UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Facultad:

CIENCIAS DE LA VIDA Y TECNOLOGÍAS

Carrera:

INGENIERÍA EN SISTEMAS

TEMA:

“AUDITORÍA INFORMÁTICA ENFOCADA AL FORTALECIMIENTO DE LA SEGURIDAD FÍSICA Y LÓGICA EN SPORTMANCAR MANTA”

Trabajo de titulación modalidad Proyecto Integrador presentado en conformidad con los requerimientos establecidos para optar por el título de Ingeniero en Sistemas.

TUTOR:

Ing. Marco Ayoví Ramírez, Ph. D.

AUTOR:

Plúa Gutiérrez Jonathan Adalberto

MANTA – MANABÍ – ECUADOR

2025(1)

DECLARACIÓN DE AUTORÍA

Yo, **PLÚA GUTIÉRREZ JONATHAN ADALBERTO** con Cédula de Identidad N.° **131498581- 1**, declaro ser el responsable del contenido del presente trabajo de titulación, cuyo tema es "AUDITORÍA INFORMÁTICA ENFOCADA AL FORTALECIMIENTO DE LA SEGURIDAD FÍSICA Y LÓGICA EN SPORTMANCAR MANTA" cuya elaboración es compartida únicamente con la dirección del tutor, Ing. Marco Wellington Ayovi Ramírez y la propiedad intelectual de la misma pertenece a la Universidad Laica Eloy Alfaro de Manabí

A si mismo, autorizo a la ULEAM para que realice la publicación de este trabajo de titulación con fines estrictamente académicos o investigativos.

Lo certifico:

Plúa Gutiérrez Jonathan Adalberto

C.I: 131498581-1

Uleam	NOMBRE DEL DOCUMENTO:* CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Facultad CIENCIAS DE LA VIDA Y TECNOLOGÍAS de INGENIERÍA EN SISTEMAS de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el Proyecto Integrador, bajo la autoría del estudiante Plúa Gutiérrez Jonathan Adalberto, legalmente matriculado/a en la carrera de INGENIERÍA EN SISTEMAS período académico 2025-2026, cumpliendo el total de 297 horas, bajo la opción de titulación de Proyecto Integrador, cuyo tema del proyecto es "AUDITORÍA INFORMÁTICA ENFOCADA AL FORTALECIMIENTO DE LA SEGURIDAD FÍSICA Y LÓGICA EN SPORTMANCAR MANTA".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Lugar, 04 de septiembre de 2025.

Lo certifico,

Ing. Marco Aydvi Ramírez. Ph.D.
Docente Tutor
Área:

AGRADECIMIENTO

Quiero agradecer a Dios por ser mi guía y luz, a mi esposa, padres y hermanos, quienes son mi motivación diaria para poder avanzar en cada meta trazada.

Agradezco también a cada lugar donde pude desempeñar mi trabajo, aprendiendo de ellos en su momento, también a Lab XXI que me ha permitido crecer y aprender de cada una de las personas que conforman esta maravillosa empresa, convirtiéndose en una familia más para mí; a todos los docentes de las etapas estudiantiles, gracias por compartir sus conocimientos.

Jonathan Adalberto Plúa Gutiérrez

DEDICATORIA

Este trabajo se lo dedico en primer lugar a Dios, quien me ayuda en cada etapa de mi vida; a mi esposa, quien desde que nos conocimos me ha impulsado a alcanzar cada meta en todos los ámbitos de mi vida; a mis padres, quienes desde mi nacimiento hacen muchas cosas por mí; mis hermanos quienes son parte de mi combustible para avanzar diariamente en este camino llamado vida; a mi hermanita en el cielo Génesis, quien me ha cuidado en todo momento de la vida; y a mi gran amigo Juan Benavides, quien siendo parte de la gran empresa LAB XXI, me ha permitido crecer y aprender de cada uno de ellos.

A cada uno de mis docentes de esta etapa de formación profesional.

Esta nueva meta alcanzada es un paso más para el trayecto trazado, Excélsior.

Jonathan Adalberto Plúa Gutiérrez

Índice de contenidos

Índice de tablas

Índice de ilustraciones

RESUMEN

El control interno es fundamental en toda organización, ya que permite la protección de los activos, prevención de fraudes y errores, esto alineado al cumplimiento de leyes y regulaciones. Al aplicar un adecuado control se obtiene una eficiencia operativa y disponibilidad de la información desde cualquier departamento de la empresa, esto permite la toma de decisiones informadas fortaleciendo la estabilidad y productividad de la empresa. Una implementación adecuada también promueve el fortalecimiento de la seguridad informática tanto física como lógica, garantizando que todos los recursos se utilicen de manera eficiente y se logren los objetivos estratégicos de la empresa. El Objetivo del presente trabajo de titulación es realizar una auditoría informática que permita identificar factores que fortalezcan la seguridad física y lógica en Sportmancar Manta, alineado a un adecuado control interno.

Para la ejecución de este trabajo, se partió desde el fortalecimiento de conocimientos en el Modelo COSO 2013, investigar las políticas internas de la empresa, seguridad informática, uso adecuado de las TI en el entorno empresarial para el cumplimiento de objetivos.

Al finalizar esta intervención se ejecutarán actividades de mejora que permitirán fortalecer el control interno, generar conciencia en los colaboradores sobre la importancia de involucrarse en la aplicación de acciones que aporten en la seguridad informática y el uso adecuado de cada equipo informático designado.

Palabras claves: control interno, disponibilidad, seguridad informática, auditoría informática, modelo COSO, equipo informático.

ABSTRACT

Internal control is fundamental to every organization, as it enables asset protection and fraud and error prevention, all in line with compliance with laws and regulations. Applying adequate control results in operational efficiency and information availability from any department within the company, enabling informed decision-making, strengthening the company's stability and productivity. Proper implementation also promotes the strengthening of both physical and logical IT security, ensuring that all resources are used efficiently and the company's strategic objectives are achieved. The objective of this thesis is to conduct an IT audit to identify factors that strengthen physical and logical security at Sportmancar Manta, aligned with adequate internal control.

This work began by strengthening knowledge of the 2013 COSO Model, investigating the company's internal policies, IT security, and the appropriate use of IT in the business environment to achieve objectives. At the end of this intervention, improvement activities will be implemented to strengthen internal control, raise employee awareness about the importance of participating in actions that contribute to IT security, and ensure the proper use of each designated IT device.

Keywords: internal control, availability, IT security, IT audit, COSO model, IT equipment.

CAPÍTULO I

Introducción

1.1 Introducción

En la actualidad, los datos que gestionan las empresas son categorizados de gran importancia para que los servicios sigan funcionando y se puedan alcanzar las metas. Cada progreso relacionado con la tecnología, así como las mejoras, permiten la eficiencia en el trabajo empresarial y su expansión, lo cual ha impulsado el uso de herramientas tecnológicas. Por esta razón, las empresas invierten en de manera considerable en la implementación de tecnologías que aseguren el acceso rápido a los datos y a su vez protejan su integridad.

Debido a la importancia de implementar mecanismos de protección y el acceso a los datos, además de ser esencial la continuidad operativa de los servicios que se brindan, resulta fundamental llevar a cabo procesos de auditoría de manera externa o interna en las empresas. Estos procesos, posibilitan que las empresas detecten vulnerabilidades, riesgos y puntos de mejora, fomentando el aprovechamiento de las tecnologías de la información, previniendo así interrupciones en la prestación de servicios o gastos excesivos en reparaciones.

Al disponer de equipos informáticos, es importante contar con un profesional en esta área, es por ello que el encargado de las TI, tiene como propósito mantener siempre disponible la información y supervisando de manera frecuente los recursos informáticos, logrando así asegurar el procesamiento, continuidad y desarrollo de los procesos internos. Para lograr estos objetivos, la ejecución de auditorías informáticas suma en gran manera, ya que permite identificar los recursos que posee la organización, analizar la seguridad de la información tanto física y lógica, dando como resultado un adecuado control interno que involucre a todos los integrantes de esta empresa.

El enfoque de una auditoría informática es fortalecer la seguridad física y lógica en toda empresa, partiendo desde un adecuado control interno. El proceso busca involucrar a

todos los colaboradores, teniendo la iniciativa el responsable de TI, con el fin de mitigar los riesgos y capacitar a todo el personal para lograr un correcto uso de las TI en el establecimiento.

Por lo antes mencionado, se desarrolla este proyecto integrador, que permitirá ejecutar una auditoría informática que permita fortalecer la seguridad física y lógica desde un adecuado control interno. De acuerdo a esto, el presente trabajo de titulación se encuentra estructurado de la siguiente forma:

En el primer capítulo, se comienza con una introducción al tema, seguido de una descripción de la localización y el contexto de la problemática, donde se destaca la razón principal para abordar el asunto mencionado. A continuación, se presenta el planteamiento del problema, que considera la definición de la problemática, el origen del mismo y su situación actual. En este contexto, se incluye un diagrama de causas y efectos del problema que facilita la identificación de sus razones y orígenes. Asimismo, se explican los objetivos del proyecto, la justificación y, al final, los impactos esperados en los ámbitos tecnológico, social y ecológico.

En el segundo capítulo, se revisan los antecedentes históricos y las investigaciones relacionadas con el tema. Esta información está respaldada por autores que proporcionan contextos relevantes y sirven como base esencial para el desarrollo de las distintas etapas del trabajo.

En el tercer capítulo, se describen las metodologías utilizadas en desarrollo de este estudio, el cual se centra principalmente en la recolección de información, así como los resultados obtenidos.

El cuarto capítulo contiene el marco propositivo, en el cual se detalla la propuesta del proyecto y se especifican los recursos empleados, incluyendo los humanos, tecnológicos y económicos.

En el quinto capítulo, se evalúan los resultados, presentando lo que se logró una vez completada la auditoría informática y, por ende, se implementaron acciones de mejora con un enfoque en fortalecer la seguridad tanto física como lógica.

Finalmente, en el sexto capítulo se ofrecen las conclusiones y recomendaciones del trabajo, donde se verifica que los objetivos planteados en el proyecto se hayan alcanzado y se sugiere que el proceso pueda ser replicado en otras organizaciones.

A continuación, se muestra en la tabla 1 el resumen del contenido del trabajo de titulación:

Tabla 1

Tabla de contenidos

N°	CONTENIDO	DETALLE
1	**Introducción**	Por medio de este capítulo, el lector podrá comprender el trabajo de titulación de manera breve y concisa.
2	**Marco Teórico de la investigación**	Permite levantar información base, que sustente la importancia de implementar una solución a la problemática identificada.
3	**Marco Investigativo**	Define las estrategias y métodos para la recolección de la información, primordial para la continuidad del trabajo.

4	**Marco Propositivo**	Este capítulo contiene las acciones de solución para el problema identificado, involucrando los diferentes recursos como humanos, tecnológicos y económicos.
5	**Evaluación de resultados**	Permite aplicar una evaluación a los resultados obtenidos luego de la implementación de las soluciones.
6	**Conclusiones y recomendaciones**	Permite conocer si los objetivos fueron cumplidos durante la ejecución del proyecto, a su vez, permite realizar recomendaciones puntuales para replicar en este o en trabajos similares.

1.2 Presentación del tema

Auditoría informática con enfoque al fortalecimiento de la seguridad física y lógica en Sportmancar Manta

1.3 Ubicación y contextualización de la problemática

El adecuado control interno, dentro de las organizaciones, es altamente importante debido a que es un punto de partida para el cumplimiento de objetivos estratégicos dentro de una institución. Para alcanzar los resultados planteados en la empresa es importante que la información esté siempre disponible y sobre todo segura, tanto física como de manera lógica.

Actualmente la seguridad informática es un tema clave en toda empresa que maneja recursos informáticos, y es por ello que para lograr mejores resultados en este ámbito se necesita involucrar a toda la organización.

Relacionado a lo mencionado anteriormente, Sportmancar Manta maneja información fundamental para el cumplimiento de los objetivos de la empresa, siendo el motivo principal

formar conductores no profesionales en la ciudad. Dicha información se basa en los datos de los estudiantes, horarios de instructores y el estado de pago de cada cliente inscrito para los cursos que se ofertan. Para la correcta ejecución de todos los procesos relacionados con TI, se cuenta con la supervisión de un profesional de en esta rama, sin embargo, hay riesgos identificados como la exposición de la estructura física de la red local y la falta de implementación de sistemas de seguridad de la información, esto podría ser un punto vulnerable para que agentes externos a la empresa puedan ingresar a todos los datos y sistemas que se maneja.

Si llegase a concretarse una vulneración de la seguridad física y lógica a las TI en Sportmancar Manta, esto llevaría a la pérdida de información de los clientes, y por consiguiente una paralización de las actividades de la empresa ocasionando también pérdidas económicas y de credibilidad.

Para resolver esta problemática se ejecuta una auditoría informática que permita fortalecer los procesos de control interno, esto a su vez potenciará la seguridad física y lógica de los recursos informáticos en la empresa, posteriormente presentar los resultados obtenidos a gerencia; con esto se incentiva a la implementación de las correcciones presentadas al final de la intervención.

1.4 Planteamiento del problema

1.4.1 Problematización

- ¿Existe un adecuado control interno que permita la continuidad de los servicios informáticos?

- ¿Qué acciones permitirán identificar mejoras en el control interno de las TI?
- ¿Se está fomentando la participación de todo el personal en el fortalecimiento de la seguridad física y lógica de los recursos informáticos?
- ¿En qué beneficia la ejecución de una auditoría informática en el fortalecimiento de la seguridad física y lógica de una empresa?

1.4.2 Génesis del problema

El control interno en el área de TI es fundamental en toda organización, siendo aún más relevante cuando su activo más valioso es la información que maneja. Al no ejecutar actividades de control específicas da como resultado el no lograr identificar riesgos y aplicar acciones de mejora dentro de un departamento o una empresa.

Es primordial la ejecución de actividades de control que permitan eliminar algunos riesgos que pueden ser: posibles vulneraciones a la red local por no implementar métodos de seguridad, ingeniería social, falta de compromiso con el uso adecuado de las TI por parte del personal de colaboradores y, por último, el acortar la vida útil de las TI en una empresa.

1.4.3 Estado actual del problema

A la fecha de ejecución de este estudio, se identifica que el no realizar acciones de control en el área de TI con enfoque a la seguridad física y lógica, ha dado como resultado el llevar un camino “a ciegas”, esto puede generar factores negativos para el cumplimiento de los procesos informáticos y un impacto en la continuidad de los servicios informáticos en Sportmancar Manta.

Hasta el momento, a pesar que se cuenta con un profesional responsable de TI, no se ha logrado implementar acciones de control interno que permitan identificar riesgos en la seguridad informática y poder ejecutar acciones que los elimine, dando como resultado la no continuidad de los servicios informáticos debido a factores que se mencionarán durante el presente trabajo de titulación.

1.5 Diagrama causa – efecto del problema

Para graficar el problema, se utiliza el método de la cebolla del problema, por medio de esta técnica podremos identificar la causa raíz del problema, y esto tiene una repercusión en la seguridad física y lógica de los recursos informáticos.

Por medio de la ilustración 1 se puede observar que, el problema central se basa en no implementar un adecuado control interno, lo que desencadena en no ejecutar acciones que permitan fortalecer la seguridad informática en Sportmancar Manta

Ilustración 1

Diagrama causa-efecto

La solución a esta problemática es la ejecución de una auditoría informática que permita fortalecer los procesos de control interno donde se involucre a todos los colaboradores de la empresa, así se logrará llevar a cabo acciones para mitigar y eliminar factores de riesgos, y por consiguiente fortalecer la seguridad física y lógica de las TI en Sportmancar Manta.

1.6 Objetivos

1.6.1 Objetivo general

Realizar una Auditoría Informática a través de la aplicación del modelo COSO 2013 para mejorar la seguridad física y lógica de la Empresa Sportmancar - Manta

1.6.2 Objetivos específicos

- Revisar la metodología del Modelo COSO 2013 para utilizar componentes del control interno que permitan mejorar las seguridad física y lógica de la empresa Sportmancar Manta
- Evaluar e implementar controles que permitan mantener la continuidad del servicio informático
- Aplicar una herramienta en la red de Sportmancar Manta que permitan identificar el tráfico de red y su acceso a servidores
- Identificar riesgos y plantear mejoras según información obtenida, realizando iniciativas que promuevan la seguridad física y lógica de las TI.
- Ejecutar una auditoría informática con enfoque a la seguridad física y lógica en Sportmancar Manta

1.7 Justificación

Hoy en día, las empresas dependen en gran porcentaje de los sistemas de información para llevar a cabo sus operaciones en todas las áreas. Esta demanda tecnológica exige la implementación de controles internos que garanticen la seguridad y continuidad de los recursos informáticos, tanto en manera física como lógica. Sportmancar Manta, dedicada a la formación de conductores no profesionales en Manta, no se exenta a estos casos; sin embargo, preocupa la carencia de controles internos eficaces en la seguridad física y lógica, aumentando su vulnerabilidad ante riesgos tecnológicos, accesos indebidos, pérdida de información y problemas en la operación continua.

La ejecución de una auditoría informática enfocada en fortalecer la seguridad física y lógica se justifica por la necesidad urgente de evaluar, identificar y corregir debilidades en el manejo de los sistemas de información de la empresa. Este tipo de auditoría permitirá no solo identificar el estado actual de la infraestructura tecnológica y sus respuestas de protección, sino también fortalecer políticas, procedimientos y controles alineados con buenas prácticas internacionales, como las propuestas por COBIT, ISO/IEC 27001 y los principios de control interno definidos por COSO.

Adicionalmente, la ejecución de una auditoría informática contribuirá a la toma de decisiones estratégicas informadas por parte de la gerencia, al brindar información objetiva y fundamentada sobre los riesgos y las oportunidades de mejora en materia de seguridad de la información. La implementación de controles internos adecuados garantizará un entorno informático confiable, protegido contra amenazas internas y externas, complementado con los objetivos empresariales de Sportmancar Manta.

Por lo tanto, este trabajo no solo responde a una necesidad operativa, sino que también se enmarca dentro de una visión preventiva y sostenible de la gestión empresarial, lo que hace relevante su realización para fortalecer la gobernanza tecnológica de la organización.

De manera concreta este proyecto se justifica debido a:

- La necesidad de identificar puntos de mejora en la empresa
- Importancia del control interno en la seguridad de la información
- Involucramiento de todo el personal en el cumplimiento de la política interna relacionada al uso adecuado de los recursos informáticos

Esto permitirá:

- Fortalecer la seguridad física y lógica en Sportmancar Manta
- Implementar acciones de control interno
- Tratamiento adecuado de riesgos
- Alcanzar sus objetivos estratégicos
- Generar el sentido de pertenencia y responsabilidad en el cumplimiento de política interna donde se menciona sobre el uso adecuado de los recursos informáticos.

Los beneficiarios de este proyecto son:

- Ejecutivos de Sportmancar Manta, como beneficiario directo; quienes usan de manera diaria los equipos informáticos para el cumplimento de sus funciones y metas internas de la empresa.
- Estudiantes y posibles clientes, quienes serían los beneficiarios indirectos; esto debido a que son quienes confían en la empresa información personal,

lo que llevará a una mayor percepción de seguridad tanto en las instalaciones (seguridad física) y el tratamiento de los datos personales e información (seguridad lógica)

1.8 Impactos esperados

A continuación, se detallan los impactos esperados en el presente trabajo de titulación, los cuales son en los ámbitos: tecnológicos, social y ecológico.

1.8.1 Impacto tecnológico

Con la ejecución de este trabajo, se podrá identificar aquellos procesos y riesgos que puedan afectar al cumplimiento de los objetivos de Sportmancar Manta, y por ende puedan afectar a la seguridad física y lógica de los recursos informáticos que posee la empresa. Durante la ejecución de este proceso, también se identificarán canales de mejora en los sistemas de protección tanto de los activos informáticos.

El enfoque de verificar la seguridad física, será el comprobar aspectos como el control de accesos físicos a áreas con acceso restringido, comprobar el funcionamiento de los sistemas de videovigilancia, aplicación de dispositivos de seguridad (cerraduras, alarmas, detectores de movimientos) y la preparación ante desastres naturales. El impacto esperado es la mejora en la protección de la infraestructura física, reduciendo la posibilidad de robos, intrusiones o daños que puedan afectar los sistemas informáticos.

En el ámbito de la seguridad lógica, analizará la gestión de contraseñas, métodos de autenticación, los sistemas de detección y respuesta ante amenazas, y la protección de datos mediante cifrado o activaciones de firewall y políticas de respaldo. El impacto tecnológico en esta área se refleja en un reforzamiento de las barreras contra ataques informáticos, minimizando

riesgos de pérdida o filtración de información relevante, accesos no autorizados y daños en los sistemas de información.

En conclusión, esta auditoría informática enfocada en la seguridad física y lógica no solo permitirá fortalecer las medidas de protección, sino que incentiva a una evolución tecnológica en la empresa, optimizando infraestructuras, fortaleciendo la defensa contra amenazas internas y externas, y elevando el nivel de protección en la gestión integral de la seguridad de la información.

Al finalizar la intervención se presentará una propuesta de mejora con contenido digital con enfoque a la seguridad física y lógica, trabajando este ámbito desde sus colaboradores siendo actores claves en el crecimiento de la empresa.

1.8.2 Impacto social

Al ejecutar este proyecto, se logrará un impacto social considerable, debido a que con esto se contribuye a la protección de la información y los recursos de TI en la organización, esto a su vez, genera confianza desde diferentes puntos tanto de los clientes como los usuarios colaboradores. Con esto se busca conseguir una protección completa, previniendo accesos no autorizados o pérdida de datos, reduciendo la percepción de vulnerabilidad y promoviendo un ambiente laboral más seguro y estable. Adicionalmente se busca asegurar la confidencialidad, integridad y disponibilidad de la información, punto clave conseguir objetivos estratégicos de Sportmancar Manta.

1.8.3 Impacto ecológico

El impacto ecológico que se conseguirá por medio de la implementación de este proyecto, principalmente es el aprovechamiento de los recursos tecnológicos y con esto se logra prolongar la vida útil de los equipos informáticos. Al mejorar el control interno por medio de esta auditoría informática, se promueve un manejo más eficiente y adecuado de los recursos informáticos, y, por ende, se reduce la emisión de residuos electrónicos contaminantes.

CAPÍTULO II

Marco teórico de la investigación

2.1 Antecedentes históricos

Manrique Plácido, JM (2019). Introducción a la auditoría. Menciona que: “La auditoría es un proceso sistemático para obtener y evaluar evidencias de una manera objetiva y se aplica en distintas actividades de la organización social: empresas privadas y públicas, entidades de otros sectores, ámbito fiscal, operacional, medioambiental, forense, informático, etc.” (página 16)

Por esto se puede comprender que la auditoría es un proceso necesario para la mejora continua de un departamento y más aún de una empresa, teniendo cobertura de supervisión y control de diferentes ámbitos de una institución, entre ellos el área de la informática.

La protección de los activos informáticos y los recursos materiales en las empresas son una prioridad en la actualidad. En este sentido, la seguridad física y lógica ejercen roles esenciales para garantizar la integridad, disponibilidad y confidencialidad de los datos y de las infraestructuras tecnológicas.

La seguridad física tiene como propósito salvaguardar los activos visibles, como equipos informáticos, servidores, documentos físicos y a las personas, ante amenazas como robos, hurtos, incendios o desastres naturales (Soto, 2020). Para ello, se implementan mecanismos como sistemas de control de acceso, videovigilancia, cerraduras, alarmas y protocolos de respuesta ante emergencias.

Por su parte, la seguridad lógica busca proteger los sistemas informáticos, redes y datos digitales de amenazas cibernéticas, accesos no autorizados, alteraciones o pérdida de información (González & Ramírez, 2021). Entre las principales herramientas de seguridad lógica

se encuentran el cifrado de datos, los firewalls, los sistemas de detección de intrusiones por medio de los circuitos de videovigilancia, aplicación de contraseñas seguras para la autenticación.

La combinación de ambas aristas de seguridad permite a las organizaciones establecer un marco integral de protección que no solo resguarda los recursos materiales, sino también los activos de información, fundamentales para la continuidad del negocio (Torres, 2019). Por tanto, es de gran importancia la implementación de estrategias que permitan disminuir o eliminar los riesgos y fortalezcan las buenas prácticas del uso de las TI, orientado a la seguridad física y lógica de las TI en la empresa.

El modelo COSO 2013 por medio de sus componentes tiene como objetivo fortalecer y dirigir el concepto de control interno en empresas de todo tipo. Su ejecución en entornos de control interno se debe principalmente a que proporciona una estructura completa y actualizada que permite a las organizaciones alcanzar objetivos internos basados en información y de cumplimiento a corto plazo, de manera adecuada.

Este modelo contiene 17 principios donde se mencionan de una manera clara los requisitos necesarios para un control interno adecuado, esto da como resultado una facilidad de comprensión, implementación y evaluación. Complementado a lo anterior, el modelo COSO 2013 tiene un enfoque en aspectos como la cultura organizacional, la evaluación de riesgos y la adaptación a los cambios. Estos elementos son importantes actualmente, donde los riesgos y la complejidad operativa exigen sistemas de control interno más dinámicos y adaptativos.

Asimismo, el marco COSO 2013 busca promover la corresponsabilidad del equipo de trabajo en el control interno entre todos los niveles de la organización, no solo la alta dirección,

esto permite obtener un control adecuado de los diferentes departamentos de la empresa. Al ser ampliamente reconocido internacionalmente, también facilita a las empresas demostrar su compromiso con buenas prácticas de gestión.

Sportmancar lleva 16 años en el mercado ecuatoriano, ofreciendo cursos de formación de conductores no profesionales con licencias tipo A o B, brindando servicios de calidad con personal capacitado para formar conductores en el Ecuador.

Su presencia en 12 provincias con atención en 42 locales distribuidos en el territorio nacional, permiten a los habitantes de ciudades como Manta acceder a cursos de conducción. Sportmancar Manta cuenta con formación de conductores para obtener licencia tipo A o B, teniendo en su personal profesionales para las diferentes áreas que comprenden la empresa ubicada en la Av. Flavio Reyes y calle 20; estas áreas son: atención al cliente, contabilidad, sistemas informáticos y administración.

Entre los modelos COSO 2013 y COSO 2017 que son usados para ejecutar una auditoría, existen cambios, sin embargo, de acuerdo al enfoque de fortalecer la seguridad física y lógica de Sportmancar Manta y el contexto de implementación, se plantea el uso del modelo COSO 2013.

Entre las ventajas del uso del modelo COSO 2013, se pueden mencionar las siguientes: Tiene un enfoque en la gestión de riesgo, siendo particularmente eficaz para organizaciones que buscan un enfoque integral en la gestión de riesgos, debido a que plantea un marco claro para la evaluación y mejora del control interno. Aunque el COSO 2017 también hace hincapié en la gestión de riesgos, el COSO 2013 lo incorpora de manera más prominente y sistemática en su estructura. Este modelo se enfoca en la identificación, evaluación y mitigación de riesgos como una parte esencial del control interno, lo que lo hace más adecuado para organizaciones con

entornos operativos complejos o cambiantes. Además, el modelo COSO 2013 proporciona una base sólida para gestionar tanto riesgos financieros como no financieros, lo que ofrece una perspectiva más amplia y adaptativa.

Claridad en sus componentes, detalla de la manera más específica los 17 principios engloban sus cinco componentes: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo. La precisión de este modelo, permite a las empresas implementar el marco de control interno de forma más efectiva, con una guía más clara sobre cómo se deben implementar cada uno de los principios.

El modelo COSO 2013 abarca en mayor proporción el ambiente empresarial, es decir no solo cubre los controles internos financieros, sino que también reconoce la importancia de los controles internos en toda la empresa. Este enfoque general permite a las instituciones gestionar el control interno de manera general, lo que resulta en mayores beneficios a largo plazo.

Este modelo se adapta a diferentes tipos de organizaciones, independiente de su tamaño o sector. El enfoque de COSO 2013, permite a las empresas realizar ajustes de acuerdo a sus necesidades, lo que lo hace ideal para diferentes tipos de empresas partiendo desde las más pequeñas hasta grandes corporaciones. Conjuntamente, al ser un marco flexible y adaptable, permite a las empresas gestionar el control interno de manera eficiente sin ser desatinadamente prescriptivo, lo que lo hace más útil en entornos dinámicos o de altos cambios.

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Tema 1: "AUDITORÍA INFORMÁTICA A METRISA METROPOLITANA RIOBAMBA CLÍNICA DE SERVICIOS MÉDICOS ESPECIALIZADOS S.A., DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO, PERÍODO 2018"

El proyecto titulado "AUDITORÍA INFORMÁTICA A METRISA METROPOLITANA RIOBAMBA CLÍNICA DE SERVICIOS MÉDICOS ESPECIALIZADOS S.A., DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO, PERÍODO 2018" desarrollado por (Cando Moreno, 2019), fundamenta la importancia de detectar falencias en el uso de las Tecnologías de la Información y Comunicación en la institución.

Para la ejecución de esta auditoría se establecieron métodos, técnicas e instrumentos de investigación las cuales se emplearon para la recolección de la información necesaria en el desarrollo de la investigación; se usaron técnicas importantes como entrevistas y cuestionarios de control interno basados en el COSO 2013 primordiales para el desarrollo de una Auditoría Informática.

Este proyecto culminó con la identificación de puntos de mejora, donde se planteó una propuesta para reducir y eliminar los riesgos, a su vez sugiriendo reestructuraciones laborales en el establecimiento médico.

Este antecedente se relaciona directamente con el proyecto actual, ya que ambos comparten el objetivo de ejecutar una auditoría informática para identificar puntos de mejora en un establecimiento.

Tema 2: "AUDITORÍA INFORMÁTICA EN SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL DISTRITO DE EDUCACIÓN 13D05 EL CARMEN"

El proyecto con título "AUDITORÍA INFORMÁTICA EN SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL DISTRITO DE EDUCACIÓN 13D05 EL CARMEN" desarrollado por (Alcívar Rivas, 2025) está orientado a comprobar y promover la seguridad lógica mediante el uso adecuado de los equipos informáticos.

Para la ejecución de este proyecto se establecieron técnicas de recopilación de información como es una encuesta estructurada, la cual permitió recopilar información relevante para la identificación de las mejoras y así lograr proponer correcciones que permitan fortalecer la seguridad física de los equipos informáticos.

Este antecedente se relaciona con el proyecto actual, debido a que ambos comparten el objetivo de identificar puntos de mejora para el fortalecimiento de la seguridad física de las TI.

Tema 3 "AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ" INGENIERÍA EN SISTEMAS"

Este proyecto que lleva por título "**"AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ" INGENIERÍA EN SISTEMAS"** desarrollado por (Ávila Cevallos, 2019) se ejecutó con el enfoque a fortalecer la seguridad lógica con información de docentes, siendo algo de gran importancia en la comunidad educativa de esta extensión.

En la ejecución de este proyecto, se planteó como punto inicial la elaboración de una encuesta diagnóstico que permitió identificar las falencias en el ámbito de la seguridad lógica en la extensión del Carmen de la "universidad Laica Eloy Alfaro de Manabí".

Este antecedente tiene relación con el proyecto actual, ya que nos permite fortalecer conocimiento en las estrategias para diagnosticar puntos de mejora en la seguridad lógica y por ende diseñar una propuesta ideal con el objetivo de presentar sugerencias para la mejora de esta área.

2.3 Definiciones conceptuales

2.3.1. Auditoría

La auditoría es un proceso sistemático, independiente y documentado que consiste en la verificación y evaluación objetiva del cumplimiento de actividades, procedimientos o estados financieros conforme a criterios previamente establecidos, tales como políticas, normativas o requisitos legales (Kawak, 2025). Según la Organización Internacional de Normalización (ISO), la auditoría permite obtener evidencia para determinar en qué medida se alcanzan dichos criterios, funcionando como un diagnóstico que identifica fortalezas, debilidades y áreas susceptibles de mejora dentro de una organización (Kawak, 2025). Este proceso debe ser

objetivo, basado en hechos sustentables y evidencias, y desarrollado con independencia e imparcialidad por profesionales capacitados (Kawak, 2025). La auditoría puede ser interna o externa y abarca diversas áreas, incluyendo la financiera, operativa, administrativa y de cumplimiento, con el fin de asegurar la precisión de la información, la eficiencia de los procesos y el cumplimiento normativo (IQS, 2024; Gadax, 2023). Además, la auditoría operacional analiza los procesos diarios para proporcionar a la dirección una visión clara que facilite la toma de decisiones estratégicas y la optimización de recursos (Captio, 2025). En definitiva, la auditoría es una herramienta esencial para garantizar la transparencia, mejorar el rendimiento organizacional y reducir riesgos, contribuyendo así a la sostenibilidad y competitividad de las empresas (Nanuk, 2024).

2.3.2. Tipos de auditoria

Existen diversos tipos de auditoría, cada una enfocada en aspectos específicos de una organización.

- **Auditoría financiera o contable**: Es la revisión de la situación financiera de una entidad para expresar una opinión sobre su razonabilidad y conformidad con principios contables. Según la *International Federation of Accountants (IFAC)*, esta auditoría busca aumentar la confianza de los usuarios sobre los estados financieros (IFAC, 2022).
- **Auditoría informática o de sistemas**: Evalúa los controles internos de los sistemas de información, la integridad de los datos y la eficiencia de los procesos informáticos. Se enfoca en garantizar la seguridad, confiabilidad y disponibilidad de los sistemas (Hurtado & Rojas, 2018).

- **Auditoría de gestión**: Examina la eficiencia, eficacia y economía con la que se utilizan los recursos de una organización. Busca mejorar los procesos administrativos y operativos (Rezaee, 2002).
- **Auditoría operativa**: Similar a la de gestión, se concentra en evaluar procedimientos operativos específicos para proponer mejoras que optimicen el desempeño organizacional (Whittington & Pany, 2012).
- **Auditoría de cumplimiento**: Verifica si una entidad cumple con leyes, regulaciones, políticas internas y otros requisitos normativos aplicables (Arens et al., 2014).

2.3.3. Auditoría interna

La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta diseñada para agregar valor y mejorar las operaciones de una organización. Su propósito es ayudar a una organización a cumplir sus objetivos mediante un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobernanza (The Institute of Internal Auditors [IIA], 2017).

Esta función actúa como un mecanismo de supervisión interna que contribuye a la transparencia, eficiencia y eficacia organizacional. A través del análisis crítico y la revisión de procedimientos, la auditoría interna no solo detecta desviaciones o riesgos potenciales, sino que también sugiere medidas correctivas y preventivas, promoviendo la mejora continua.

2.3.4. Auditoría externa

La auditoría externa es un proceso independiente y sistemático de evaluación que realiza un auditor externo con el fin de verificar la razonabilidad, exactitud y cumplimiento normativo del estado de una entidad. Este procedimiento se efectúa conforme a normas internacionales de auditoría y busca brindar confianza a los usuarios externos —como inversionistas, entidades gubernamentales o acreedores— sobre la veracidad de la información financiera presentada. A diferencia de la auditoría interna, la auditoría externa es ejecutada por profesionales ajenos a la organización y su informe final tiene valor legal y contable (Arens, Elder & Beasley, 2018).

2.3.5. Auditoría informática

La auditoría informática es un proceso donde se busca analizar y evaluar los sistemas de información y a su vez la infraestructura tecnológica de una empresa u organización con el objetivo de evaluar su estado, seguridad y eficiencia en el uso de los recursos informáticos. Su objetivo principal es verificar que los sistemas salvaguarden los activos de la empresa, mantengan la integridad de los datos y cumplan con las leyes y normativas vigentes, además de asegurar que los recursos tecnológicos se utilicen de manera óptima para apoyar los objetivos organizacionales (Icesi, 2023). Este tipo de auditoría abarca tanto los activos físicos, como hardware y software, como las prácticas y controles implementados para proteger la información y garantizar la continuidad operativa (Economipedia, 2020). La auditoría informática también se caracteriza por ser preventiva, identificando vulnerabilidades y riesgos antes de que se materialicen, lo que permite tomar acciones correctivas oportunas para minimizar impactos negativos (Ibaiscanbit, s.f.). Para su ejecución, es fundamental que los auditores cuenten con formación específica en tecnología y auditoría, ya que deben evaluar desde la configuración

técnica hasta el uso adecuado por parte del personal (Economipedia, 2020; Ikusi, 2023). Además, la aplicación de estándares como lo son COBIT, ITIL o COSO facilita la ejecución de auditorías efectivas y alineadas a normativas internacionales. En definitiva, la auditoría informática es una herramienta clave para garantizar la seguridad, eficiencia y cumplimiento normativo en el entorno digital de las organizaciones, contribuyendo a la protección de sus activos y a la mejora continua de sus procesos tecnológicos (World Campus Saint Leo, 2024).

2.3.6. Control interno

El control interno informático es un sistema integrado dentro del proceso administrativo que abarca la planeación, organización, dirección y supervisión de las operaciones relacionadas con los recursos tecnológicos, con el propósito de proteger dichos recursos y optimizar la economía, eficiencia y efectividad de los procesos automatizados (Pinilla, 2025). Según el Informe COSO, el control interno se define como el conjunto de normas, procedimientos, prácticas y estructuras organizativas diseñadas para proporcionar una seguridad razonable de que los objetivos de la organización se cumplirán, y que los eventos no deseados serán prevenidos, detectados y corregidos (Plattini, citado en Scribd, 2025). En el ámbito informático, este control se materializa a través de controles manuales, realizados por el personal, y controles automáticos, incorporados en el software y sistemas de gestión, que buscan prevenir, detectar y corregir errores o irregularidades que puedan afectar el funcionamiento y la seguridad de los sistemas (Noris14, 2011). Además, el control interno informático incluye la definición y cumplimiento de políticas, normas y procedimientos que regulan la operación de sistemas, la seguridad informática, la administración de redes y el desarrollo de software, garantizando la confiabilidad, integridad y disponibilidad de la información (Universidad Nacional José Faustino Sánchez Carrión, 2024). Este sistema debe ser dinámico, adaptándose a los cambios tecnológicos y

organizacionales mediante un ciclo continuo de identificación de riesgos, evaluación de controles, pruebas y optimización, para asegurar la eficacia y eficiencia de los procesos tecnológicos (GBTEC, 2024). En suma, el control interno informático es esencial para proteger los activos digitales, asegurar la continuidad operativa y apoyar el cumplimiento normativo dentro de las organizaciones modernas.

El control interno informático es un sistema integrado dentro del proceso administrativo que abarca la planeación, organización, dirección y supervisión de las operaciones relacionadas con los recursos tecnológicos, con el propósito de proteger dichos recursos y optimizar la economía, eficiencia y efectividad de los procesos automatizados (Pinilla, 2025). Según el Informe COSO, el control interno se define como el conjunto de normas, procedimientos, prácticas y estructuras organizativas diseñadas para proporcionar una seguridad razonable de que los objetivos de la organización se cumplirán, y que los eventos no deseados serán prevenidos, detectados y corregidos (Plattini, citado en Scribd, 2025). En el ámbito informático, este control se materializa a través de controles manuales, realizados por el personal, y controles automáticos, incorporados en el software y sistemas de gestión, que buscan prevenir, detectar y corregir errores o irregularidades que puedan afectar el funcionamiento y la seguridad de los sistemas (Noris14, 2011). Además, el control interno informático incluye la definición y cumplimiento de políticas, normas y procedimientos que regulan la operación de sistemas, la seguridad informática, la administración de redes y el desarrollo de software, garantizando la confiabilidad, integridad y disponibilidad de la información (Universidad Nacional José Faustino Sánchez Carrión, 2024). Este sistema debe ser dinámico, adaptándose a los cambios tecnológicos y organizacionales mediante un ciclo continuo de identificación de riesgos, evaluación de controles, pruebas y optimización, para asegurar la eficacia y eficiencia de los procesos

tecnológicos (GBTEC, 2024). En suma, el control interno informático es esencial para proteger los activos digitales, asegurar la continuidad operativa y apoyar el cumplimiento normativo dentro de las organizaciones modernas.

2.3.7. Tipos de control

Los controles informáticos son mecanismos, políticas y procedimientos implementados para proteger los sistemas de información de una organización, garantizando la confidencialidad, integridad y disponibilidad de los datos. Estos controles se clasifican comúnmente en tres tipos principales: controles preventivos, identificativos y correctivos.

- Los controles preventivos, buscan impedir que ocurran incidentes o accesos no autorizados. Ejemplos promover el uso de contraseñas seguras, firewalls y la capacitación en seguridad.

- Los controles identificativos, tienen como objetivo identificar y alertar sobre la ocurrencia de incidentes o irregularidades. Entre ellos se encuentran los sistemas de monitoreo, auditorías y registros de eventos.

- Los controles correctivos son los que se ejecutan una vez concretado un riesgo, con el fin de mitigar sus efectos y restaurar la normalidad. Esto incluye planes de recuperación ante desastres y respaldo de información.

Estos controles son fundamentales en el marco de la auditoría de sistemas y la gestión de riesgos tecnológicos, y están alineados con estándares internacionales como COBIT y NIST (Romney & Steinbart, 2021).

2.3.8. Riesgos

Los riesgos en seguridad informática se refieren a las posibles amenazas, vulnerabilidades o debilidades presentes en los sistemas, redes, aplicaciones y datos de una organización que pueden ser explotados por atacantes para causar daños, pérdidas o interrupciones en las operaciones (Ticnova, 2024). Estos riesgos incluyen una amplia variedad de ataques como malware, ransomware, phishing, ataques de denegación de servicio (DDoS), y accesos no autorizados, que ponen en peligro la confidencialidad, integridad y disponibilidad de la información (Bitso, 2023; InvGate, 2024). La vulnerabilidad en los sistemas, entendida como debilidades en el diseño, implementación o gestión, facilita la explotación de estos riesgos, lo que puede derivar en pérdidas financieras significativas, daños a la reputación y violaciones a la privacidad (Smowl, 2025). Por ello, es fundamental que las organizaciones implementen programas de gestión de riesgos y vulnerabilidades que permitan identificar, evaluar y mitigar estos peligros, garantizando así la continuidad operativa y el cumplimiento normativo en un entorno digital cada vez más complejo y sofisticado (Worldsys, 2023; Innevo, 2024). En suma, comprender y gestionar los riesgos en seguridad informática es clave para proteger los activos digitales y mantener la confianza de usuarios y clientes frente a las crecientes amenazas cibernéticas.

2.3.9. metodología MAGERIT

MAGERIT es un método destinado al análisis y manejo de riesgos, que fue desarrollado como un estudio de riesgos y el procedimiento establecido por el Consejo Superior de Administración Electrónica de España. Proporciona un enfoque específico para examinar los riesgos asociados con el uso de innovaciones en datos y comunicación para implementar las medidas de control más eficaces que ayuden a reducir estos riesgos. Además, dispone de un

documento exhaustivo que compila tácticas y ejemplos sobre cómo llevar a cabo el análisis de riesgos.

Según Gusmán (2019), MAGERIT se fundamenta en separar el impacto que una amenaza de seguridad puede ocasionar en una organización, con el objetivo de identificar los riesgos que pueden afectar a la entidad y las vulnerabilidades que pueden ser explotadas por estos riesgos, logrando así una base razonable y clara de las acciones preventivas y correctivas más apropiadas.

2.3.10. COSO 2013

Según (Martinez, 2014) indica que la Metodología COSO "se dedica a desarrollar marcos y orientaciones para mejorar el desempeño organizacional y la supervisión, con el objetivo de reducir riesgos" (página 4)

La metodología COSO 2013 tiene los siguientes componentes:

I. Ambiente de Control, en el cual se desarrollan todas las actividades bajo la gestión administrativa, este ambiente de control es influenciado por ambientes internos y externos, en el cual intervienen factores como la historia de la empresa, sus valores, el mercado y el ambiente competitivo. En este componente se evalúan los riesgos para el cumplimiento de objetivos de la empresa.

II. Evaluación de Riesgo, este componente permite identificar los riesgos y evaluarlos desde dos perspectivas: probabilidad e impacto de estos, por lo cual es importante analizarlos de manera individual.

III. Actividades de Control, se constituye por políticas y procedimientos que permiten llevar respuestas inmediatas de la gerencia ante los riesgos identificados. En

estas actividades se ven involucradas todas las áreas de la empresa donde se ejecutan diferentes actividades de control que permiten la continuidad de las actividades.

IV. Sistema de Información y Comunicación, en este componente se identifica, obtiene y comunica de manera adecuada la información dentro de un margen corto de tiempo, esto permite llevar a cabo las responsabilidades a cada miembro que conforma el departamento o empresa.

V. Actividades de Monitoreo o Supervisión, una vez que se lograron identificar los riesgos, este componente permite monitorear y revisar la correcta ejecución de cada tarea.

Por medio de la ilustración 2, se puede analizar cada componente del modelo COSO 2013.

Ilustración 2

Modelo COSO 2013

Nota. Adaptada de MARCO INTEGRADO DE CONTROL INTERNO. MODELO COSO III (p. 15), por C. P. Rafael González Martínez, 2014

2.3.11. Norma de estandarización ISO 27002

La norma ISO 27002 para los sistemas de gestión de seguridad de la información es fácil de poner en práctica, automatizar y mantener utilizando la plataforma tecnológica de ISO Tools. Con ISO Tools, se satisfacen todos los requisitos que giran en torno al ciclo PHVA, que representa planificar, ejecutar, verificar y actuar. Para que esto se logre, es necesario establecer, llevar a cabo, conservar y mejorar el sistema de gestión de la seguridad de la información, así como cumplir de manera complementaria con las buenas prácticas o controles descritos en la ISO 27002. (De Santiago Bartolomé, 2019) La seguridad de la información según la norma ISO 27001, se fundamenta en proteger su confidencialidad, integridad y disponibilidad, así como la de los sistemas utilizados para su manejo.

• Confidencialidad: la información se mantiene lejos del alcance y no trasciende a personas, organizaciones o procesos sin autorización.

• Integridad: permite asegurar que la información y sus técnicas permanezcan intactos y completos a lo largo del proceso.

• Disponibilidad: permite el acceso y uso de la información a sistemas por parte de los usuarios o procesos autorizados siempre que se necesite.

2.3.12. Seguridad de la información

La seguridad de la información se define como el conjunto de medidas, procedimientos y tecnologías destinadas a proteger la información contra accesos no autorizados, uso indebido, alteraciones, interrupciones o destrucciones, garantizando así su confidencialidad, integridad y disponibilidad (Microsoft, 2024). Esta disciplina abarca todas las aristas de la informática, tanto físicas como lógicas. IBM (2024) señala que la seguridad de la información protege activos

críticos como datos financieros, personales o confidenciales a lo largo de todo su ciclo de vida, supervisando infraestructura, software y procesos de auditoría y archivado. Además, la seguridad de la información evoluciona continuamente para enfrentar un panorama de amenazas en constante cambio, requiriendo la colaboración de múltiples equipos para actualizar tecnologías y procedimientos (IBM, 2024). Telefónica (2024) destaca que sus elementos clave incluyen la seguridad física, el control de acceso, la ciberseguridad, la criptografía y la recuperación ante desastres, lo que permite a las organizaciones mantener la continuidad operativa y la confianza de sus usuarios. En suma, la seguridad de la información es esencial para proteger la privacidad individual y organizacional, evitar fraudes y pérdidas económicas, y garantizar el cumplimiento normativo en un mundo cada vez más interconectado (Slack, 2024).

2.3.13. Encuesta

Según Cabrera, D. (2013). La encuesta es usada como herramienta de investigación, permitiendo obtener información esencial al momento de ejecutar un levantamiento de línea base, esto permite recolectar las diferentes perspectivas de la población encuestada en un tema específico.

Por esto es importante el uso de esta herramienta para la recolección de información desde los colaboradores vinculados al lugar donde se está implementado el proceso de auditoría.

2.3.14. Nmap.

Según (Nmap, s.f.). indica que “es una herramienta de código abierto para exploración de red y auditoría de seguridad”. Esto permite explorar redes, comprobando su tráfico y seguridad de una manera eficiente. Su fuerte es analizar redes amplias, sin embargo, permite el escaneo de

un equipo único. Nmap actúa enviando paquetes IP “crudos” para poder identificar qué dispositivos están activos, qué sistemas operativos están corriendo en estos equipos y de manera complementaria si existe algún cortafuegos activo. Esta es una herramienta usada en auditorías de seguridad informática y de uso cotidiano en el levantamiento de inventario de activos, generando reportes generales o detallados.

2.3.15. WireShark.

De acuerdo a (WireShark.org, s.f.) es un analizador de paquetes de red, que permite ver a detalle todo lo que circula por una red, permitiendo capturar cada conexión de un determinado rango. Siendo su función principal la captura de paquetes, permite al usuario observar de manera clara y detallada, un paquete en específico, logrando ser entendible para quienes elijan esta herramienta como complemento en un proceso de análisis de red.

Adicionalmente, permite filtrar, explorar y comprender diferentes protocolos como TCP, UDP, HTTP, entre otros; generando una oportunidad para descubrir qué hay detrás de cada conexión generada en la red, lo que convierte a esta herramienta como un apoyo profesional tanto como una herramienta de aprendizaje.

2.4 Conclusiones relacionadas al marco teórico

Según los estudios realizados en relación con el marco teórico, se presentan a continuación las conclusiones relevantes divididas en secciones:

Antecedentes históricos:

La evolución de la auditoría informática se alinea en un contexto histórico de creciente dependencia entre la tecnología y digitalización en las empresas. De manera inicial, una auditoría se concentraba en aspectos financieros y físicos, pero con los avances tecnológicos y la incorporación de nuevos sistemas informáticos, surge la necesidad de aplicar estos métodos hacia la seguridad de la información y los sistemas automatizados. En el caso específico de Sportmancar Manta, esta evolución refleja la necesidad relevante de incorporar controles internos que no solo protejan los activos físicos (equipos, infraestructuras), sino que también salvaguarden la integridad, confidencialidad y disponibilidad de la información digital. En este marco histórico se muestran cómo las amenazas informáticas, desde accesos no autorizados hasta fallos en los sistemas, han obligado a las empresas a ejecutar auditorías más completas y adaptadas a la realidad tecnológica, promoviendo un enfoque completo que fortalezca todas las áreas donde se usa de manera esencial los recursos informáticos.

Investigaciones relacionadas al tema:

Las investigaciones mencionadas en el marco teórico resaltan el impacto positivo que tiene la ejecución de auditorías informáticas con enfoque a la seguridad de la información. Diversas fuentes indican que cuando se aplican controles internos adecuados y se adoptan estándares reconocidos internacionalmente (como ISO 270012 o COBIT), las empresas logran reducir en gran volumen las vulnerabilidades relacionadas a las amenazas internas y externas. En específico, en el caso de pequeñas y medianas empresas semejantes a Sportmancar Manta, se evidencia que el fortalecimiento integral

de la seguridad física y lógica reduce la probabilidad de incidentes que puedan comprometer la continuidad de las operaciones y la credibilidad organizacional. Asimismo, la bibliografía revisada valida que la capacitación del personal y la auditoría frecuente son factores importantes para mantener la efectividad en el control interno, sugiriendo que la ejecución de auditorías informáticas formales se relacione de manera directa en beneficios específicos como la mitigación y eliminación de riesgos, optimización de recursos informáticos y una mejora en la toma de decisiones informadas.

Definiciones conceptuales:

El análisis de las definiciones teóricas brinda una perspectiva clara y detallada del entorno general que involucra una auditoría informática. Los conceptos vinculados a la seguridad física y lógica tienen relación entre sí: por una parte, la seguridad física protege los elementos tangibles como la infraestructura, los equipos informáticos y las entradas físicas a cualquier departamento de una empresa, por otra parte, la protección lógica incluye estrategias de protección de los sistemas, software y datos manejados de manera digital, mediante el uso de herramientas como firewall, antivirus, controles de acceso y validación de datos. Igualmente, se puntualizan ideas relacionadas a la gestión de peligros, los controles internos y las normas aplicables, que forman la estructura fundamental para llevar a cabo la auditoría. Esta base conceptual muestra la conexión entre la identidad, la integridad, la accesibilidad y la privacidad de los datos, lo cual ayuda a que la auditoría no solo identifique vulnerabilidades, sino que también permita identificar estratégicas contextualizadas para fortalecer la seguridad de la información en Sportmancar Manta de manera completa y sostenible.

CAPÍTULO III

Marco investigativo

3.1 Introducción

En este capítulo se detallan los tipos y métodos de investigación utilizados para la recopilación y análisis de datos. Posteriormente, estos datos fueron tabulados para generar indicadores que permitan definir parámetros orientados a mejorar la seguridad informática dentro de la institución. Las estrategias empleadas para la recolección y aplicación de la información son fundamentales, ya que permiten focalizarse en el área específica de estudio dentro del problema general, facilitando un análisis progresivo desde una visión amplia hacia aspectos particulares. Esto contribuye a tomar decisiones informadas para definir buenas prácticas de control interno en seguridad física y lógica. Entre los instrumentos utilizados para recopilar los datos se emplearon entrevistas y encuestas: la entrevista se realizó al responsable de TI, quien posee la experiencia necesaria para ejercer dicha función y aportar con información valiosa para obtener resultados efectivos. Por otro lado, las encuestas fueron dirigidas a los colaboradores de la empresa, quienes constituyen un grupo objetivo de la auditoría y fuentes de información debido a la metodología aplicada para este proceso.

3.2 Tipo de investigación

3.2.1. Investigación bibliográfica

La investigación bibliográfica es una metodología fundamental que permite recopilar, analizar y sintetizar información proveniente de fuentes documentales confiables, facilitando así la construcción del conocimiento teórico necesario para el desarrollo de un estudio (Matos, 2020). Este tipo de investigación se centra en revisar libros, artículos, tesis y otros materiales ya existentes, con el propósito de fundamentar el problema de investigación y justificar su relevancia.

Con la finalidad de obtener datos verídicos de textos y publicaciones relacionados a una auditoría informática y otros elementos tanto físicos como lógicos que apoyan el enfoque del proyecto, se empleó este enfoque investigativo para examinar la bibliografía relacionada con el tema en cuestión.

3.2.2. Investigación cuantitativa

De acuerdo con Neill y Suárez (2018), la investigación cuantitativa es un método organizado para reunir y examinar datos provenientes de diversas fuentes de recolección, con la finalidad de obtener información sólida a través del análisis estadístico, presentándola en forma de gráficos y cifras representativas. Este tipo de investigación sigue un formato preestablecido, bien estructurado y analizado para que la recolección de datos sea más efectiva, eficiente y asegure su utilidad.

De acuerdo con lo mencionado anteriormente sobre la investigación cuantitativa, en el presente trabajo se aplicó este método para la recolección y análisis de datos y así evaluar la implementación de acciones luego de la ejecución de la auditoría informática.

Este análisis cuantitativo se manifiesta en la recogida de información, análisis e interpretación de los datos obtenidos por medio de una encuesta llevada a cabo a través de un cuestionario en línea que se encuentra en el anexo 1

3.3 Método de investigación

Basándonos en los tipos de estudios realizados y descritos previamente, podemos reconocer los enfoques de investigación aplicados en este trabajo, los cuales son:

3.3.1. Método analítico

El enfoque analítico, por otro lado, se fundamenta en la evaluación, fragmentación y examen minucioso de un objeto, por lo que este enfoque inicia con un análisis general y descompone la información en componentes más reducidos para investigar las causas y consecuencias del estudio en curso. Posteriormente, este enfoque conecta cada acción, elaborando un resumen general del caso o fenómeno que se está investigando. (Sosa, 2018)

Método utilizado en esta auditoría que consiste en examinar y analizar minuciosamente los temas investigados y la recopilación de datos que resultaron ser de gran relevancia. Esto facilita la identificación de aspectos más profundos relacionados con el fortalecimiento de la seguridad física y lógica, ya que a través de este método se clasifica la información adquirida de forma detallada, permitiendo así reducirla únicamente en lo esencial.

3.3.2. Método deductivo

Utilizando datos estadísticos obtenidos a través de la observación, el registro y el análisis comparativo durante la investigación, se aplica la técnica inductiva en el proceso de establecer conexiones universales a partir de situaciones particulares. De acuerdo con Westrecher (2020), el enfoque deductivo se asemeja más a la aplicación de la lógica para alcanzar un resultado, ya que la validez de la conclusión final dependerá de la precisión de las premisas que se han utilizado como fundamento. Este enfoque puede emplearse de

manera directa o indirecta y consiste en deducir una conclusión a partir de premisas que se consideran verdaderas.

Método utilizado para reunir información, ya que realiza un estudio amplio de los datos para que puedan ser examinados desde una perspectiva general y, de esta forma, se obtiene información más concreta acerca procesos de control interno, riesgos y amenazas que anteriormente se mencionaron como puntos importantes en esta auditoría.

3.4 Fuente de información de datos

3.4.1. Fuentes primarias

Para el desarrollo de este trabajo, se identificó la necesidad de aplicar fuentes primarias de información, tales como la entrevista y una encuesta estructurada. Las herramientas en mención, se destacan por el hecho de que su mecanismo es de vinculación directa entre el entrevistador y la fuente, facilitando la obtención de respuestas objetivas y claras, evitando palabras redundantes o intermediarios durante su ejecución.

Adicionalmente, se considera relevante lo siguiente:

- Información resultante de la observación directa ejecutada en el trabajo en campo para la obtención de información relevante y esencial.
- Resultados cuantitativos de la encuesta.

Por otro lado, se consideraron como fuentes secundarias todos los sitios web, libros, artículos de revistas, proyectos de titulación de tercer y cuarto nivel, blogs, entre otros, como

herramientas para recopilar información tanto documental como teórica, esto permitió el enriquecimiento de la investigación llevada a cabo.

3.5 Estrategia operacional para recolectar datos

3.5.1 Población – segmentación

Para la recopilación de datos, se tomó como población a los colaboradores de Sportmancar Manta, quienes desempeñan funciones administrativas, operativas y tecnológicas dentro de la institución. Su participación fue clave para identificar las prácticas actuales en materia de seguridad informática y control interno, así como para detectar falencias y necesidades específicas en el manejo de los recursos tecnológicos.

3.5.2. Técnica de muestreo

La técnica de muestreo se realizó mediante la aplicación de una entrevista al responsable de TI en conjunto a la aplicación de una encuesta dirigida a los colaboradores de la empresa, esto permite obtener información específica que fortalece la investigación que se realiza.

3.5.3. Tamaño de muestra

Los instrumentos de muestreo fueron aplicados a 15 colaboradores de la empresa Sportmancar Manta, que, por medio de las respuestas obtenidas, permitieron establecer estrategias para fortalecer la seguridad física y lógica en la institución.

3.5.4. Análisis de las herramientas de recolección de información

A continuación, se analizan los métodos utilizados en este trabajo para recopilar datos, con un enfoque especial en la encuesta, evidenciando su efectividad y la veracidad en la adquisición de información.

Encuesta: Con el objetivo de obtener información relevante actual relacionada a la seguridad física y lógica de Sportmancar Manta, se implementó un formulario en línea el cual consta de preguntas claves que dan como resultados datos reales y claros.

Complementando lo anterior, según Torres, Paz, & Salazar (2020), señalan a la encuesta como un método importante para la recolección de datos en una investigación, proporcionando una visión periférica más profunda sobre el tema a tratar y a su vez permite obtener una información versátil y eficaz.

Entrevista: Dentro de cada entrevista hay dos papeles: el entrevistador y el entrevistado. El entrevistador hace preguntas basadas en sus intereses, mientras que el entrevistado se encarga de responder. En el transcurso de una entrevista, el entrevistado puede ofrecer la información necesaria, explicar o argumentar datos; a veces, simplemente puede compartir su perspectiva o relatos relacionados (Seid, 2016).

En el desarrollo de este trabajo de titulación, se llevó a cabo una entrevista con el encargado de TI, con el fin de obtener información relevante sobre aspectos de seguridad o deficiencias que presente la institución.

3.6 Análisis y presentación de resultados

Los resultados obtenidos que se detallan a continuación, fueron recopilados mediante la entrevista y la encuesta; por una parte, por medio de la entrevista se buscó recopilar información necesaria sobre el estado actual de las situaciones vinculadas al control interno, por otra parte, a través de la encuesta se busca identificar el nivel de conocimiento del personal relacionado a la seguridad de la información y los reglamentos internos, quienes usan los recursos informáticos diariamente.

3.6.1. Presentación y descripción de los resultados obtenidos

3.6.1.1 Entrevista: La entrevista está dirigida al responsable de TI de Sportmancar Manta, el cual es un punto clave dentro del control interno relacionado al uso de los equipos informáticos, a continuación, en la tabla 2 se detallan las preguntas con sus respectivas respuestas, alineadas al modelo COSO 2013.

Tabla 2

Resultados de la entrevista

N°	Preguntas relacionadas a la seguridad de la información	Respuesta
1	En los últimos dos años ¿cuántas veces se ha ejecutado una auditoría informática?	En ninguna ocasión, únicamente se verifica de manera interna en lo posible que todo marche de manera adecuada.
2	¿Cómo describiría las condiciones actuales de los equipos informáticos?	Los equipos en su mayoría tienen varios años de funcionamiento, actualmente

		se ha logrado adquirir nuevos equipos, pero estos solo representan un 30% de la totalidad.
3	¿Se han reportado problemas técnicos por parte de los colaboradores?	Si, en su mayoría reportan fallas en la conexión a internet, esto debido a que existen cables de red que no cuentan con un empaquetado adecuado o se encuentran visibles.
4	¿Cuáles son los problemas técnicos más comunes que han enfrentado?	Hemos presentado caída del servicio de internet en la red local, mal funcionamiento de los equipos de impresión y por último fallas en las computadoras usadas por el área de atención al cliente.
5	¿Qué medidas de seguridad se implementan para proteger la información y datos almacenados en las computadoras?	Actualmente no existen controles de acceso a las ubicaciones del rack de videovigilancia y sus servidores. En los equipos que funcionan como servidores para el área de caja y base de datos de estudiantes, se encuentran dentro del área de TI, esto permite salvaguardar de manera parcial estos activos.

6	¿Cómo se gestiona y controla el acceso a Internet en la empresa?	Existen 3 redes locales, una destinada únicamente para estudiantes, la segunda para colaboradores de la empresa relacionados al área de atención al cliente y por último una tercera red correspondiente al área de TI. Cada una maneja una contraseña diferenciada la cual se actualiza de manera recurrente para prevenir accesos no autorizados, se ha solicitado a Gerencia la compra de equipos de mayor nivel de seguridad que permitan fortalecer la red local, esto está por ejecutarse en los próximos 4 meses.
7	¿Existen políticas claras sobre el uso de los equipos pertenecientes a la empresa?	Desconozco, al momento no tengo conocimiento de aquello.
8	¿Se realiza algún tipo de mantenimiento preventivo en las computadoras de la empresa? ¿Con qué frecuencia se lleva a cabo este mantenimiento?	Si, los mantenimientos preventivos se los realiza mínimo una vez al año para optimizar los equipos y alargar su vida útil, sin embargo, esto no queda registrado para un seguimiento adecuado.

9	¿Existe un plan de contingencia en caso de fallas significativas?	Si, existe un plan general de la empresa, sin embargo, no se ha actualizado a las modificaciones estructurales de las instalaciones. En los próximos 4 meses se hará una reestructuración física en la empresa por ende servirá para adecuar todo lo relacionado al plan de contingencia.
N°	**Preguntas relacionadas a los componentes del Modelo COSO 2013**	**Respuesta**
10	¿El responsable de TI supervisa el desarrollo y desempeño del control interno relacionado al uso de los equipos informáticos?	Si se realizan actividades de control interno, sin embargo, no existe ningún tipo de bitácora que respalde lo mencionado.
11	¿El área de TI ha establecido procesos para evaluar la probabilidad e impacto de los riesgos?	A la fecha no, considero que es un punto clave de mejora para nuestra área.
12	¿El área de TI ha implementado controles para mitigar los riesgos identificados?	Si, se ejecutan acciones, pero no existe ningún respaldo en documentos para respaldar lo mencionado.
13	¿El responsable de TI ha establecido actividades de control para prevenir o detectar errores, fallas o irregularidades relacionadas a los equipos informáticos?	Se realizan verificaciones semanales del correcto funcionamiento de los equipos, desde los usados en el área de atención al cliente, sistema de videovigilancia y demás, pero como mencionaba no se ha incorporado ningún mecanismo para el registro de las actividades de control.
14	¿Se documentan y comunican las actividades de control de la seguridad física y lógica?	No, no existen medios de verificación.

15	¿La información relevante se comunica de manera oportuna y efectiva a las partes interesadas, siendo estas Gerencia, Supervisión o Área de TI?	Los medios usados para comunicación de preferencia son vía WhatsApp, no se ha implementado ningún medio formal para la comunicación interna, se ha sugerido la compra de licencias para el uso de correo corporativo.
16	¿Existe un canal de comunicación o medio formal para reportar problemas relacionados a los equipos informáticos?	No, actualmente no se usa ningún medio formal.
17	¿El responsable de TI realiza evaluaciones periódicas del correcto funcionamiento de los equipos informáticos y la seguridad de la información?	Si, como lo mencionaba, se ejecutan de manera semanal.

3.6.1.2 Encuesta

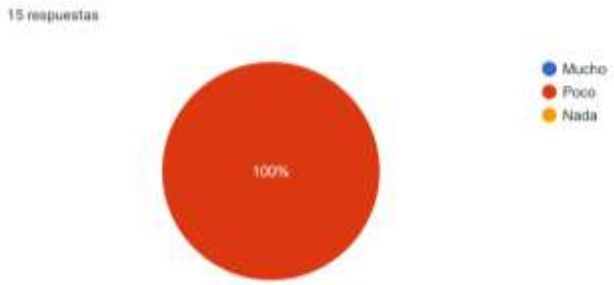
La encuesta consta de 10 preguntas, la cual está dirigida a todo el personal de Sportmancar que usa los equipos informáticos, y por ende es un punto clave en la seguridad de la información de manera interna.

Esta encuesta se ejecuta con el objetivo de identificar la necesidad de capacitar a todo el personal en buenas prácticas de uso de los recursos informáticos, seguridad de la información y cuidados de los equipos; lo cual permitirá fortalecer desde dentro del entorno de los colaboradores y a su vez generar conciencia sobre la importancia de involucrar a todos en el control interno de la empresa, iniciando desde las buenas prácticas de cada colaborador.

Pregunta 1: ¿Conoce sobre la seguridad informática?

Ilustración 3

Resultados pregunta 1 Encuesta



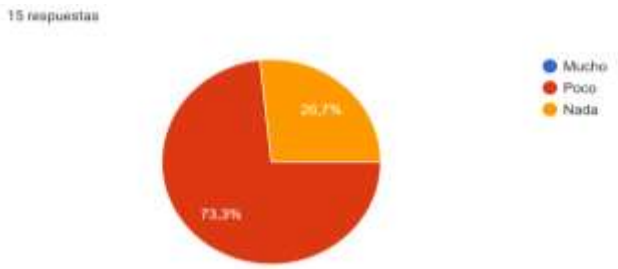
Análisis: De acuerdo a la ilustración 3, el 100% de los encuestados menciona que conoce poco sobre la seguridad informática.

Interpretación: Por medio de este resultado, se puede interpretar que la totalidad de las personas que trabajan en Sportmancar Manta, tienen poco conocimiento sobre la seguridad informática y cómo se relaciona con la protección de los activos.

Pregunta 2: ¿Conoce qué es ingeniería social?

Ilustración 4

Resultados pregunta 2 Encuesta



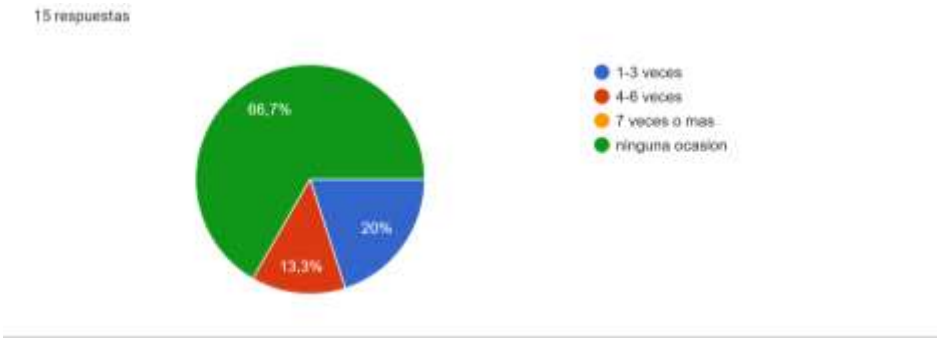
Análisis: Según la ilustración 4, el 26,7% de los encuestados menciona que no tiene conocimiento sobre ingeniería social, mientras el 73,3% menciona que conoce poco sobre su concepto.

Interpretación: A través de este resultado, se puede interpretar que la mayoría tiene poco conocimiento sobre ingeniería social, sin embargo, no son conscientes del impacto que puede causar un ataque mediante ingeniería en la empresa.

Pregunta 3: ¿Con qué frecuencia al año, ha sido infectado por un malware el equipo que usa en la empresa?

Ilustración 5

Resultados pregunta 3 Encuesta



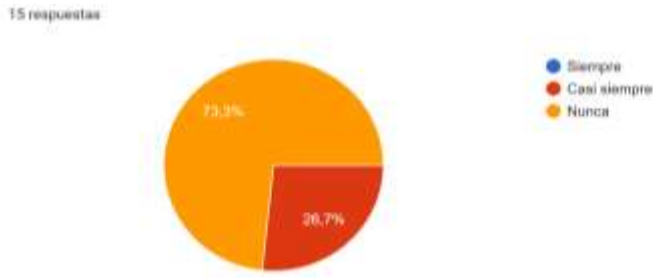
Análisis: De acuerdo a la ilustración 5, el 66,7% de los encuestados menciona que el equipo que usa en la empresa no ha sido infectado en alguna ocasión por malware, el 20% entre 1 a 3 ocasiones, y por último el 13,3% indica que su equipo se ha infectado entre 4 a 6 ocasiones durante el año.

Interpretación: A través de este resultado, se puede interpretar que la mayoría de colaboradores indica que el equipo usado en las actividades de la empresa, nunca ha sido infectado, mientras el 33,3% indica que al menos en 1 ocasión ha sido infectado el equipo informático.

Pregunta 4: ¿Ha instalado herramientas o programas sin darlo a conocer al responsable de TI?

Ilustración 6

Resultados pregunta 4 Encuesta



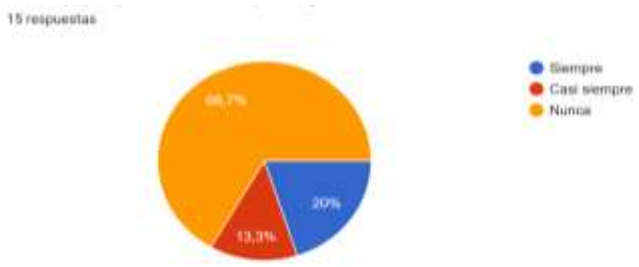
Análisis: Mediante la ilustración 6, se observa que el 73,3% de los encuestados menciona nunca ha instalado herramientas o programas en los equipos sin darlo a conocer al responsable de TI, mientras que el 26,7% casi siempre lo ha hecho.

Interpretación: Se puede interpretar que, en su mayoría, no tiene por práctica instalar software sin antes darlo a conocer al responsable de TI, sin embargo, existe un porcentaje de encuestados que al menos en alguna ocasión lo ha realizado.

Pregunta 5: El equipo que usa en la empresa, ¿cuenta con antivirus?

Ilustración 7

Resultados pregunta 5 Encuesta



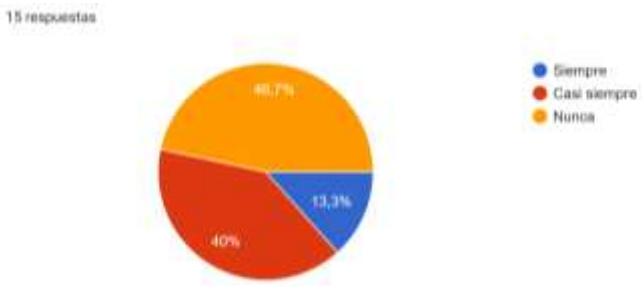
Análisis: Por medio de la ilustración 7, se entiende que el 66,7% de los encuestados indica el equipo que usa en las actividades laborales, nunca cuenta con antivirus, el 13,3% casi siempre cuenta con antivirus, y por último el 20% cuenta siempre con un antivirus en su equipo.

Interpretación: Por medio de estos resultados, se puede interpretar que la mayoría de los equipos nunca cuenta con un software antivirus que proteja a los equipos que son parte de la empresa.

Pregunta 6: ¿Se ha brindado mantenimiento periódico al equipo informático que usa en la empresa?

Ilustración 8

Resultados pregunta 6 Encuesta



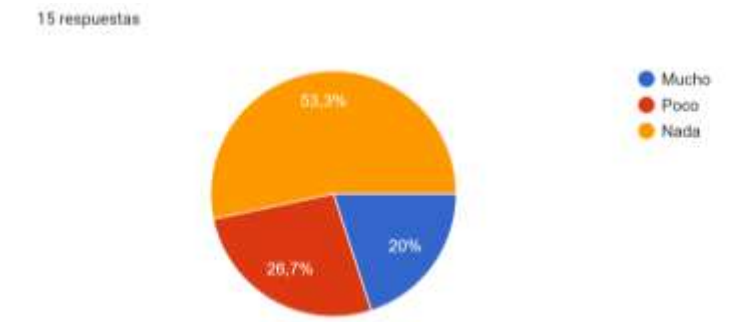
Análisis: La ilustración 8 indica que el 46,7% de los colaboradores menciona que nunca se ha brindado mantenimiento al equipo brindado por la empresa para el desarrollo de sus actividades, el 40% indica que casi siempre le han brindado un mantenimiento, y el 13,3% siempre le han realizado un mantenimiento a su equipo.

Interpretación: A través de estos resultados, se interpreta que a la mayoría de los equipos nunca se le ha realizado un mantenimiento que permita optimizar y por ende alargar la vida útil de estos dispositivos.

Pregunta 7: ¿Conoce cuáles son las recomendaciones para establecer una contraseña robusta?

Ilustración 9

Resultados pregunta 7 Encuesta



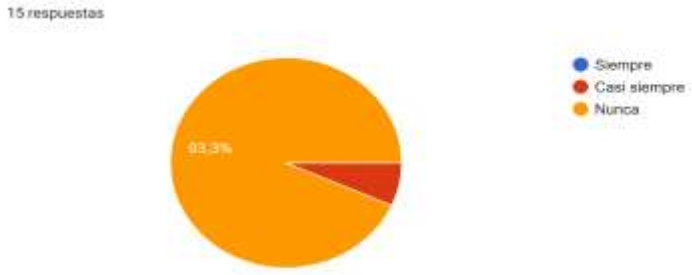
Análisis: Mediante la ilustración 9, se observa que el 53,3% de los colaboradores indica que no tiene conocimiento sobre las recomendaciones para establecer una contraseña robusta, el 26,7% tiene poco conocimiento sobre las recomendaciones y el 20% tiene mucho conocimiento acerca de las recomendaciones para una contraseña robusta.

Interpretación: Se puede interpretar por medio de estos resultados, que la mayoría de encuestados no tiene conocimiento sobre cómo establecer contraseñas seguras, esto relacionado a las contraseñas establecidas para el inicio de sesión en los equipos informáticos que usan en la empresa.

Pregunta 8: ¿Cambia la contraseña de ingreso al equipo informático de la empresa periódicamente?

Ilustración 10

Resultados pregunta 8 Encuesta



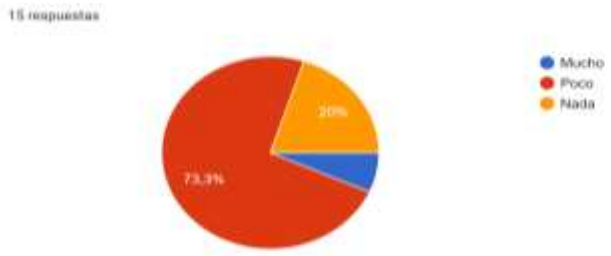
Análisis: Mediante la ilustración 10, vemos que el 93,3% de los encuestados nunca ha cambiado la contraseña de su equipo brindado por la empresa, mientras que el 6,7% casi siempre la cambia.

Interpretación: Se puede interpretar por medio de estos resultados, que la mayoría de encuestados no tiene como buena práctica el cambiar la contraseña en su equipo, mientras que una minoría lo realiza de manera poca frecuente.

Pregunta 9: ¿Conoce las recomendaciones para un buen uso de los equipos informáticos de la empresa?

Ilustración 11

Resultados pregunta 9 Encuesta



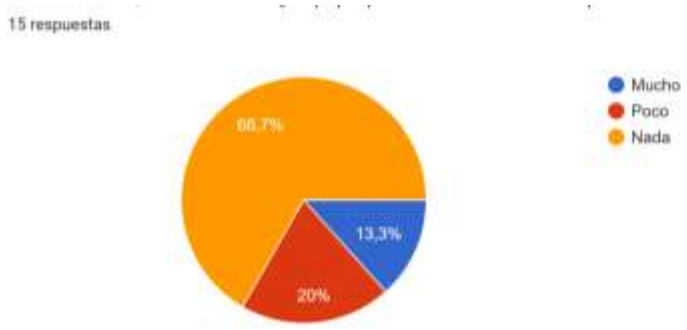
Análisis: A través de la ilustración 11, entendemos que el 73,3% de los encuestados tiene poco conocimiento sobre las recomendaciones para un buen uso de los equipos informáticos, el 20% no tiene conocimiento sobre estas recomendaciones, por último, el 6,7% tiene mucho conocimiento sobre las recomendaciones para un buen uso de los equipos informáticos.

Interpretación: Se puede interpretar que la mayoría de los encuestados tiene poco conocimiento sobre las recomendaciones para el buen uso de los equipos brindados por la empresa.

Pregunta 10: Conoce la existencia en el reglamento de Sportmancar Manta, donde se menciona el buen uso de los bienes, instalaciones y equipo pertenecientes a la empresa.

Ilustración 12

Resultados pregunta 10 Encuesta



Análisis: La ilustración 12 nos indica que el 66,7% de los encuestados no conoce sobre este apartado dentro del reglamento interno de la empresa, el 20% conoce poco y el 13,3% conoce mucho.

Interpretación: A través de estos resultados se puede interpretar que en su mayoría no conocían sobre la existencia de este reglamento y mucho menos de este literal, el porcentaje restante conoce sobre la existencia de este reglamento mas no del apartado en donde menciona la importancia de involucrar a todo el personal en el buen uso de los equipos de Sportmancar

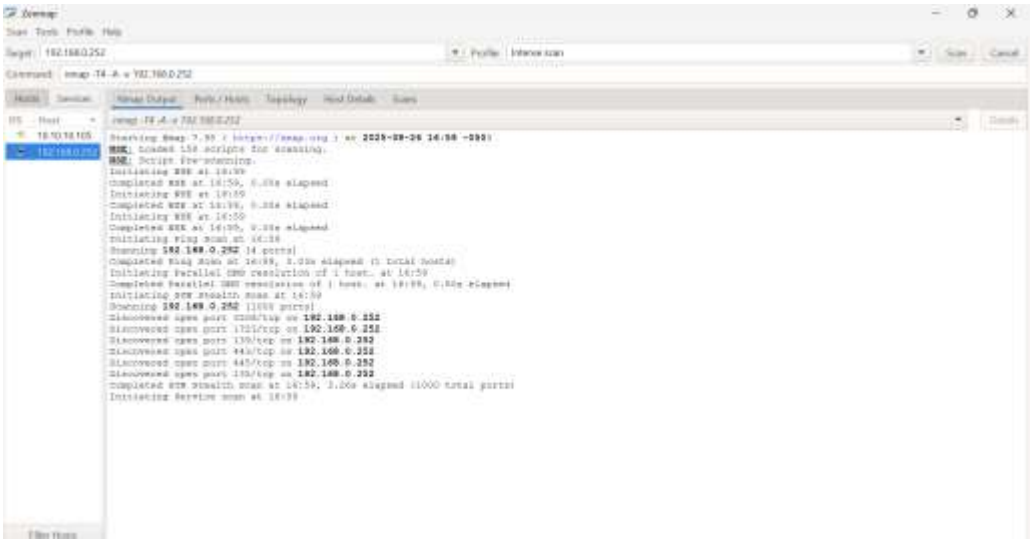
3.6.1.3 Análisis de resultados obtenidos en herramienta Nmap (tráfico de red y acceso a servidores):

Por medio de la aplicación de Nmap en las redes locales de Sportmancar Manta, se pudo determinar que la conexión a los servidores de estudiantes por un usuario con un dominio externo, es factible.

A continuación, se muestra el resultado en la ilustración 13, 14 y 15 relacionadas a la conexión hacia el servidor Estudiantes en Sportmancar Manta:

Ilustración 13

Ping realizado al servidor Estudiantes



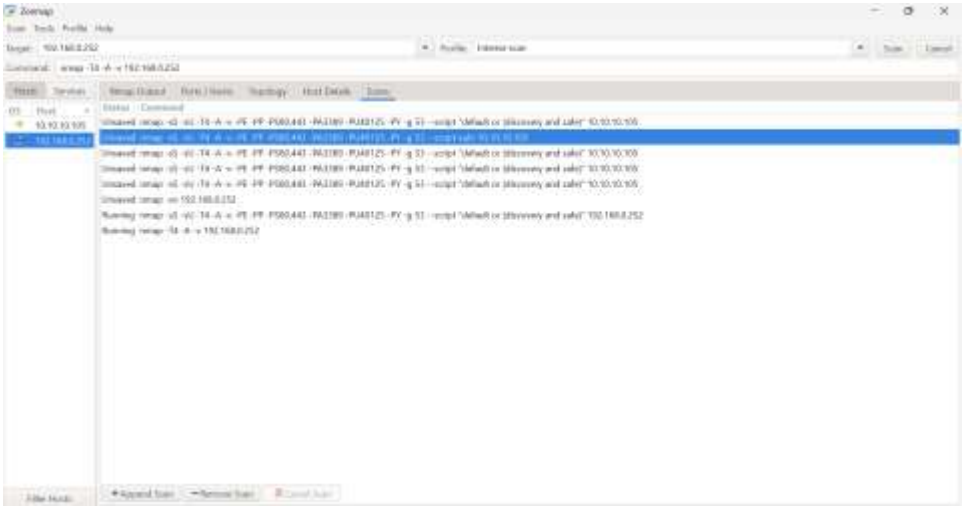
Nota. Por medio de esta ilustración, se comprueba que una maquina externa puede enviar paquetes hacia el servidor donde se encuentran alojados los datos de los estudiantes.

Ilustración 14

Topología de conexión a servidor Estudiantes

Ilustración 15

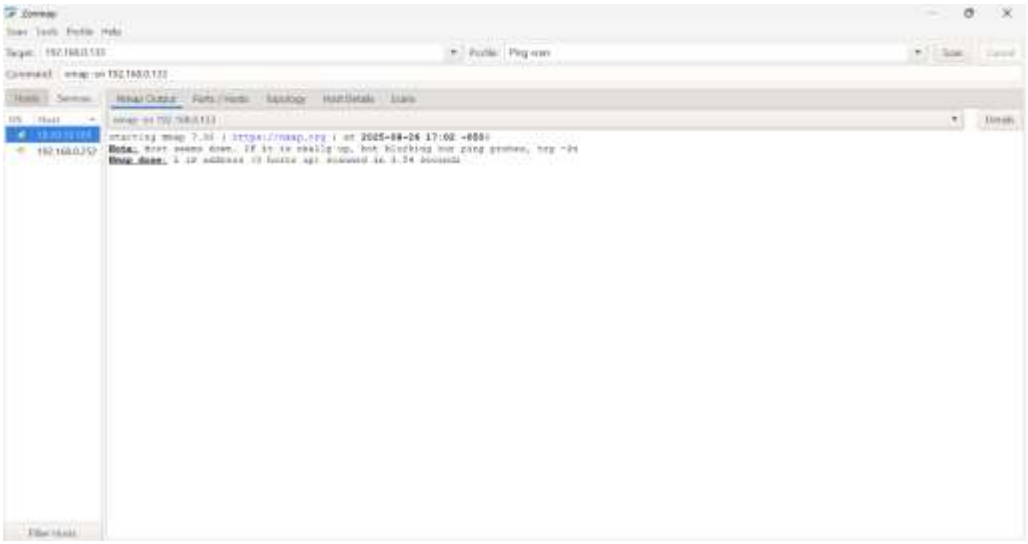
Resultados de escaneo mediante Nmap



Por otra parte, en las ilustraciones 16, 17 y 17 se muestran los resultados de la conexión al servidor contable:

Ilustración 16

Ping ejecutado a Servidor Contable



Nota. El ping enviado desde el computador de prueba con acceso hacia el servidor Contable fue rechazado, indica que se implementa un Firewall de protección

Ilustración 17

Puertos abiertos en Servidor Contable

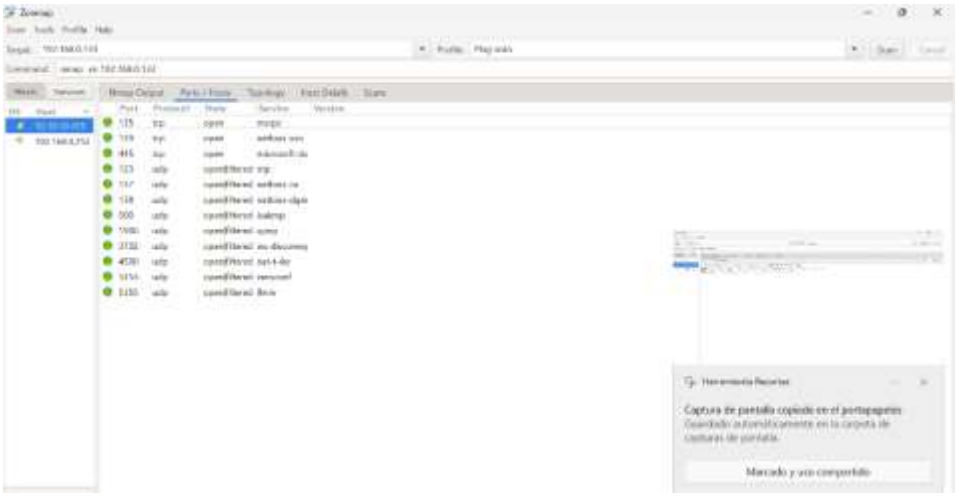
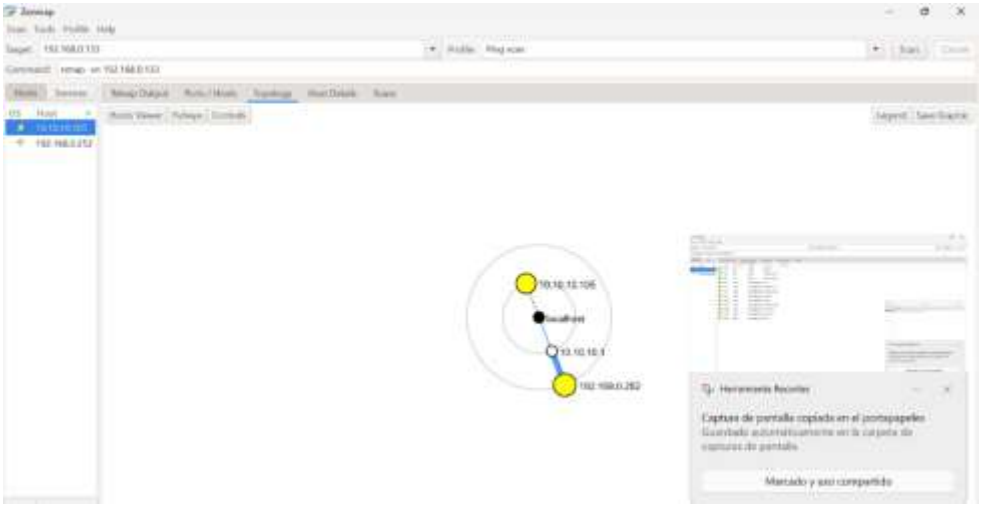


Ilustración 18

Topología de red de conexión a Servidor Contable



A través de este análisis implementando la herramienta Nmap, se puede identificar que la conexión hacia el servidor estudiantes es permitida debido a la falta de implementación de

firewall, por otra parte, el servidor Contable bloquea la señal debido a la protección que se brinda al activar el cortafuegos.

3.6.1.4 Análisis de resultados obtenidos en herramienta WireShark (conexión a puertos de la red local):

Por medio de las ilustraciones 19 y 20, se puede observar la falta de conexión a diferentes puertos de la red, local, esto quiere decir que existen equipos con intermitencia o inclusive terminales de puertos que no están en uso actualmente, dejando así una puerta abierta a la red.

Ilustración 19

Conexión a servidor estudiantes, paquete 5

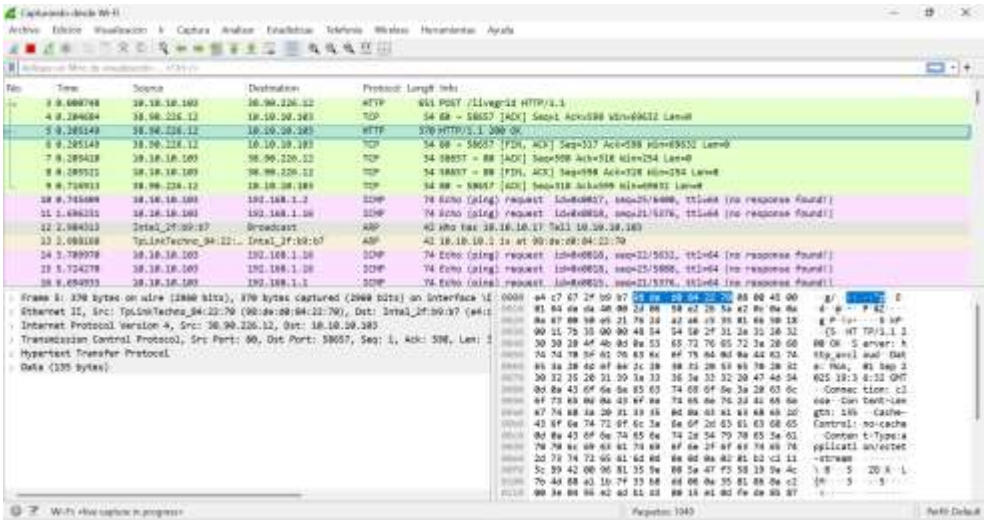
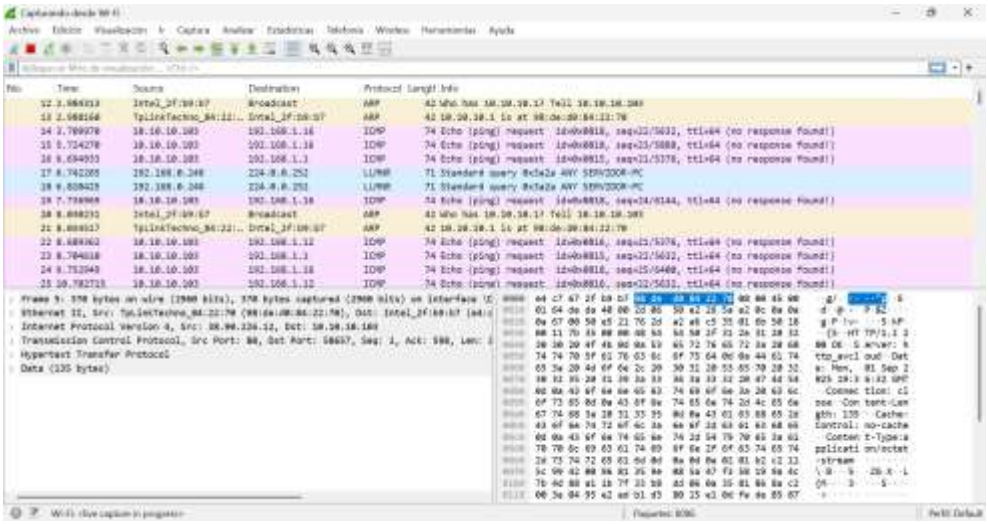


Ilustración 20

Puertos sin respuestas-paquetes 14-16



Por medio de la aplicación de la herramienta WireShark, se puede comprender que al momento existen puertos sin conexión debido a conexiones estructuradas sobre redes antiguas, es importante corregir este problema para optimizar la conexión entre dispositivos locales.

CAPÍTULO IV

Marco propositivo

4 Marco propositivo

4.1. Introducción

Se realizó un levantamiento de información esencial para identificar la problemática desde la raíz con el enfoque al fortalecimiento de la seguridad informática en Sportmancar Manta. Tras estructurar los datos, se avanzó con la ejecución de la auditoría. En esta sección de la investigación, se detallan los elementos que se utilizan en el proyecto, así como la metodología adoptada, en la cual se explican las diferentes etapas.

La presente propuesta tiene como objetivo ejecutar una auditoría informática en Sportmancar Manta, escuela de conducción ubicada en la ciudad de Manta, con el fin de fortalecer la seguridad física y lógica de sus sistemas informáticos y de su infraestructura tecnológica.

Este proceso se enmarca en el Modelo COSO 2013, el cual proporciona un marco integral para la evaluación del control interno, orientado a mejorar la eficacia operativa, la confiabilidad de la información financiera y el cumplimiento normativo. En complemento, se empleará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que permite identificar, analizar y gestionar los riesgos tecnológicos, proporcionando un enfoque estructurado para la toma de decisiones en materia de seguridad de la información.

La combinación de estos dos enfoques busca no solo evaluar la situación actual de los controles implementados en Sportmancar Manta, sino también proponer medidas correctivas y preventivas que contribuyan a la protección integral de los activos informáticos. De esta manera,

se busca garantizar un entorno tecnológico seguro, confiable y alineado con los objetivos institucionales, fortaleciendo al mismo tiempo la cultura organizacional hacia la gestión del riesgo y la mejora continua del control interno.

4.2. Descripción de la propuesta

En relación con el problema de investigación, se llevó a cabo la propuesta de la solución alineada al enfoque de la intervención el cual es fortalecer la seguridad física y lógica en las TI en Sportmancar Manta. Para la ejecución de este proyecto, fue necesario reunir información bibliográfica, la cual resultó fundamental para una investigación efectiva. En conjunto, se ejecutaron encuestas y entrevistas, ya que son herramientas que permiten conseguir datos precisos respecto al problema que se pretende resolver. Posterior a identificar los riesgos e identificar puntos de mejora, el próximo paso es implementar registros de control interno de mantenimientos y controles diarios en las TI, en paralelo para involucrar a todo el personal de acuerdo a lo indicado al Modelo COSO 20213, se capacita a todo el personal en dos contenidos:

- Cuidado y buen uso de las TI
- Seguridad Informática desde los diferentes roles

En este apartado se mencionan las vulnerabilidades identificadas y evalúa el riesgo asociado a cada una. Posteriormente, se explican los procedimientos a seguir para implementar buenas prácticas de seguridad informática.

En la ejecución de este trabajo, se basa en el Modelo COSO 2013, con el objetivo de identificar puntos de mejora en el control interno; en conjunto a la metodología MAGERIT, esta por su enfoque al análisis y a la administración de riesgos relacionados con la informática. La complementación de ambas permite englobar dos puntos fundamentales para el fortalecimiento de la seguridad física y lógica en Sportmancar Manta.

4.3 Determinación de recursos

4.3.1. Humanos

A continuación, en la tabla 3, se presenta un resumen de los recursos humanos involucrados en el desarrollo del presente trabajo de titulación.

Tabla 3

Tabla de recursos humanos

Recurso humano	Función	Especificaciones
Ing. Marco Ayoví Ramírez, PhD.	Docente facultad Ciencias de la vida y Tecnologías	Tutor del Proyecto de Titulación
Jonathan Adalberto Plúa Gutiérrez	Autor del Proyecto de Titulación.	Desarrollo del proyecto de titulación
Personal administrativo y de planta Sportmancar Manta	Encuestados - beneficiarios	Muestra de encuesta

4.3.2. Tecnológicos

En la tabla 4, se mencionan los recursos tecnológicos usados en el desarrollo del trabajo de titulación:

Tabla 4

Tabla de recursos tecnológicos

Recurso Tecnológico	Especificaciones	Servicios Externos
Computadora Portátil Lenovo	12th Gen Intel(R) Core (TM) i3-1215U (1.20 GHz) 8,00 GB (7,73 GB usable)	Internet Servicio de electricidad

4.3.3. Económicos

Para el desarrollo del presente trabajo fue necesario el uso de los siguientes recursos, detallados en las tablas 5 y 6:

Tabla 5

Recursos económicos-humanos

Recursos humanos	**Cantidad (horas)**	**Valor x hora**	**Total (dólares)**
Desarrollador del proyecto	400	$2,81	$1.124
Tutor del proyecto	60	$18,54	$1.118,40
	Total		$2.242,40

Tabla 6

Recursos económicos-tecnológicos

Recursos Tecnológicos	**Cantidad**	**Precio unitario**	**Total (dólares)**
Computador	1	$400	$400
Servicios externos	**Cantidad**	**Precio unitario**	**Total (dólares)**
Servicio de internet	1	$23	$23
Energía Eléctrica	1	$22	$22
	Total		$455

4.4 Etapas de acción para el desarrollo de la propuesta

En la ejecución de la auditoría se usa como base el Modelo COSO 2013, que permite analizar el control interno de la seguridad informática desde sus diferentes componentes, y a su vez permite involucrar a todo el personal de la empresa, a su vez se complementa con la metodología Magerit, debido a su enfoque de analizar y gestionar los riesgos de los sistemas de información.

Los activos de las empresas son recursos necesarios para la ejecución y desarrollo de las actividades diarias enfocadas al cumplimiento de objetivos internos, es por esto que es relevante fortalecer la seguridad física y lógica en Sportmancar Manta, esto partiendo desde un adecuado control interno diario e involucrar a todo el personal. De acuerdo al levantamiento de información inicial se permitió identificar que la implementación y desarrollo de esta auditoría basada en las metodologías en mención, permitirá controlar, reducir y eliminar riesgos y por consiguiente fortalecer la seguridad informática.

Por una parte, COSO 2013 permite:

- Evaluar el ambiente de control dentro de la organización
- Identificar y gestionar riesgos tecnológicos
- Establecer actividades de control efectivas para la seguridad física y lógica
- Asegurar la calidad de la información y la comunicación interna
- Monitorear continuamente la eficacia del control interno

Todo ello con el objetivo de fortalecer la protección de los activos informáticos

Por otra parte, la metodología Magerit se enfoca a los siguientes objetivos:

- Sensibilizar a quienes manejan los sistemas de información sobre la presencia de peligros y la importancia de administrarlos a tiempo.

- Proporcionar un enfoque estructurado para examinar los diferentes riesgos.
- Facilitar la identificación y la planificación de las acciones adecuadas para mantener los peligros controlados.
- Fortalecer a la organización en todas las áreas involucradas en la protección de los recursos informáticos.

De acuerdo lo antes mencionado, se puede identificar que el complementar el modelo COSO 2013 con la metodología MAGERIT en una auditoría informática brinda múltiples ventajas, entre las que destacan:

- La integración de un enfoque estructurado de control interno con uno especializado en análisis y gestión de riesgos tecnológicos.
- La posibilidad de identificar amenazas y vulnerabilidades específicas que afectan la seguridad física y lógica.
- La generación de planes de acción concretos para mitigar riesgos, alineados con los objetivos institucionales.
- El fortalecimiento de la toma de decisiones basadas en riesgos, promoviendo la mejora continua en los sistemas de información.
- La contribución al cumplimiento normativo y regulatorio, mediante controles documentados y que puedan ser monitoreados.

4.4.1. Análisis de Riesgos

En el análisis de riesgos se identifican y valoran los diversos elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

El análisis del riesgo contempla lo siguiente:

- Identificación de activos de información.
- Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
- Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

4.4.2. Inventario de activos

Dentro de una auditoría informática, el inventario de activos consiste en la identificación, clasificación y documentación detallada de todos los recursos tecnológicos que posee la organización, los cuales son fundamentales para el funcionamiento de sus sistemas de información. Este inventario incluye tanto activos físicos, como servidores, computadoras, routers, switches, y dispositivos de almacenamiento; como activos lógicos, tales como software, licencias, bases de datos, sistemas operativos y configuraciones. El objetivo principal de este proceso es conocer con precisión qué recursos existen, dónde se encuentran, quién los utiliza y cuál es su nivel de criticidad para las operaciones institucionales. Tener un inventario actualizado permite evaluar adecuadamente los riesgos asociados a cada activo, establecer controles específicos y diseñar planes de contingencia que aseguren la disponibilidad, integridad y confidencialidad de la información. Además, es un insumo esencial para metodologías de gestión de riesgos como MAGERIT y para el fortalecimiento del control interno según marcos como COSO 2013.

4.4.3. Amenazas y vulnerabilidades

La detección de amenazas y vulnerabilidades es un aspecto fundamental en la presente auditoría informática, teniendo aún mayor relevancia que se está aplicando el modelo COSO 2013 junto con la metodología MAGERIT, esto permite una evaluación completa de los peligros que afectan la seguridad tanto física y lógica de los sistemas de información. Dentro del marco de COSO 2013, esta evaluación se conecta con el componente de "Evaluación de riesgos", que destaca la necesidad de identificar eventos, tanto internos como externos, que podrían perjudicar el cumplimiento de los objetivos de la institución. Al complementar con MAGERIT, se añade un componente técnico y especializado que ayuda a identificar amenazas concretas, como accesos no autorizados, fallos en el hardware, pérdida de información o ataques cibernéticos, así como vulnerabilidades susceptibles de ser aprovechadas, tales como configuraciones inadecuadas, ausencia de políticas de seguridad o la falta de controles físicos. Esta estrategia combinada no solo permite identificar puntos de mejora, sino que también establece la importancia de los proteger los activos, evalúa el impacto potencial y prioriza las acciones correctivas basándose en un análisis de riesgos. De esta manera, se refuerza el sistema de control interno, se mejora la capacidad de respuesta ante incidentes y se asegura una gestión más eficiente de la seguridad de la información, contribuyendo a la continuidad de las operaciones, la protección de los datos de la institución y el cumplimiento de las normativas y regulaciones pertinentes.

4.5 Fase I: Planificación de la auditoría.

4.5.1. Beneficiarios

Esta auditoría informática será aplicada a Sportmancar Manta, tiene como objetivo fortalecer la seguridad física y lógica en la institución, esto a su vez beneficia a la empresa en

alcanzar los objetivos internos por medio de la continuidad de sus servicios en el uso diario de los recursos informáticos.

4.5.2. Alcance

Este proceso tiene como alcance los recursos informáticos de Sportmancar Manta usados en los procesos de formación de conductores, departamento de TI, atención al cliente, recaudación y Psicosensométricos. Esta auditoría fue llevada a cabo en Julio y agosto del 2025

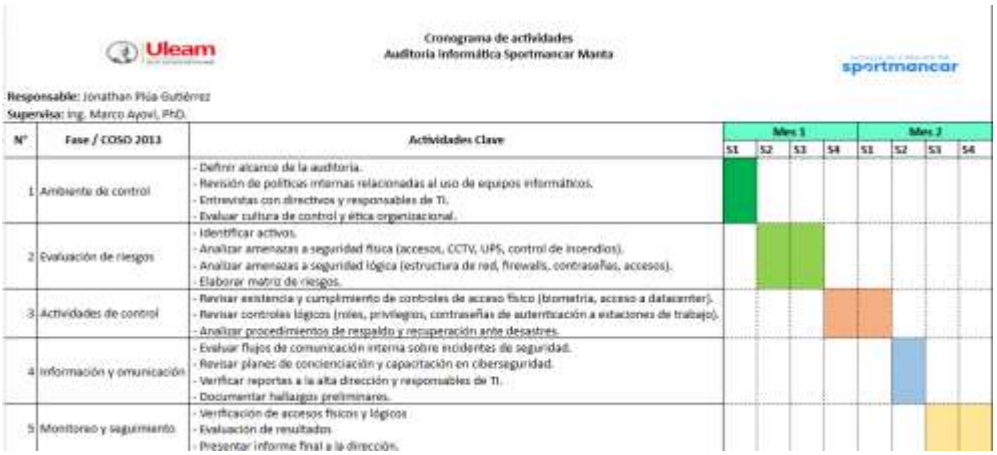
4.5.3. Equipo de trabajo

Para la ejecución de la Auditoría Informática, es fundamental identificar los diferentes roles y actividades que desempeñan los involucrados en este proyecto, en la parte ejecutora y de campo se encuentra Jonathan Plúa, estudiante de la carrera de ingeniería en sistemas quien cuenta con el conocimiento elemental para el desarrollo de estas actividades, en conjunto está el Ing. Marco Ayoví, PhD. Docente a cargo de la supervisión de las actividades ejecutadas en la auditoría informática aplicada a Sportmancar Manta.

4.5.4. Cronograma de trabajo

Ilustración 21

Cronograma de actividades



Cronograma de actividades
Auditoría Informática Sportmancar Manta

Responsable: Jonathan Plúa Gutiérrez
Supervisa: Ing. Marco Ayovi, PhD.

N°	Fase / COSO 2013	Actividades Clave	Mes 1				Mes 2			
			S1	S2	S3	S4	S1	S2	S3	S4
1	Ambiente de control	- Definir alcance de la auditoría. - Revisión de políticas internas relacionadas al uso de equipos informáticos. - Entrevistas con directivos y responsables de TI. - Evaluar cultura de control y ética organizacional.								
2	Evaluación de riesgos	- Identificar activos. - Analizar amenazas a seguridad física (accesos, CCTV, UPS, control de incendios). - Analizar amenazas a seguridad lógica (estructura de red, firewalls, contraseñas, accesos). - Elaborar matriz de riesgos.								
3	Actividades de control	- Revisar existencia y cumplimiento de controles de acceso físico (biometría, acceso a datacenter). - Revisar controles lógicos (roles, privilegios, contraseñas de autenticación a estaciones de trabajo). - Analizar procedimientos de respaldo y recuperación ante desastres.								
4	Información y comunicación	- Evaluar flujos de comunicación interna sobre incidentes de seguridad. - Revisar planes de concienciación y capacitación en ciberseguridad. - Verificar reportes a la alta dirección y responsables de TI. - Documentar hallazgos preliminares.								
5	Monitoreo y seguimiento	- Verificación de accesos físicos y lógicos - Evaluación de resultados - Presentar informe final a la dirección.								

Por medio de la ilustración 21, se observa el plan de trabajo alineado al modelo COSO 2013, complementado con Magerit. El establecer este cronograma de actividades permite tener una visión clara de las actividades y tiempos establecidos para el cumplimiento de la auditoría informática.

4.6 Fase II: Levantamiento de información.

4.6.1. Acerca de Sportmancar Manta

Sportmancar Manta es una escuela de conducción no profesional, cuyo enfoque es la formación y capacitación a personas que optan por una licencia de conducir, está situada en la ciudad de Manta, en la provincia de Manabí, Ecuador. Desde sus inicios, se ha establecido como una reconocida institución a nivel local, destacándose por su dedicación a la formación de

calidad, la educación vial y la seguridad vial. La institución proporciona formación teórica como práctica, siguiendo las normativas vigentes regularizadas por la Agencia Nacional de Tránsito (ANT) y los reglamentos nacionales. Sportmancar Manta dispone de un equipo de instructores capacitados y aptos para ejercer, aulas con tecnología acorde a las necesidades y sistemas informáticos que administran la información académica, administrativa y operativa de sus estudiantes y colaboradores. A través de su crecimiento en infraestructura tecnológica y el volumen de información que maneja, surgen nuevos retos en cuanto a la seguridad de la información y el control interno. Esta situación permite identificar la necesidad de establecer acciones que fortalezcan la protección de sus recursos digitales y físicos, garantizando así la continuidad operativa y la credibilidad de sus usuarios.

4.6.2. Activos informáticos

En la tabla 7, se muestra la lista de activos de Sportmancar Manta

Tabla 7

Lista de activos de la empresa

Lista de Activos informático			**Referencia A**
N°	**Nombre**	**Descripción**	**Tipo de activo**
A1	**Computadoras de escritorio**	Equipo usado en las actividades de atención al cliente, Exámenes psicosensométricos, departamento TI y cobros.	Equipo informático de escritorio
A2	**Equipo Psicosensométrico**	Usado para la toma de exámenes	Equipo Psicosensométrico

		psicosensométricos a los estudiantes de conducción	
A3	**Cámaras de vigilancia**	Usadas para la videovigilancia de las instalaciones	Videovigilancia
A4	**Equipo de proyección**	Usado en el aula para clases teóricas, parte de los módulos de capacitación	Equipo de proyección
A5	**Sistema Operativo**	Windows 10	Software
A6	**Navegador Web**	Aplicación que permite acceder a la web	
A7	**Paquete Office**	Herramienta de escritorio para el manejo de información en estaciones de trabajo	
A8	**Router y red**	Interconexión por medio de una red local con topología bus	Servicio
A9	**Servicio de Internet**	Servicio con proveedor externo	

4.6.3. Implementación MODELO COSO 2013 como análisis

De acuerdo a una visita realizada a las instalaciones de Sportmancar Manta, por medio del uso de las técnicas de observación directa y entrevista, se pudo levantar una línea base de información que se detalla a continuación las cuales se alinean a los 5 componentes del modelo COSO 2013.

I. Ambiente de Control

El ambiente de control de Sportmancar Manta está compuesto por los siguientes puntos:

- Objetivos de la empresa
  - Misión

"Nuestro compromiso mediante la formación de conductores responsables con un gran dominio vehicular, leyes de tránsito y respeto al peatón; es aportar al desarrollo del País"

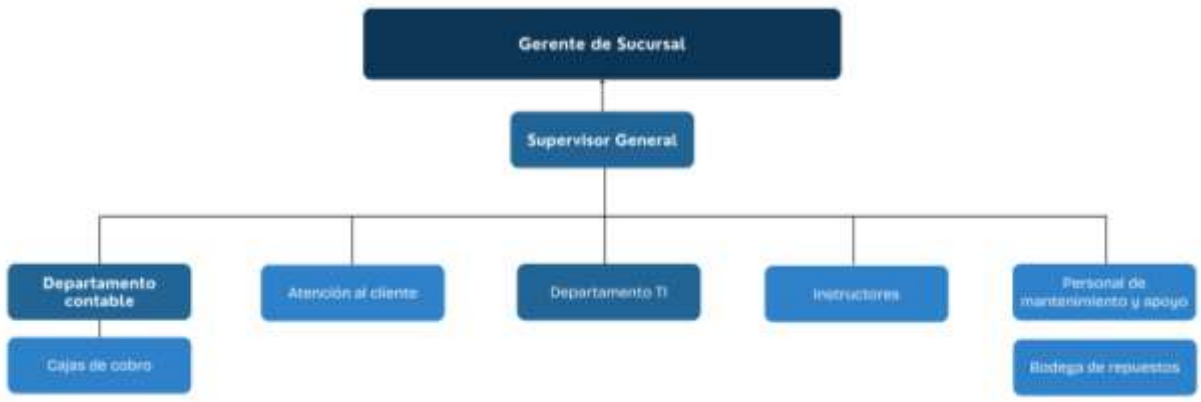
  - Visión

"Basados en pedagogías innovadoras con alta tecnología de punta, formamos conductores responsables que aporten y sobre todo respeten a la sociedad"

- En la ilustración 22, se muestra la Estructura Administrativa

Ilustración 22

Organigrama jerárquico



- Sistema de registro de estudiantes, este sistema desarrollado de manera local e implementado desde el 2018 con el objetivo de permitir registrar estudiantes, asignarle su horario e instructor, a este sistema tienen acceso con todos los privilegios el gerente, el encargado de TI, el supervisor general y con privilegios de registro y estado de pago el personal de atención al cliente.

- Existencia en el reglamento interno de Sportmancar Manta, que menciona lo siguiente:

"Art. 7.- Será responsabilidad de los jefes de Área las siguientes actividades:

d.- Incentivarán al personal bajo su cargo sobre la Prevención de Riesgos Laborales y concienciar sobre el buen uso de las instalaciones, equipos y bienes de propiedad de SPORTMANCAR CIA. LTDA." (Sportmancar CIA LTDA, 2020)

II. Evaluación de riesgos

Enmarcado a este componente, se pudieron identificar a través de la entrevista, observación directa y la encuesta los diferentes riesgos relacionados a los equipos informáticos y de manera estructural, este último puede afectar de manera directa la continuidad de los servicios informáticos en la empresa de manera considerable.

En complemento de lo antes mencionado se detalla la tabla 8, una matriz de los activos con sus amenazas y vulnerabilidades identificadas.

Tabla 8

Amenazas y vulnerabilidades

Amenazas y vulnerabilidades			**Referencia B**
N°	**Nombre**	**Amenazas**	**Vulnerabilidades**
A1	**Computadoras de escritorio**	- Pérdida o robo del equipo - Falla en el funcionamiento - Infección por virus - Desconocimiento en el cuidado de los equipos	- Poca o nula seguridad en inicio de sesión - Falta de mantenimiento - Equipos desactualizados
A2	**Equipo Psicosensométrico**	- Clima - Falta de conocimiento sobre el manejo	- Ubicación en un punto no protegido ante eventos climáticos
A3	**Cámaras de vigilancia**	- Pérdida o robo de los equipos - Falla en su funcionamiento	- Falta de mantenimiento - Actualización de equipos
A4	**Equipo de proyección**	- Pérdida o robo de los equipos - Falla en su funcionamiento	- Falta de mantenimiento
A5	**Sistema Operativo**	- Caída o daño del sistema - Robo de Información	- Hardware incompatible con versiones del sistema - Errores de configuración

A6	**Navegador Web**	- Acceso a sitios web maliciosos - Accesos a archivos en línea contaminados	- Falta de implementación de antivirus - Enlaces maliciosos
A7	**Paquete Office**	- Error de activación	- Uso de software no oficial
A8	**Router y red**	- Daño de la estructura - Mal estado del cableado de la red - Paralización del servicio	- Desastres naturales - Estructura de red visible - Equipos de red básicos - Contraseñas de accesos fáciles
A9	**Servicio de Internet**	- Paralización del servicio - Fallo en los enlaces de comunicación	- Falla eléctrica - Desastres naturales

Por medio de la metodología MAGERIT, se toman de referencia las siguientes ilustraciones 23 y 24.

Ilustración 23

Escala de riesgo-probabilidad

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Nota. Adaptada de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (p. 7), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónic, 2012

Ilustración 24

Clasificación de amenazas

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Nota. Adaptada de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (p. 7), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónic, 2012

Teniendo estas referencias, se elabora la tabla de tratamiento de riesgo alineado a MAGERIT, que se muestra en la ilustración 25.

Ilustración 25

Categorización de riesgos-Metodología MAGERIT

Riesgos		Probabilidad				
		MB	B	M	A	MA
Impacto	MA		- Seguridad de red	- Falla en el funcionamiento de las cámaras de videovigilancia - Paralización del servicio de internet	- Daños en la estructura de red	
	A	- Pérdida o robo del equipo - Falla en el funcionamiento Infección por virus	- Equipos sin antivirus - Equipos Obsoletos	- Contraseñas de autenticación a los equipos sencillas	- Desconocimiento en el cuidado de los equipos - Daños del SO - Acceso a sitios web maliciosos - Accesos a archivos en línea contaminados	- Filtraciones por clima
	M					
	B					
	MB			- Falta de mantenimientos preventivos a los equipos		

III. Actividades de control

Por medio de la entrevista, se pudieron levantar los siguientes resultados, estos relacionados a este componente, de los cuales se identifica que no se están implementando acciones de manera frecuente que permitan identificar riesgos y el desarrollo de controles como:

- Mantenimientos preventivos o correctivos realizados.
- Controles de acceso robustos y confiables hacia el área donde se encuentran los equipos físicos que funcionan como servidores para el sistema contable y el sistema de registro de estudiantes.
- Bitácoras de registro que permitan un control de mantenimientos o supervisión del correcto funcionamiento de equipos.

IV. Sistema de información y Comunicación

Por medio de la entrevista se pudo evidenciar puntos a corregir:

- No se comunican por medios formales las incidencias con equipos informáticos.

- Las solicitudes de compra de repuestos o adquisición de equipos no se manejan por medios formales.

Esto limita a que exista una buena comunicación y que los departamentos o áreas involucradas obtengan de manera eficiente información necesaria para la toma de decisiones o cumplimiento de objetivos de la empresa.

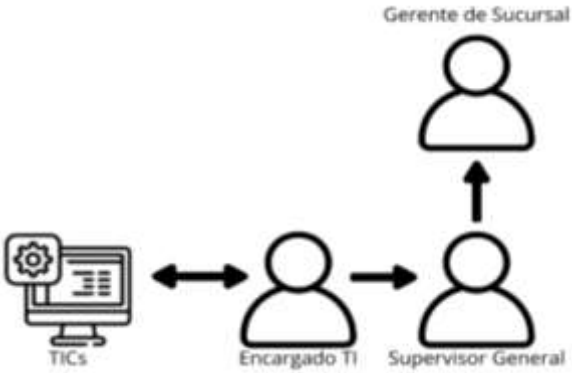
V. Actividades de monitoreo o supervisión

El encargado de TI realiza de manera frecuente una supervisión de todos los equipos, quien al encontrar alguna incidencia comunica a supervisión en caso de ser necesario; sin embargo, no existe un formato de formulario de manejo de incidencias.

Esto se muestra en la ilustración 26.

Ilustración 26

Organigrama de comunicación interna



4.7 Acciones correctivas

4.7.1. Capacitación al personal

De acuerdo a los resultados obtenidos y la aplicación del modelo COSO 2013, se identifica la importancia y necesidad de capacitar al personal de Sportmancar Manta quienes usan diariamente los equipos informáticos para generar la cultura en la implementación de buenas prácticas y el uso adecuado de los equipos informáticos complementado por la importancia de la seguridad de la información y como ellos son actores clave en la empresa.

Los temas impartidos fueron generados de acuerdo a la encuesta aplicada y los resultados de la necesidad de impartir temas que aporten a la empresa, estos se mencionan a continuación:

- Buenas prácticas en seguridad de la información, portada mostrada en la ilustración 27 y ubicada en el Anexo 2.

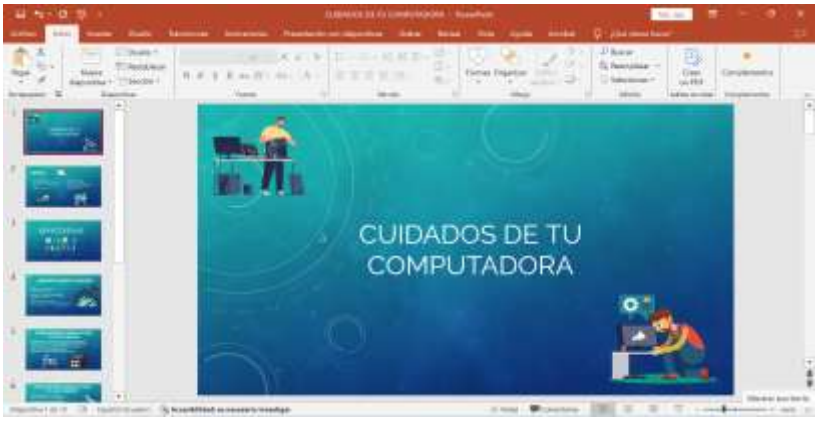
Ilustración 27

Portada de presentación Seguridad de la información

- Cuidados de tu computadora, portada mostrada en la ilustración 28 y ubicada en el Anexo 3.

Ilustración 28

Portada presentación Cuidados de la computadora



4.7.2. Creación de registros digitales

De acuerdo a los hallazgos se identifica la necesidad de facilitar a la empresa documentos que permitan dar inicio a la verificación adecuada a los controles internos que se realizan relacionados a los equipos informáticos, es por ello que se generan los siguientes documentos:

- Registro semanal de control interno de equipos informáticos, referencia en la ilustración 29, documento ubicado en el Anexo 4.

Ilustración 29

Registro de control interno

Registro de control interno semanal a equipos informáticos Sportmancar Manta

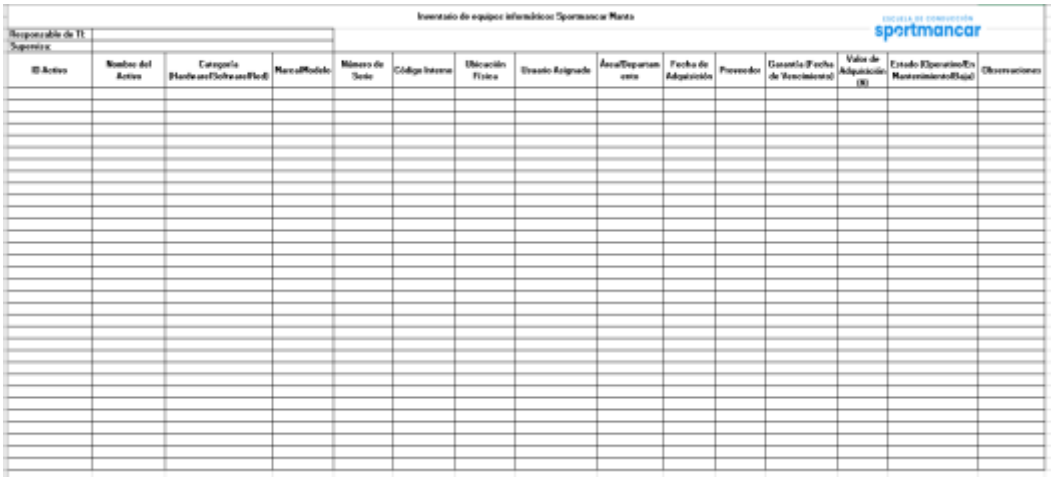
ESCUELA DE CONDUCCIÓN sportmancar

Responsable de TI:					
Supervisa:					
Fecha	Equipo	Área	Responsable	Estado	Observaciones

- Matriz de activos informáticos, referencia en la ilustración 30, documento ubicado en el Anexo 5.

Ilustración 30

Inventario de activos informáticos



- Bitácora de mantenimientos a equipos informáticos, referencia en la ilustración 31, documento ubicado en el Anexo 6.

Ilustración 31

Bitácora de mantenimientos

- Formulario de solicitud de compra de equipos o repuestos informáticos, referencia en la ilustración 32, documento ubicado en el Anexo 7.

Ilustración 32

Formulario de solicitud de compra

FORMULARIO DE SOLICITUD DE COMPRA DE EQUIPOS / REPUESTOS INFORMÁTICOS

Fecha de Solicitud:	
Nombre del Solicitante:	
Área / Departamento:	
Cargo:	
Correo Electrónico:	
Teléfono de Contacto:	

ESCUELA DE CONDUCCIÓN sportmancar

DETALLE DE EQUIPOS O REPUESTOS SOLICITADOS

N°	Descripción del Equipo/Repuesto	Cantidad	Especificaciones Técnicas	Proveedor Sugerido	Justificación

Firmas:	Responsable de TI		Gerente Sucursal		Supervición
CI:					
Nombre y apellido:					

Observaciones adicionales:

CAPÍTULO V

Evaluación

5 evaluación de resultados

5.1 Introducción

El presente capítulo tiene como objetivo presentar los resultados obtenidos mediante la ejecución de una auditoría informática, esta fue aplicada en la Escuela de conducción Sportmancar Manta. En relación a la implementación del modelo COSO 2013 y los hallazgos, se detallan cada resultado a continuación:

5.2 Presentación y monitoreo de resultados

5.2.1. Hallazgos

Los resultados se detallan a través, de las tablas 9 a la 16, que se muestran a continuación:

Tabla 9

Hallazgo 01

Resultados obtenidos	
Hallazgo N° 01	Las contraseñas de inicio de sesión en computadoras incumplen parámetros para ser contraseñas seguras.
Descripción	Las contraseñas de acceso a los equipos informáticos, que son usados por los trabajadores de Sportmancar Manta para las diferentes actividades y considerados como activos importantes, no cumplen con los parámetros determinados para una contraseña segura.
Consecuencia	Personas no autorizadas pueden ingresar ante un mínimo descuido lo cual podría causar un robo, manipulación o daño de la información.
Recomendación	Establecer contraseñas de acuerdo a las recomendaciones vistas durante la capacitación, cambiando de manera recurrente las contraseñas de todos los equipos.

Tabla 10

Hallazgo 02

Resultados obtenidos	
Hallazgo N° 02	**Falta de controles de acceso al área de servidores y CCTV**
Descripción	Inexistencia de controles de accesos biométricos o cerraduras que únicamente permitan el acceso a personal autorizado en la empresa
Consecuencia	Personas no autorizadas pueden ingresar a través de engaños y esto podría terminar en robo, manipulación o daño de la información y de los equipos informáticos.
Recomendación	Implementar mecanismos y tecnologías como tarjetas únicas de acceso a los espacios donde se ubican servidores o rack de CCTV.

Tabla 11

Hallazgo 3

Resultados obtenidos	
Hallazgo N° 03	Falta de activación de Firewall en servidores
Descripción	Falta de activación de firewall en servidores de estudiantes, estos contienen toda la información relacionada a las inscripciones y estatus de los estudiantes
Consecuencia	Pérdida de datos por medio de una intrusión, falta de datos para la toma de decisiones y posible paralización de la continuidad de los servicios
Recomendación	Activación de firewall en servidor Estudiantes

Tabla 12

Hallazgo 04

	Resultados obtenidos
Hallazgo N° 04	Estructura de red en malas condiciones y visible
Descripción	Existe cableado de red visible y algunos que no se encuentran en uso, esto es visible ante toda persona que llega a la empresa, y en ocasiones pausa la continuidad de servicio en el área de atención al cliente.
Consecuencia	La continuidad de los servicios podría verse afectada, causando en mayor impacto pérdidas económicas y de credibilidad por los usuarios.
Recomendación	Eliminación de cables sin uso, reestructuración de la red local empaquetando los cables de manera adecuada.

Tabla 13

Hallazgo 05

	Resultados obtenidos
Hallazgo N° 05	Desconocimiento del reglamento interno, misión y visión
Descripción	Desconocimiento de estos por parte del personal sobre la existencia del reglamento interno y sus artículos vinculados a las buenas prácticas y seguridad.
Consecuencia	Desconocimiento y en casos falta de compromiso en el cumplimiento de los objetivos de la empresa.
Recomendación	Socialización del reglamento interno, misión y visión a todo el personal y la importancia de la aplicación de estos como estrategia clave para el crecimiento de la empresa.

Tabla 14

Hallazgo 06

	Resultados obtenidos
Hallazgo N° 06	Fallas en la estructura física de la empresa
Descripción	Existencia de filtraciones de agua en algunas áreas cercanas al departamento de TI
Consecuencia	Daños en los equipos y a su vez pérdida de información
Recomendación	Reparación de grietas y filtraciones en las áreas afectadas por la lluvia de manera visible

Tabla 15

Hallazgo 07

	Resultados obtenidos
Hallazgo N° 07	Implementación de documentos para respaldo de actividades de control
Descripción	Inexistencia de formatos o documentos que permitan respaldar los diferentes controles internos aplicados vinculados al área de TI
Consecuencia	Falta de información para la toma de decisiones, falta de documentación requerida para futuras auditorías
Recomendación	Aplicar la documentación facilitada, iniciando con las buenas prácticas en el registro de las diferentes actividades realizadas vinculadas a la seguridad física y lógica en la empresa

Tabla 16

Hallazgo 08

	Resultados obtenidos
Hallazgo N° 08	Desconocimiento de existencia de plan de contingencia en el área de TI
Descripción	Desconocimiento sobre la existencia sobre un plan de contingencia en la empresa aplicable para la continuidad de los servicios brindados por Sportmancar Manta
Consecuencia	Discontinuidad de los servicios ante algún evento natural o causado
Recomendación	Creación de plan de contingencia para la continuidad de los servicios informáticos y la protección de los activos

5.3 Interpretación objetiva

Por medio del apartado anterior, se puede interpretar que existen varios puntos a fortalecer vinculados tanto a la seguridad física como a la seguridad lógica, iniciando por un punto clave como es el control interno, donde se parte y se identifica la necesidad mejorarlo.

De acuerdo a los datos obtenidos por medio de las diferentes técnicas se puede concluir que la mayoría del personal que usa equipos informáticos de Sportmancar Manta, no implementa acciones desde su rol que incidan de manera positiva en la seguridad física y lógica. Esto a su vez vinculado a que no se lleva un control interno y registro histórico adecuado en el área de TI sobre los mantenimiento, adquisiciones y reparaciones ejecutadas en los diferentes años que lleva en funcionamiento la empresa.

Por otra parte, no se ha logrado generar una inversión importante relacionada a la adquisición de equipos nuevos y actualizados que permitan fortalecer la seguridad de la información. Esta

inversión se relaciona de manera directa a la seguridad lógica ya que por medio de estas estaciones de trabajo se maneja información importante de los estudiantes y ante lo cual es relevante aplicar políticas internas de protección de datos de acuerdo a las leyes vigentes.

El desconocimiento ha sido un punto importante identificado a mejorar, ya que se identifica que la mayoría del personal no conoce cuales son los reglamentos de la empresa vinculado al buen uso de los equipos facilitados por la empresa para el desempeño de las actividades.

CAPÍTULO VI

Conclusiones y recomendaciones

6.1 Conclusiones

- Por medio de la investigación bibliográfica sobre la metodología COSO 2013, se pudo comprender que esta permite identificar riesgos y puntos de mejora para lograr el cumplimiento de los objetivos de la empresa, integrando cada departamento y por ende cada miembro del equipo de trabajo.
- A través de la entrevista y la visita a las instalaciones se identificó la necesidad de establecer controles de acceso a los servidores de estudiantes, como punto clave para la continuidad de los servicios prestados en Sportmancar Manta.
- Por medio de la aplicación de la herramienta Nmap se determina que el servidor de estudiantes no tiene protección de un firewall y por ende es importante sugerir que se debe aplicar de manera inmediata.
- Se elaboró una matriz de riesgos y se proponen mejoras para reducirlos o eliminarlos, iniciando la ejecución de actividades que incentiven al fortalecimiento de la seguridad física y lógica en la empresa a través del involucramiento de todo el personal.
- Se ejecutó la auditoría informática y se determinan los hallazgos de la misma.

6.2 Recomendaciones

Las recomendaciones que se redactan a continuación, van dirigidas a Sportmancar Manta.

- Asignar tareas específicas y roles a cada miembro del equipo de trabajo, ya que al no contar con esto se desaprovecha el factor tiempo en el cumplimiento de tareas correspondientes a cada área.

- Se sugiere la reestructuración de la red local en las instalaciones, esto permitirá potenciar los recursos informáticos con los que actualmente se cuenta, y mejoras en el cumplimiento de tareas específicas.
- Identificar puntos estructurales a mejorar para así evitar el daño de equipos informáticos de alto valor puedan dañarse debido a situaciones climáticas.
- Implementación de formularios para el control de los procesos correspondientes a TI.
- Promover el uso de canales oficiales para reportes de incidencias, por ejemplo, correo institucional.
- Activar firewall a todos los equipos de la empresa, para fortalecer la protección en los mismos.
- Actualización recurrente de contraseñas y que estas cumplan los parámetros sugeridos para prevenir acceso no autorizados.
- Socializar en un lugar visible la misión y visión de la empresa, promoviendo así el apropiamiento de los miembros del equipo de trabajo con los objetivos a alcanzar de la empresa.
- Considerar la actualización de equipos informáticos para mejoras de seguridad informática y salvaguarda de la información.

Bibliografía

Martinez, R. G. (2014).

https://www.ofstlaxcala.gob.mx/

González, M., & Ramírez, L. (2021). *Seguridad informática: Principios y aplicaciones*. Editorial Universitaria.

Soto, J. (2020). *Protección física de activos tecnológicos*. Ediciones Técnicas.

Torres, R. (2019). *Gestión integral de la seguridad en organizaciones*. Grupo Editorial Norma.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework: Executive summary*. https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

PricewaterhouseCoopers. (2013). *Understanding the COSO 2013 Framework*. https://www.pwc.com/us/en/risk-assurance-services/assets/understanding-the-coso-2013-framework.pdf

Nmap. (s.f.). *Nmap.org*. Obtenido de https://nmap.org/man/es/index.html

Sportmancar CIA LTDA. (2020). Reglamento Interno. Loja.

WireShark.org. (s.f.). *wireshark.org*. Obtenido de

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

Protiviti. (2013). *Frequently asked questions—2013 COSO Internal Control–Integrated Framework*. https://www.protiviti.com/sites/default/files/united_states/insights/2013-coso-framework-faq.pdf

Hurtado, J. A., & Rojas, H. M. (2018). Auditoría de sistemas informáticos: Principios y aplicaciones. *Revista de Tecnología*, 17(2), 45-58.

IFAC. (2022). *Normas Internacionales de Auditoría*. International Federation of Accountants. https://www.ifac.org/

Rezaee, Z. (2002). *Financial Statement Fraud: Prevention and Detection*. John Wiley & Sons.

Whittington, O. R., & Pany, K. (2012). *Principles of Auditing and Other Assurance Services* (18th ed.). McGraw-Hill Education.

Arens, A. A., Elder, R. J., & Beasley, M. S. (2018). *Auditoría: Un enfoque integral* (15.ª ed.). Pearson Educación.

Gusmán, V. (2019). Evaluación de seguridad de la información aplicado al sistema de evaluación de docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la metodología magerit V3. Ibarra- Ecuador.

http://repositorio.utn.edu.ec/handle/123456789/9535

Seid, G. (2016). Procedimientos para el análisis cualitativo de entrevistas. Una propuesta didáctica. ISSN 2408-3976. Obtenido https://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.8585/ev.8585.pdf

IBM. (2024). *¿Qué es la seguridad de la información (InfoSec)?* https://www.ibm.com/es-es/topics/information-security

Microsoft. (2024). *¿Qué es la seguridad de la información (InfoSec)?* https://www.microsoft.com/es-ar/security/business/security-101/what-is-information-security-infosec

Slack. (2024). *¿Qué es la seguridad de la información y por qué importa?* https://slack.com/intl/es-es/blog/transformation/que-es-la-seguridad-de-la-informacion-y-por-que-importa

Telefónica. (2024). *Qué es la seguridad de la información.* https://www.telefonica.com/es/sala-comunicacion/blog/seguridad-informacion-que-es/

Captio. (2025). Auditoría empresarial: ¿en qué consiste? https://www.captio.net/blog/auditoria-empresarial-en-que-consiste

Gadax. (2023). ¿Qué es una auditoría empresarial y por qué es importante? https://gadaxrd.com/que-es-una-auditoria-empresarial-y-por-que-es-importante/

IQS. (2024). Técnicas de auditoría y sus técnicas. https://iqs.edu/es/blog/que-es-una-auditoria-y-cuales-son-sus-tecnicas/

Kawak. (2025). Auditoría, conceptos y definiciones clave. https://landing.kawak.net/conceptos-y-definiciones-clave-de-auditoria

Nanuk. (2024). Auditorías empresariales. https://nanuk.mx/servicios/normatividad-cumplimiento/auditoria-empresarial/

Economipedia. (2020). Auditoría informática. https://economipedia.com/definiciones/auditoria-informatica.html

Ibaiscanbit. Auditoría informática de sistemas - ¿Qué es y sus ventajas? https://ibaiscanbit.com/ibaiscanbit/auditoria-informatica-de-sistemas-que-es-y-sus-ventajas/

Ikusi. (2023). Auditoría informática: ¿Qué es y cómo hacer una con éxito? https://www.ikusi.com/mx/blog/auditoria-informatica/

World Campus Saint Leo. (2024). ¿Qué es una auditoría informática y cuáles son sus fases? https://worldcampus.saintleo.edu/blog/fases-de-una-auditoria-informatica-y-en-que-consisten

Matos, A. A. (23 de octubre de 2020). Investigación Bibliográfica: Definición, Tipos, Técnicas. Obtenido de Investigación Bibliográfica: Definición, Tipos, Técnicas: https://www.lifeder.com/investigacion-bibliografica/

De Santiago Bartolomé, I. (13 de agosto de 2019). ANÁLISIS DE MAGERIT Y PILAR. Valladolid.

//uvadoc.uva.es/bitstream/handle/10324/37736/TFG-213.pdf?sequence=1&isAllowed=y

Neill, D. A., & Suárez, L. C. (2018). Procesos y fundamentos de la investigación científica. Machala, Ecuador: UTMACH. http://repositorio.utmachala.edu.ec/bitstream/48000/14232/1/Cap.4-Investigaci%C3%B3n%20cuantitativa%20y%20cualitativa.pdf

Sosa, A. (21 de diciembre de 2018). Prezi. Obtenido de https://prezi.com/c3cu3jwuax79/elmetodo-analitico-sintetico/Westrecher, G. (14 de agosto de 2020). Definición de técnica.

https://economipedia.com/definiciones/metodo-deductivo.html

GBTEC. (2024). Sistema de Control Interno.

https://www.gbtec.com/es/wiki/grc/sistema-de-control-interno-1/

Noris14. (2011). Control Interno Informático - Auditoría de Sistemas.

https://noris14.wordpress.com/2011/06/10/control-interno-informatico/

Pinilla, J. D. (2025). *Auditoría Informática - Aplicaciones en Producción*.

https://es.scribd.com/doc/38921087/Control-Interno-Informatico

Plattini, M. G. (2025). *Auditoría Informática - Un Enfoque Práctico*

https://es.scribd.com/doc/38921087/Control-Interno-Informatico

Universidad Nacional José Faustino Sánchez Carrión. (2024). Control Interno Informático y la eficiencia.

https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/4568/Domingo%20Ra%C3%BAl%20MORALES%20LOZAa%20%202.pdf?sequence=1&isAllowed=y

ADR Formación. (2023, noviembre 29). *Tipos de riesgos en Ciberseguridad*.

https://www.adrformacion.com/knowledge/ciberseguridad/tipos_de_riesgos_en_ciberseguridad.html

Bitso. (2023, octubre 30). *¿Cuáles son los tipos de riesgos de ciberseguridad más comunes?* https://blog.bitso.com/es-co/seguridad-co/tipos-de-riesgos-de-ciberseguridad

InvGate. (2024, septiembre 6). *Ciberseguridad: definición, tipos, amenazas y empleos*. https://blog.invgate.com/es/ciberseguridad

Innevo. (2024, noviembre 1). *4 tipos de Riesgos Informáticos Prioritarios en las Empresas*. https://innevo.com/blog/tipos-de-riesgos-informaticos

Smowl. (2025, mayo 7). *Vulnerabilidad en la seguridad informática: definición, tipos y consejos*. https://smowl.net/es/blog/vulnerabilidad-en-la-seguridad-informatica/

Ticnova. (2024, febrero 8). *Principales riesgos de seguridad informática en las empresas*. https://ticnova.es/blog/riesgos-seguridad-informatica/

Worldsys. (2023, junio 22). *3 tipos de riesgos informáticos a los que se exponen las empresas*. https://worldsys.io/3-tipos-de-riesgos-informaticos-a-los-que-se-exponen-las-empresas/

Anexos

Anexo 1. Encuesta dirigida a colaboradores

Encuesta obtenida de acuerdo al muestreo de 15 trabajadores relacionados a Sportmancar Manta, quienes usan diariamente los equipos informáticos.

Preguntas del formulario

1.- ¿Conoce sobre la seguridad informática?

- Mucho
- Poco
- Nada

2.- ¿Conoce qué es ingeniería social?

- Mucho
- Poco
- Nada

3.- ¿Con qué frecuencia al año, ha sido infectado por un malware el equipo que usa en la empresa?

- 1-3 veces
- 4-6 veces
- 7 veces o más

- Ninguna ocasión

4.- ¿Ha instalado herramientas o programas sin darlo a conocer al responsable de TI?

- Siempre
- Casi siempre
- Nunca

5.-El equipo que usa en la empresa, ¿cuenta con antivirus?

- Siempre
- Casi siempre
- Nunca

6.- ¿Se ha brindado mantenimiento periódico al equipo informático que usa en la empresa?

- Siempre
- Casi siempre
- Nunca

7.- ¿Conoce cuáles son las recomendaciones para establecer una contraseña robusta?

- Mucho
- Poco

- Nada

8.- ¿Cambia la contraseña de ingreso al equipo informático de la empresa periódicamente?

- Siempre
- Casi siempre
- Nunca

9.- ¿Conoce las recomendaciones para un buen uso de los equipos informáticos de la empresa?

- Mucho
- Poco
- Nada

10.- Conoce la existencia en el reglamento de Sportmancar Manta, donde se menciona el bueno uso de los bienes, instalaciones y equipo pertenecientes a la empresa

- Mucho
- Poco
- Nada

Anexo 2. Buenas prácticas relacionadas a la seguridad de la información

Reglamento Sportmancar Manta

Art. 7

d.- Incentivarán al personal bajo su cargo sobre la Prevención de Riesgos Laborales y concienciar sobre el buen uso de las instalaciones, equipos y bienes de propiedad de SPORTMANCAR CIA. LTDA.

¿Qué es la seguridad informática?

La práctica de proteger las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos se conoce como ciberseguridad. También se conoce como seguridad de datos electrónicos o seguridad de tecnología de la información. El término se usa en una variedad de contextos, desde los negocios hasta la informática móvil, y se puede dividir en varias categorías comunes.

Seguridad de red

Proteger una red informática de los intrusos

01

Seguridad de las aplicaciones

Mantener el software y los dispositivos libres de amenazas

02

Seguridad de la información

Protege la integridad y la privacidad de los dato

03

04

Seguridad operativa

Protege los recursos de datos

05

Recuperación ante desastres y la continuidad del negocio

Intentar operar sin determinados recursos.

06

Capacitación del usuario final

Temas que impulsen a las buenas prácticas de seguridad

Vulnerabilidades

Las vulnerabilidades en ciberseguridad son fallas o debilidades en sistemas y aplicaciones informáticas, redes o software que pueden ser explotadas por actores malintencionados para acceder, robar, alterar o destruir información sensible. Los errores de software, las configuraciones incorrectas, las prácticas de seguridad inadecuadas o las tecnologías obsoletas pueden ser la causa de estas vulnerabilidades. Para proteger los activos digitales y mantener la integridad y confidencialidad de los datos en el mundo conectado de hoy, es esencial su identificación y corrección.

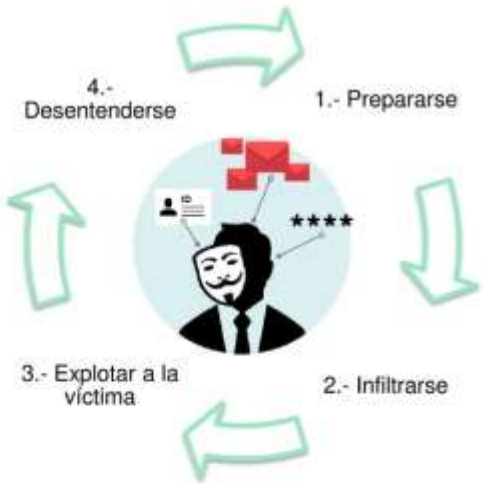
- Control de acceso débil
- Vulnerabilidades de inyección SQL
- Vulnerabilidades de denegación de servicio
- Vulnerabilidades por uso de componentes vulnerables

¿QUÉ ES LA INGENIERÍA SOCIAL?

INGENIERÍA SOCIAL

La ingeniería social es una forma de manipulación que utiliza el error humano para recopilar datos privados, acceso a sistemas u objetos valiosos. En el contexto del crimen cibernético, estas acciones de "hackeo de humanos" suelen llevar a los usuarios a exponer datos, propagar infecciones de malware o permitir el acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, en persona o a través de otras interacciones.

¿CÓMO FUNCIONA LA INGENIERIA SOCIAL?



El ciclo del ataque les da a estos criminales un proceso confiable para engañarlo. El ciclo de ataque de ingeniería social suele usar los siguientes pasos:

RASGOS DE LOS ATAQUES DE INGENIERÍA SOCIAL

Intensificación de las emociones

- Es mucho más probable que realice acciones irracionales o arriesgadas

Urgencia

- Es posible que se sienta motivado a comprometerse ante aparentes problemas graves

Confianza

- Ha investigado lo suficiente sobre usted como para crear una historia fácil de creer

ATAQUES DE PHISHING

Los atacantes que usan el phishing se hacen pasar por una institución o un individuo de confianza en un intento de persuadirlo de que exponga datos personales y otros objetos de valor.

- **Spam de phishing**
- **Spear de phishing**

Phishing (vishing) por voz

Mediante llamadas telefónicas

01

Los mensajes de texto de phishing (smishing)

Mensajes de aplicaciones móviles pueden incluir un enlace web

02

Phishing por correo electrónico

Utiliza un correo electrónico que le insta a responder o hacer un seguimiento por otros medios.

03

04

El phishing de Angler

EL atacante finge ser del equipo de servicio al cliente de una empresa de confianza.

05

El phishing en buscadores

Intenta colocar enlaces a sitios web falsos en la parte superior de los resultados de búsqueda.

06

Phishing URL

Tientan a visitar sitios web de phishing

ATAQUES DE CEBO

Los ataques de cebo abusa de su curiosidad natural para convencerlo de que se exponga a un atacante. Por lo general, el potencial de recibir algo gratis o exclusivo es la manipulación utilizada para explotarlo. El ataque por lo general implica termina infectándolo con malware.

- Unidades USB dejadas en espacios públicos, como bibliotecas y estacionamientos.
- Archivos adjuntos de correo electrónico que incluyen detalles sobre una oferta gratuita o software gratuito fraudulento.

ATAQUES DE ACCESO FÍSICO

Los ataques de acceso físico involucran a los atacantes que se presentan en persona, haciéndose pasar por alguien que tiene derecho de acceso a áreas o información restringidas.

ATAQUES QUE USAN PRETEXTOS

Los ataques que usan pretextos echan mano de una identidad engañosa como "pretexto" para ganarse la confianza. Por ejemplo, pueden hacerse pasar por un proveedor o un empleado de la compañía.

ATAQUES DE "ACCESO A CUESTAS"

Es el acto de seguir a un miembro del personal autorizado a un área de acceso restringido.

ATAQUES DE SCAREWARE O INTIMIDACIÓN

Scareware es una forma de malware que se utiliza para asustarlo y hacer que realice una acción. Este malware engañoso utiliza advertencias alarmantes sobre infecciones de malware falsas o afirman que una de sus cuentas se ha visto comprometida.

CONSEJOS

- **Actualizar el software y el sistema operativo:** esto significa que aprovechará las últimas revisiones de seguridad.
- **Utilizar software antivirus:** las soluciones de seguridad, como los antivirus, detectarán y eliminarán las amenazas. Se recomienda mantener el software actualizado para obtener el mejor nivel de protección.
- **Utilizar contraseñas seguras:** asegúrese de que sus contraseñas no sean fáciles de adivinar.
- **No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos:** podrían estar infectados con malware.
- **No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos:** es una forma común de propagación de malware.
- **Evitar el uso de redes Wi-Fi no seguras en lugares públicos:** las redes no seguras lo dejan vulnerable a ataques del tipo "Man-in-the-middle".


PREGUNTAS


GRACIAS

Anexo 3. Cuidados de tu computadora

TEMA 1

¿POR QUÉ CUIDAR TU EQUIPO?

- Mejorar su rendimiento
- Evitar robo de datos
- Estética con buena presentación
- Alargar la vida útil
- Evitar costos monetarios
- Tener un equipo en optimas condiciones

TEMA 2

CONSEJOS PARA ALARGAR LA VIDA ÚTIL DE TU EQUIPO

- Mantén limpio tu ordenador y el área donde se encuentra
- Protege tu equipo de subidas y bajadas de tensión eléctrica
- Evita descargas de archivos de sitios web no oficiales
- Evita el sobrecalentamiento del equipo
- Evita tener comida o bebida cerca de tu equipo

TEMA 2

CONSEJOS PARA ALARGAR LA VIDA ÚTIL DE TU EQUIPO

- Mantén actualizado tu equipo
- Borra archivos que no necesites
- Protege tu equipo con antivirus
- Evita conectar dispositivos que no son confiables
- Realiza mantenimiento preventivo

TEMA 3

CÓMO SABER CUANDO SE NECESITA SOPORTE TÉCNICO

- Problemas de batería
- Se apaga inesperadamente
- Pantalla azul
- Error al iniciar un programa
- Sobrecalentamiento

TEMA 3

CÓMO SABER CUANDO SE NECESITA SOPORTE TÉCNICO

- Problemas de conexión WiFi o Bluethooth
- El ventilador hace mucho ruido
- Fallas en el teclado
- No se visualiza imagen
- Equipo infectado por virus o malware

DUDAS O PREGUNTAS


GRACIAS

Anexo 4. Registro semanal de control interno de equipos informáticos

Registro de control interno semanal a equipos informáticos Sportmancar Manta					
Responsable de TI:					
Supervisa:					
Fecha	Equipo	Área	Responsable	Estado	Observaciones

Anexo 5. Matriz de activos informáticos

Inventario de equipos informáticos Sportmancar Manta														
Responsable de TI:														
Supervisa:														
ID Activo	Nombre del Activo	Categoría (Hardware/Software/Red)	Marca/Modelo	Número de Serie	Código Interno	Ubicación Física	Usuario Asignado	Área/Departamento	Fecha de Adquisición	Proveedor	Garantía (Fecha de Vencimiento)	Valor de Adquisición	Estado (Operativo/En Mantenimiento/Baja)	Observaciones

Anexo 6. Bitácora de mantenimiento a equipos informáticos

Bitacora de Mantenimiento a equipos informáticos Sportmancar Manta

ESCUELA DE CONDUCCIÓN sportmancar

Responsable:
Supervisor:

ID Equipo	Nombre del Equipo	Usuario Responsable	Área/Departamento	Tipo de Mantenimiento (Preventiva/Correctiva)	Fecha de Mantenimiento	Descripción de la Actividad	Técnico Responsable	Firma	Próxima Fecha de Mantenimiento	Observaciones

Anexo 7. Formulario de solicitud de compra de equipos o repuestos informáticos

FORMULARIO DE SOLICITUD DE COMPRA DE EQUIPOS / REPUESTOS INFORMÁTICOS

Fecha de Solicitud:	
Nombre del Solicitante:	
Área / Departamento:	
Cargo:	
Correo Electrónico:	
Teléfono de Contacto:	

ESCUELA DE CONDUCCIÓN sportmancar

DETALLE DE EQUIPOS O REPUESTOS SOLICITADOS

N°	Descripción del Equipo/Repuesto	Cantidad	Especificaciones Técnicas	Proveedor Sugerido	Justificación

Firmas: _____ Responsable de TI _____ Gerente Sucursal _____ Supervición

CI:

Nombre y apellido:

Observaciones adicionales: