puertos inseguros: no cuenta con seguridad y se encuentran los puertos activos por default
Interpretación de resultados	Con el escaneo nos muestra información sobre los puertos que están habilitados en el pc, son los puertos que vienen por default. De igual manera nos muestra los dispositivos que se encuentran conectados en dicha red dándonos una idea de cómo detectar actividad sospechosa.

	
Recomendaciones	De acuerdo con la sección 11.4. Protección del puerto de diagnóstico y configuración remoto: “Los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad comercial, deberían ser desactivados o removidos”. 1. Realizar un procedimiento de soporte para asegurar que los puertos de diagnóstico y configuración sólo sean accesibles entre el gerente del servicio de cómputo y el personal de soporte de hardware/software que requiere acceso Considerando el punto 10.8.1 de la ISO 17799, se recomienda, mantener inhabilitados los puertos cuando no estén en uso.

El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 48. Prueba de instalación de software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

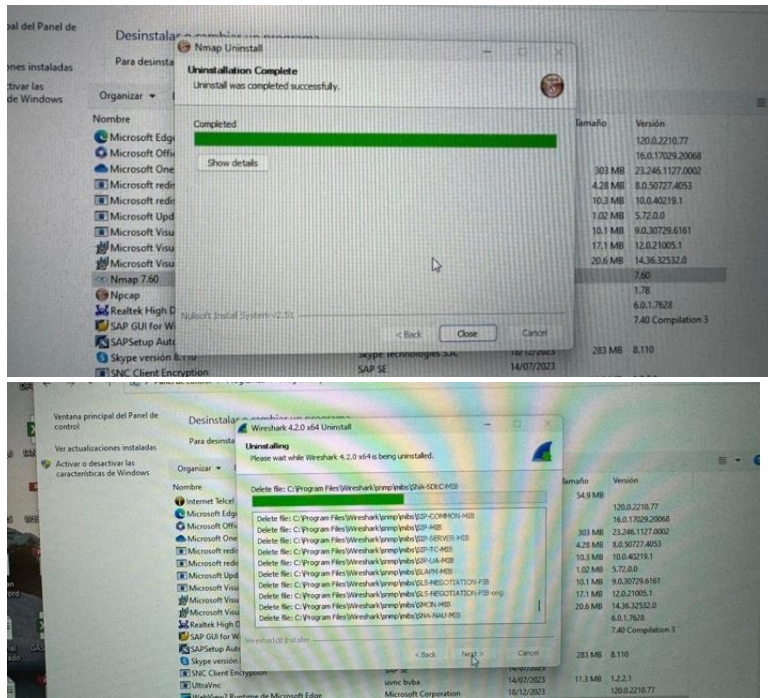
- **Funciona excelente:** La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.
- **Funciona muy bien:** En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados.
- **Funciona bien:** La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas.
- **Funciona suficiente:** La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto. Se requiere una mayor atención para garantizar que solo se instalen softwares autorizados y que estén plenamente funcionales.
- **Deficiente:** La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino.

Esto con el objetivo de evaluar la **Instalación de Software** en el activo.

Tabla 48. Desarrollo de prueba de instalación de software (Auxiliar de soporte 3)

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 3)	
Objetivo de la prueba	Observar y analizar el proceso de instalación de cualquier software en los equipos de cómputo del laboratorio de cisco para verificar su seguridad y facilidad en la instalación.
Descripción de la prueba y Valor esperado	La realización de esta prueba se ejecuta para comprobar y analizar el procedimiento de instalación de softwares en los equipos de cómputo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la Instalación de algún software en cualquier equipo de cómputo
Herramientas Requeridas	Memoria USB, laptop y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino. Funciona muy bien: En general, la instalación de software se realiza de manera eficiente y adecuada. Se siguen los procedimientos recomendados y se verifica que los softwares estén funcionando correctamente después de la instalación. Existe un registro de los softwares instalados, aunque puede haber algunas inconsistencias menores. Se toman medidas para garantizar que solo se instalen softwares autorizados. Funciona bien: La instalación de software cumple con los requisitos básicos. Se siguen los procedimientos establecidos y se instalan los softwares necesarios. Aunque en su mayoría los softwares funcionan correctamente, puede haber algunos casos en los que se presenten problemas menores después de la instalación. Existe un registro de los softwares instalados, aunque puede requerir actualizaciones periódicas. Funciona suficiente: La instalación de software cumple con los requisitos mínimos, pero puede haber áreas que necesiten mejoras. Se siguen los procedimientos básicos de instalación, pero pueden existir problemas ocasionales después de la instalación. El registro de los softwares instalados puede ser limitado o incompleto.

Tabla 48 (continuación). Desarrollo de prueba de instalación de software (Auxiliar de soporte 3)

Desarrollo de Prueba de Instalación de Software (Auxiliar de soporte 3)	
	Deficiente: La instalación de software presenta deficiencias graves. Los procedimientos de instalación no se siguen adecuadamente, lo que resulta en softwares mal instalados o que no funcionan correctamente. No se lleva un registro de los softwares instalados o el registro está desactualizado. No se implementan medidas de seguridad adecuadas para evitar la instalación de software no autorizado o potencialmente dañino
Criterios de Terminación / Valor obtenido	Funciona excelente: La instalación de software se realiza de manera impecable. Se siguen los procedimientos estándar y las mejores prácticas de instalación. Todos los softwares se instalan correctamente y están plenamente funcionales. Se lleva un registro actualizado de los softwares instalados y se implementan medidas de seguridad para evitar la instalación de software no autorizado o potencialmente dañino.
Interpretación de resultados	El proceso de instalación se muestra de manera correcta siguiendo el procedimiento adecuado, sin interrupciones ni contratiempos. 
Recomendaciones	1. Antes de proceder con la instalación, revisar los requisitos del sistema especificados por el fabricante del software y verificar que el equipo cumpla con los

	requisitos mínimos de hardware, sistema operativo y otros componentes necesarios. 2. Descargar el software únicamente de fuentes confiables y oficiales. Evitar sitios web no verificados o descargas de dudosa procedencia, ya que pueden contener versiones modificadas, malware u otros problemas de seguridad. 3. Leer atentamente las instrucciones de instalación proporcionadas por el desarrollador del software y seguir los pasos de instalación recomendados.
--	--

El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 49. Prueba de licencias de software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

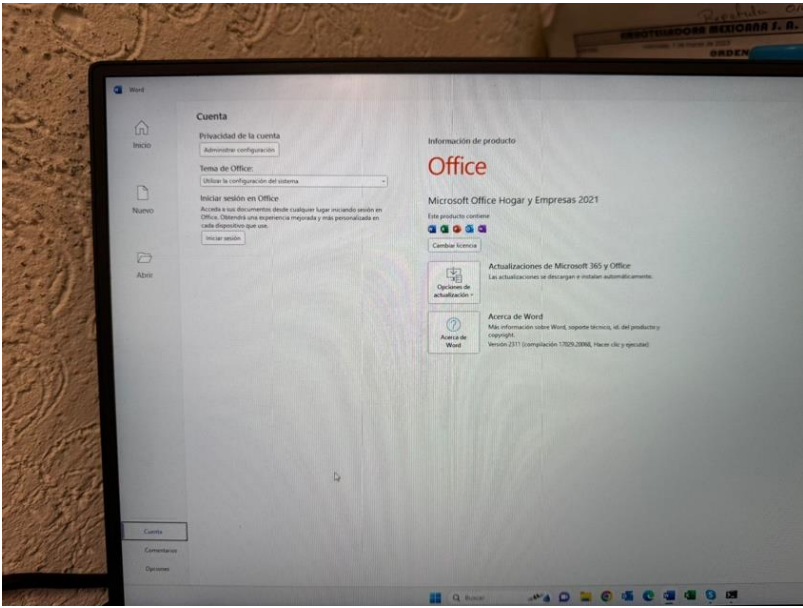
- **Funciona excelente:** Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna.
- **Funciona muy bien:** En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas.
- **Funciona bien:** Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias.
- **Funciona suficiente:** Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas.
- **Deficiente:** El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Esto con el objetivo de evaluar el estado de las **Licencias de Software** que se encuentra en el activo.

Tabla 49. Prueba de licencias de software. Auxiliar 3.

Desarrollo de Prueba de Licencias de Software (Auxiliar de mantenimiento 3)	
Objetivo de la prueba	Observar que la instalación de los softwares en el equipo de cómputo y los softwares ya instalados cuenten con la licencia correspondiente para su uso adecuado.
Descripción de la prueba y Valor esperado	La prueba se realiza para verificar que cada uno de los softwares instalados en el equipo de cómputo cuenten con sus respectivas licencias de uso.
Técnica	1. Ingresar al departamento de sistemas 2. Buscar en la configuración de los softwares la licencia de estos y verificar que dichas licencias se encuentren activas.
Herramientas Requeridas	Equipo de cómputo y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna. Funciona muy bien: En general, las licencias de software se adquieren y gestionan de manera adecuada. Existe un proceso establecido para la adquisición y activación de las licencias, y se mantiene un registro actualizado de las mismas. Funciona bien: Las licencias de software se adquieren y gestionan cumpliendo con los requisitos básicos. Existe un proceso establecido para la adquisición y activación de licencias, y se realiza un seguimiento razonable de las mismas. Sin embargo, puede haber algunas áreas de mejora, como la falta de un registro completo o actualizado de las licencias. Funciona suficiente: Las licencias de software cumplen con los requisitos mínimos establecidos, pero existen algunas deficiencias significativas. Puede haber falta de documentación adecuada, como la ausencia de registros o falta de información detallada sobre las licencias adquiridas. Deficiente: El cumplimiento de las licencias de software presenta deficiencias graves. No se adquieren ni gestionan las licencias de manera adecuada. Puede haber un uso generalizado de software no autorizado o licencias caducadas. No se mantiene un registro adecuado de las licencias adquiridas.

Tabla 49 (continuación). Prueba de licencias de software (Auxiliar de mantenimiento 3)

Desarrollo de Prueba de Licencias de Software (Auxiliar de mantenimiento 3)	
Criterios de Terminación / Valor obtenido	Funciona excelente: Todas las licencias de software se encuentran correctamente adquiridas, activadas y documentadas. Se realiza un seguimiento riguroso de las licencias y se cuenta con un sistema eficiente para gestionar y renovar las licencias de manera oportuna.
Interpretación de resultados	Se observa que el software más utilizado por el personal (Microsoft Word, Excel y Power Point) cuenta con la licencia activa y el usuario la utiliza de esta manera, contando con todas las funciones que este proporciona. 
Recomendaciones	De acuerdo con la sección 15.1.2. Derechos de propiedad intelectual (IPR) de la norma ISO 17799, se recomienda: 1. “Mantener prueba y evidencia de la propiedad de las licencias” 2. “Llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia” Evitar el uso de software pirata o copias no autorizadas, ya que esto puede violar los derechos de autor y generar consecuencias legales.

El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 50. Prueba de seguridad de software), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura.
- **Funciona muy bien:** En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones.
- **Funciona bien:** El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general.
- **Funciona suficiente:** El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente.
- **Deficiente:** El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.

Esto con el objetivo de evaluar la **Seguridad de Software** que se encuentra en el activo.

Tabla 50. Desarrollo de prueba de seguridad del software (Auxiliar de soporte 3)

Desarrollo de Prueba de Seguridad del Software (Auxiliar de soporte 3)	
Objetivo de la prueba	Analizar y comprobar la seguridad del software en los equipos de cómputo para verificar que se cuente con autenticación y protección de datos.
Descripción de la prueba y Valor esperado	La realización de esta prueba es para verificar que todos los equipos de cómputo de laboratorio cisco cuenten con la seguridad de los softwares deseada y así evitar daños al equipo.
Técnica	1. Ingresar al departamento de sistemas 2. Analizar la seguridad del software en los equipos de cómputo
Herramientas Requeridas	Equipos de cómputo, memoria USB y dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: El software cumple con los más altos estándares de seguridad. Se han implementado medidas de seguridad robustas en todas las capas del software, desde el diseño y desarrollo hasta el despliegue y operación. Se han identificado y mitigado proactivamente las vulnerabilidades conocidas, y se siguen las mejores prácticas de codificación segura. Funciona muy bien: En general, el software cuenta con una sólida postura de seguridad. Se han implementado medidas efectivas de seguridad en la mayoría de las áreas críticas del software. Las vulnerabilidades conocidas se abordan de manera adecuada, y se sigue un enfoque de seguridad en el desarrollo y en las operaciones. Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general. Funciona suficiente: El software cumple con los requisitos mínimos de seguridad. Se han implementado algunas medidas básicas de seguridad, pero pueden existir deficiencias significativas. Puede haber vulnerabilidades conocidas que aún no se han abordado adecuadamente. Deficiente: El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el

	software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.
Criterios de Terminación / Valor obtenido	Funciona bien: El software cumple con los requisitos básicos de seguridad. Se han implementado medidas estándar de seguridad y se abordan las vulnerabilidades conocidas de manera adecuada. Si bien pueden existir algunas áreas de mejora, se siguen buenas prácticas de seguridad en general
Interpretación de resultados	Se observó que cuenta con la protección de windows defender, básica protección contra amenazas, además de contar con un antivirus extra SYMANTEC.
Recomendaciones	1. Implementar mecanismos de autenticación y autorización robustos para controlar el acceso al software y a los datos sensibles. 2. Asignar los permisos de acceso adecuados para cada usuario y evita el uso de privilegios excesivos. 3. Adquirir un medio de protección adicional.

El equipo del auxiliar de soporte y mantenimiento 3 (véase tabla 51. Prueba de autenticación), se analizó utilizando la técnica de Observación, se utilizó un dispositivo móvil con cámara para fotografiar el equipo y se tomaron en consideración ciertos criterios para determinar el valor obtenido conforme a los siguientes procesos de medición:

- **Funciona excelente:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
- **Funciona muy bien:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico
- **Funciona Regular:** La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.

Esto con el objetivo de evaluar el tipo de **Autenticación** que se encuentra en el activo.

Tabla 51. Desarrollo de prueba de autenticación (Auxiliar de soporte 3)

Desarrollo de Prueba de Autenticación (Auxiliar de soporte 3)	
Objetivo de la prueba	El objetivo de la prueba de autenticación es verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso en particular. Esta prueba tiene como objetivo principal garantizar la seguridad y protección de los datos y recursos al asegurarse de que solo usuarios autorizados puedan acceder a ellos. Algunos objetivos específicos de la prueba de autenticación incluyen:
Descripción de la prueba y Valor esperado	La prueba de autenticación es un proceso mediante el cual se evalúa la efectividad de los mecanismos utilizados para verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o recurso. Esta prueba busca detectar posibles debilidades en los métodos de autenticación utilizados y garantizar que solo los usuarios autorizados puedan acceder a la información y los recursos protegidos.
Técnica	Es utilizada y consiste en que el usuario proporcione una contraseña secreta que solo él o ella debe conocer. La contraseña se compara con la almacenada previamente en el sistema para verificar la identidad del usuario.
Herramientas Requeridas	Equipo de cómputo, memoria USB, dispositivo móvil con cámara.
Proceso de medición	Funciona excelente: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus. Funciona muy bien: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus básico Funciona Regular: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, y los equipos no están protegidos con antivirus.
Criterios de Terminación / Valor obtenido	Funciona excelente: La autenticación de cada equipo es segura y que cada usuario cuente con una cuenta diferente, que los equipos estén protegidos con antivirus.
Consideraciones especiales	Los equipos deberían estar protegidos con contraseñas o algún método de autenticación para proteger la información que contienen.
Interpretación de resultados	Se puede observar que al intentar ingresar al equipo del usuario pide una contraseña para verificar la identidad del personal.

	
Recomendaciones	En la sección 11.5.3. Sistema de gestión de claves secreta, de la norma ISO 17799, “Las claves secretas son uno de los principales medios para validar la autoridad del usuario para tener acceso a un servicio de cómputo.” Por lo que se recomienda: 1. Utilizar contraseñas de al menos 8 caracteres alfanuméricos y caracteres especiales (\$#%&) 2. No compartir la contraseña con ninguna persona fuera de la autorización.

CAPÍTULO IV

RESULTADOS

Auditoria Informática de la empresa Embotelladora Mexicana S.A de C.V

Informe Final de Auditoria

Objetivo General. Diagnosticar el funcionamiento general y control interno de la seguridad de TI de la empresa Embotelladora Mexicana S.A de C.V

Alances. Evaluar el estado de las instalaciones físicas del departamento de sistemas de la empresa Embotelladora Mexicana S.A de C.V, incluyendo la disponibilidad y calidad de los equipos de cómputo, la conectividad de red y la disposición de mobiliario, así como las medidas de seguridad implementadas, como sistemas de control de acceso, protección contra virus y malware.

La auditoría se llevó a cabo en el departamento de sistemas ubicado en la Embotelladora Mexicana S.A de C.V con el objetivo de realizar un diagnóstico y evaluación integral del estado de las instalaciones físicas y lógicas. El propósito de la auditoría es identificar posibles deficiencias, evaluar el nivel de seguridad implementado y ofrecer recomendaciones para mejorar la protección de los activos y datos en el laboratorio.

Para llevar a cabo la evaluación, se utilizó una métrica que clasifica el estado de las instalaciones y medidas de seguridad en cuatro niveles: Excelente, Muy bien, Bien, Suficiente y Deficiente. Cada nivel refleja el grado de cumplimiento de los estándares y buenas prácticas de seguridad establecidos.

- Excelente: Instalaciones y medidas de seguridad son óptimas, se han implementado de manera adecuada y se encuentran en pleno funcionamiento. No se identifican deficiencias significativas y se cumplen todos los requisitos de seguridad.
- Muy bien: Las instalaciones y medidas de seguridad están en buen estado y se han implementado correctamente. Se han identificado solo algunas deficiencias menores que no representan un riesgo significativo para la seguridad.
- Bien: Aunque las instalaciones y medidas de seguridad cumplen con los requisitos básicos, se han detectado algunas deficiencias que requieren atención y mejoras. Estas deficiencias pueden tener un impacto moderado en la seguridad.
- Suficiente: Si bien se han implementado algunas medidas de seguridad, se han identificado deficiencias significativas que representan un riesgo para la seguridad de las instalaciones y los activos. Se requieren mejoras sustanciales para garantizar una protección adecuada.
- Deficiente: Se han identificado múltiples deficiencias graves que comprometen la seguridad de las instalaciones y los activos. Se requiere una intervención inmediata para corregir estas deficiencias y garantizar un entorno seguro.

Mediante la métrica de evaluación mencionada anteriormente, se podrá determinar el nivel de seguridad actual del departamento de sistemas y proporcionar recomendaciones específicas para mejorar el estado de las instalaciones físicas y lógicas, así como fortalecer las medidas de seguridad implementadas.

HALLAZGOS DE SEGURIDAD FÍSICA

Hallazgo 1. Acceso físico

Con el análisis de las respuestas que se obtuvieron en el cuestionario, se determinó que el departamento cuenta con información donde muestra el nombre de las personas que tienen acceso físico, con datos como el día, hora, nombre completo y firma, sin embargo, este registro no es únicamente del departamento, si no de la empresa completa.

1. Riesgos/efectos probables.

- a) Sin un sistema de autenticación, cualquier persona puede ingresar al departamento sin restricciones. Esto aumenta el riesgo de que individuos no autorizados accedan a equipos, datos sensibles u otros recursos del laboratorio.
- b) La ausencia de seguridad física puede permitir el robo de equipos o el vandalismo de estos. Esto no solo implica la pérdida de recursos valiosos, sino también la interrupción del trabajo y la pérdida de datos importantes.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

- 3. **Bien:** El laboratorio si cuenta con información sobre las personas que están designadas a ingresar y se les pide autorización a los trabajadores del departamento para permitir el ingreso de los visitantes.

4. Recomendaciones

- a) Establecer supervisión minuciosa o incluso agregar cámaras de seguridad.
- b) Contar con un algún medio de autenticación que sea solo para el ingreso al departamento de sistemas.

Hallazgo 2. Uso de aire acondicionado

Se observó que el departamento cuenta con 2 aires acondicionados en solo 2 de 4 oficinas (véase tabla 14. Desarrollo de prueba de uso de aire acondicionado). El aire abarca gran cantidad de la oficina, sin embargo, en las dos oficinas restantes no existe aire acondicionado o ventiladores.

1. Riesgos/efectos probables.

- a) Sobrecalentamiento de equipos: Los equipos informáticos generan calor cuando están en funcionamiento. Si no se proporciona una ventilación adecuada, el calor puede acumularse en la oficina, lo que aumenta el riesgo de sobrecalentamiento de los equipos y esta situación puede dañar los componentes internos de las computadoras, reducir su vida útil y provocar fallas frecuentes.
- b) Disminución del rendimiento: Las altas temperaturas en la oficina pueden afectar el rendimiento de los equipos informáticos. Los componentes internos pueden funcionar a temperaturas subóptimas, lo que puede ralentizar el procesamiento de datos y causar errores en las operaciones.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Bien: El departamento cuenta con al menos de 2 a 4 aires acondicionados, los cuales son grandes y el rango de aire abarca gran parte de la oficina, están semilimpios, pero permite el flujo de aire limpio en su totalidad y se encuentran en buen estado generalmente.

3. Recomendaciones

- a) Los aires acondicionados deben estar limpios, libres de polvo o pelusa que pueda dañar cualquier equipo dentro del laboratorio.
- b) Los aires acondicionados deben estar en excelentes condiciones y enfocarse más a los equipos de cómputo para mantener un equilibrio de temperaturas dentro de las instalaciones causadas por dichos equipos.

Hallazgo 3. LAPTOPS

Se pudo observar y analizar que la mayoría de las computadoras portátiles se encuentran en buen estado, a excepción de algunas que presentan daños externos atribuibles a un uso muy frecuente (véase tabla. Desarrollo de prueba laptop encargado de FROG, tabla. Desarrollo de prueba de laptop de encargada de departamento, tabla. Desarrollo de prueba de laptop de encargada de soporte y mantenimiento 3, tabla. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 4 y tabla. Desarrollo de prueba de laptop de auxiliar de soporte y mantenimiento 5).

1. Riesgos/efectos probables

- a) **Deterioro funcional:** Los daños externos pueden afectar el funcionamiento interno de la laptop, causando problemas en componentes esenciales como la pantalla, el teclado, los puertos USB, etc.
- b) **Impacto en la productividad:** Una laptop dañada externamente puede dificultar o imposibilitar su uso normal, lo que afectaría la productividad del usuario.
- c) **Estética y profesionalismo:** Una laptop dañada externamente puede afectar la percepción estética y profesional del usuario, especialmente en entornos laborales o académicos.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Bien: Indica un nivel aceptable de cumplimiento de los estándares de seguridad. Aunque las instalaciones y medidas de seguridad cumplen con los requisitos básicos, se han detectado algunas deficiencias que requieren atención y mejoras. Estas deficiencias pueden tener un impacto moderado en la seguridad.

3. Recomendaciones

- a) **Mantenimiento regular:** Realizar revisiones periódicas para asegurar que todos los componentes estén en buen estado. Limpiar el polvo y la suciedad de los puertos y ventiladores, y considerando la instalación de protectores de pantalla y teclado para evitar caída de teclas y derrames.
- b) **Superficie segura:** Colocar la laptop sobre superficies estables y planas. Evitar dejarla en bordes o lugares elevados donde pueda caerse fácilmente.
- c) **Reemplazo:** Si el equipo se encuentra bastante dañado, lo ideal será reemplazarlo.

Hallazgo 4. CPU

Se pudo constatar y analizar que la mayoría de las unidades centrales de procesamiento (CPU) se encuentran en condiciones óptimas, dejando de lado la suciedad y la falta de mantenimiento que presentan algunos de estos dispositivos (véase tabla. Desarrollo de prueba de CPU del encargado de soporte y mantenimiento 1, tabla. Desarrollo prueba de CPU de becarios, tabla. Desarrollo de prueba de CPU de encargada de soporte y mantenimiento 2 y tabla. Desarrollo de prueba de CPU de analista de datos SAP).

1. Riesgos / efectos probables:

- a) **Sobrecalentamiento:** La acumulación de suciedad en las CPU puede obstruir los sistemas de refrigeración, llevando a un aumento de la temperatura y potencial sobrecalentamiento del dispositivo.
- b) **Daño a componentes:** La suciedad puede causar daño físico a los componentes internos de la CPU, como ventiladores, disipadores de calor y placas de circuito, afectando su funcionalidad y durabilidad.
- c) **Fallas del sistema:** La acumulación de suciedad puede provocar fallos inesperados del sistema, lo que podría resultar en pérdida de datos o interrupción de las operaciones normales.
- d) **Problemas de conectividad:** La suciedad en los puertos y conectores puede interferir con la conectividad de periféricos y dispositivos externos, generando dificultades en la transferencia de datos.

2. Índice / grado de importancia de acuerdo con la métrica establecida:

Bien: Indica un nivel aceptable de cumplimiento de los estándares de seguridad. Aunque las instalaciones y medidas de seguridad cumplen con los requisitos básicos, se han detectado algunas deficiencias que requieren atención y mejoras. Estas deficiencias pueden tener un impacto moderado en la seguridad.

3. Recomendaciones:

- a) **Mantenimiento regular:** Implementar limpieza y mantenimiento por lo menos 1 vez por mes, para eliminar la acumulación de polvo y suciedad en la CPU y sus componentes.
- b) **Ubicación adecuada:** Colocar el CPU en un lugar limpio y bien ventilado para reducir la exposición a partículas de polvo y mantener una temperatura ambiente adecuada.
- c) **Espacios elevados:** Evita colocar el CPU directamente sobre el suelo para reducir la exposición a partículas de polvo y facilitar la limpieza de la zona de al rededor.

Hallazgo 5. Inventario

Se observó que el departamento de sistemas no cuenta con un inventario detallado y actualizado de la planta Tultitlán, cedis de la zona Metropolitana, zona Hidalgo y Morelos.

1. Riesgos/efectos probables.

- a) Pérdida de activos: Sin un inventario adecuado, es más difícil realizar un seguimiento de los equipos y recursos de la empresa. Esto aumenta el riesgo de pérdida de activos, ya sea por robo, extravío o mal uso. Sin un registro de los activos existentes, también puede ser más difícil identificar y recuperar los elementos perdidos.
- b) Dificultad para la conservación: Un inventario de activos es fundamental para realizar un mantenimiento adecuado de los equipos. Sin una lista actualizada de los activos y su estado, es difícil programar y realizar tareas de mantenimiento preventivo, como actualizaciones de software, reemplazo de componentes o limpieza.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Deficiente: El departamento no cuenta con algún inventario de activos actualizado.

3. Recomendaciones

- a) El departamento debería tener un control de inventario de activos internos con especificaciones de cada uno de los activos como: algún 'ID', nombre del activo, cantidad, modelo, marca, capacidad y que sea supervisado por lo menos 1 vez por mes por el encargado.
- b) Con un inventario actualizado, es más fácil programar y realizar tareas de mantenimiento preventivo. Puedes identificar rápidamente los equipos que necesitan actualizaciones de software, reemplazo de componentes o limpieza.

Hallazgo 6. Nobreak

Durante la auditoría, se identificaron varios problemas relacionados con el uso y mantenimiento de los nobreak.

1. Riesgos/efectos probables.

- a) Estos dispositivos son cruciales para mantener la continuidad operativa durante interrupciones del suministro eléctrico. Los problemas detectados podrían afectar la capacidad de la empresa para responder adecuadamente a cortes de energía, poniendo en riesgo la integridad de los sistemas y la continuidad de las operaciones.
- b) Las interrupciones eléctricas pueden causar daños físicos a los componentes electrónicos debido a picos de voltaje o apagados abruptos, lo que requerirá reparaciones costosas o reemplazos, aumentando los costos operativos.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Deficiente: El departamento no cuenta con nobreak en buen estado

3. Recomendaciones (2 mínimo)

- a) Implementar un programa de mantenimiento regular, incluyendo revisiones trimestrales y pruebas de carga para asegurar el buen funcionamiento
- b) Realizar análisis de carga para los nobreak y si es necesario, reemplazarlos por unidades de mayor capacidad o redistribuir la carga entre varios dispositivos para asegurar una protección adecuada.
- c) Proporcionar capacitación específica al personal sobre el mantenimiento, pruebas y manejo de nobreak, incluyendo formación sobre los procedimientos de emergencia en caso de fallo del dispositivo.

HALLAZGOS DE SEGURIDAD LÓGICA

Hallazgo 1. Licencias del software

Se comprobó que solo un equipo de cómputo del departamento de sistemas no cuenta con licencia de office activa para su uso

1. Riesgos/efectos probables.

- a) Al utilizar software sin las licencias correspondientes, se está infringiendo la propiedad intelectual del desarrollador del software. Esto puede llevar a demandas legales, multas significativas y dañar la reputación. Además, el uso de software no autorizado puede generar incompatibilidades, falta de actualizaciones y soporte, así como un mayor riesgo de exposición a malware y vulnerabilidades de seguridad, lo que pone en peligro la integridad y confidencialidad de los datos.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Muy bien: El que solo un equipo de cómputo no cuente con licencia de office activa no representa riesgos significativos para la seguridad.

3. Recomendaciones

- a) Mantener actualizado el inventario con el que ya cuenta el departamento, que este sea detallado y centralizado de todas las licencias de software utilizadas. Esto incluye registrar la información relevante de cada licencia, como el nombre del software, número de licencia, fecha de adquisición, proveedor, términos de uso y fechas de renovación. Esto facilitará la gestión y seguimiento de las licencias, evitando la pérdida de licencias o el uso no autorizado de software.
- b) Establecer un sistema de seguimiento para recordar las fechas de renovación de licencias y tomar las acciones necesarias para renovarlas a tiempo. Evitar el uso de licencias caducadas o vencidas.

Hallazgo 2. Seguridad del software

Se observó que no se cuenta con las actualizaciones necesarias para la protección contra los virus y amenazas.

1. Riesgos/efectos probables.

El riesgo de no contar con seguridad de software es la exposición a amenazas cibernéticas y ataques maliciosos. Al no implementar medidas de seguridad adecuadas, el equipo y los datos almacenados en él están más vulnerables a ser comprometidos. Podría existir una infección por malware, pérdida de datos, acceso no autorizado, etc.

2. Índice/grado de importancia de acuerdo con la métrica establecida.

Deficiente: El software presenta deficiencias graves en términos de seguridad. Se han implementado medidas de seguridad insuficientes o inadecuadas, lo que expone el software a riesgos significativos. Pueden existir numerosas vulnerabilidades conocidas sin resolver.

3. Recomendaciones

- 1) Mantener el software del equipo de cómputo actualizado con las últimas versiones y parches de seguridad. Esto incluye el sistema operativo, programas y aplicaciones utilizadas. Las actualizaciones de software suelen incluir correcciones de vulnerabilidades y mejoras de seguridad, por lo que es importante instalarlas de manera regular y oportuna.
- 2) Implementar soluciones de seguridad confiables en el equipo de cómputo, como software antivirus, firewalls y herramientas de detección de malware. Asegurarse de utilizar soluciones de seguridad de reputación reconocida y mantenerlas actualizadas regularmente. Estas soluciones ayudan a proteger el equipo contra amenazas cibernéticas, detectar y eliminar malware, y proporcionar una capa adicional de seguridad para bloquear ataques maliciosos.

Al finalizar con la identificación de hallazgos, se puede concluir que la Embotelladora Mexicana S.A de C.V se encuentran bastante bien respecto a la seguridad lógica, sin embargo, la seguridad física es donde se ven ciertas deficiencias. La atención inmediata a estos hallazgos es esencial para fortalecer la seguridad física y la gestión de activos en la empresa. La implementación de medidas correctivas específicas, como mejoras en los controles de acceso, programas de mantenimiento de activos y gestión rigurosa de licencias de software, será crucial para mitigar riesgos, garantizar la conformidad y promover una infraestructura segura y eficiente.

Tabla 52. Lista de recomendaciones/contramedidas de acuerdo con la norma ISO 17799

LISTA DE RECOMENDACIONES / CONTRAMEDIDAS DE ACUERDO CON LA NORMA ISO 17799
1. Mantener los sistemas actualizados con los últimos parches y actualizaciones de seguridad
2. Implementar soluciones de seguridad actualizadas y realizar análisis periódicos de virus y actualizaciones automáticas
3. Educar y concienciar a los usuarios sobre las mejores prácticas de seguridad, como evitar descargar archivos de fuentes no confiables y utilizar políticas de filtrado de contenido web
4. Realizar evaluaciones periódicas de riesgos para identificar y evaluar las amenazas y vulnerabilidades asociadas a la seguridad de la información en el departamento de TI y tomar medidas para mitigar los riesgos identificados
5. Implementar políticas que prohíban el uso de software pirateado o no licenciado y realizar auditorías periódicas para asegurar el cumplimiento de las licencias de software
6. Implementar soluciones de seguridad web que realicen análisis y filtrado de contenido malicioso, como bloqueo de sitios web peligrosos o sospechosos
7. Establecer políticas de respaldo regulares y realizar pruebas periódicas de restauración de datos para asegurar su integridad y disponibilidad en caso de infección o pérdida de datos
8. Implementar controles de acceso físico y lógico, como autenticación multifactor, gestión de usuarios y privilegios, y políticas basadas en roles
9. Implementar sistemas de gestión de registros de eventos que registren y monitoreen las actividades de los sistemas para detectar actividades sospechosas o no autorizadas
10. Establecer políticas y procedimientos para identificar, manejar y responder a incidentes de seguridad, incluyendo infecciones de virus, y tener un equipo o persona responsable de la gestión de incidentes
11. Educar a los usuarios sobre la importancia de descargar archivos únicamente de fuentes confiables y utilizar soluciones de seguridad web que bloqueen el acceso a sitios web maliciosos
12. Establecer políticas que prohíban o restrinjan el uso de dispositivos externos no confiables y realizar escaneos antivirus antes de permitir su uso en los sistemas del departamento
13. Implementar políticas que prohíban el uso de software no autorizado o pirateado y realizar auditorías periódicas para garantizar el cumplimiento de las licencias de software
14. Establecer políticas que requieran el uso de software con soporte activo y realizar auditorías periódicas para garantizar que se estén utilizando las versiones actualizadas de los programas

15. Establecer políticas y procedimientos de configuración segura, realizar auditorías periódicas de configuración y aplicar controles de cambio para prevenir configuraciones incorrectas o inseguras

16. Implementar políticas y procedimientos para realizar copias de seguridad periódicas de las configuraciones de los dispositivos de red y mantener una copia de seguridad fuera del sitio para facilitar la recuperación en caso de infección o pérdida de datos

EVIDENCIAS

Hallazgo 5. Inventario

El departamento de sistemas de la empresa Embotelladora Mexicana S.A de C.V no contaba con un inventario actualizado de los equipos (monitor, cpu) que son entregados a los usuarios, ni sobre los servicios que deben contar, como las licencias office.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	ID	VERIFICAR	USUARIO	MODELO	SERIE	MONITOR	MODELO2	WINDOWS	WIN KEY	OFFICE	OFFICE KEY	PROCESADOR	VELO		
27	EMF026		DAMARIS JUAREZ	OPTIPLEX 3080	9Y2R2C3	HP	ELITE DISPLAY E201	WIN 10 PRO	DIGITAL	H & B 2019	paola.castrejon@agamexico.com.mx	CORE I5-10500	3.10		
28	EMF027		VACANTE 2	OPTIPLEX 3080	9Y1T2C3	SAMSUNG	953SNPLUS	WIN 10 PRO	DIGITAL	H & B 2019	paola.castrejon@agamexico.com.mx	CORE I5-10500	3.10		
29	EMF028		NORMA MENDOZA	OPTIPLEX 3080	9Y0R2C3	HP	ELITE DISPLAY E201	WIN 10 PRO	DIGITAL	H & B 2019	paola.castrejon@agamexico.com.mx	CORE I5-10500	3.10		
30	EMF029		RETIRADA	OPTIPLEX 3080	7C9FIB3	HP	L2208	WIN 10 PRO	DIGITAL	H & B 2019	licencioffice03@agamexico.com.mx	CORE I5-10500	3.10		
31	MPT005		RETIRADA	SASCOO	MJ0A221E	DELL	E2417H	WIN 10 PRO	DIGITAL	H & B 2019	lic_18m@hotmail.com	CORE I7-870T	2.4		
32	MPT006		RETIRADA	VOSTRO 3470	J89GR2	DELL	E1916HW	WIN 10 PRO	DIGITAL	H & B 2019	lic_5m@hotmail.com	CORE I5-8400	2.80		
33	MPT007		RETIRADA	OPTIPLEX 3070	55G53R3	DELL	E1920H	WIN 10 PRO	DIGITAL	H & B 2019	licaga204t@hotmail.com	CORE I5-9500	3.3		
41	MPT010		ANA GONZALEZ	OPTIPLEX 3080	5CFXIB3	HP	ELITE DISPLAY E201	WIN 10 PRO	DIGITAL	H & B 2019	licencioffice03@agamexico.com.mx	CORE I5-10500	3.10		
42	MPT012		EDUARDO NEVAREZ	OPTIPLEX 3040	84Q9HB2	DELL	P2014HT	WIN 10 PRO	DIGITAL	H & B 2021	lic_32m@hotmail.com	CORE I5-6500	2.5		
43	MPT015		JOSE LUIS MENDOZA	L15		N/A	N/A	WIN 10 PRO	DIGITAL	H & B 2019	lic_83m@hotmail.com	CORE I7-1165G7	2.80		
44	MPT016		GENARO SILVA	LATITUDE 5500	J1KL13	N/A	N/A	WIN 10 PRO	DIGITAL	H & B 2019	licgsilvapetaga@hotmail.com	CORE I7-8665U	1.9		
89	MPT086		VACANTE (DIANA)	OPTIPLEX 3070	6H40522	DELL	E1914HC	WIN 10 PRO	DIGITAL	H & B 2019	lic_may192020@hotmail.com	CORE I5-6500T	2.50		
91	MPT088		JANET REYES	LATITUDE E6440	JVNOM12	N/A	N/A	WIN 10 PRO	DIGITAL	16 PRO	NO REQUIERE	I5			
92	MPT089		GABRIELA ANGELES	LATITUDE E6440	17YRN72	N/A	N/A	WIN 10 PRO	DIGITAL	16 PRO	NO REQUIERE	I5			
93	MPT090		PAMELA ORDUÑO	LATITUDE E7450	2X62J72	N/A	N/A	WIN 10 PRO	DIGITAL	16 PRO	NO REQUIERE	I5			
94	MPT091		RETIRADA	LATITUDE 7480	JMRKZM2	N/A	N/A	WIN 10 PRO	DIGITAL	16 PRO	SIN	I5			
95	MPT092		RETIRADA	LATITUDE 5590	3LXJNV2	N/A	N/A	WIN 10 PRO	DIGITAL	H & B 2019	C7979-NC6VT-WWYFX-K2XTF-QGM	CORE I7-8650U	1.90		
100	MPT098		AMELALI ORTIZ	LATITUDE 7480	HRFTN12	N/A	N/A	WIN 10 PRO	DIGITAL	16 PRO	NO REQUIERE	I5			
104	MPT103		NESTOR ENRIQUEZ	MUONXW7	DELL	E1916HV		WIN 10 PRO	DIGITAL	H & B 2019	lic_65m@hotmail.com	CORE I5-10500	3.10		
105	MPT104		ELIZABETH ESCOBEDO LAP TOP	XPS 15 9560	9VP3BH2	N/A	N/A	WIN 10 PRO	DIGITAL	2013 Pro P11	NO REQUIERE	INTEL CORE I7-7700HQ	2.80		
114	MPT113		ELIZABETH ESCOBEDO	THINKCENTRE M70	MJ04RRV			WIN 10 PRO	DIGITAL	H & B 2019	lic_18m@hotmail.com	CORE I7-10700	2.90		
117	MPT116		RICARDO VILLAMAR	T14	PF3K4KTJ	N/A	N/A	WIN 10 PRO	DIGITAL	H & B 2021	lic_159m@hotmail.com	CORE I7-1165G7	2.80		
132	MPT131		LAURA CRUZ	OPTIPLEX 7010 SFI	8P55G04			WIN 11 PRO	DIGITAL	H & B 2019	lic_5m@hotmail.com	CORE I5-13500	2.50		
139															
140															
			PLANTA TUTILITAN	COCOYOC	TUTILITAN RCO	COORDRATIVO	OBELISCO	ECATEPEC	IXMQUILPAN	AZCAPO RCO	COYOACAN	ERMITA	C ...		
			LISTO MODIFICAR	ELIMINAR											

Figura 3. Evidencia de inventario desactualizado

Al realizar las observaciones a los encargados del departamento de sistemas, se comenzaron con las actualizaciones del inventario por cada bodega con las que cuenta la empresa. Para un inventario más completo, se tomaron los siguientes datos: ID de la bodega, nombre del usuario, área, tipo de máquina (laptop o de escritorio), marca, modelo, número de serie, sistema operativo, licencia office, IP, si cuenta con monitor y nobreak o regulador.

ID	USUARIO	AREA	TIPO	MARCA	MODELO	SERIE	LO	OFFICE	IP	MONITOR	NOBREAK/REGULADOR
1	LAURA CRUZ	CONTABILIDAD	DESK	DELL	VOSTRO 3470	J95GR2	CL	CL	192.168.107.29	DELL	NOBREAK
2	DANIEL VELAZQUEZ	PRODUCCION	DESK	DELL	OPTIPLEX 3080	449VC1	CL	CL	192.168.106.64	DELL	NOBREAK
4	PROYECTO SIMPSON	PRODUCCION	DESK	DELL	OPTIPLEX 3080	CE1TM2	CL	CL	192.168.106.58	HP	SIN
5	JUAN BARNES	PRODUCCION	LAPTOP	LENOVO	20PVA0SLM	PFOKVTX	CL	CL	192.168.106.119	N/A	NOBREAK
6	LUIS DAVID	COORDINADOR DE LINEA	DESK	DELL	OPTIPLEX 3080	448P2C3	CL	CL	192.168.106.128	HP	SIN
7	JOSE HERNANDEZ CRUZ	SUPERVISOR MANT. PREVENTIVO	DESK	DELL	OPTIPLEX 3080	192Q2C3	CL	CL	192.168.106.25	SAMSUNG	SIN
8	ARACELI GASTARDA	SERVICIO MEDICO	DESK	DELL	OPTIPLEX 3080	CPC001	CL	CL	192.168.106.170	DELL	NOBREAK
9	VICTOR GONZALEZ	ALMACEN	DESK	DELL	OPTIPLEX 3080	194K2C3	CL	CL	192.168.106.161	DELL	NOBREAK
10	MAURICIO TREJO	JEFE DE TERRITORIO	LAPTOP	DELL	LATITUDE 7480	17N88H2	CL	CL	192.168.106.4	N/A	SIN
11	MARIA GARDUÑO	VENTAS	DESK	DELL	OPTIPLEX 9020	2MPC352	CL	CL	192.168.106.103	DELL	NOBREAK
12	PEDRO JIMENEZ	VENTAS	DESK	DELL	OPTIPLEX 3080	194P2C3	CL	CL	192.168.106.129	DELL	NOBREAK
13	JOSE EMANUEL GARCIA	TICKETS 3	DESK	DELL	OPTIPLEX 3010	CJ58G1	CL	SN	192.168.106.242	DELL	NOBREAK
14	JOSE EMANUEL GARCIA	TICKETS 1	DESK	DELL	OPTIPLEX 3020	4R02R22	CL	SN	192.168.106.34	DELL	NOBREAK
15	OSCAR TELLEZ	MONITORIO	DESK	DELL	OPTIPLEX 3080	6U22C3	CL	SN	192.168.106.32	DELL	NOBREAK
16	MIGUEL ANGELLOS	MESA DE CONTROL LOGISTICA	LAPTOP	LENOVO	20KX0LUP	PC04X0P8	CL	CL	192.168.107.27	N/A	SIN
17	PAOLA SANDOVAL	MESA DE CONTROL LOGISTICA	LAPTOP	LENOVO	20H55YB00	PC04X0P8	CL	CL	192.168.106.59	N/A	REGULADOR COMPARTIDO
18	REBECA ANDRADE	CARTA PORTE	DESK	DELL	OPTIPLEX 3080	GT0CKL3	CL	CL	192.168.106.92	DELL	NOBREAK
19	YADIRA AYALA	CARTA PORTE	DESK	DELL	OPTIPLEX 3080	8H0JL13	CL	CL	192.168.106.228	DELL	NOBREAK
20	JESUS CRUZ	SUPERVISOR TRAFICO	DESK	DELL	OPTIPLEX 3080	194V2C3	CL	CL	192.168.106.205	DELL	NOBREAK
21	MAGDA ROSAS	ASISTENTE DE DIRECCION AUTOMOTRIZ	DESK	DELL	OPTIPLEX 3080	6G0HWM3	CL	CL	192.168.106.83	DELL	NOBREAK
22	MAYRA	OPERADORA SAP FLEET	DESK	LENOVO	18ANAD0SL	CF2B7H2	CL	CL	192.168.106.251	LENOVO	NOBREAK
23	PABLO VILLALBOS	CONTROL VENCULAR	LAPTOP	DELL	LATITUDE 7480	CF2B7H2	CL	CL	192.168.106.189	N/A	NOBREAK
24	JOEL GONZALEZ	GERENTE DE AUTOMOTRIZ	DESK	DELL	OPTIPLEX 3010	83P8N01	CL	CL	192.168.106.98	DELL	NOBREAK
25	JOEL GONZALEZ	GERENTE DE AUTOMOTRIZ	LAPTOP	LENOVO	20L652V00	6X30V23	CL	CL	192.168.106.19	N/A	NOBREAK
26	ALBERTO SANCHEZ	AUXILIAR DE ALMACEN REFACC.	DESK	DELL	OPTIPLEX 3080	195V2C3	CL	CL	192.168.106.46	DELL	NOBREAK
27	JOSUE CORTEZ	ENCARJADO DE COMBUSTIBLE	DESK	LENOVO	18ACX0T80	8A2708P9	CL	CL	192.168.106.131	LENOVO	NOBREAK
28	FERNANDO MOTA	RECIBIDORES	DESK	DELL	OPTIPLEX 3080	18AM0322	CL	CL	192.168.106.195	HP	NOBREAK
29	TIBERIO MARTINEZ	TRAFICO PET	LAPTOP	LENOVO	20PVA0SLM	PFOKVTX	CL	CL	192.168.106.127	N/A	SIN
30	GUADALUPE VARGAS	COMPRA	LAPTOP	LENOVO	20KX0LUP	PC04X0P8	CL	CL	192.168.106.18	N/A	SIN
31	OSWALDO CASTAÑO	COMPRA	LAPTOP	DELL	LATITUDE 7450	8F0H22	CL	CL	192.168.106.166	N/A	NOBREAK
32	MIGUEL HERNANDEZ	JEFE DE COMPRA	LAPTOP	LENOVO	20L652V00	PC04X0P8	CL	CL	192.168.106.66	N/A	NOBREAK
33	CLAUDIA BARNES	NOMINAS	DESK	DELL	OPTIPLEX 3080	18C0HWM3	CL	CL	192.168.106.118	DELL	REGULADOR
34	JENNIFER ALMARAZ	AUXILIAR DE RH	DESK	DELL	OPTIPLEX 790	8F0H22	CL	CL	192.168.106.118	ACER	NOBREAK
35	DANIA LOPEZ	ENCARJADA DE NOMINA	DESK	DELL	OPTIPLEX 7010	C9K0G22	CL	CL	192.168.106.126	DELL	NOBREAK
36	DIEGO DURAN	PRODUCCION	DESK	DELL	LATITUDE 3420	11BM0K3	CL	CL	192.168.106.126	DELL	NOBREAK
37	ALBA BECERRA MAYEN PAZ	CONTABILIDAD	DESK	DELL	OPTIPLEX 3080	191T2C3	CL	CL	192.168.107.24	DELL	NOBREAK

Figura 4. Inventario actualizado

Hallazgo 5. Nobreak

El departamento de sistemas contaba con algunos nobreak en mal estado, a los cuales no se les realizaba un mantenimiento adecuado para su buen funcionamiento.



Figura 5. Nobreak

Al realizar esta observación, los encargados del departamento comenzaron a realizar pruebas con los nobreak, para revisar su funcionamiento y comenzar a reemplazar los que tuvieran daños mayores por unos nuevos.



Figura 6. Nobreak nuevos

CONCLUSIONES

Conclusión general

Al finalizar la evaluación y análisis de riesgos físicos y lógicos dentro de la auditoría de seguridad de los activos de TI realizada en el departamento de sistemas de la Embotelladora Mexicana S.A de C.V, con el fin de identificar activos críticos y vulnerabilidades se puede destacar que la ISO 17799 no se limita a una evaluación técnica de la infraestructura y seguridad de TI, sino también fortalece la resiliencia de la empresa frente a las amenazas lógicas y físicas, mejora la continuidad de la seguridad de la información del departamento, concientizando la participación del personal que se involucra en la preservación de la integridad, protección y gestión de los datos y activos.

Dentro de los hallazgos y recomendaciones planteadas, se pudo reconocer un área de oportunidad para la empresa de percibir y afrontar lo antes posible las amenazas identificadas, mejorando el mobiliario para la organización de activos, realizando un mantenimiento más minucioso y mejorando los controles del entorno operativo ajustando las prácticas de seguridad, políticas y normativas de uso para la reducción de probabilidad de incidentes como fuga de datos, ataques lógicos y pérdida de información.

Los objetivos planteados al inicio del proyecto se lograron alcanzar diseñando un plan de auditoría donde se incluyó el análisis de vulnerabilidades, revisiones del estado general de la infraestructura del departamento, la aplicación de cuestionarios a los trabajadores, así como la ejecución de procedimientos específicos, como las revisiones de acceso y análisis de los equipos de cómputo para la evaluación del funcionamiento y eficacia de los controles de seguridad internos.

Conclusiones personales

Después de analizar los resultados obtenidos al realizar la auditoria y haber identificado algunas fortalezas como áreas de mejora para el departamento, sin dejar a un lado la existencia de puntos vulnerables que requieren atención adicional, la auditoría permitió familiarizarse más en profundidad con los controles de seguridad establecidos por la norma ISO 17799, principalmente en cuanto a controles relacionados con la gestión de activos, la seguridad física y lógica y la gestión de incidentes. Adquiriendo así una perspectiva integral sobre la importancia de la seguridad de la información y la gestión de riesgos en el entorno empresarial que se vive actualmente.

Por otra parte, al realizar el informe detallado sobre la auditoría realizada se permitió desarrollar las habilidades de comunicación. Aprendiendo a presentar los resultados de manera clara y comprensible, facilitando la comprensión de los hallazgos por parte del personal encargado del departamento.

En general, la realización una auditoría de seguridad de activos proporciono beneficios significativos al departamento de sistemas y para las personas encargadas de la auditoria, permitiendo una evaluación profunda de la infraestructura y por otro lado ayudando a garantizar la integridad, confidencialidad de la información.

- Aguirre Olmos Katia Elizabeth

La elaboración de una auditoría de seguridad de activos de TI conforme a la norma ISO 17799 en la Embotelladora Mexicana S.A de C.V, ha proporcionado una visión estructurada de la postura de seguridad de los recursos tecnológicos. A través de este proceso, se han identificado áreas clave que requieren atención y mejoras para fortalecer la seguridad de los activos de tecnología de la información.

Por la parte práctica, la realización del proyecto permite obtener experiencias que van más allá de la evaluación de procesos y controles, ya que a través de estos se adquieren conocimientos significativos sobre las empresas/organizaciones auditadas, comprendiendo la cultura, estructura y procesos operativos, así como aprender a identificar y evaluar riesgos, vulnerabilidades, etc, que pueden afectar la seguridad e integridad de los datos o activos de TI.

Por la parte teórica se desarrollan habilidades analíticas al examinar los documentos, procesos y controles, además de mejorar la habilidad para comunicarse de manera efectiva tanto escrita como verbalmente y a su vez ayuda a desarrollar una mayor sensibilidad hacia las necesidades, permitiendo la adaptación de enfoques y recomendaciones identificando las oportunidades de mejora.

- Pantoja Hernández Karla Celeste

COMPETENCIAS DESARROLLADAS

Asignatura	Competencias
Fundamentos de investigación	• Capacidad de investigación • Habilidad de procesar y analizar información procedente de diversas fuentes • Habilidad en el uso de tecnologías de la información • Capacidad de trabajar en equipo • Recolección y tratamiento de datos • Análisis de resultados
Taller de ética	• Facilita el desarrollo de habilidades para tomar decisiones informadas y fundamentadas en principios éticos
Cultura empresarial	• Analiza los conceptos de la empresa para identificar vulnerabilidades y oportunidades de mejoras.
Arquitectura de computadoras	• Conoce los componentes y el funcionamiento en diferentes modelos de arquitectura en los equipos de cómputo.
Administración de la seguridad en comunicaciones	• Comprender principios y practicas necesarias para gestionar de manera efectiva la seguridad de comunicaciones. • Aprender a garantizar la confiabilidad e integridad de las comunicaciones, así como proteger los activos e información crítica. • Comprender el uso de herramientas para realizar escaneos sobre las aplicaciones/servicios de los equipos de cómputo
Administración de la función informática	• Manejo de los fundamentos lógicos de la seguridad informática para su aplicación • Uso e interpretación de lineamientos y marcos referenciales • Uso de técnicas y herramientas de software para comprender el ambiente de seguridad • Proponer medidas de seguridad basadas en lineamientos y estándares actuales

Normalización de software y hardware	• Analizar y comparar los distintos lineamientos actuales sobre el hardware, software y telecomunicaciones para aplicar su uso • Identifica los contenidos de los estándares generales de hardware • Identifica la arquitectura de comunicaciones y los contenidos de los estándares generales de los mismos
Auditoria informática y desarrollo de proyectos y aplicaciones	• Manejar los fundamentos teóricos de auditoría general, informática y tecnologías de la información. • Identificar, interpretar y usar lineamientos, estándares, técnicas y otros conceptos que contemplen la unión del conocimiento para la auditoria, realizando búsquedas sobre los tipos de pruebas de cumplimiento, pruebas sustantivas, los tipos y características de las evidencias, así como técnicas de recopilación de información (análisis, investigaciones, FODA, cuestionarios, etc) • Conocer las herramientas aplicables a la auditoria, a fin de proponerlas en el desarrollo de la planificación, ejecución y entrega de resultados, con la ayuda del plan de auditoria en donde se desarrollan los objetivos y alcances. • Comprender el entorno del control interno de la Embotelladora Mexicana S.A de C.V y su concepción en una normativa internacional. • Argumentar las metodologías para la seguridad y auditoria informática, a fin de incorporar en el proceso de la auditoria
Administración y seguridad en aplicaciones	• Comprender y analizar conceptos como seguridad de la información, vulnerabilidades, amenazas y ataques.

FUENTES DE INFORMACIÓN

- Alatrasta, M. (16 de 01 de 2019). *Auditool*. Obtenido de <https://www.auditool.org/blog/auditoria-externa/tecnicas-y-procedimientos-de-auditoria-lo-que-todo-auditor-debe-conocer>
- ALTP. (25 de 01 de 2018). *GSITIC*. Obtenido de <https://gsitic.wordpress.com/2018/01/25/bii11-auditoria-informatica-objetivos-alcance-y-metodologia-tecnicas-y-herramientas-normas-y-estandares/>
- Camejo. (27 de 04 de 2022). *Negocios y empresas*. Obtenido de <https://negociosyempresa.com/importancia-de-la-auditoria-en-empresas/>
- Cardoso Arteaga, C., & Zuluaga Contreras, M. G. (2007). *Aplicación de los estándares ISO 17799 y 27001 para el diagnóstico de la seguridad física y lógica en laboratorios de informática*. Bogotá.
- Castillo, J. (s.f). *ISO 17799: GESTIÓN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN*. Obtenido de https://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/estudios_ciencias/v1n1/a16_p277.pdf
- Cherres Jiménez, G. J. (2020). *Auditoría de seguridad de información y riesgos de tecnología de información en una cooperativa de ahorro y crédito*. Lima, Perú.
- Chicano, E. (2022). *Auditoría de seguridad informática*. IC Editorial, Segunda Edición.
- Coppola, M. (s.f). *HUBSPOT*. Obtenido de <https://blog.hubspot.es/website/que-es-seguridad-informatica>
- Coppola, M. (s.f). *HUBSPOT*. Obtenido de <https://blog.hubspot.es/website/auditoria-de-seguridad>
- Escudero, J. (s.f). *iedg*. Obtenido de <https://www.iedge.eu/juan-manuel-escudero-herramientas-tecnicas-para-la-auditoria-informatica>
- Fuenzalida, D. I. (2005). *Aplicación de la norma ISO/IEC 17799: Tesis, Universidad de Santiago de Chile*.
- Gómez Vieites, Á. (2011). *Enciclopedia de la seguridad informática*. RA-MA.
- Gómez, A. (2011). *Auditpría de seguridad informática (MF0487_3)*. Starbook Editorial, S.A.
- Hernández Jiménez, R. (2011). *Administración de la unficón informática, factor AFI*. Trillas.
- IBM. (s.f). *IMB*. Recuperado el 2024, de <https://www.ibm.com/mx-es/topics/data-security>

- ISO/IEC. (2005). *Estándar internacional 17799, Tecnología de la información*. Obtenido de <https://auditoriasistemasucb.pbworks.com/f/iso-17799-2005-castellano.pdf>
- Jarritos. (s.f). *Jarritos oficial*. Obtenido de <https://jarritosmexico.com/>
- Mendoza, M. (18 de 06 de 2015). *Universidad Veracruzana*. Obtenido de https://www.uv.mx/infosegura/general/conocimientos_ciberseguridad-2/
- Menendez Arante, S. C. (2022). *Auditoría de seguridad informática*.
- Mora Marín, G. (2006). *Directrices del plan director de seguridad: ISO 17799*. Sevilla.
- Morales Garcés, J. L., & Valle Romero, M. L. (2014). *Auditoría Informática de la seguridad de la información bajo las normas ISO/IEC 17799, en la red de estructura de finanzas populares y solidarias de Chimborazo (Refich). Periodo 2012*. Riobamba, Ecuador.
- Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales*. México: Pearson Education.
- Piattini, M., & Del Peso, E. (1998). *Auditoría Informática Un Enfoque Práctico (2a ed.)*. México: Alfaomega.
- Quiroga, S. (31 de 05 de 2021). *Linkedin*. Obtenido de <https://es.linkedin.com/pulse/seguridad-de-la-informaci%C3%B3n-acuerdo-las-iso-2700213-lic-quiroga>
- Sisteseg. (s.f). *Política seguridad física*. Bogotá.

ANEXOS

Anexo 1. Cuestionario

Infraestructura

1. ¿Cuántos racks tienes en tu infraestructura?
2. ¿Los racks están ubicados en un espacio con condiciones adecuadas de temperatura y humedad?

Si / No

3. ¿Cuántos routers y switches tienes en tu infraestructura?

Routers_____ Switches_____

4. ¿Cuál es la marca y modelo de los routers y switches utilizados?
5. ¿Los routers y switches tienen mantenimiento frecuente?

Sí, frecuencia_____ / No

6. ¿Se realizan inspecciones regulares de los equipos para detectar daños y problemas de funcionamiento?

Si, ¿Cuándo? ¿Quién?

Inventario

1. ¿Se cuenta con un registro detallado de los dispositivos?
2. ¿Existe un sistema de etiquetado e identificación para cada dispositivo?
3. ¿Existe un procedimiento para dar de baja dispositivos obsoletos o fuera de servicio?

Si / No

4. ¿Existe un registro de los softwares y licencias instaladas?

Si / No

5. ¿Existe un inventario separado para periféricos como cables, pantallas, teclados y mouses?

Si / No

6. ¿Se lleva un registro de los incidentes de seguridad relacionado con los dispositivos?

Si / No

Seguridad física

1. ¿Cómo se supervisa y controla el acceso a los componentes del departamento de sistemas?
2. ¿Cuáles son las medidas de seguridad implementadas para prevenir el robo de equipos?
3. ¿Existe algún sistema de vigilancia o cámaras de seguridad instaladas en el departamento?
4. ¿Cómo se realiza la supervisión y control de los visitantes que ingresan al departamento?
5. ¿El departamento cuenta con extintores contra incendios y señalamientos de evacuación?
6. ¿Qué tipo de sanciones existen en caso de dañar un dispositivo, periférico o instalación del departamento?

Seguridad Lógica

1. ¿Existen procedimientos establecidos para la seguridad lógica?

Sí, ¿Cuáles? No

2. ¿Se siguen procedimientos para la creación, modificación y eliminación de cuentas de usuarios?

Sí, ¿Cuáles? No

3. ¿Se utilizan contraseñas seguras y se requiere que los usuarios las cambien periódicamente?

Sí / No

4. ¿Se brinda capacitación regular a los usuarios sobre las mejores prácticas de seguridad lógica, cómo el uso de contraseñas seguras y la identificación de correos electrónicos?

Sí, frecuentemente Sí, ocasionalmente No, nunca

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

Sí, frecuentemente Sí, ocasionalmente No, nunca

Servicios

1. ¿Se han presentado problemas físicos con el servicio del aire acondicionado?

Sí, frecuentemente Sí, ocasionalmente No, nunca

2. ¿Cómo calificas la velocidad del servicio de WiFi?

Muy lento Lento en ocasiones Aceptable Rápido y estable

3. ¿Cómo defines el servicio eléctrico del laboratorio?

Muy bueno Estable Malo No existe

4. ¿A qué autoridad debes acudir en caso de encontrar fallas en el servicio de internet y qué actividades se realizan para recuperar la conectividad?

5. ¿A qué autoridad debes acudir en caso de encontrar fallas en el servicio eléctrico y qué actividades se realizan para recuperar la electricidad?

6. ¿Cómo se supervisa y monitorea el rendimiento de la red y los sistemas?