UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 PARA EL CONTROL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA EPC-COMPU DE LA CIUDAD DE AMBATO.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del Título de Ingeniera en Tecnologías de la Información.

ÁREA: Seguridad

LÍNEA DE INVESTIGACIÓN: Seguridad informática

AUTOR: Soraya Cristina Sailema Fiallos

TUTOR: Ing. Julio Enrique Balarezo, PhD

Ambato – Ecuador

agosto - 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 PARA EL CONTROL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA EPC-COMPU DE LA CIUDAD DE AMBATO, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Soraya Cristina Sailema Fiallos estudiante de la Carrera de Ingeniera en Tecnologías de la Información., de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, agosto 2023

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Enrique Balarezo, PhD

TUTOR

AUTORÍA

El presente trabajo de titulación titulado: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 PARA EL CONTROL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA EPC-COMPU DE LA CIUDAD DE AMBATO, es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023

Soraya Cristina Sailema Fiallos

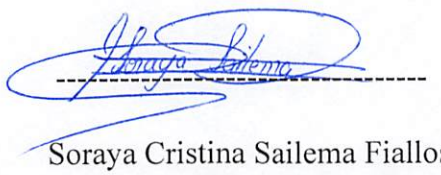
C.C.180546555-4

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, agosto 2023



Soraya Cristina Sailema Fiallos

C.C. 180546555-4

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Soraya Cristina Sailema Fiallos, estudiante de la Carrera de Ingeniería en Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 PARA EL CONTROL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA EPC-COMPU DE LA CIUDAD DE AMBATO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
MARCO VINICIO GUACHIMBOZA VILLALVA

Ing. Mg. Marco Vinicio Guachimboza Villalva
PROFESOR CALIFICADOR

Firmado electrónicamente por:
EDISON HOMERO ALVAREZ MAYORGA

Ing. Mg. Edison Homero Álvarez Mayorga
PROFESOR CALIFICADOR

DEDICATORIA

Dedico este logro académico y profesional a todas las personas que creyeron en mi desde el principio en especial a mis padres Ángel y Martha que fueron mis pilares fundamentales en este logro de la vida. y con sus consejos han formado la persona que soy.

A mis hermanos con los que comparto mis conocimientos y fueron mi inspiración y ganas de superarme, hasta conseguir esta meta.

Soraya Cristina Sailema Fiallos

AGRADECIMIENTO

Agradezco a Dios por ser uno de los pilares fundamentales en mi vida y permitirme llegar hasta donde estoy, a mi madre por brindarme su apoyo incondicional porque fue el motor para no darme por vencida, a mi padre por enseñarme a ser la mejor y obligarme a tomar el camino más difícil para demostrarme que aquello que se veía imposible hoy ha dado frutos, a mi abuelito que es el ángel que me cuido durante todo este proceso y a mi familia por sus palabras de aliento. Solo me queda decir, meta cumplida

Soraya Cristina Sailema Fiallos

ÍNDICE DE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

En la actualidad los datos se han convertido en un valioso recurso para las organizaciones y su control demanda un análisis minucioso con el fin de resguardarlos de posibles riesgos a los que están expuestos. De este modo, se busca asegurar la integridad, confidencialidad y accesibilidad de la información.

El presente proyecto de investigación tiene como objetivo implementar un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001 para el control de la seguridad informática de la empresa EPCCOMPU en la ciudad de Ambato.

Primero, se realizó un estudio de la ISO 27001 para crear un manual basado en la norma ISO 27001:2013, el cual contiene los puntos necesarios que se deben seguir para implementar correctamente un Sistema de Gestión de Seguridad de la Información, después se realizó un análisis del estado actual de la seguridad informática mediante la recopilación de información de entrevistas y ficha de observación que permitieron obtener un punto de partida para el diseño del SGSI, también se hizo un análisis de los procesos críticos de la empresa EPC-COMPU para realizar la evaluación de riesgos con la finalidad de identificar y analizar las vulnerabilidades y amenazas que intervienen en la gestión de la seguridad de la información para este análisis se seleccionó los controles necesarios de la norma ISO 27001, luego se hizo la gestión de riesgos identificando prevención, detección y corrección por consecuencia detallado en el plan de contingencia. Finalmente se elaboró procesos de seguimiento y control para definir las actividades con sus respectivos responsables.

Palabras clave: Integridad, confidencialidad, disponibilidad, Norma ISO 27001, gestión de la seguridad, evaluación de riesgos, procesos, SGSI

ABSTRACT

Actually, data has become a valuable resource for organizations and its control demands a thorough analysis in order to protect them from possible risks to which they are exposed. In this manner, it seeks to ensure the integrity, confidentiality and accessibility of information.

The present research proyect aims to implement an information security management system (ISMS) based on the ISO 27001 standard for the control of computer security of the company EPCCOMPU in Ambato city.

First, a study of ISO 27001 was carried out to create a manual based on the ISO 27001:2013 standard, which contains the necessary points that must be followed to correctly implement an Information Security Management System, then an analysis of the current state of computer security through the collection of information from interviews and an observation sheet that allowed obtaining a starting point for the design of the ISMS, an analysis of the critical processes of the company EPC-COMPU to perform risk assessment in order to identify and analyze the vulnerabilities and threats involved in the management of information security for this analysis, the necessary controls of the ISO 27001 standard were selected, then risk management was carried out identifying prevention, detection and correction by consequence detailed in the contingency plan. Finally, monitoring and control processes were developed to define the activities with their respective managers.

Keywords: Integrity, confidentiality, availability, ISO 27001 Standard, security management, risk assessment, processes, ISMS

CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema de investigación

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001, PARA EL CONTROL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA EPC-COMPU DE LA CIUDAD DE AMBATO

1.1.1 Planteamiento del problema

Las organizaciones utilizan la tecnología como un medio de procesamiento, almacenamiento y para salvaguardar la información, especialmente en tiempos de pandemia, la tecnología desempeña un papel fundamental en el funcionamiento de sus procesos, pero al mismo tiempo, estos están expuestos a numerosos riesgos y amenazas informáticas. Existen varios países que actualmente consideran una prioridad la prevención de los ciberataques, existiendo un ranking de 193 países comprometidos a enfrentar los ciberataques, el ranking fue detallado por la Unión Internacional de Telecomunicaciones. Ecuador entra en los países latinoamericanos del ranking, se encuentra en el puesto número 66 a nivel mundial como parte de este listado, siendo considerado como un país que si cuenta con estudios y avances respecto a la ciberseguridad [1].

La mayoría de los robos o pérdidas de información en Latinoamérica recaen sobre el sector empresarial, pues Aguilar-Antonio (2019) explica que estos incidentes se deben a las insuficientes medidas de protección, lo que causa pérdidas de productividad, credibilidad, competitividad y perjuicios financieros que comprometen la continuidad de la organización [2].

Toda organización está expuesta cada vez más a amenazas y es vulnerable a cualquier ataque informático (Caamaño y Gil, 2020); es decir, la variedad de amenazas en contra de sus activos puede causar la pérdida, manipulación o la no disponibilidad de la información (Gil y Gil, 2017). Paralelamente, pueden ocasionar cuantiosas pérdidas económicas, tal como dicen Wiley et al. (2020), el Foro Económico Mundial, en 2018,

reportó que el 65 % de organizaciones australianas fueron víctimas de ataques, una de 6 cada diez sufrió pérdidas superiores a $ 1 millón. En el Ecuador existen algunas empresas públicas y privadas que tratan la información como un asunto técnico, por lo que es necesario tomar las medidas correspondientes para proteger uno de los activos más valiosos como es la información. La seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada [3].

La información es uno de los activos principales de las organizaciones y empresas, existen diferentes tipos de amenazas que atentan contra el buen funcionamiento de estos entes, como los virus, los malware, cibercriminales, spyware y un sinnúmero de amenazas existentes, diariamente se utilizan diferentes equipos en especial móviles que están conectados a internet, la mayor fuente de amenazas para la seguridad [4].

A medida que avanza la tecnología, surgen nuevas formas de afectar la seguridad de la información, lo que hace necesario el análisis de vulnerabilidades. Esto puede existir en los sistemas informáticos, por lo que se pueden desarrollar sistemas de gestión de seguridad de la información, y el mismo sistema está diseñado para minimizar los riesgos que puedan surgir de formas fraudulentas para ayudar a controlarlo mejor.

Dentro de la empresa EPC-COMPU de la cuidad de Ambato-Ecuador, se trabaja con información confidencial, por lo que es muy importante contar con un sistema de seguridad de la información teniendo en cuenta aspectos fundamentales como: confidencialidad, integridad y disponibilidad, la empresa presenta un deficiente control en la seguridad de la información debido a la ausencia de políticas de seguridad, la limitada capacitación del personal y una infraestructura inadecuada, estas carencias han creado un entorno vulnerable que expone la información a riesgos y ha ocasionado pérdidas económicas.

1.2 Antecedentes Investigativos

Al realizar una investigación bibliográfica se pudo encontrar la siguiente información:

Según Muñoz Pinto Oscar Gabriel [5], en su trabajo investigativo denota que: El diseño del Sistema de Gestión de la Seguridad de la Información aplicando los estándares que se indica en la norma ISO 27001 fueron de vital importancia ya que cumplen con las necesidades dentro de cualquier institución, permitiendo tener una mejor seguridad en cuanto a la disponibilidad y una seguridad de la información más confiable. Además, la aplicación del Sistema de Gestión de la Seguridad de la información que fue diseñado ayuda a tener un mejor control en el manejo de la seguridad de la información como de los activos este será exclusivamente del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito indígena SAC quien será el encargado de hacer cumplir cada una de las normas que indica la norma ISO 27001.

Según Guevara Tucta Ramiro Alejandro [6] menciona en su tesis que: Al Implementar un Sistema de Gestión de Seguridad de la información ayuda a supervisar y monitorear periódicamente toda actividad relacionada con la seguridad de la información. Además, gracias a la aplicación del Sistema de Gestión de Seguridad de la información los parámetros de seguridad de los sistemas institucionales, los archivos y documentos se encuentran correctamente respaldados y documentados.

Según Guamán Seis Joseph Alexander [7]:

La norma ISO 27001 está diseñada y elaborada para ser compatible con otras normas reconocidas de sistemas de gestión. Además, es perfecta para su integración con sistemas y procesos de gestión. También el Sistema de gestión de la Seguridad de la Información en conjunto con la Norma ISO 27001 permite determinar establecer políticas y los objetivos de gestión de la seguridad de la información. Además, con el Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.; así como la identificación del riesgo, identificación de las amenazas y vulnerabilidades; permite el cálculo del riesgo; tratamiento de riesgo; y, revisión de los riesgos y reevaluación de los activos de información.

Remigio Leonel Chagmana Pomaquero [8] en su trabajo investigativo dice que:

La aplicación de la Norma ISO 27001 es fundamental ya que permite determinar existen riesgos informáticos en una organización y además permite encontrar vulnerabilidades en los sistemas informáticos, garantizando la confidencialidad, integridad y disponibilidad de la información en el Departamento de TIC's del Centro de Investigación y Desarrollo FAE. Además, la implementación de las políticas de seguridad basada en la norma ISO 27001 determinan un porcentaje de satisfacción óptimo de cumplimiento lo cual permite el adecuado funcionamiento del SGSI.

Según Jaime Fernando Vásquez Escalante [9] en su tesis denota que: Con la aplicación del sistema de gestión permite identificar los activos de información importantes para el negocio, así como los riesgos y el impacto sobre los mismos, asimismo permite elaborar planes de trabajo con los controles adecuados para su mitigación y reducir los niveles de riesgos a un nivel aceptable. También al contar con una política de seguridad de la información y que esta sea difundida y de conocimiento de todo el personal, permite a la organización tener una visión de cómo con sus actividades diarias y como estas pueden contribuir a la mejora del sistema de gestión. Además, la norma ISO 27001:2013 puede integrarse a las diversas normas debido a su estructura a las demás normas ISO 9001, ISO 14000, etc.

Según José Gregorio Arévalo Ascanio [10]:

El éxito en la implantación de un SGSI desde cualquier perspectiva empresarial depende del compromiso y la mentalidad de cambio de los niveles ejecutivos y directivos en las organizaciones, por tanto, el alcance del sistema para todas las organizaciones es elaborar estratégicas y tácticas con respecto a la seguridad de la información. También la definición del SGSI se hace de manera formal en la norma ISO 27001 donde se recogen los estándares y mejores prácticas de seguridad de la información con la finalidad de identificar los activos de información, responsables, documentación, y posteriormente se establece las políticas de seguridad que permiten resguardar la seguridad de la información lo cual permitirá la obtención de la certificación internacional de Norma ISO 27001.

Aníbal Rubén Mantilla Guerra [11] en su artículo científico denota que: La norma ISO27001:2013 es una herramienta efectiva para manejar un Sistema de Gestión de Seguridad de la Información en cualquier organización, sin importar a que se dedique

esta, debido a que es un tema de extrema trascendencia y permanente actualidad. Es de uso global y además es certificable. Además, la seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional, inherente a toda actividad humana; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

Según Harry Vite Cevallos [12] en su artículo científico denota que: El cumplimiento de normas de calidad en materia del aseguramiento de la información, a futuro permite tener un mejor control de los recursos hardware, software que facilite un análisis de amenazas y vulnerabilidades que puedan presentar sobre los activos de la institución. Además, la implementación de sistemas de Gestión de Seguridad de la Información permite establecer e identificar los elementos de seguridad en los activos de información a utilizarse con el hecho de mejorar las actividades académicas que se pueden ejecutar en las universidades.

1.3 Fundamentación Teórica

Tecnología de la Información

Son todas las tecnologías que permiten dar soporte a la construcción y operación de los sistemas de información, y son tecnologías de hardware, software, de almacenamiento y de comunicaciones. Estas tecnologías forman la infraestructura tecnológica de la empresa, que provee una plataforma en la cual la compañía construye y opera los sistemas de información [13].

Seguridad Informática

Intenta proteger el almacenamiento, procesamiento y transmisión de información digital, la era de la información, con Internet como principal exponente, ha mejorado el nivel de vida y la convivencia en este planeta. La información es poder, luego hay que protegerla. Sus elementos son susceptibles de ser atacado por un saboteador o,

simplemente, fallar. La seguridad informática intenta evitarlo y, en caso de que ocurra, minimizar los daños para recuperar el servicio lo antes posible.

La seguridad informática comprende:

Equipos. Robo; evitar intentos de conectar equipos externos a la empresa, mantenimiento preventivo. Aplicaciones. Limitar privilegios, revisar vulnerabilidades conocidas, descargar aplicaciones de fuentes fiables. Datos. Almacenamiento redundante, copias de seguridad y cifrado. Comunicaciones. Utilizaremos canales cifrados para proteger la información cuando es transmitida por nuestra red interna y, sobre todo, por Internet [14].

Auditoria Informática

La auditoría de seguridad informática propone detectar las vulnerabilidades expuestas en la red de datos y en los sistemas de información y, verificar los niveles de riesgos que conllevan al explotar un fallo de seguridad mediante herramientas de código abierto; para después implementar un sistema de correlación de eventos que permita monitorear actividades de origen desconocido y que este proceda a bloquearlas [14].

Sistema de seguridad de la información

Es un Sistema de Gestión de Seguridad de la Información (Information Security Management System, por sus siglas en inglés). Un SGSI es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo. Éste garantiza que las empresas tomen medidas sistemáticamente para mantener seguros los datos y la información; puede ser cualquier tipo de información, como datos de clientes, procesos internos o detalles de pago. Un Sistema de Gestión de Seguridad de la Información (SGSI) es el primer paso para la certificación, puesto que proporciona las mejores prácticas de seguridad de información y permite a la organización desarrollar, implementar y medir la práctica eficaz de gestión de la seguridad en todas sus áreas unificadas en sus operaciones

(comúnmente el día a día de la organización) con el fin de alinearse al cumplimiento de los objetivos de la misma y para minimizar los riesgos existentes [15].

Norma ISO 27001

Es un estándar internacional que permite el aseguramiento, confidencialidad e integridad de los datos y los sistemas que los procesan. Los requisitos de la norma ISO 27001 nos proporcionan un Sistema de Gestión de la Seguridad de la Información (SGSI), que incluye medidas diseñadas para proteger la información, independientemente de su formato, de cualquier amenaza, de manera que podamos 13 garantizar la continuidad de las actividades de nuestra empresa en todo momento. Una forma de garantizar la seguridad de la información es conocer las normativas que engloban los SGSI: las ISO 27001. Las empresas deben estar al tanto de estas normas y formar al personal en ellas, desde el director a los operarios que manejarán el sistema. Asimismo, es importante contar con asesores que estén permanentemente actualizados para descubrir cualquier grieta dentro del sistema la norma ISO 27001 proporciona un conjunto de controles para la seguridad de la información que una organización debe implementar en función de los resultados de una evaluación de riesgos y los requisitos de las partes interesadas. Es decir, para cada riesgo a tratar se implementará una combinación de diferentes tipos de controles. Para la implementación de la norma ISO 27001 recurre a ciclo de Deming que se encarga en el continuo mejoramiento de la seguridad de la información. Podemos concluir que: un SGSI actúa como un eje centralizado para salvaguardar y gestionar toda la información de una organización en un solo lugar [16].

Control de la Información

El control de la información es la evaluación de las acciones para detectar posibles riesgos o inconvenientes que serán subsanados mediante el uso del sistema de gestión Computadora. Los controles internos de seguridad tienen por finalidad garantizar que todos los activos, sistemas, instalaciones, datos y archivos relacionados con el uso de

la Tecnología de Información se encuentran protegidos contra accesos no autorizados, daños eventuales y uso indebido o ilegal que se encentran operables, seguros y protegidos en todo momento. La planificación de controles de seguridad informática definirá controles técnicos a implementarse en la infraestructura tecnológica y servicios informáticos institucionales, según requerimientos establecidos por el Plan Director de Seguridad de la Información, el plan de seguridad informática histórico, reportes de análisis de monitoreo de la plataforma, análisis ethical hacking, leyes, reglamentos, normas, eventos e incidentes de seguridad informática [17].

Seguridad de la Información

El propósito de la seguridad informática es proteger la información de una variedad de amenazas para garantizar la continuidad del negocio, minimizar el costo del daño potencial para el negocio y maximizar el retorno de la inversión sin dejar de ser competitivo a través de un mejor posicionamiento competitivo para aprovechar la oportunidad [18]

Seguridad

La seguridad es la capacidad de identificar y abordar las vulnerabilidades, se debe hacer hincapié en la necesidad de proteger las fortalezas de una organización, incluida la información y los dispositivos físicos, como las propias computadoras. Es importante la preservación de los bienes y servicios a través de normas de confianza para con el fin de evitar algún daño o riesgo [19].

Gestión de Seguridad

La gestión de la seguridad de la información es muy extensa, pero sin duda alguna, uno de sus puntos claves es la adecuada gestión del riesgo. Administrar y monitorear la integridad y privacidad de la información procesada por la infraestructura tecnológica de la organización [20].

1.4 Objetivos

1.4.1 Objetivo general

Implementar un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001 para el control de la seguridad informática de la empresa EPCCOMPU de la ciudad de Ambato.

1.4.2 Objetivos específicos

- Realizar un diagnóstico de la seguridad de información de la empresa EPC-COMPU de la ciudad de Ambato, con la finalidad de evidenciar falencias de seguridad informática.
- Determinar la existencia de políticas de seguridad y el cumplimiento de normas en los procesos de seguridad informática de la empresa EPC-COMPU de la ciudad de Ambato, con la finalidad de garantizar la seguridad de la información.
- Diseñar un sistema de gestión de seguridad de la información (SGSI) aplicando la norma ISO 27001, para el control de la seguridad informática de la empresa EPC-COMPU.

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

Para la recolección de la información del presente proyecto se utilizó dos entrevistas, la primera dirigida al Gerente y la segunda al personal de sistemas y una ficha de observación.

Guía de entrevista dirigida al Gerente de la empresa EPC-COMPU

ENTREVISTA AL GERENTE EPC - COMPU			
Objetivo: Recolectar información sobre el manejo de la seguridad de la información en la institución y la seguridad de la información de los clientes de EPC-COMPU			
Fecha:			
Entrevistado:		Entrevistadora: Cristina Sailema	
Cargo:			
N°	Preguntas	Respuestas	Observación
1	¿Qué presupuesto se ha asignado a la seguridad de la información?		
2	¿Existe algún plan de contingencia para enfrentar cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución?		
3	¿Se ha enterado de los planes de contingencia que se ha realizado?		

4	¿Se realiza un análisis de riesgos en cuanto a la seguridad de la información dentro de la institución?		
5	¿Existe algún tipo de responsabilidad de los empleados a nivel de contrato si se llega a perder información de algún cliente?		
6	¿En caso de alguna perdida tienen algún seguro para reparar los equipos?		
8	¿Se han realizado capacitaciones a todo el personal en caso de alguna eventualidad?		
9	¿Usted ha identificado proveedores para responder rápidamente en caso de alguna perdida de equipos?		
10	¿Ha existido alguna perdida de información de los clientes que han dejado sus equipos, y que es lo que ha sucedido?		
11	¿Los clientes han sido informados que al		

	momento de formatear su equipo se perderá su información?		
12	¿La empresa cuenta con Licencias de Antivirus actualizados en los equipos informáticos?		
13	¿La empresa cuenta con equipos de Firewall?		
14	¿Cuenta la empresa con un Sistema de Gestión de Seguridad de la Información (SGSI)?		
15	¿Le gustaría implementar un SGSI?		
16	¿Conoce usted acerca de un Sistema de Gestión de seguridad de la información (SGSI)?		
Conclusión:			

Tabla 1. Guía de Entrevista al Gerente

Elaborado por: Investigador

Guía de entrevista dirigida al Personal de Sistemas

ENTREVISTA AL PERSONAL DE SISTEMAS EPC - COMPU	
Objetivo: Recolectar información sobre el manejo de los activos de información en EPC - COMPU	
Fecha:	Entrevistadora: Cristina Sailema

Entrevistado Preguntas	Jefe del Departamento de TICS	Desarrollador de Software	Asistente de Tecnología	Jefe de Mantenimiento de Informática
1.- ¿Qué tipo de activos de información utilizan en la empresa?				
2.- ¿Cuáles son las vulnerabilidades más comunes en los activos de información que se han presentado?				
3.- ¿Actualmente la empresa cuenta con políticas de seguridad? ¿Si cuenta con políticas cuáles son?				
4.-¿Utilizan proxys en los equipos informáticos para restringir el contenido de sitios web?				

5.-¿Como cuantifica los impactos de las amenazas de los activos de información?				
6.-¿Cuál es el procedimiento para manejar los respaldos de la información?				
7.-¿Con que programas complementan la seguridad de los equipos informáticos en la institución?				
8.-¿La empresa cuenta con equipos de Firewall?				
9.-¿Cuántos computadores tienen en la empresa?				
10.- ¿Los cables de los equipos informáticos tienen etiquetas?				
11.-¿Tienen algún servidor de				

seguridad en internet, o directamente conectado el servidor de base de datos al internet?				
12.-¿Tienen redes Wireless?				
13.-¿Los dispositivos conectados a red tienen algún nivel de seguridad?				
14.-¿Que motores de base de datos utilizan?				
15.- ¿Las computadoras están conectadas a UPC, regletas o reguladores y cuál es su voltaje en microvoltio amperios?				
16.-¿Cuenta la empresa con un SGSI?				

Tabla 2. Guía de entrevista dirigida al Personal de Sistemas

Elaborado por: Investigador

Guía de la Ficha de observación

Objetivo: Realizar observaciones dentro de la empresa EPC-COMPU, con la finalidad de obtener una impresión de cómo se llevan a cabo los procesos informáticos

Escala de valoración

5=Excelente, 4= Muy Bueno, 3=Bueno, 2=Regular, 1=Insuficiente

Aspectos	Valoración					Observaciones
	1	2	3	4	5	
Activos de información seguros						
Uso de los equipos de cómputo.						
Actualización de sistemas en servidores y clientes						
El cableado de los computadores que atienden a los clientes posee seguridad						
Equipos de respaldos bajo llave						
Ubicación de los dispositivos de red						

Estado de dispositivos contraincendios						
Organización del cableado estructurado con canaletas y de los equipos informáticos						
Conclusión:						

Tabla 3. Guía de la Ficha de observación

Elaborado por: Investigador

2.2 Métodos

2.2.1 Modalidad de la Investigación

La presente investigación se contextualizo en la modalidad de investigación de campo y bibliográfica-documental.

Investigación de campo

La investigación será de campo ya que se realiza la investigación en el lugar en el que se presenta el problema es decir en la empresa EPC-COMPU, determinando los inconvenientes que se presenta dentro de la misma.

Investigación bibliográfica-documental

La investigación será bibliográfica ya que se utilizarán fuentes como libros, artículos los mismos que serán un aporte vital para el análisis y la identificación de las amenazas informáticas para la elaboración de un modelo de gestión adecuado que asegure un adecuado tratamiento de la información dentro de la empresa.

2.2.2 Población y Muestra

Población: Para la presente investigación se tomó como población al Gerente, al personal del departamento de Tecnologías de la Información también se incluye a sus clientes actuales de la empresa EPC - COMPU.

Población	Numero	Porcentaje
Gerente General	1	16.67%
Jefe del Departamento de TICS	1	16.67%
Desarrollador de software	1	16.67%
Asistente de tecnología	1	16.67%
Jefe de Mantenimiento de Informática	2	33.33%
TOTAL	6	100%

Tabla 4. Población empresa EPC- COMPU

Elaborado por: El Investigador

2.2.3 Recolección de Información

2.2.3.1 Resultados de las Entrevistas

ENTREVISTA AL GERENTE **EPC - COMPU**			
Objetivo: Recolectar información sobre el manejo de la seguridad de la información en la institución y la seguridad de la información de los clientes de EPC-COMPU			
Fecha:17/04/2023			
Entrevistado: Ing. Ricardo Quispe		Entrevistadora: Cristina Sailema	
Cargo: Gerente			
N°	Preguntas	Respuestas	Observación
1	¿Qué presupuesto se ha asignado a la seguridad de la información?	No hemos asignado ningún presupuesto, si se requiere la adquisición de algún software o hardware se realiza un informe por parte del jefe de sistemas para aprobar o denegar la compra a	

		través de un análisis con los involucrados.	
2	¿Existe algún plan de contingencia para enfrentar cualquier eventualidad que pueda suceder o amenazar a los sistemas de información dentro de la institución?	Si existe un plan de contingencia anual	
3	¿Se ha enterado de los planes de contingencia que se ha realizado?	Si, yo mismo realizo los controles necesarios de los planes de contingencia además están aprobados por la SEPS (Superintendencia de Economía Popular y Solidaria) hasta el momento.	Se puede notar que el gerente está al tanto de los planes de contingencia que se realiza en la empresa.
4	¿Se realiza un análisis de riesgos en cuanto a la seguridad de la información dentro de la institución?	No se ha realizado ningún análisis de riesgos, no hemos tenido una perspectiva de un análisis de riesgos de la seguridad de la información	Se determina que no tienen conocimiento de cómo realizar un análisis de riesgos de la seguridad de la información.
5	¿Existe algún tipo de responsabilidad de los empleados a nivel de contrato si se llega a perder información de algún cliente?	Si, en el contrato solo se establece la confidencialidad, además de los apartados y normas que los empleados aceptan, si un empleado es responsable de la perdida de información será el único	

		responsable y se elaborará un informe.	
6	¿En caso de alguna perdida tienen algún seguro para reparar los equipos?	No contamos con ningún seguro	
8	¿Se han realizado capacitaciones a todo el personal en caso de alguna eventualidad?	No se han realizado ninguna capacitación.	
8	¿Usted ha identificado proveedores para responder rápidamente en caso de alguna perdida de equipos?	Si ha identificado algunos proveedores, pero no tenemos los suficientes recursos económicos para contratarlos.	Se puede evidenciar que el gerente ha observado algunos proveedores, pero no cuentan con los suficientes recursos económicos para contratar proveedores en caso de pérdida de equipos
9	¿Ha existido alguna perdida de información de los clientes que han dejado sus equipos, y que es lo que ha sucedido?	Si, en algunos casos, pero se ha podido solucionar con éxito.	

10	¿Los clientes han sido informados que al momento de formatear su equipo se perderá su información?	Si, el cliente es informado además hay clientes que piden que no se saque un respaldo y de los clientes que se saca el respaldo se guarda dicha información por 6 meses en caso de que el cliente lo necesite.	
11	¿La empresa cuenta con Licencias de Antivirus actualizados en los equipos informáticos?	No, contamos únicamente con un antivirus AVAST gratuito y actualizado.	Se puede determinar que cuentan con un antivirus gratuito sin licenciamiento.
12	¿La empresa cuenta con equipos de Firewall?	No contamos con equipos Firewall	Se puede evidenciar que no tienen a su disposición los dispositivos Firewall
13	¿Cuenta la empresa con un Sistema de Gestión de Seguridad de la Información (SGSI)?	No tenemos un SGSI.	Se puede notar que la empresa no tiene el Sistema de Gestión de la seguridad de la Información
14	¿Le gustaría implementar un SGSI?	Por supuesto, ya que nos hace mucha falta un sistema para controlar la seguridad de la información en nuestra empresa	

15	¿Conoce usted acerca de un Sistema de Gestión de seguridad de la información (SGSI)?	Si, tales como: · Sistemas de encriptación de discos PGP · Active Directory	El gerente tiene conocimientos de varios (SGSI).
Conclusión: Se evidenció que la seguridad de los activos de información en la empresa está expuesta a riesgos por tal motivo es de suma importancia implementar un Sistema de Gestión de Seguridad de la Información para resguardar dichos activos. No se ha mostrado un interés por asignar un presupuesto para mejorar la seguridad de la información. Hasta el momento no se brindado ninguna capacitación al personal en caso de alguna eventualidad. Existe desconocimiento sobre la importancia del Sistema de Gestión de la Seguridad de la Información por falta de revisión, esto implica un aspecto negativo dentro de la empresa, ya que existen problemas con las tecnologías de la información sin resolver. No existe un análisis de riesgos, lo cual es muy importante para identificar y evaluar las posibles amenazas y vulnerabilidades que enfrenta la empresa en términos de seguridad.			

Tabla 5. Matriz de resultados de la entrevista al Gerente

Elaborado por: El investigador

ENTREVISTA AL PERSONAL DE SISTEMAS EPC - COMPU				
Objetivo: Recolectar información sobre el manejo de los activos de información en EPC - COMPU				
Fecha:17/04/2023		Entrevistadora: Cristina Sailema		
Entrevistado Preguntas	Jefe del Departamento de TICS	Desarrollador de Software	Asistente de Tecnología	Jefe de Mantenimiento de Informática
1.- ¿Qué tipo de activos de información utilizan en la empresa?	Bases de Datos, Documentos	Bases de Datos, Documentos	Bases de Datos, Documentos	Bases de Datos, Documentos
2.-¿Cuáles son las vulnerabilidades más comunes en los activos de información que se han presentado?	Software y otros equipos sin documentar Falta de segregación de las redes No disponen de dispositivos Firewall	Descargas e instalaciones desde internet no controladas	Falta de controles para acceder a los sistemas de información	Falta de monitoreo a los sistemas y activos de información

3.- ¿Mencione las amenazas más comunes que han ocurrido en los activos de información en la empresa?	Malware Pishing Daños a los equipos informáticos	Malware Pishing Spyware	Malware	Malware
4.- ¿Actualmente la empresa cuenta con políticas de seguridad? ¿Si cuenta con políticas cuáles son?	No contamos con políticas de seguridad, solo con controles básicos	No	No	No
5.- ¿Utilizan proxys en los equipos informáticos para restringir el contenido de sitios web?	No	No	No	No
6.-¿Cuál es el procedimiento para acceder a los dispositivos de la base de datos y archivos?	Con claves de autenticación	Usuario y Contraseña	Usuario y Contraseña	Usuario y Contraseña

7.- ¿Como cuantifica los impactos de las amenazas de los activos de información?	No cuantificamos, solo analizamos los reportes de los antivirus	No realizamos ningún análisis de riesgos	No realizamos ninguna cuantificación	No realizamos ninguna cuantificación de las amenazas
8.-¿Cuál es el procedimiento para manejar los respaldos de la información?	Se realizan copias en los USB, discos duros externos y en la nube	Se realizan copias en los discos duros externos	Se realizan copias en la nube	Se realizan copias en los USB y discos duros externos
9.-¿Con que programas complementan la seguridad de los equipos informáticos en la institución?	Paquete de Antivirus Firewall de Windows	Antivirus	Antivirus	Antivirus
10.- ¿La empresa cuenta con equipos de Firewall?	No	No	No	No
11.-¿Cuántos computadores tienen en la empresa?	9	9	9	9
12.- ¿Los cables de los equipos informáticos tienen etiquetas?	No	No	No	No

13.-¿Que sistemas operativos utilizan los clientes y servidores?	Para clientes: Windows 8.1, 10,11, Linux Para servidores: Windows Server 2012, 2015 y Linux	Clientes: Windows 8.1, 10,11, Linux Servidores: Windows Server y Linux	Clientes: Windows 8.1, 10,11 Servidores: Windows Server y Linux	Clientes: Windows 8.1, 10,11 Servidores: Windows Server y Linux
14.- ¿Tienen algún servidor de seguridad en internet, o directamente conectado el servidor de base de datos al internet?	Directo al servidor de base de datos al internet	Directo	Directo	Directo
15.- ¿Tienen redes Wireless?	Si	Si	Si	Si
16.- ¿Las redes Wireless tienen políticas para la configuración de seguridad de redes?	Manejamos el estándar WPA2, 802.1X	Manejarnos estándares de seguridad, WPA2, 802.1X	WPA2 802.1X	WPA2 802.1X
17.- ¿Los dispositivos conectados a red tienen algún nivel de seguridad?	No manejamos ningún otro nivel de seguridad	Ninguno	Ninguno	Ninguno

18.-¿Las redes Wireless manejan subdominios?	No	No	No	No
19.-¿Los clientes se conectan con un dominio?	Algunos equipos si se conectan con un dominio	No	No	No
20.-¿Que motores de base de datos utilizan?	Mysql	Mysql	Mysql	Mysql
21.- ¿Las computadoras están conectadas a UPC, regletas o reguladores y cuál es su voltaje en microvoltio amperios?	Están conectadas al UPC de 110v de 2500W Amperios	Están conectas a un regulador UPC de 110v de 2500W Amperios	Están conectas a un regulador UPC de 110v de 2500W Amperios	Están conectas a un regulador UPC de 110v de 2500W Amperios
22.- ¿Cuenta la empresa con un SGSI?	No	No	No	No
23.- ¿Se han descargado e instalado programas sin licencia original?	Si	Si	Si	Si

Tabla 6. Matriz de resultados de la entrevista al Personal de Sistemas

Elaborado por: El Investigador

Conclusiones:

- Se ha suscitado problemas internos de la empresa con correos mal intencionados que contienen archivos adjuntos con el objetivo de borrar la información, siendo un problema muy perjudicial y como factor la gestión de contraseñas no seguras
- No existe un proceso para cuantificar los impactos de las amenazas de los activos de información, lo que no se tendría en conocimiento de cuál es el nivel del riesgo suscitado
- No cuentan con políticas de seguridad, solo tiene a su disposición controles básicos, los cuales limitan mucho a la seguridad de la información y no son suficientes para garantizar que la información esté asegurada.
- Existe la falta de controles para acceder a los sistemas de información, especialmente para acceder al sistema de información principal el cual debe contar con algún factor de doble autenticación.
- Las redes Wireless de la empresa tienen seguridad WPA2, pero no están auditadas.
- Los servidores no cuentan con dispositivos firewall, solo tienen a su disposición de software antivirus y no es suficiente, además no son monitoreados periódicamente por lo que son vulnerables a ataque cibernéticos, es indispensable contar con estos dispositivos y realizar seguimiento periódico de los servidores para supervisar todo el tráfico de red y para identificar y bloquear el tráfico no deseado.
- No tienen ningún otro nivel de seguridad en las redes lo que podría ocasionar que ciberdelincuentes accedan a la información sin autorización, especialmente en archivos compartidos.
- Se evidenció que se han descargado programas piratas sin licencia de algunos sitios web, lo que podría ocasionar que el equipo se infecte con algún tipo de malware.
- No cuentan con un SGSI, pero están interesados en que se implemente en la empresa ya que es indispensable para resguardar la información en la empresa.

2.2.3.2 Resultados de la Ficha de Observación

FICHA DE OBSERVACIÓN

EPC - COMPU

Objetivo: Realizar observaciones dentro de la empresa EPC-COMPU, con la finalidad de obtener una impresión de cómo se llevan a cabo los procesos informáticos

Escala De Valoración

5 = Excelente, 4 = Muy Bueno, 3 = Bueno, 2 = Regular, 1 = Insuficiente

Aspectos	**Valoración**					**Observaciones**
	1	2	3	4	5	
Activos de información seguros		X				Se pudo evidenciar que los activos de información carecen de seguridad
Uso de los equipos de cómputo.			X			
Actualización de sistemas en servidores y clientes			X			Se evidencio que en algunos equipos aún tienen Sistemas Operativos sin actualizar
El cableado de los computadores que atienden a los clientes posee seguridad		X				El cableado de los computadores que atienden a los clientes no tiene algún tipo de seguridad, lo que podría ocasionar el robo de algún dispositivo.
Equipos de respaldos bajo llave				X		

Ubicación de los dispositivos de red		X				Se observó que los dispositivos de red se encuentran en un escritorio sin ningún tipo de seguridad
Estado de dispositivos contraincendios			X			
Organización del cableado estructurado con canaletas y de los equipos informáticos		X				El cableado de los dispositivos de red tiene una topología de anillo y cuentan con algunos cables con etiquetas envolventes de Brady y otros cables no están cubiertos por canaletas.
Conclusión: Los activos de información presentan ciertas vulnerabilidades y amenazas, también se evidencio la falta de actualización de los sistemas operativos en clientes y servidores, los dispositivos de red se encuentran en una mesa sin ningún tipo de seguridad, La mayoría de los archivos se encuentran en una carpeta compartida en la red de la empresa, que pueden ser manipulados por los mismos empleados y no empleados sin ninguna restricción, además se pudo notar que los cables de red no se encuentran separados de los cables de energía lo que podría ocasionar algún perjuicio y otros cables no cuentan con etiquetas envolventes de Brady.						

Tabla 7. Matriz de resultados de la Ficha de Observación

Elaborado por: El Investigador

2.2.4 Procesamiento y Análisis de Datos

De acuerdo con los resultados obtenidos de la entrevista al Gerente, se determinaron los siguientes aspectos:

- La Gerencia desconoce acerca de las revisiones periódicas en sus sistemas informáticos, esto se debe a la falta de planificación por parte del área de Sistemas.
- La empresa EPC COMPU no tiene a su disposición un Análisis de Riesgos que permita a la empresa cuantificar el riesgo y las acciones que deban llevarse a cabo.
- EPC- COMPU cuenta con normas de seguridad básicas que no permiten el correcto aseguramiento de los activos de información; por tal razón es recomendable utilizar una normativa estricta y confiable que garantice la confidencialidad y seguridad de la información.

De acuerdo con los resultados obtenidos de la entrevista al Personal de Sistemas, se determinaron los siguientes aspectos:

- El sistema de información que se maneja en la empresa no requiere la utilización de caracteres especiales, letras y números; por este motivo el personal de la institución crea contraseñas simples, dando paso a que personal no autorizado y malintencionado pueda acceder sin consentimiento realizando cambios al sistema.
- Se requiere fortalecer los procesos de capacitación, acuerdos de confidencialidad, procedimientos de desvinculación laboral que garanticen la inhabilitación de usuarios a los sistemas,
- La empresa debe establecer esfuerzos para capacitar a los empleados en materia de seguridad de la información, formular recomendaciones respecto a las vulnerabilidades técnicas de los equipos, protección contra malware, procesos de inicio y cierre seguro de sesiones, confidencialidad respecto a la información que se manipula internamente y concientización sobre la responsabilidad de notificar cuando se detecta una vulnerabilidad en el proceso de acceso y el manejo de la información.

De acuerdo con la ficha de observación aplica en la empresa se demostró que:

- Las instalaciones físicas no cuentan con las seguridades respectivas que brinden el aseguramiento de los recursos existentes en EPC-COMPU.

- Es fundamental etiquetar todos los cables y ordenar el cableado de los computadores que atienden a los clientes.

2.2.5 Metodología desarrollada para el presente trabajo

Para cumplir el desarrollo del proyecto de investigación, se creó una planificación la cual se llevará a cabo de forma secuencial con las siguientes actividades:

1. Comparación de metodologías para la evaluación de riesgos.

2. Desarrollar el Sistema general de Gestión de Seguridad de la Información en base a parámetros de la Norma ISO 27001 para disminuir la ocurrencia de amenazas.

- Análisis de la norma ISO 27001.
- Descripción de los dominios del anexo A
- Creación de un manual basado en la Norma ISO 27001:2013

3. Diseñar el Sistema de Gestión de Seguridad de la Información para la empresa EPC COMPU.

4. Establecer una metodología de evaluación y mejoramiento continuo del SGSI lo cual garantice un adecuado tratamiento de la información.

- Monitorización e implementación de mejoras

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de resultados

3.1.1 Metodologías para la evaluación de riesgos

Escala de valoración

5=Excelente, 4= Muy Bueno, 3=Bueno, 2=Regular, 1=Deficiente

Metodologías Características	Cramm	Magerit	OCTAVE
Alcance y aplicabilidad	3	5	5
Metodología	3	4	3
Ventajas	4	5	3
Limitaciones	3	3	3
Sumatoria	13	**17**	14
Como se puede evidenciar en la sumatoria del cuadro de caracterización Magerit es la metodología más indicada para la evaluación de riesgos.			

Tabla 8. Metodologías para la evaluación de riesgos

Elaborado por: Investigador

3.1.2 Desarrollar el Sistema general de Gestión de Seguridad de la Información en base a parámetros de la Norma ISO 27001 para disminuir la ocurrencia de amenazas

- **Análisis de la norma ISO 27001**

La norma ISO 27001 es una norma emitida por la Organización Internacional de Normalización (ISO) que determina como proteger la seguridad de la información de una empresa, es un estándar certificable por lo tanto cualquier empresa que tenga implementado un SGSI puede solicitar una auditoría externa a una empresa acreditada y recibir la certificación en ISO 27001 esto permite tener una ventaja comercial por

tener controles que van a garantizar a los clientes mantener su información protegida reduciendo así el impacto de las amenazas relacionadas a los activos informáticos.

El objetivo de la ISO 27001 es la prevención de incidentes de seguridad siendo estos grandes o pequeños evitarlos le ahorrará mucho dinero a la empresa garantizando la continuidad laboral. Se basa en un ciclo de vida PDCA(Plan-Do-Check-Act, su significado es Planear, Hacer, Verificar y Actuar) el cual se aplica para organizar los procesos del SGS. Para realizar este objetivo esta norma ha creado clausulas y anexos los que incluyen objetivos de control y controles.

Estándar ISO 27001:2013

Permite a las empresas grandes y pequeñas evaluar el riesgo y el uso de controles necesarios para mitigar las amenazas esta última versión del 2013 refuerza las mejoras continuas del ciclo Deming.

Descripción de los controles del anexo A

El anexo A indica los controles y objetivos de control a poner en marchar a través de los 18 dominios fundamentales que se detallan a continuación:

- A. 5 Políticas de seguridad

Proporciona orientación y apoyo por parte de la dirección a la seguridad informática de acuerdo con las normativas correspondientes.

- A. 6 Organización de la seguridad

Crear un sistema de gestión para controlar el funcionamiento de la seguridad y la implementación dentro de la empresa.

- A. 7 Seguridad de los recursos humanos

Garantizar que los empleados tengan claro sus responsabilidades y si son idóneos para el rol para que se desempeñan.

- A. 8 Gestión de activos

Establecer los activos definiendo las responsabilidades de protección.

- A. 9 Control de acceso

Restringir el acceso a la información y al equipo de procesamiento de la información.

- A. 10 Criptografía

Asegurar el adecuado uso de la criptografía para resguardar la información.

- A. 11 Seguridad física y del entorno

Evitar el acceso no autorizado a las instalaciones de información de la empresa.

- A.12 Seguridad de las operaciones

Respaldar el funcionamiento correcto y seguro de los equipos.

- A. 13 Seguridad de las comunicaciones

Proteger la información en línea y del soporte de procesamiento de la información.

- A. 14 Adquisición, desarrollo y mantenimientos de sistemas

Garantizar que la seguridad informática sea parte importante de los sistemas informáticos incluyendo los requisitos de los sistemas que prestan servicios en una red pública.

- A. 15 Relación con los proveedores

Resguardar la protección de los activos que estén disponibles a los proveedores de la empresa

- A. 16 Gestión de incidentes de seguridad de la información

Garantizar un planteamiento adecuado y coherente de la gestión de problemas de seguridad incluidas las comunicaciones sobre los incidentes de la seguridad y vulnerabilidades.

- A. 17 Aspectos de seguridad de la información de la gestión continua de negocio

Se requiere continuidad de la seguridad informática y esto se debe integrar en los diferentes sistemas de gestión de la continuidad del negocio.

- A. 18 Cumplimiento

Eludir el incumpliendo de responsabilidades legales, reglamentos y de cualquier requisito de la seguridad.

3.1.2.1 Creación de un manual basado en la Norma ISO 27001

MANUAL GENERAL DE LA NORMA ISO 27001

Análisis de la situación actual de la empresa

Se solicita al gerente la información más relevante de la empresa en cuanto a los servicios que ofrece y sus datos empresariales, para plasmar la información se utiliza el siguiente formato.

Nombre de la empresa	
Ubicación	
Introducción a la Empresa	
Servicios	

Tabla 9. Matriz Información de la empresa

Elaborado por: Investigador

Con la ayudar del jefe de TIC se procede a identificar los sistemas de información de la empresa para asi documentarla en el siguiente formato.

Sistema/Sofware	Definición	Características

Tabla 10. Matriz Sistemas de información de la empresa

Elaborado por: Investigador

- Para el análisis de seguridad de la red de la empresa es necesario utilizar herramientas de seguridad informática, para seleccionar la que mejor se adapta a los requerimientos de la empresa.
- Se utilizan los siguientes formatos de tablas.

- Para el análisis del sondeo de puertos se sugiere realizar una comparación de las siguientes herramientas, para elegir la que mejor se adapte a los requerimientos empresariales.

Herramientas **Características**	**Nmap**	**SuperScan6**	**Advanced Port Scanner**	**arp-scan**
Escaneo de puertos	Si	Si	Si	Si
Escaneo de servicios	Si	Si	No	No
Escaneo de vulnerabilidades	Si	No	No	No
Licencia	Open Source	De paga	De paga	Open Source
Plataformas	Multiplataforma	Windows	Windows	Multiplataforma
Documentación	Amplia	Limitada	Limitada	Amplia
De acuerdo con el análisis realizado podemos concluir que las mejores herramientas para realizar el sondeo de puertos es **Nmap y arp-scan**				

Tabla 11. Matriz de Sondeo de puertos

Elaborado por: Investigador

- De igual manera se realiza la comparación de herramientas para el análisis de vulnerabilidades en aplicaciones web como se muestra a continuación.

Herramientas **Características**	**Acunetix**	**Nessus**	**OWASP**
Escaneo de vulnerabilidades	Detecta vulnerabilidades en aplicaciones web	Búsqueda de vulnerabilidades en host y aplicaciones web	Detecta vulnerabilidades en aplicaciones web

			proporcionando una guía de solución para mejorar la seguridad.
Plataformas	Multiplataforma	Multiplataforma	Multiplataforma
Licencia	De paga	Open Source	Open Source
Reportes	Permite generar informes de las vulnerabilidades encontradas para su posterior solución	Permite generar informes detallados de las vulnerabilidades encontradas para solucionarlas.	Permite generar informes en diferentes formatos como pdf, html, xls de las vulnerabilidades encontradas para darle solución.
Soporte Técnico	Actualizaciones disponibles	Actualizaciones disponibles	Profesionales de seguridad activos
Dificultad de uso	Avanzado	Avanzado	Fácil
Se puede concluir que la herramienta **OWASP** es la óptima para realizar el análisis de vulnerabilidad de aplicaciones web.			

Tabla 12. Matriz Vulnerabilidades en aplicaciones web

Elaborado por: Investigador

Cuadros comparativos de Herramientas de Explotación

- Se realiza una comparativa entre las herramientas de phishing permitiendo que se puede seleccionar la mejor.

Herramientas	**Zphisher**	**Nexphisher**	**SocialBox**

Características			
Enfoque	Crea y envía correos electrónicos de phishing y clonación de páginas web	Crea y envía correos electrónicos de phishing	Realiza pruebas de penetración
Personalización	Personaliza correos electrónicos y páginas web de phishing	Personaliza plantillas de phishing	No utiliza personalización para realizar ataques de phishing
Documentación	Presenta documentación completa sobre el uso y configuración de la herramienta	Ofrece documentación básica	Proporciona informacion limitada
Con respecto a las características **Zphisher** es la herramienta ideal para realizar ataques de phishing.			

Tabla 13. Cuadro comparativo de herramientas de phishing.

Elaborado por: Investigador

- Para la creación de códigos maliciosos se realiza una comparación de las siguientes herramientas.

Herramientas **Características**	**Metasploit**	**Darkcommet Rat**	**Quasar Rat**
Funcionalidad	Pentesting y explotación de vulnerabilidades	Control remoto no autorizado a los sistemas	Control remoto no autorizado a los sistemas
Exploits y vulnerabilidades	Extensa colección de exploits actualizados	No está orientado en exploits	No está orientado en exploits

Personalización	Personaliza y desarrolla módulos y scripts	Personalización por defecto	Personalización por defecto
Uso ético	Se utiliza de manera ética y legal	Tiene fines mal intencionados	Tiene fines mal intencionados
Según el análisis de las características **Metasploit** es la herramienta que se usa de manera legal sin fines de lucro.			

Tabla 14. Cuadro comparativo de creación de código malicioso.

Elaborado por: Investigador

- En el siguiente cuadro se presenta una comparación entre las herramientas para realizar ataques de sniffing.

Herramientas **Características**	**Wireshark**	**Burpsuite**	**Ettercap**
Captura de paquetes	Analiza y captura todo el tráfico de la red en tiempo real.	Analiza el tráfico web	Manipula el tráfico de la red
Protocolos	Permite la funcionalidad de varios protocolos de red	Soporta protocolos HTTP Y HTTPS	Incluye protocolos ARP Y TCP
Análisis de tráfico	Brinda herramientas para examinar el tráfico en la red	Analiza y manipula solicitudes de respuesta	Análisis de los paquetes de red.
Documentación	Dispone de una documentación completa	Incluye documentación básica	Brinda documentación básica
De acuerdo con las características, **Wireshark** es la herramienta más indicada para realizar ataques de sniffing.			

Tabla 15. Cuadro comparativo de ataques de sniffing.

Elaborado por: Investigador

- Comparativa de herramientas para la ofuscación de malware.

Herramientas **Características**	**Dotfuscator**	**ProGuard**	**DexGuard**
Funcionalidad	Permite ofuscar y proteger aplicaciones .NET	Ofusca aplicaciones en Java	Ofusca aplicaciones en Android
Ofuscación de código	Tiene métodos avanzados de ofuscación ocultando la lógica del código.	Brinda ofuscación de código protegiendo la lógica del código.	Brinda ofuscación de código protegiendo la lógica del código.
Soporte y documentación	Brinda una amplia documentación y un completo soporte técnico	Soporte limitado	Soporte limitado
Después del análisis de las características, se determina que la mejor herramienta es **Dotfuscator.**			

Tabla 16. Cuadro comparativo de herramientas de ofuscación de malware

Elaborado por: Investigador

- Una vez seleccionada la herramienta a utilizar en la empresa se realiza la recopilación de las vulnerabilidades es importante que el proceso sea lo más detallado posible.
- Los activos de información se definen como los recursos utilizados por los sistemas operativos es decir las bases de datos, correo electrónico y los sistemas de información.

- Para obtener información de la empresa y de sus activos informáticos se sugiere utilizar una ficha de observación.

Aspectos	Observaciones
Listar activos de información	
Estado de los equipos de cómputo	
Identificación de los sistemas operativos	
Estado de la red	
Sistemas de seguridad por equipo	

Tabla 17. Información de la empresa y de sus activos informáticos

Elaborado por: Investigador

Identificar la infraestructura informática y los procesos críticos de la empresa.

- Se debe realizar visitar a la empresa para observar su infraestructura e ir recolectando la información.
- La ayuda del Personal del Departamento de TIC's es importante para definir los procesos críticos de la empresa.
- Una vez obtenida la información detalla anteriormente se procese a clasificarla y documentarla.

Investigar cómo está estructurada la empresa.

- Solicitar el organigrama a la empresa

Determinar las políticas Existentes en la empresa

- Solicitar documentación de políticas de seguridad a la empresa
- Documentar las políticas existentes
- En caso de no contar con políticas listar los controles básicos

Diseño del SGSI

Definir el alcance

Se describe el propósito del SGSI para el cual está siendo diseñado. En el alcance se define los aspectos más importantes de la empresa como:

- Control de activos
- Control de recursos humanos
- Gestión de acceso
- Controlo de las operaciones y comunicación

Definir la política de seguridad

Se establece un objetivo general que abarque las necesidades relacionadas a la gestión de la seguridad de la información en la empresa.
Con el propósito de llevar a cabo la política de seguridad se establecen los siguientes objetivos:

- Evaluar la seguridad de la información, con la finalidad de optimizar los niveles de seguridad de la información.
- Establecer una evaluación de riesgos para detectar vulnerabilidades en los activos de información para optimizar el control de la seguridad.
- Implementar el sistema de gestión de la seguridad de la información para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Supervisar el SGSI para garantizar el correcto tratamiento de la información

Análisis de riesgos

Existen diferentes tipos de riesgos que se pueden presentar en las empresas

- Riesgos de seguridad informática

Entre los riesgos se puede enlistar los siguientes:
Malware: revisar que los equipos tengan antivirus para evitar que se infecte.
Robo de datos: evitar visitar sitios no seguros y no ingresando los datos personales.
DoS: verificar que el servidor cuente con firewall.

Pishing: evitar abrir correos con contenidos de spam.

- Riesgos de pérdida de datos

Pueden ser causados por:

  - Errores humanos

Realizar copias de seguridad en caso de pérdida de datos por error.

  - Evitar que el usuario descargue archivos desconocidos.
  - Errores Físicos

Realizar copias de seguridad en caso de fallos en el disco duro

  - Fallos de los sistemas de respaldo
- Realizar un monitoreo de los sistemas de respaldo.
  - Desastres naturales.
    - Contar con clúster de base de datos
    - Mantener un convenio vigente con varios proveedores para la sustitución de los activos informáticos.
    - Tener un plan de contingencia ante desastres naturales.

- Riesgos operativos
  - Falta de capacidad
    - Mejorar la capacidad de los equipos mediante la implementación de discos sólidos y aumento de memoria ram.
  - Riesgos de reputación
    - Incidentes de seguridad
      - Disponer de señalización en áreas restringidas.

Metodología Magerit para la evaluación de riesgos

Esta metodología es útil para enforcar esfuerzos en los riesgos más críticos relacionados con los sistemas de información de la empresa. Su objetivo principal es

identificar y aplicar las medidas de control más adecuadas para mitigar las vulnerabilidades de manera efectiva.

En la **Tabla 8,** se puede observar la comparación de las metodologías

Las fases de esta metodología son:

Identificación de activos

- Obtener información del activo mediante la observación
- Clasificar el activo
- Utilizar el siguiente formato de tabla

Nª	Activo	Clasificación del Activo

Tabla 18. Formato de Identificación y Clasificación de activos

Elaborado por: Investigador

Tasación de los activos

Sirve para ver la relevancia que tienen los activos en la empresa.

Menos importante	1
Poco Importante	2
Algo importante	3
Importante	4
Muy importante	5

Tabla 19. Valoración de activos de acuerdo a su importancia.

Elaborado por: Investigador

Aplicar las directrices de confiabilidad, integridad y disponibilidad de los activos teniendo en cuenta el proceso de valoración de activos que varía de 1 a 5, siendo un valor de 5 el más importante y un valor de 1 el menos importante como se muestra a continuación.

Se procede a calcular el promedio del total del riesgo. Utilizando el siguiente formato de tabla.

Activo	Confidencialidad	Disponibilidad	Integridad	Valor del activo

Tabla 20. Formato de Tasación de activos

Elaborado por: Investigador

Identificación de amenazas

- Identificar las amenazas y vulnerabilidades a los que están expuestos los activos mencionados
- Definir la frecuencia de ocurrencia de la amenaza de manera mediante la siguiente tabla

Casi nunca	1
Algunas veces	2
A menudo	3
Casi siempre	4
Siempre	5

Tabla 21. Frecuencia de ocurrencia de la amenaza

Elaborado por: Investigador

- Calcular el riesgo total teniendo en cuenta la obtención del valor del activo en la tabla de tasación de activos por la probabilidad de la amenaza.
- Utilizar el siguiente modelo de tabla

Activo	Amenazas	Vulnerabilidades	Valoración de activo	Frecuencia de ocurrencia de la Amenaza	Riesgo total

Tabla 22. Formato Calculo del riesgo total de activos.

Elaborado por: Investigador

Selección de Controles

A continuación, se presentan los 18 dominios de la norma ISO 27001:2013

- A.5 Políticas de seguridad de la información
- A.6: Organización de la Seguridad de la información
- A 7 Seguridad de los recursos humanos
- A.8 Gestión de Activos
- A 9 Control De Acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimientos de sistemas
- A.15 Relación con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio
- A.18 Cumplimiento

Se utiliza el siguiente formato de tabla para relacionar los controles definidos en la norma ISO 27001:2013, tomando como referencia los activos con mayor índice de riesgo.

Activo	Amenazas	Vulnerabilidades	Valoración del Activo	Frecuencia de ocurrencia de la Amenaza	Riesgo Total	Objetivo de Control

Tabla 23. Modelo Selección de Controles.

Elaborado por: Investigador

Declaración de la aplicabilidad

Se utiliza el siguiente formato de tabla para elaborar la Declaración de Aplicabilidad – SOA (Arquitectura Orientada a Servicios) el cual es un documento basado en los apartados de la norma ISO 27001 (Ver ANEXO 1), siendo uno de los puntos de partida para la aplicación del SGSI.

A.5 Políticas de seguridad de la información				
A.5.1 Directrices establecida por la dirección para la seguridad de la información				
SECCIÓN	CONTROLES ISO 27001:2013	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	

Tabla 24. Modelo Declaración de Aplicabilidad – SOA.

Elaborado por: Investigador

El proceso consiste en identificar los controles que se implementaran, así como la justificación necesaria de aquellos que no sean aplicables. La declaración de aplicabilidad debe ser revisada y aprobada por el jefe encargado del Área o Departamento de Sistemas

Análisis del cumplimiento de los controles

- Realizar de manera conjunta con el jefe de sistemas
- Elaborar la gráfica de cumplimiento para cada área en la que se detallan los porcentajes obtenidos.

Establecer Políticas y controles para la seguridad de la información para la empresa EPC COMPU

- Definir las políticas de seguridad de la Información en base al análisis de cada uno de los controles que son aplicables

Definir los procesos de seguimiento de los controles establecidos

- Para verificar el seguimiento de los controles se definen los responsables y sus actividades, posteriormente se definen los procesos con los cuales se dará cumplimientos de dichos controles

Elaboración del Manual del Plan de Contingencia

Se establece un plan de contingencia el cual permitirá aplicar medidas de seguridad ante la presencia de riesgos, con la finalidad de minimizar o evitar que los mismos se materialicen y de esta manera resguardar la seguridad de la información.

Monitorear y Revisar el SGSI

Una vez que el Sistema de Gestión de Seguridad este implementado se debe realizar un monitoreo para detectar posibles falencias del SGSI y poder mantener un nivel elevado de seguridad, por eso es necesario recolectar datos que ayuden a revisar el estado actual en la empresa.
Para reflejar lo antes mencionado se plantea seguir con los siguientes pasos:

- Monitorear el SGSI de manera anual
- Definir procedimientos de monitoreo y revisión.

Dar a conocer el SGSI a la dirección

Una vez que se dé por terminado el diseño del SGSI se dará a conocer a la gerencia para que den su aprobación.

Capacitación al personal para conocer el Sistema de Gestión de Seguridad de la información y el plan de contingencia

Se debe brindar capacitaciones al personal y a los nuevos empleados que ingresen a laborar en EPC COMPU de idéntica manera deben ser capacitados sobre la

importancia del Sistema de Gestión de la Seguridad de la Información y el plan de contingencia como se observa en el **ANEXO 5.**

3.2 Desarrollo de la propuesta

3.2.1 Diseñar el Sistema de Gestión de Seguridad de la Información para la empresa EPC COMPU.

3.2.1.1 Análisis de la situación actual de la empresa

Se realizó un análisis para evaluar el estado actual de la empresa por la cual se obtuvo la información de la empresa.

Información de la Empresa

Beneficiario	EPC COMPU
Ubicación	Ecuador Tungurahua / Ambato
Introducción a la Empresa	EPC-COMPU es una empresa enfocada a brindar el servicio de mantenimiento y reparación de dispositivos electrónicos como: Impresoras, Portátiles, CPU, Tablets y Monitores dentro de la ciudad de Ambato. Para mejora del servicio ofrecido, dispone a sus clientes la entrega y recepción de su dispositivo electrónico de puerta a puerta mediante la gestión georreferenciada, así como la gestión de la gestión de mantenimiento y reparación se la emplea mediante el sitio web ECP-COMPU.
Servicios	Mantenimiento: se lo realiza después de un diagnóstico previo del dispositivo electrónico, estimando un mantenimiento preventivo o correctivo. Reparación: se lo realiza después de un diagnóstico previo del dispositivo electrónico, identificando la parte

	a repararse y definiendo el elemento de cambio con el fin de solucionar el problema.

Tabla 25. Información de la empresa.

Elaborado por: Investigador

Organigrama

Se puede observar cómo se divide y organiza la jerarquía interna, mostrando los diferentes niveles de autoridad, responsabilidad y relaciones entre los distintos departamentos y empleados.

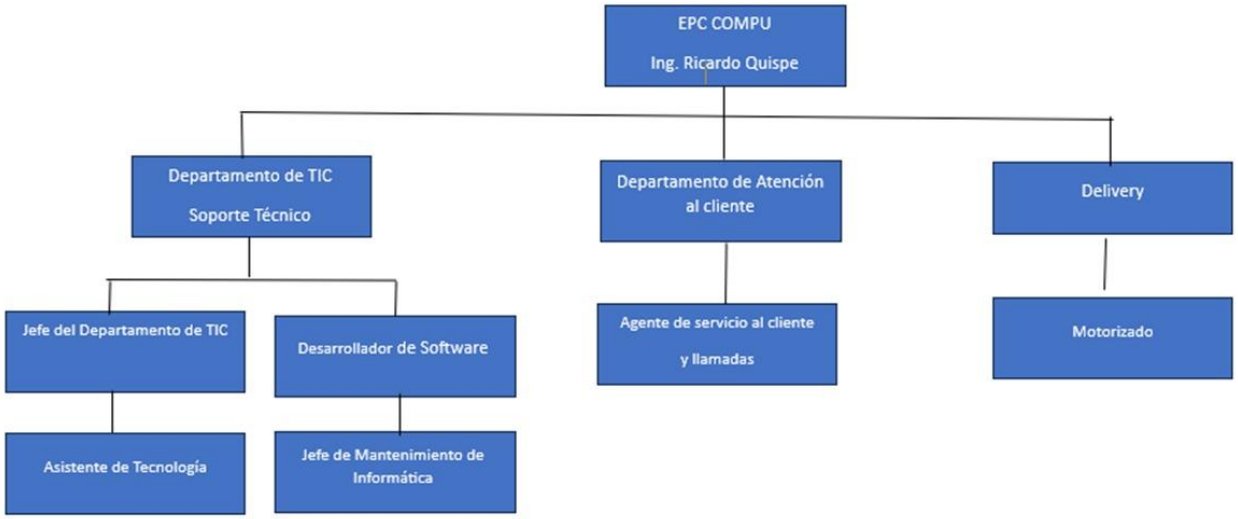


Figura 1. Organigrama

Para el crecimiento del entorno empresarial he desarrollado una propuesta que tiene como objetivo fortalecer la capacidad para enfrentar los desafíos actuales y futuros con mayor eficiencia y agilidad. Ver **ANEXO 6**

Estructura Física

En el siguiente plano se puede determinar que hay una ineficiente distribucion de los espacios que componen la empresa por lo que habia cierta incomodidad por parte de la secretaria al no contar con un espacio para ella al igual el echo de que no exista dos baños tambien era un problemay es ese motivo que se plantea una nueva ingraestructura.

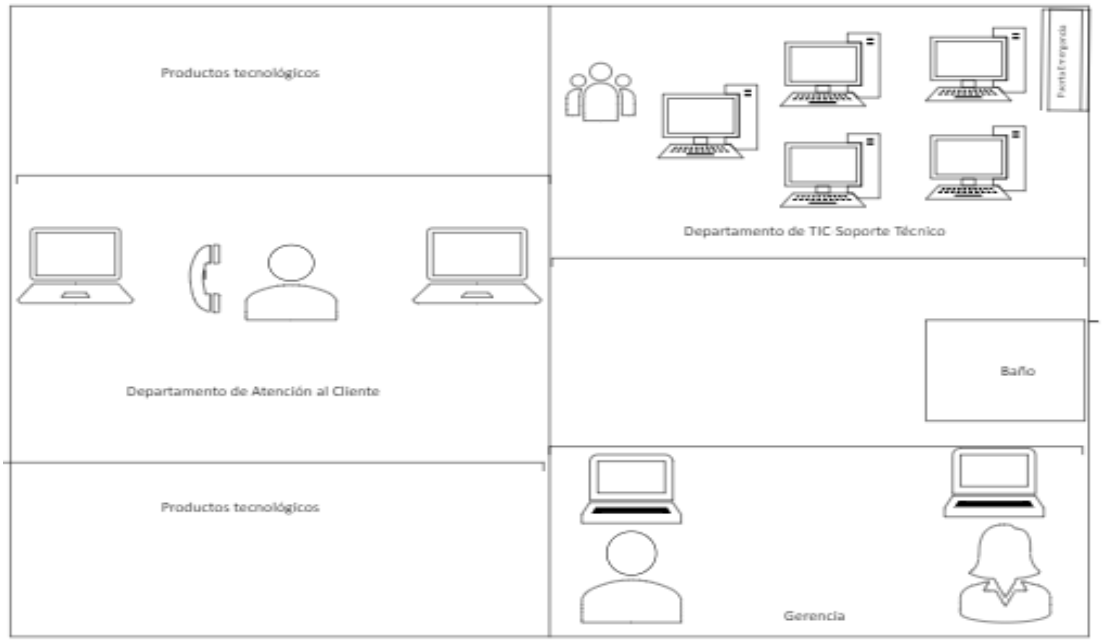


Figura 2.Estructura Física

Debido a la falta de departamentos y organización de los empleados, se propone una nueva infraestructura física donde el espacio de trabajo principal está compuesto por áreas de trabajo compartidas donde los equipos trabajan en estaciones abiertas equipadas con escritorios ajustables. Estas áreas fomentan la colaboración informal y permiten a los empleados cambiar fácilmente de entorno según sus necesidades. Se ha creado áreas de descanso cómodas y atractivas donde los clientes pueden tomar un descanso también están equipadas con una infraestructura tecnológica sólida, cada estación de trabajo tiene acceso a conexiones de red de alta velocidad y enchufes de energía convenientemente ubicados el precio de la nueva infraestructura física seria alrededor de 2 mil dólares. Ver **ANEXO 8**

En la siguiente tabla identificamos los sistemas de información y software utilizados en los equipos de la empresa EPC COMPU

Sistema / Software	Definición	Características
Sistema web para la gestión de servicio técnico	Es un sistema realizado en .NET que utiliza la base de datos SQL Server. Permite realizar la gestión de soporte técnico para optimizar entregas y recepciones de equipos de tal manera que permite optimizar el trabajo en la empresa. [21]	• Permite solicitar la entrega y recepción de dispositivos a domicilio por lo cual se lo implemento utilizando georreferenciación. [21]
Avast Antivirus	Es una tecnología para monitorizar las aplicaciones para encontrar cualquier indicio de peligro de software malicioso en el equipo. [22]	• Análisis inteligente • Protección Del Equipo • Mayor facilidad de uso • Escudos en tiempo real de avast • AutoSandbox • Antispam. [22]

Zoom	Es una plataforma online de web conference, permite realizar video-llamadas en alta definición, con la funcionalidad de compartir escritorio, pizarra, chat, grabar la conferencia, compartir documentos, y poder acceder desde cualquier lugar ya que está disponible para dispositivos móviles.[23]	• Videoconferencia • Sala De Videoconferencia • Compartir Pantalla • Chat. [23]
AnyDesk	Es una herramienta de control y acceso remoto entre dispositivos. En CEIP la vamos a utilizar para poder acceder a cualquier computadora (que lo tenga habilitado) desde cualquier dispositivo con conexión a Internet (tablet, celular, PC, etc.) que podamos tener a nuestro alcance desde fuera de la oficina. Funciona como alternativa a la herramienta TeamViewer**.** [24]	• Acceso remoto bidireccional entre Windows, macOS, Linux y FreeBSD. • acceso unidireccional desde las plataformas móviles Android y iOS • protocolo seguro TLS-1.2 • transferencia de archivos. • chat cliente a cliente. • integración portapapeles. • registro de sesiones.[24]

Office	Microsoft Office es una suite ofimática creada por la empresa Microsoft. Funciona oficialmente bajo los sistemas operativos Microsoft Windows y Apple Mac OS, aunque también lo hace en Linux si se utiliza un emulador como Wine o CrossOver Office. Además de aplicaciones incluye servidores y servicios basados en Web. [25]	• Aplicaciones móviles. • Skype Empresarial. • Servicio de hosting web. • Servicio de correo integrado. • Integración con Active Directory. • Integración con otros productos Microsoft. ... • Servicio de copia de seguridad automática. [25]
VirtualBox	Es un software de virtualización a nivel de sistema operativo actualmente desarrollado por Oracle Corporation que puede simular arquitecturas de 32 bits (x86) y 64 bits (x64) y sistemas operativos Linux, Windows, Mac OS, etc. Con este programa podremos tener nuestro "propio pc" con varios sistemas operativos en uno. [26]	• Portabilidad: • Herramientas adicionales o Guest Additions • Gran soporte de hardware. [26]

Microsoft Visual Studio 2019	Visual Studio es una herramienta de desarrollo eficaz que permite completar todo el ciclo de desarrollo en un solo lugar. Es un entorno de desarrollo integrado (IDE) completo que puede usar para escribir, editar, depurar y compilar el código y, luego, implementar la aplicación. Aparte de la edición y depuración del código, Visual Studio incluye compiladores, herramientas de finalización de código, control de código fuente, extensiones y muchas más características para mejorar cada fase del proceso de desarrollo de software. [27]	• Desarrolle su código • Compilación de la aplicación • Colaboración con otros usuarios • Depurar el código • Prueba del código • Control de versiones • Implementación de la aplicación. [27]
SQL Server	Microsoft SQL Server es uno de los principales sistemas de gestión de bases de datos relacional del mercado que presta servicio a un amplio abanico de aplicaciones de software destinadas a la	• Inteligencia en todos sus datos con clústeres de Big Data: • Elección de Lenguaje y Plataforma • Capacidades de bases de datos inteligentes**:** • Cifrado de datos y cumplimiento normativo • BI móvil y escalabilidad. [28]

	inteligencia empresarial y análisis sobre entornos corporativos. Basada en el lenguaje Transact-SQL, incorpora un conjunto de extensiones de programación propias de lenguaje estándar y su aplicación está disponible para usarse tanto a nivel on premise o bajo una modalidad cloud. [28]	
Putty	En general, Putty no es más que una terminal de simulación *open source* que fue desarrollado para actuar como cliente de conexiones seguras a través de protocolos raw TCP, Telnet, rlogin y portal serial. Por lo tanto, este software se indica para establecer conexiones seguras de acceso remoto a servidores a través de Shell Seguro (SSH y para construir canales encriptados entre servidores.	• Software sin costo • Conexiones seguras • Varias posibilidades de edición • Compatibilidad • Sin impacto en los servicios de alojamiento. [29]

	De esta manera, Putty fue desarrollado para el uso, principalmente de programadores y administradores de red, ya que su interfaz es prácticamente configurable y cuenta con numerosas opciones de ajuste de conexiones. [29]	
Xampp	XAMPP es una distribución de Apache completamente gratuita y fácil de instalar que contiene MariaDB, PHP y Perl. El paquete de instalación de XAMPP ha sido diseñado para ser increíblemente fácil de instalar y usar. [30]	• **Multiplataforma** • Versión estándar y una versión completa. • El usuario puede iniciar y finalizar toda la pila del servidor web más la base de datos con un solo comando. • Alojamiento web. [30]
CPU-Z	CPU-Z es un programa de detección de hardware gratuito para el sistema operativo Windows de Microsoft. **Se** trata de una aplicación que ayuda a recopilar información del sistema, y luego muestra los detalles en una sola pantalla. CPU-Z es desarrollado por CPUID y actualizado	• Caché de nuestro procesador • Datos de nuestra placa base • Nuestra memoria RAM al detalle • Podemos saber que tarjeta gráfica tenemos • Incorpora un benchmark muy liviano. [31]

	regularmente, gracias a lo cual es compatible con la mayoría de los procesadores y chipsets, incluso los más nuevos. [31]	
Adobe Reader	El software Adobe Reader DC es la versión más moderna de la herramienta creada para leer los documentos en formato PDF. Las siglas 'DC' indican 'Document Cloud', que nos agrega la función de sincronizar documentos en todos los dispositivos mediante la nube. Una función está solo disponible mediante el sistema Cloud de Adobe, que permite compartir, firmar y almacenar documentos de manera segura. [32]	• Adobe Sign: Permite firmar documentos legalmente y entregarlos en cualquier dispositivo. La firma se realiza mediante el dedo en una pantalla táctil o bien mediante certificados digitales • Adobe Send & Track: Mediante Document Cloud podemos mandar grandes archivos de manera segura y evitar adjuntar archivos a los correos. • Export PDF: Permite la conversión de cualquier documento PDF a formatos Word. [32]

Tabla 26. Sistemas de información y software.

Elaborado por: Investigador

Diagrama de Red

La empresa está diseñada por una topología anillo en donde solo existe un segmento de red en donde solo existe un dominio de red en el cual se da la comunicación de todos los equipos de la red, esta red es vulnerable porque permite compartir todos los recursos de la red sin ningún límite de restricciones y no se puede controlar el acceso a la información.

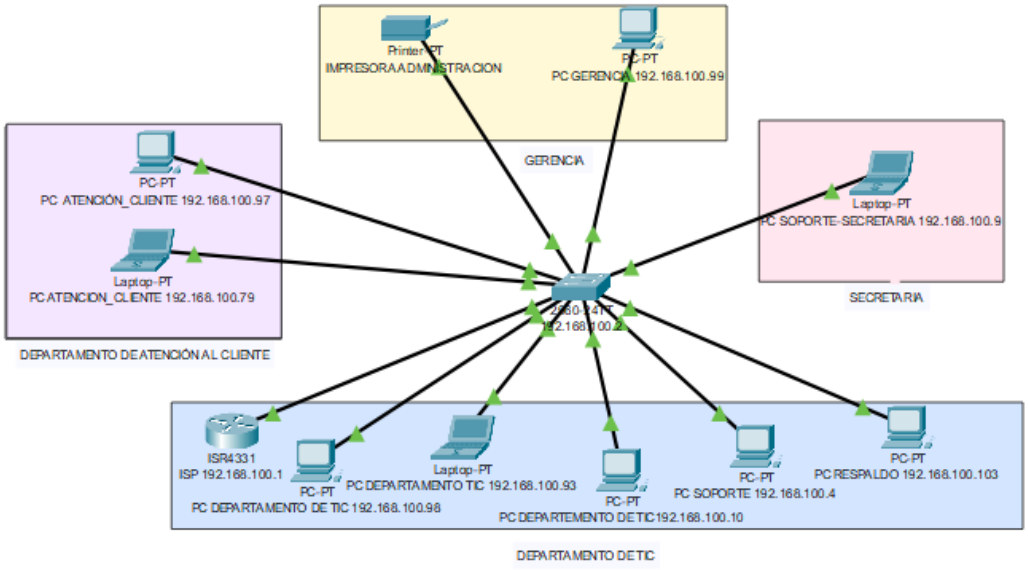


Figura 3. Diagrama de Red

Elaborado por: Investigador

Como solución al diagrama de red se plantea contar con dispositivos que sean gestionables y permitan una mejor gestión y aseguren la red. Para un mejor rediseño de la red se optó por crear VLAN en donde no se va a permitir compartir información dentro de la red LAN y están dentro de un switch, las ACL son políticas de control de acceso que están implementadas dentro del router que van a denegar el tráfico de datos provenientes de internet o dentro de la red LAN hacia el internet permitiendo la seguridad al limitar cierto tráfico para evitar ataques cibernéticos. Ver **ANEXO7**

Estado actual de la empresa

Para determinar el estado actual de la seguridad de la red dentro de EPC COMPU se realizó una comparación entre varias herramientas que se puede ver en la **Tabla 11** donde se consideró utilizar arp scan y Nmap porque son óptimas para el sondeo de toda la red estas herramientas permiten detectar los hosts en línea y locales, puertos

abiertos, servicios, aplicaciones versiones del sistema operativo, DNS, direcciones MAC, de idéntica manera soportan direcciones IPv4 e IPv6, y reconocimientos de sistemas.

3.2.1.2 Resultados de las herramientas de sondeo de puertos

Sondeo de Red

Con el debido permiso de la empresa se procedió a obtener las direcciones IP de toda la red, estas fueron analizadas por la herramienta arp-scan-l de Kali Linux, para esto se realizará una búsqueda en la red.

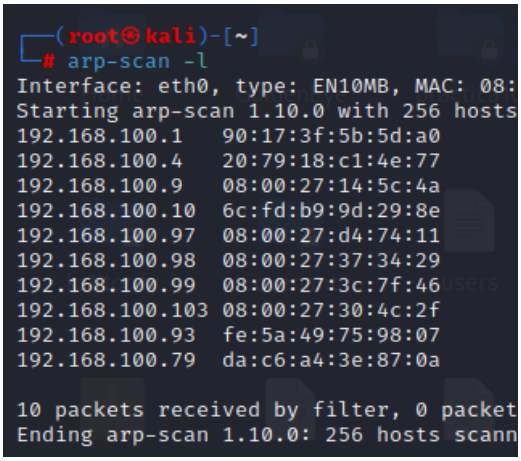


Figura 4. Lista de dispositivos conectados a la red

Elaborado por: Investigador

Análisis de Vulnerabilidades con Nmap

Puertos Abiertos en el Equipo con Windows Server 2012

Figura 5. Puertos Abiertos en el Equipo con Windows Server 2012.

Elaborado por: Investigador

Este equipo maneja el gerente, la Figura 5 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión.

Puertos Abiertos en el Equipo con Ubuntu

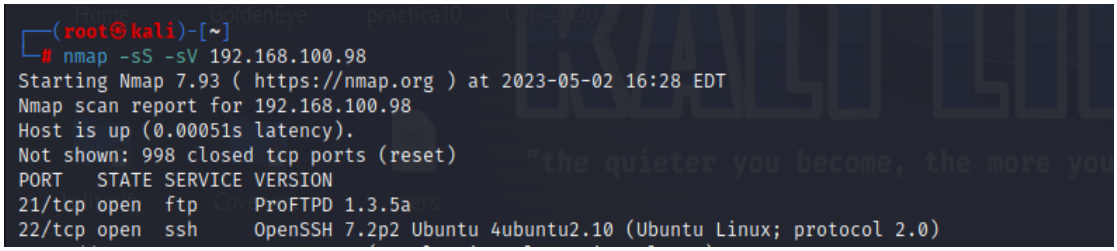


Figura 6.Puertos Abiertos en el Equipo con Ubuntu.

Elaborado por: Investigador

Este equipo funciona como un servidor local en el que se almacena información relevante de la empresa, pruebas de sitios web, la Figura 6 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión

Puertos Abiertos en el Equipo con Windows 10

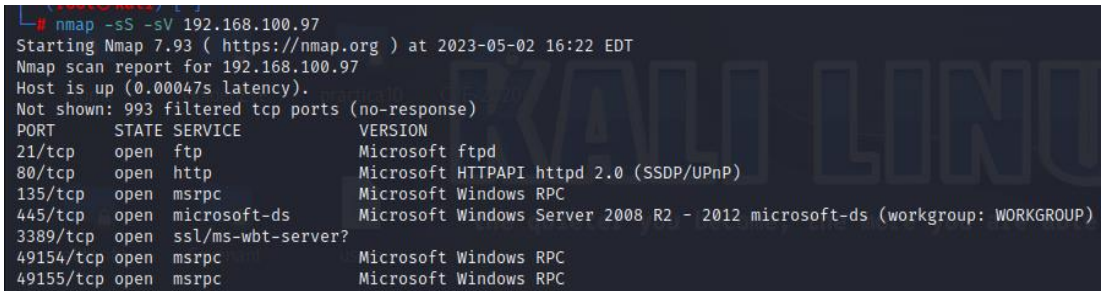


Figura 7. Puertos Abiertos en el Equipo con Windows 10.

Elaborado por: Investigador

Este equipo funciona como cliente y atención a los clientes de la empresa, la Figura 7 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión

Puertos Abiertos en el Equipo con Windows 11

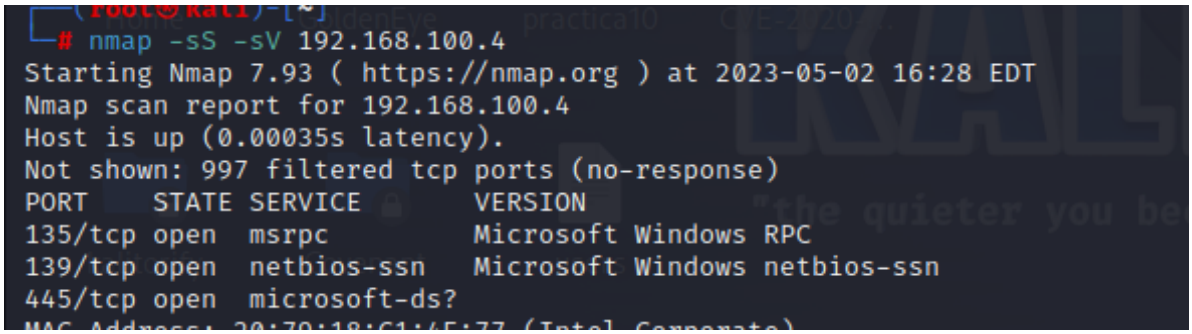


Figura 8. Puertos Abiertos en el Equipo con Windows 11.

Elaborado por: Investigador

Este equipo funciona como máquina de soporte técnico, la Figura 8 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión.

Puertos Abiertos en el Equipo con Windows 8.1

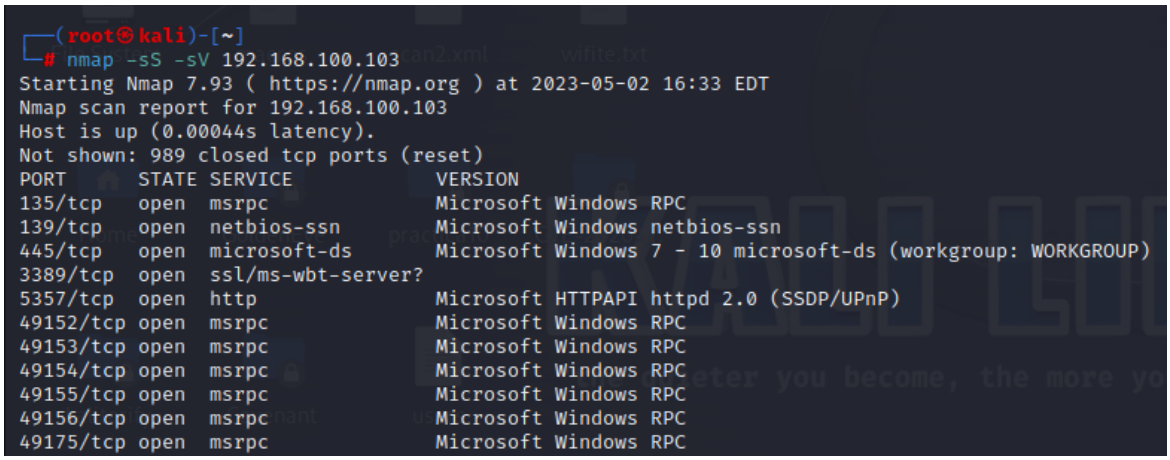


Figura 9.Puertos Abiertos en el Equipo con Windows 8.1.

Elaborado por: Investigador

Este equipo funciona para sacar respaldo de la información, la Figura 9 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión.

Puertos Abiertos en el Equipo con Windows 7

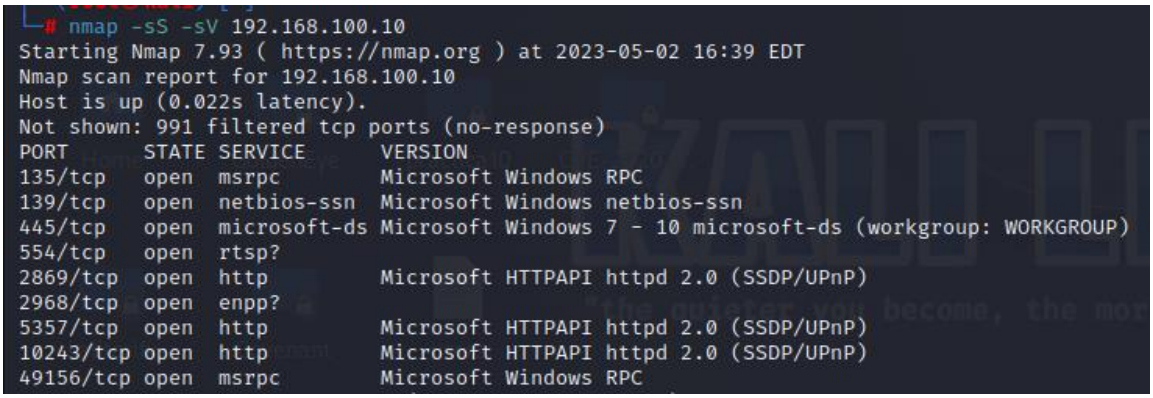


Figura 10. Puertos Abiertos en el Equipo con Windows 7.

Elaborado por: Investigador

Este equipo lo maneja el departamento de TIC, la Figura 10 muestra el escaneo del equipo con NMAP en el que se detallan los puertos, el estado y su servicio con su correspondiente versión

Una vez analizada la **Tabla 12**, referente a las herramientas para la obtención de vulnerabilidades se optó OWASP dicha herramienta permite realizar escaneos avanzados además cuentan con varias funciones como análisis de vulnerabilidades, análisis web, detección de recursos, escaneo de redes, evaluación de vulnerabilidades, además, cuentan con reportes flexibles y de fácil interpretación.

3.2.1.3 Resultados del análisis de vulnerabilidades al Sistema Web con OWASP

Se identificaron vulnerabilidades en la aplicación web “Sistema Web Para La Gestión De Servicio Técnico Aplicando Georreferenciación Para La Recepción Y Entrega De Dispositivos Tecnológicos” de la empresa EPC COMPU.

PROBLEMA	RIESGO	DESCRIPCION	SOLUCION
Ausencia de tokens anti-CSRF	Medio	Los ataques CSRF son efectivos en una serie de situaciones, que incluyen:	Utilice el control de gestión de sesiones ESAPI. Este control

		La víctima tiene una sesión activa en el sitio de destino. La víctima se autentica mediante autenticación HTTP en el sitio de destino. La víctima está en la misma red local que el sitio de destino.	incluye un componente para CSRF. No utilice el método GET para ninguna solicitud que desencadene un cambio de estado. Verifique el encabezado HTTP Referer para ver si la solicitud se originó en una página esperada. Esto podría interrumpir la funcionalidad legítima, ya que los usuarios o los representantes pueden haber deshabilitado el envío del Recomendado por motivos de privacidad.
Encabezado de política de seguridad de	Medio	La Política de seguridad de contenido (CSP) es una capa	Asegúrese de que su servidor web, servidor de

contenido (CSP) no establecido		adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java,	aplicaciones, balanceador de carga, etc. esté configurado para establecer el encabezado de política de seguridad de contenido.

		ActiveX, archivos de audio y video.	
Falta el encabezado antisecuestro de clics	Medio	La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra los ataques de 'ClickJacking'.	Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web devueltas por su site/app.
Vulnerable JS Library	Medio	El programa de arranque de biblioteca identificado, versión 3.3.5, es vulnerable.	Actualice a la última versión de bootstrap.
Inclusión de archivos fuente de JavaScript entre dominios	Bajo	La página incluye uno o más archivos de script de un dominio de terceros.	Asegúrese de que los archivos fuente de JavaScript se carguen solo desde fuentes confiables y que los usuarios finales de la aplicación no puedan controlar las fuentes.
El servidor filtra información a través de los campos de	Bajo	El servidor web/aplications está filtrando información a través de uno o más	Asegúrese de que su servidor web, servidor de aplicaciones,

encabezado de respuesta HTTP "X-Powered-By"		encabezados de respuesta HTTP "X-Powered-By". El acceso a dicha información puede facilitar a los atacantes la identificación de otros marcos/componentes de los que depende su aplicación web y las vulnerabilidades a las que dichos componentes pueden estar sujetos.	equilibrador de carga, etc. esté configurado para suprimir los encabezados "X-Powered-By".
Encabezado de respuesta de la versión X-AspNet	Bajo	El servidor filtra información a través de los campos de encabezado de respuesta HTTP "X-AspNet-Version"/"X-AspNetMvc-Version".	Configure el servidor para que no devuelva esos encabezados.
Falta el encabezado X-Content-Type-Options	Bajo	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no se configuró en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de	Asegúrese de que aplication/web establezca el encabezado de tipo de contenido correctamente y que establezca el encabezado X-Content-Type-Options en 'nosniff'

		la respuesta, lo que podría causar que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido diferente al tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se ha configurado uno), en lugar de realizar un análisis MIME.	para todas las páginas web.
Divulgación de información - Comentarios sospechosos	Informativo	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante. Nota: Las coincidencias realizadas dentro de los bloques de secuencias de comandos o archivos se refieren a todo el contenido, no solo a los comentarios.	Elimine todos los comentarios que devuelvan información que pueda ayudar a un atacante y solucione cualquier problema subyacente al que se refieran.

Tabla 27: Vulnerabilidades al Sistema Web con OWASP

Elaborado por: Investigador

Una vez analizados los cuadros comparativos de las herramientas de explotación se seleccionó Zpisher como se observa en la **Tabla 13**, para la creación del código

malicioso se seleccionó Metasploit como se observa en la **Tabla 14**, se elige Wireshark para hacer sniffing como se observa en la **Tabla 15** y finalmente Dotfuscator para realizar ofuscación de malware como se observa en la tabla **Tabla 16.**

3.2.1.4 Resultados de la explotación de vulnerabilidades en los equipos mediante ataques de seguridad informática

PROBLEMA	DIAGNÓSTICO	SOLUCIÓN
Pishing con email	Se utilizó el sistema operativo Kali Linux con la herramienta Zpisher porque se evidencio la presencia de pishing en los correos de los empleados. Mensaje ilegitimo de correo con enlace, clonación de página web, robo de Credenciales de correo Gmail.	No abrir correos electrónicos de remitentes que no sean oficiales, si recibe un correo electrónico de una fuente navegue anónimamente y verifique que la URL de la página comienza con "HTTPS" en lugar de simplemente "HTTP". La "S" significa "seguro". Se debe tomar en cuenta que no es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Además, verifique que la pagina es segura dando click en candado y que tenga certificado SSL
Pishing con email y archivo adjunto	Se utilizó el sistema operativo Kali Linux con la	No abrir correos electrónicos de remitentes

	herramienta Metasploit porque se evidencio la presencia de pishing en los correos de los empleados con archivos adjuntos. Mensaje ilegitimo de correo con enlace, Enlace con archivo pdf adjunto	que no sean oficiales y no descargar archivos adjuntos
Malware	Se utilizó el sistema operativo Kali Linux con la herramienta Metasploit porque se evidencio la presencia de malware en los equipos Escalamiento de privilegios, Acceso remoto no autorizado del equipo	Si se descarga algún documento pdf asegurarse que tenga la extensión, pdf,, Es recomendable subir cualquier archivo descargado de internet a virus total
Pishing y Malware	Se utilizó el sistema operativo Windows con la herramienta cmd para crear el malware indetectable y se utilizó netcat de Kali Linux porque se evidencio la presencia de malware en los equipos Servicios desconocidos ejecutándose en segundo plano	Realizar un seguimiento de todos los equipos informáticos con la suit de Microsoft Sysinternals Suite para monitorear todos los procesos de un computador y matar los procesos desconocidos que son utilizados por malware
Sniffing	Se utilizó la herramienta Wireshark, porque se evidencio la falta de control en las redes.	Es necesario que sistema contrate otro dominio y maneje la seguridad con el protocolo HTTPS y con el

	Obtención de las credenciales del usuario administrador a través de http. Falta de controles para acceder al sistema de información	certificado SSL, Establecer contraseñas robustas para los administradores y usuarios, Utilizar Gestores de contraseñas, Establecer en el sistema empresarial un factor de doble autenticación
Escritorio remoto RDP	Se utilizó el Sistema Operativo Kali Linux con la herramienta Metasploit Pantallazo Azul en Windows 7	Actualización del Sistema Operativo
Ataque de fuerza bruta con diccionarios	Se utilizó el Sistema Operativo Kali Linux con la herramienta Metasploit Escalamiento de privilegios a través del puerto ssh 22 del servidor Ubuntu	Actualizar el Sistemas Operativo a la versión actual de Ubuntu, Establecer contraseñas robustas para los administradores y usuarios, utilizar Dispositivos Firewall en el servidor para brindar seguridad de red para restringir el tráfico de Internet entrante, saliente o dentro de una red privada.
Vulnerabilidad smb(MS17-010)	Se utilizó el Sistema Operativo Kali Linux con la herramienta Metasploit	Descargar parches de seguridad de Soporte de Microsoft, Actualizar el Sistemas Operativo,

	Escalamiento de privilegios a través del puerto smb 445 del servidor Windows Server 2012 R2	utilizar Dispositivos Firewall en el servidor para brindar seguridad de red para restringir el tráfico de Internet entrante, saliente o dentro de una red privada.
Falta de segregación de las redes y seguridad en los servidores	Se utilizó el Sistema Operativo Kali Linux con la herramienta Arp-Scan, nmap Equipos conectados a una sola red El acceso no autorizado de terceros a la red Puertos Abiertos sin monitorear Incidentes de seguridad en la red	Segmentar la red en áreas de: sistemas, atención al cliente y mantenimiento. Monitorear los servidores y cerrar puertos innecesarios. Adicionalmente se puede utilizar sistemas IDS, IPS para detecta amenazas potenciales en la red. se puede utilizar Proxy para restringir el contenido de sitios web en los clientes, Utilizar redes VPN

Tabla 28:Vulnerabilidades en los equipos mediante ataques de seguridad informática

Elaborado por: Investigador

3.2.2 Identificar la infraestructura informática y los procesos críticos de la empresa.

El proceso crítico de la empresa es un:

Sistema Web Para La Gestión De Servicio Técnico Aplicando Georreferenciación Para La Recepción Y Entrega De Dispositivos Tecnológicos

Los procesos informáticos que tiene la empresa EPC COMPU como infraestructura de TI a nivel de software son:

- **Elementos del Sistema**
  - Framework .NET
  - Cuentas de Usuario
  - Base de Datos SQL Server
  - Dispositivos pasivos y activos de red

Procesos del Sistema

- Ingreso de credenciales al sistema
- El cliente solicita el retiro de la reparación o mantenimiento de su equipo y realiza el pago

Elementos a nivel de Hadware

- Computador
- Servidores
- Swiches
- Routers

En la siguiente figura se muestra la Descripción del Proceso de Soporte Técnico en la que maneja el sistema de la empresa EPC COMPU

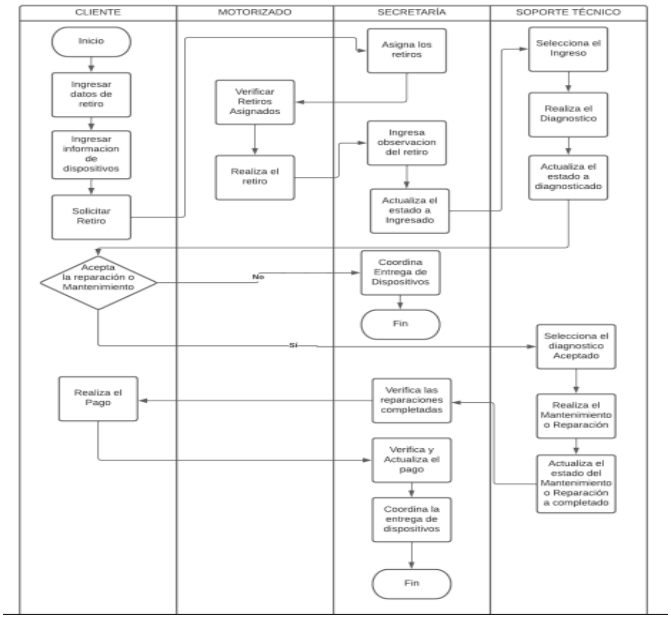


Figura 11. Descripción del Proceso de Soporte Técnico en la Empresa EPC COMPU.

Elaborado por: EPC COMPU

3.2.3 Determinar las políticas Existentes en la empresa

La empresa EPC COMPU de la ciudad de Ambato no cuenta con políticas establecida para realizar diferentes procesos que garanticen la seguridad de la información, la empresa en mención cuenta con varias normas para cubrir diferentes procesos que deberían contar con una política clara y concisa. Entre las normas que cumple dicha empresa se encontraron las siguientes:

- Mantenimiento anual preventivo de activos informáticos.
- Inventario anual y control de Bienes.
- Esquemas de autorización y autenticación para las diferentes plataformas de la organización.
- Generación Respaldos de la información.
- Administración de usuarios.

3.2.4 Diseño del SGSI

3.2.4.1 Alcance del SGSI

EPC COMPU define el alcance del SGSI a los servicios y sistemas que manejan información relacionada con los procesos de la empresa.

A continuación, se detalla cada uno de los procesos que se contemplaran el alcance:

- Control de activos. - Ayudará a un mejor manejo de la seguridad de la información, así como brindar responsabilidades al personal que hace uso de cada uno de los activos en relación con las vulnerabilidades y riesgos dentro de la empresa.
- Control de recursos humanos. – Brindará un control adecuado y capacitaciones oportunas al personal de EPC COMPU, así como el compromiso del recurso humano ayudará a que exista un mejor control de la seguridad de la información, como una mejor gestión en los recursos durante el periodo laboral también de la culminación del mismo.
- Gestión de acceso. – Es importante tener un mejor control y una adecuada verificación previo a ingresar, así como el control de acceso a cualquiera de los recursos de la empresa ayudará a conservar la integridad y confianza de la información.
- Control de las operaciones y comunicación. – Es necesario garantizar la comunicación y la funcionalidad de los sistemas de información, ante cualquier eventualidad que pudiera ocurrir dentro de la empresa, para así garantizar la disponibilidad de la información

3.2.4.2 Política de Seguridad

"Fomentar hábitos y destrezas en EPC COMPU para asegurar el manejo adecuado de los procesos informáticos a través de un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y de mejora constante que mantenga la confidencialidad, integridad, y disponibilidad de la información".

3.2.4.3 Análisis de Riesgos

3.2.4.3 Metodología de evaluación de riesgos

La metodología que se utilizará en la evaluación de riesgos es Magerit porque interpreta sus resultados de manera cuantitativa esto va a facilitar a las empresas una mejor toma de decisiones.

A continuación, se presenta un esquema de la metodología Magerit:

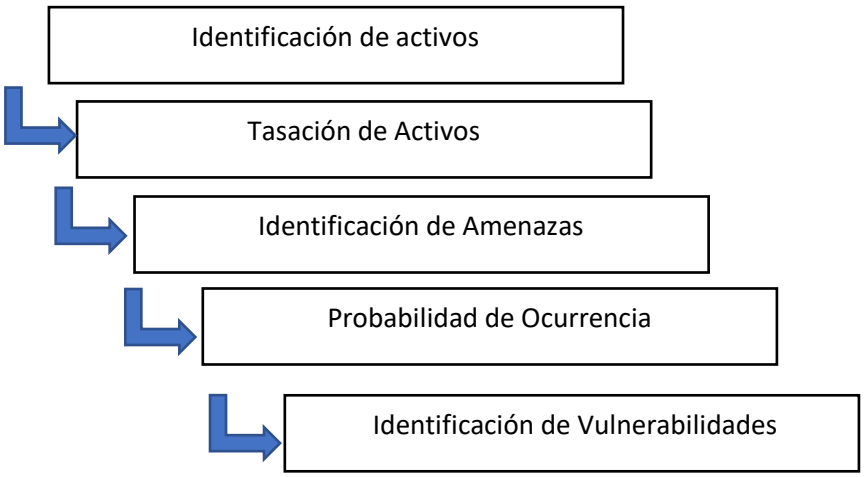


Figura 12. Metodología Magerit.

Elaborado por: Investigador

3.2.4.4 Identificación de Activos

Para la identificación de los activos se utilizaron datos proporcionados por el jefe de sistemas del departamento de Tecnologías de la Información y Comunicación de EPC COMPU

N°	Activo	Clasificación del Activo
1	Sistema Web	Software
3	Correo	
4	Cuentas de Usuario	
5	Computadores de escritorio y laptops	
6	Impresoras Multifunción	
7	Swiches	
8	Router	
9	Red LAN	Comunicaciones
10	Telefonía	

Tabla 29: Activos

Elaborado por: Investigador

3.2.4.5 Tasación de activos

Para la tasación de activos el proceso de valoración se realizó con la metodología de Delphi incluyendo el criterio de 3 personas siendo estas el Jefe del departamento de

TICS, Jefe de Mantenimiento de Informática y la investigadora, se aplicó las directrices de confiabilidad, integridad y disponibilidad de los activos que varía en un rango de 1 a 5, y después se obtiene el promedio de cada activo en base a las directrices, la valoración de activos se aplicó de acuerdo a su importancia como se muestra a continuación:

Menos importante	1
Poco Importante	2
Algo importante	3
Importante	4
Muy importante	5

Tabla 30: Valoración de activos de acuerdo a su importancia.

Elaborado por: Investigador

Con la explicación realizada anteriormente se presenta la tasación de activos:

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Sistema Web	3	4	3	3,33
Correo	5	5	4	4,67
Cuentas de Usuario	4	4	4	4
Computadores de escritorio y laptops	5	5	5	5
Impresoras Multifunción	3	3	2	2,66
Switches	3	4	3	3,33
Router	4	4	4	4
Telefonía	2	4	3	3

Tabla 31: Tasación de Activos

Elaborado por: Investigador

3.2.4.6 Identificación de Amenazas

Se procedió a identificar los Activos Informáticos con un resultado mayor o igual a 3 y se toma la media del rango indicado para realizar la evaluación de riesgos.

Seguidamente, se definió la frecuencia de ocurrencia de la amenaza bajo los siguientes criterios utilizando la metodología de Delphi.

Casi nunca	1
Algunas veces	2
A menudo	3
Casi siempre	4
Siempre	5

Tabla 32: Frecuencia de ocurrencia de la amenaza

Elaborado por: Investigador

Luego se procedió a calcular el riesgo total con la siguiente formula:

Riesgo Total = Valoración del Activo * Frecuencia de ocurrencia de la Amenaza

Con la explicación realizada anteriormente se muestran los activos pertenecientes a EPC COMPU, destacando las amenazas y vulnerabilidad a la que están expuestos estos activos:

Activo	Amenazas	Vulnerabilidades	Valoración del Activo	Frecuencia de ocurrencia de la Amenaza	Riesgo Total
Sistema Web	Información no verificada o alterada	Falta de políticas de seguridad	3,33	3	9,99
	Exceso de privilegios	Carencia de revisiones de privilegios de ingreso	3,33	2	6,66
Correo	Hurto de información	Falta de control de acceso	4,67	3	14,01
		Falta de monitoreo del sistema			
	Sniffing	Falta de cifrado y autenticación débil	4,67	3	14,01
	Phishing	Correo no deseado	4,67	3	14,01
		Archivos adjuntos maliciosos			
		Ingeniería social			

	Fuga de información	Carencia de control de acceso	4,67	3	14,01
		Carencia de cifrado			
	Spam	Estafas y fraudes	4,67	3	14,01
	Caída del sistema	Falta de control en el uso de recursos	4,67	3	14,01
Cuentas de Usuario	Alteración o eliminación de cuentas	Control de acceso inadecuado	4	2	8
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso	4	2	8
	Licencias Vencidas y desactualizadas	Sistema operativo desactualizado	3	4	12
		Carencia de políticas de licencias de software			
	Falla en el disco duro	Falencias en las particiones del disco duro	3	2	6
	Daños en la fuente de poder	Piezas deficientes de fábrica	3	2	6

Computadores de escritorio y laptops	Daños en los ventiladores	Presencia de basura	3	1	3
	Sismo	Carencia de plan antisísmico	3	3	9
	Incendio	Falta de control en los reguladores de voltaje	3	1	3
	Robo	Falta de sistemas de seguridad	3	2	6
	Falla en la tarjeta de red	Mala configuración	3	3	9
	Falla de cableado y conectores	Malas instalaciones y deterioro	3	4	12
	Fallas en la BIOS	Desactualización del firmware	3	2	6
	Fallas de Hardware	Deterioro físico por el tiempo del equipo informático	3	3	9
	Malware	Uso inadecuado del internet	3	3	9
		Libre acceso en la internet			

	Errores de arranque	Carencia de mantenimientos preventivos	3	2	6
	Fallas en la memoria RAM	Falencias en el mantenimiento, lectura/escritura incorrecta	3	2	6
	Fallas del procesador	Carencia de límites y controles en utilizar recursos	3	2	6
	Pésima Resolución de pantalla	Mala configuración	3	1	3
	Acceso no autorizado	Ingresos indebidos	3	2	6
	Corte de servicio eléctrico	Fallas en los suministros de energía	3	3	9
	Filtración de Agua	Fallas en la infraestructura física	3	1	3
Impresoras Multifunción	Sustracción de documentos	Uso y acceso no autorizado	2,66	2	5,32
	Daño en los cartuchos y cabezales	Falta de mantenimiento	2,66	2	5,32

	Agotamiento de tinta	Falta de revisión de los cartuchos de tinta.	2,66	2	5,32
	Atascamiento de papel	Carga incorrecta de papel.	2,66	1	2,66
		Uso de papel inadecuado.			
	Sismo	Carencia de plan antisísmico.	2,66	1	2,66
	Incendio	Falta de control en los reguladores de voltaje	2,66	1	2,66
	Robo	Falta de sistemas de seguridad	2,66	1	2,66
	Corte de servicio eléctrico	Fallas en los suministros de energía	2,66	3	7,98
	Filtración de Agua	Fallas en la infraestructura física	2,66	1	2,66
Switches	Daño físico	Falta de revisiones	3,33	3	9,99
	Sobrecalentamiento	Cambios del suministro eléctrico	3,33	3	9,99
	Bajo rendimiento	Falta de mantenimiento	3,33	4	13,32

	Denegación de servicio distribuido	Falta de monitoreo del tráfico y escasa actualización y configuración del firmware	3,33	2	6,66
	Spoffing de ARP	Intercepción de paquetes	3,33	2	6,66
	Intrusión de dispositivos ilegítimos en la red	Carencia de monitoreo de las direcciones MAC	3,33	4	13,32
	Puertos abiertos y mal configurados	Deficiente monitoreo de los puertos y configuraciones de los switches	3,33	4	13,32
	Acceso no autorizado	Falta de autenticación segura para acceder al switch	3,33	3	9,99
	Sismo	Carencia de plan antisísmico	3,33	1	3,33
	Incendio	Falta de control en los reguladores de voltaje	3,33	1	3,33
	Robo	Falta de sistemas de seguridad	3,33	1	3,33

	Corte de servicio eléctrico	Fallas en los suministros de energía	3,33	3	9,99
	Filtración de Agua	Fallas en la infraestructura física	3,33	1	3,33
Router	Bajo rendimiento	Falta de Mantenimiento	4	2	8
	Recalentamiento	Cambios del suministro eléctrico	4	2	8
	Conexión intermitente	Mala ubicación del dispositivo	4	3	12
	Denegación de servicio distribuido	Falta de monitoreo del tráfico y escasa actualización y configuración del firmware	4	2	8
	Envenenamiento de DNS	Deficiente monitoreo del tráfico DNS y configuración del router	4	1	4
	Acceso no autorizado	Falta de autenticación segura para acceder al router	4	3	12

	Sismo	Carencia de plan antisísmico	4	1	4
	Incendio	Falta de control en los reguladores de voltaje	4	1	4
	Robo	Falta de sistemas de seguridad	4	1	4
	Corte de servicio eléctrico	Fallas en los suministros de energía	4	2	8
	Filtración de Agua	Fallas en la infraestructura física	4	1	4
Telefonía	Daños físicos	Falta de mantenimiento	3	3	9
	Perdida de conexión	Configuración inadecuada en central telefónica	3	2	6
	Sismo	Carencia de plan antisísmico	3	1	3
	Incendio	Falta de control en los reguladores de voltaje	3	1	3
	Robo	Falta de sistemas de seguridad	3	1	3

	Corte de servicio eléctrico	Fallas en los suministros de energía	3	2	6
	Filtración de Agua	Fallas en la infraestructura física	3	1	3

Tabla 33: Identificación de Amenazas

Elaborado por: Investigador

3.2.4.7 Selección de Controles

El siguiente paso para el desarrollo del SGSI es relacionar los controles definidos por la norma ISO 27001:2013 con los activos de mayor valoración en cuanto al factor riesgo reflejados en las tablas anteriores.

A continuación, se detalla los dominios que conforman la norma ISO 27001:2013

- A.5 Políticas de seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones.
- A.14 Adquisición, desarrollo y mantenimientos de sistemas.
- A.15 Relación con los proveedores.
- A.16 Gestión de incidentes de seguridad de la información.
- A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- A.18 Cumplimiento.

La norma mencionada está establecida por 18 dominios, 35 objetivos de control y 114 controles (Ver Anexo 1)

A continuación, se elaboró la columna “Objetivo de Control” la misma que contiene los dominios que corresponden con las amenazas detalladas en cada activo informático:

Activo	Amenazas	Vulnerabilidades	Valoración del Activo	Frecuencia de ocurrencia de la Amenaza	Riesgo Total	Objetivos de Control
Sistema Web	Información no verificada o alterada	Falta de políticas de seguridad	3,33	3	9,99	A.9: Control de acceso.
	Exceso de privilegios	Carencia de revisiones de privilegios de ingreso	3,33	2	6,66	A.6: Organización de la Seguridad de la Información
Correo	Hurto de información	Falta de control de acceso	4,67	3	14,01	A.9: Control de acceso.
		Falta de monitoreo del sistema				A.12 Seguridad de las operaciones
	Sniffing	Falta de cifrado y autenticación débil	4,67	3	14,01	
	Phishing	Correo no deseado	4,67	3	14,01	

		Archivos adjuntos maliciosos				
		Ingeniería social				
	Fuga de información	Carencia de control de acceso	4,67	3	14,01	
		Carencia de cifrado				
	Spam	Estafas y fraudes	4,67	3	14,01	
Cuentas de Usuario	Alteración o eliminación de cuentas	Control de acceso inadecuado	4	3	12	A.9: Control de acceso.
	Exceso de privilegios de ingresos	Carencia de revisiones continuas de privilegios de ingreso	4	2	8	
	Licencias Vencidas y desactualizadas	Sistema operativo desactualizado	3	2	6	A.9: Control de acceso. A.11 Seguridad física y del entorno.
		Carencia de políticas de licencias de software				

Computadores de escritorio y laptops	Falla en el disco duro	Falencias en las particiones del disco duro	3	2	6	A.12 Seguridad de las operaciones A.13 Seguridad de las comunicaciones
	Daños en la fuente de poder	Piezas deficientes de fábrica	3	2	6	
	Daños en los ventiladores	Presencia de basura	3	2	6	
	Sismo	Carencia de plan antisísmico	3	1	3	
	Incendio	Falta de control en los reguladores de voltaje	3	3	9	
	Robo	Falta de sistemas de seguridad	3	1	3	
	Falla en la tarjeta de red	Mala configuración	3	2	6	
	Falla de cableado y conectores	Malas instalaciones y deterioro	3	3	9	
	Fallas en la BIOS	Desactualización del firmware	3	4	12	

	Fallas de Hardware	Deterioro físico por el tiempo del equipo informático	3	2	6	
	Malware	Uso inadecuado del internet	3	3	9	
		Libre acceso en la internet				
	Errores de arranque	Carencia de mantenimientos preventivos	3	2	6	
	Fallas en la memoria RAM	Falencias en el mantenimiento, lectura/escritura incorrecta	3	2	6	
	Fallas del procesador	Carencia de límites y controles en utilizar recursos	3	2	6	
	Pésima Resolución de pantalla	Mala configuración	3	2	6	

	Acceso no autorizado	Ingresos indebidos	3	1	3	
	Corte de servicio eléctrico	Fallas en los suministros de energía	3	2	6	
	Filtración de Agua	Fallas en la infraestructura física	3	3	9	
Impresoras Multifunción	Sustracción de documentos	Uso y acceso no autorizado	2,66	1	2,66	A.9: Control de acceso.
	Daño en los cartuchos y cabezales	Falta de mantenimiento	2,66	2	5,32	A.11 Seguridad física y del entorno.
	Agotamiento de tinta	Falta de revisión de los cartuchos de tinta.	2,66	2	5,32	
	Atascamiento de papel	Carga incorrecta de papel.	2,66	2	5,32	A.12 Seguridad de las operaciones.
		Uso de papel inadecuado.				
	Sismo	Carencia de plan antisísmico.	2,66	1	2,66	
	Incendio	Falta de control en los reguladores de voltaje	2,66	1	2,66	

	Robo	Falta de sistemas de seguridad	2,66	1	2,66	
	Corte de servicio eléctrico	Fallas en los suministros de energía	2,66	1	2,66	
	Filtración de Agua	Fallas en la infraestructura física	2,66	3	2,66	
Switches	Daño físico	Falta de revisiones	3,33	1	3,33	A.9: Control de acceso A.8 Gestión de activos. A.11 Seguridad física y del entorno A.13 Seguridad de las comunicaciones
	Sobrecalentamiento	Cambios del suministro eléctrico	3,33	3	9,99	
	Bajo rendimiento	Falta de mantenimiento	3,33	3	9,99	
	Denegación de servicio distribuido	Falta de monitoreo del tráfico y escasa actualización y configuración del firmware	3,33	3	9,99	
	Spoffing de ARP	Intercepción de paquetes	3,33	2	6,66	

	Intrusión de dispositivos ilegítimos en la red	Carencia de monitoreo de las direcciones MAC	3,33	2	6,66	A.12 Seguridad de las operaciones A.16 Gestión de incidentes de seguridad de la información.
	Puertos abiertos y mal configurados	Deficiente monitoreo de los puertos y configuraciones de los swiches	3,33	4	13,32	
	Acceso no autorizado	Falta de autenticación segura para acceder al swich	3,33	4	13,32	
	Sismo	Carencia de plan antisísmico	3,33	3	9,99	
	Incendio	Falta de control en los reguladores de voltaje	3,33	1	3,33	
	Robo	Falta de sistemas de seguridad	3,33	1	3,33	
	Corte de servicio eléctrico	Fallas en los suministros de energía	3,33	1	3,33	

	Filtración de Agua	Fallas en la infraestructura física	3,33	3	9,99	
Router	Bajo rendimiento	Falta de Mantenimiento	4	1	4	A.8 Gestión de activos. . A.9: Control de acceso A.11 Seguridad física y del entorno A.13 Seguridad de las comunicaciones. A.12 Seguridad de las operaciones
	Recalentamiento	Cambios del suministro eléctrico	4	2	8	
	Conexión intermitente	Mala ubicación del dispositivo	4	2	8	
	Denegación de servicio distribuido	Falta de monitoreo del tráfico y escasa actualización y configuración del firmware	4	3	12	
	Envenenamiento de DNS	Deficiente monitoreo del tráfico DNS y configuración del router	4	2	8	

	Acceso no autorizado	Falta de autenticación segura para acceder al router	4	1	4	
	Sismo	Carencia de plan antisísmico	4	3	12	
	Incendio	Falta de control en los reguladores de voltaje	4	1	4	
	Robo	Falta de sistemas de seguridad	4	1	4	
	Corte de servicio eléctrico	Fallas en los suministros de energía	4	1	4	
	Filtración de Agua	Fallas en la infraestructura física	4	2	8	
Telefonía	Daños físicos	Falta de mantenimiento	3	1	3	A.9: Control de acceso A.11 Seguridad física y del entorno
	Perdida de conexión	Configuración inadecuada en central telefónica	3	3	9	

	Sismo	Carencia de plan antisísmico	3	2	6	A.12 Seguridad de las operaciones
	Incendio	Falta de control en los reguladores de voltaje	3	1	3	
	Robo	Falta de sistemas de seguridad	3	1	3	
	Corte de servicio eléctrico	Fallas en los suministros de energía	3	1	3	
	Filtración de Agua	Fallas en la infraestructura física	3	2	6	

Tabla 34: Selección de Controles

Elaborado por: Investigador

3.2.4.7 Declaración de la aplicabilidad

A continuación, se desarrolló la declaración de aplicabilidad (SOA), siendo unos de los puntos más importantes dentro del SGSI, el mismo que se basa en las áreas y dominios de la ISO 27001:2013, (Ver Anexo 1) dicho documento se realizó con cada uno de los controles aplicables a la situación actual de EPC COMPU.

Su finalidad consistió en identificar los controles que se implementaran, así como la justificación necesaria de aquellos que no sean aplicables.

La presente Declaración de Aplicabilidad fue revisada y aprobada por el Jefe del Departamento de TIC's.

Principalmente la declaración de Aplicabilidad constituye de:

- Dominios de control de la norma ISO 27001:2013
- Objetivos de control correspondientes a cada dominio.
- Objetivos de control seleccionados con su correspondiente justificación

La presente declaración de aplicabilidad fue revisada y aprobada por el Ing. Carlos López Encargado del departamento de TICS

A.5 Políticas de seguridad de la información				
A.5.1 Directrices establecidas por la dirección para la seguridad de la información				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.5.1.1	Políticas para la seguridad de la información	X		Es de suma importancia elaborar un documento en donde se establezcan las políticas de seguridad, siendo la información el bien más preciado de la empresa, dicho documento debe ser aprobado por la alta dirección
A.5.1.2	Revisión de las políticas de seguridad de la información	X		Es importante revisar periódicamente el documento de las políticas de seguridad y mantenerla actualizada constantemente
A.6: Organización de la Seguridad de la información				
A 6.1 Organización Interna				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.6.1.1	Funciones y responsabilidades de la Seguridad de la información	X		Es necesario definir las responsabilidades de cada empleado en relación a la Seguridad de la

				información. Además, se debe comunicar a cada persona implicada en la Seguridad de la Información sus roles y responsabilidades.
A.6.1.2	Separación de deberes	X		Es importante evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan es decir los activos de información mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad en el puesto de trabajo.
A.6.1.3	Contacto con las autoridades	X		En caso de incidentes de seguridad de la información se debe mantener informadas a las autoridades de la dirección con el fin de monitorear todos los procesos que se llevan a cabo.
A.6.1.4	Contacto con grupos de interés especial		**X**	No es aplicable debido a que la empresa no tiene contacto con terceros, es decir la información se maneja internamente.
A.6.1.5	Seguridad de la información en la gestión de proyectos	**X**		Es importante que la seguridad de la información se involucre en todos los procesos de la organización ya

				sean procesos del Negocio, procesos internos, Servicios o productos, Procesos TI etc.
A 6.2 Dispositivos Móviles y Teletrabajo				
A 6.2.1	Política para dispositivos móviles	**X**		Es de vital importancia adoptar políticas de seguridad para reducir el riesgo que representan los dispositivos móviles.
A 6.2.2	Teletrabajo		**X**	No es aplicable debido que todas las actividades que se realiza en la empresa se realizan de manera presencial
A 7 Seguridad de los recursos humanos				
A 7.1 Antes de asumir el empleo				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A 7.1.1	Selección	**X**		Se debe tener un proceso de selección de acuerdo a la hoja de vida del postulante con certificados laborales y cursos de capacitación comprobables en el área correspondiente

A 7.1.2	Términos y condiciones del empleo	**X**		Es necesario incluir en los contratos con los empleados las obligaciones y responsabilidades ligadas a la Seguridad de la Información.
A 7.2 Durante la ejecución del empleo				
A 7.2.1	Responsabilidades de la dirección	**X**		Es muy importante que la dirección exija a los empleados el cumplimiento de las políticas, normas y procedimientos establecidos para la Seguridad de la Información en la empresa. Es primordial realizar capacitaciones al personal de la empresa con respecto a la seguridad de la información de manera adecuada y periódica mientras labore en la empresa, de tal manera que se pueda resguardar la información.
A 7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**X**		Se debe motivar, formar concientizar suficientemente a los empleados, además impartir actualizaciones regulares en políticas y procedimientos organizacionales para que cumplan con sus obligaciones eficientemente en la empresa.

A 7.2.3	Proceso disciplinario	**X**		Es necesario implantar un sistema disciplinario para los incumplimientos de la seguridad de la información. Un procedimiento que sea formal y comunicado a todos los empleados.
7.3 Terminación o cambio de empleo				
7.3.1	Terminación o cambio de responsabilidades de empleo	**X**		Es muy importante establecer y comunicar al empleado las responsabilidades sobre la seguridad de la información después de finalizar su contrato o ante el cambio de empleo en el cual debe Incluir las responsabilidades de la desvinculación.
A.8 Gestión de Activos				
A 8.1 Responsabilidad por los activos				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
8.1.1	Inventario de Activos		**X**	La empresa cuenta actualmente con un inventario de activos.

8.1.2	Propiedad de Los Activos		**X**	La empresa cuenta con el personal encargado que tiene a disposición de gestionar todos los activos informáticos.
8.1.3	Uso Aceptable de los Activos	**X**		Es de vital importancia documentar el uso adecuado de la información describiendo los requisitos de seguridad de la información de los activos.
8.1.4	Devolución de Activos	**X**		Es necesario establecer un control para que todos los empleados devuelvan los activos de información una vez finalizado el periodo de su utilización, o contrato laboral.
8.2 Clasificación de la Información				
8.2.1	Clasificación de la Información	**X**		Es de vital importancia elaborar un esquema de clasificación de acuerdo a su valor, requisitos legales, y nivel de protección necesario.
8.2.2	Etiquetado de la Información	**X**		Es primordial llevar un etiquetado adecuado de clasificación de los activos que contienen información clasificada como sensible o crítica.

8.2.3	Manejo de activos	**X**		Se debe establecer un control que exija el desarrollo de procedimientos de manejo de activos que tengan en cuenta la clasificación de los activos de información.
8.3 Manipulación de Soportes				
8.3.1	Gestión de medios removibles	**X**		Se debe establecer un control para gestionar unidades de almacenamiento extraíble tales como unidades USB, Discos duros.
8.3.2	Disposición de los medios	**X**		Es importante establecer procedimientos para la eliminación segura de los dispositivos de almacenamiento a la finalización de su uso para evitar que los datos sensibles o confidenciales puedan ser recuperados una vez que el dispositivo se da de baja mediante procedimientos de eliminación segura.
8.3.3	Transferencia de medios físicos	**X**		Es necesario establecer un control seguro para proteger la información cuando los soportes necesitan ser transferidos o transportados entre distintas ubicaciones.

A 9 Control De Acceso				
A 9.1 Requisitos del negocio para control de acceso				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A 9.1.1	Política de control de acceso	**X**		Es necesario elaborar un documento en el que se establezca la política de control de acceso es decir los Privilegios a las instalaciones como a los sistemas de información de la empresa para garantizar permisos de acceso a usuarios autorizados.
A 9.1.2	Política sobre el uso de los servicios de red	**X**		Es importante gestionar la autorización de los usuarios que acceden a los recursos de red mediante identificación y autenticación.
A 9.2 Gestión de acceso de usuarios				
A 9.2.1	Registro De Usuarios y cancelación del Registro	**X**		Es necesario establecer un proceso de altas y bajas que permita los derechos de acceso a los sistemas de información.

9.2.2	Suministro de acceso de usuarios	**X**		Se debe establecer un proceso formal para asignar y revocar los accesos a sistemas y servicios.
9.2.3	Gestión de derechos de acceso privilegiado	**X**		Se debe establecer un proceso que identifique accesos privilegiados de cada sistema o proceso, además se debe definir la caducidad de los permisos.
9.2.4	Gestión de información de autenticación secreta de usuarios	**X**		Es de vital importancia establecer Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso en especial de las contraseñas.
9.2.5	Revisión de los derechos de acceso de usuarios	**X**		Es necesario establecer un Control para una revisión periódica de los permisos de accesos de los usuarios.
9.2.6	Retiro o ajuste de los derechos de acceso	**X**		Es importante definir un control para garantizar que se modifican los derechos de acceso a los sistemas.
A 9 3 Responsabilidades de los usuarios				
9.3.1	Uso de la información de autenticación secreta	**X**		Se debe establecer normas para la utilización de contraseñas.
A 9 4 Control de acceso a sistemas y aplicaciones				

9.4.1	Restricción del Acceso a la Información	**X**		Es necesario establecer restricciones de control de acceso para prevenir accesos no autorizados a sistemas y aplicaciones.
9.4.2	Procedimiento de ingreso seguro	**X**		Es indispensable establecer un control para establecer inicios de sesión seguros en los equipos y en los sistemas de información.
9.4.3	Sistema de gestión de contraseñas	**X**		Se deben establecer cambios de contraseñas periódicamente, se debe utilizar dichos cambios para asegurar la calidad de las contraseñas.
9.4.4	Uso de programas utilitarios privilegiados	**X**		Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema del equipo y los controles de las aplicaciones.
9.4.5	Control de acceso a códigos fuente de programas	**X**		Es importante restringir el acceso a los códigos fuente de los programas.
A.10 Criptografía				
A.10.1 Controles criptográficos				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	

A.10.1.1	Política sobre el uso de controles criptográficos	**X**		Es primordial desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	**X**		Es muy importante implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.
A.11 Seguridad física y del entorno				
A.11.1 Áreas seguras				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.11.1.1	Perímetro de seguridad física	**X**		Se debe establecer un control para usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica.
A.11.1.2	Controles físicos de entrada	**X**		Es de suma importancia que las áreas seguras estén protegidas mediante controles de entrada apropiados para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**X**		Se debe diseñar y aplicar seguridad física a oficinas, y a todas las instalaciones.

A.11.1.4	Protección contra amenazas externas y ambientales		**X**	No es aplicable debido a que disponen de un plan de contingencia.
A.11.1.5	Trabajo en áreas seguras	**X**		Es importante aplicar procedimientos para el trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	**X**		Es indispensable establecer un proceso para controlar los puntos de acceso tales como áreas de despacho y de carga, también otros puntos en donde pueden ingresar personas no autorizadas, y además, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2 Equipos				
A.11.2.1	Ubicación y protección de los equipos	**X**		Es importante establecer un control para que los equipos estén ubicados y protegidos para reducir los riesgos de amenazas y peligros del ambiente.
A.11.2.2	Servicios de suministro	**X**		Es necesario un control para que los equipos estén protegidos contra fallas de energía o de los suministros.

A.11.2.3	Seguridad del cableado	**X**		Es muy importante establecer un control para que el cableado de potencia y de red estén seguros contra interceptaciones, interferencias o daños.
A.11.2.4	Mantenimiento de equipos	**X**		Es indispensable elaborar un documento en el que consten los registros del mantenimiento de los equipos.
A.11.2.5	Retiro de activos	**X**		Es importante establecer un control para que todos los equipos, información o software no se deban retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		**X**	No aplica debido a que no se tiene el permiso para trabajar fuera de las instalaciones de la organización
A.11.2.7	Disposición segura o reutilización de equipos	**X**		Se debe establecer un control para que los equipos que tengan unidades de almacenamiento deben revisarse para asegurar que todos los datos se hayan removido en su totalidad.
A.11.2.8	Equipos de usuario desatendidos	**X**		Es importante establecer un control para los usuarios que usan los equipos y deben recibir la protección correspondiente.

A.11.2.9	Política de escritorio limpio y pantalla limpia	**X**		Es necesario aplicar una política de escritorio limpio para los papeles y medios de almacenamiento removibles para evitar divulgación de información.
A.12 Seguridad de las operaciones				
A.12.1 Procedimientos operacionales y responsabilidades				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.12.1.1	Procedimientos de operación documentados	**X**		Es importante documentar para poner a disposición de todos los usuarios.
A.12.1.2	Gestión de cambios	**X**		Es necesario establecer un control para monitorear los cambios en la organización y en toda la infraestructura tecnológica.
A.12.1.3	Gestión de capacidad	**X**		Se debe realizar un seguimiento del uso de los recursos, ajustes, y proyecciones de los requisitos sobre la capacidad futura para posteriormente asegurar el desempeño requerido.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**X**		Es muy importante establecer un control para separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso.

A.12.2 Protección contra códigos maliciosos				
A.12.2.1	Controles contra códigos maliciosos	**X**		Es indispensable implementar controles de detección, de prevención y de recuperación contra código malicioso, combinados con la toma de conciencia de los usuarios, para proteger los activos de información.
A.12.3 Copias de respaldo				
A.12.3.1	Respaldo de información	**X**		Es de vital importancia implementar controles para realizar copias de respaldo de la información en los equipos informáticos mediante la elaboración de un documento con las directrices de política.
A.12.4 Registro y seguimiento				
A.12.4.1	Registro de eventos	**X**		Es muy importante establecer un control para monitorear todas las actividades del usuario en el equipo mediante el visor de eventos en Windows y mediante el registro de logs en Linux para detectar fallas y eventos de seguridad. También se puede utilizar software para obtener las actividades de usuario.

A.12.4.2	Protección de la información de registro	**X**		Es esencial definir controles para proteger el acceso a las instalaciones de la organización, así como también el registro de toda la información.
A.12.4.3	Registros del administrador y del operador	**X**		Se debe establecer un control para revisar periódicamente las tareas del usuario administrador en los equipos y en los sistemas de información.
A.12.4.4	Sincronización de relojes		**X**	No aplicable debido a que la empresa no posee demasiada infraestructura de TI.
A.12.5 Control de software operacional				
A.12.5.1	Instalación de software en sistemas operativos	**X**		Es primordial establecer un control para controlar la instalación de software en los equipos.
A.12.6 Gestión de la vulnerabilidad técnica				
A.12.6.1	Gestión de las vulnerabilidades técnicas	**X**		Es muy importante documentar oportunamente información acerca de las vulnerabilidades técnicas de los equipos y en los sistemas de información que se usen en la empresa para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	**X**		Es importante establecer un control y documentar las reglas para la instalación de software en los equipos
A.12.7 Consideraciones sobre auditorias de sistemas de información				

A.12.7.1	Información controles de auditoría de sistemas	**X**		Se debe elaborar un plan de auditoria para todos los activos informáticos y los sistemas de información con el fin de minimizar riesgos.
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de la seguridad de las redes				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.13.1.1	Controles de redes	**X**		Es muy importante establecer un control para toda la infraestructura de la red para proteger a los equipos y sistemas de información.
A.13.1.2	Seguridad de los servicios de red	**X**		Es necesario elaborar un documento en el que se pueda registrar y dar un seguimiento a todos los servicios de red.
A.13.1.3	Separación en las redes	**X**		Es indispensable segmentar las redes por áreas o por departamentos para optimizar el rendimiento de la red.
A.13.2 Transferencia de información				
A.13.2.1	Políticas y procedimientos de transferencia de información	**X**		Se debe elaborar un documento en el que se establezcan los controles para proteger la transferencia

				de información usando medios de comunicación segura.
A.13.2.2	Acuerdos sobre transferencia de información	**X**		Se deben elaborar acuerdos para la transferencia segura de información entre la organización.
A.13.2.3	Mensajería electrónica	**X**		Es muy importante establecer un control para proteger adecuadamente la mensajería de correo electrónico.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**X**		Es muy importante elaborar una documentación en el que se identifiquen, y revisen los requisitos para los acuerdos de confidencialidad o de no divulgación de la información.
A.14 Adquisición, desarrollo y mantenimientos de sistemas				
A.14.1 Requisitos de seguridad de los sistemas de información				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**X**		Se debe verificar que los requisitos relacionados con seguridad de la información se deban incluir en los requisitos para nuevos sistemas de información o para mejorar a los sistemas de información.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	**X**		Es importante establecer un control para proteger la información de actividades fraudulentas que pasan sobre redes públicas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	**X**		Es indispensable elaborar un control para proteger las transacciones de los servicios de aplicaciones para evitar trasmisiones incompletas y alteraciones no autorizadas en la información.
A.14.2 Seguridad en los procesos de desarrollo y soporte				
A.14.2.1	Política de desarrollo seguro	**X**		Es necesario establecer y aplicar reglas para el desarrollo de software y de sistemas en la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	**X**		Se deben elaborar procedimientos formales de control de cambios dentro del ciclo de vida de desarrollo de software.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**X**		Se debe elaborar un documento en el que consten las revisiones técnicas de los procesos críticos que posee la organización además hay que tener en cuenta que todos sistemas se cambian las plataformas de

				operación, para asegurar que no haya impacto negativo a un futuro.
A.14.2.4	Restricciones en los cambios a los paquetes de software	**X**		Se debe establecer un control para remover las modificaciones a los paquetes de software para limitar a cambios necesarios.
A.14.2.5	Principios de construcción de sistemas seguros	**X**		Es muy importante documentar los principios para la construcción de sistemas seguros.
A.14.2.6	Ambiente de desarrollo seguro	**X**		Es necesario establecer un control para proteger los ambientes de desarrollo seguros para las tareas de desarrollo de software e integración de sistemas.
A.14.2.7	Desarrollo contratado externamente		**X**	No aplica debido a que la empresa no contrata sistemas externos.
A.14.2.8	Pruebas de seguridad de sistemas	**X**		Es muy importante llevar un control para las pruebas de funcionalidad de seguridad durante el desarrollo del software.
A.14.2.9	Prueba de aceptación de sistemas		**X**	No aplica debido a que no poseen muchos sistemas de información.
A.14.3 Datos de prueba				

A.14.3.1	Protección de datos de prueba	**X**		Se debe tener un control para seleccionar, proteger y controlar los datos de prueba.
A.15 Relación con los proveedores				
A.15.1 Seguridad de la información en las relaciones con los proveedores				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		**X**	No aplica debido a la empresa no mantiene ninguna relación con proveedores.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		**X**	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		**X**	
A.15.2 Gestión de la prestación de servicios con los proveedores				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		**X**	No aplica debido a que la empresa no presta sus servicios a proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores		**X**	
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información				

SECCIÓN	CONTROLES ISO 27001:2013	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
A.16.1.1	Responsabilidad y procedimientos	**X**		Es muy importante establecer un control para cumplir con las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida y eficaz a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	**X**		Se debe elaborar un informe de los eventos de seguridad de la información y comunicarlos de manera urgente y precisa por los canales de gestión.
A.16.1.3	Reporte de debilidades de seguridad de la información	**X**		Es muy importante establecer un control y generar un reporte de debilidades de seguridad de la información por parte de todos los empleados cuando se sospeche que los sistemas estén comprometidos.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**X**		Es necesario evaluar los eventos de seguridad de la información clasificarlos como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	**X**		Es muy importante dar respuesta inmediata a los todos incidentes de seguridad de la información de acuerdo a los lineamientos establecidos.

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**X**		El análisis y resolución de los incidentes de seguridad de la información debe permitir reducir el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	**X**		Es muy importante establecer procedimientos para la identificación, recolección, y resguardo de información que puedan servir como evidencia.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio				
A.17.1 Continuidad de seguridad de la información				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**X**		Es necesario determinar establecer una planificación para la seguridad de la información y la continuidad de la gestión de la seguridad de la información durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**X**		Es muy importante documentar e implementar todos los procesos y controles para asegurar el nivel de continuidad para la seguridad de la información.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**X**		Es muy importante verificar los controles de continuidad de la seguridad de la información establecidos mediante intervalos de tiempo.
A.17.2 Redundancias				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	**X**		Es necesario cumplir con los requisitos de disponibilidad y con redundancia suficiente de la información.
A.18 Cumplimiento				
A.18.1 Cumplimiento de requisitos legales y contractuales				
SECCIÓN	**CONTROLES ISO 27001:2013**	**APLICABILIDAD**		**JUSTIFICACIÓN**
		SI	**NO**	
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	**X**		Se importante elaborar un documento en el que consten reglamentos, estatutos para todos los sistemas de información en la organización y sobre todo mantenerlos actualizado.
A.18.1.2	Derechos de propiedad intelectual	**X**		Es necesario establecer procedimientos para garantizar el cumplimiento de los reglamentos sobre el uso de recursos y de software patentado.

A.18.1.3	Protección de registros	**X**		Es muy importante proteger los registros contra perdida, destrucción, alteración, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos.
A.18.1.4	Privacidad y protección de datos personales	**X**		Se debe asegurar la privacidad y la protección de la información de datos personales de acuerdo al reglamento.
A.18.1.5	Reglamentación de controles criptográficos	**X**		Es indispensable implementar controles criptográficos, en cumplimiento de todos los acuerdos y legislación.
A.18.2 Revisiones de seguridad de la información				
A.18.2.1	Revisión independiente de la seguridad de la información	**X**		Es necesario planificar una revisión independiente de la seguridad de la información es decir todos los controles, políticas y procedimientos aplicados para brindar seguridad a la información especialmente cuando susciten cambios.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**X**		Es muy importante la revisión periódica por parte de la alta dirección del cumplimiento y procedimientos, con las políticas y normas de seguridad apropiadas.

A.18.2.3	Revisión del cumplimiento técnico	**X**		Es muy importante establecer un control para revisar periódicamente los sistemas de información para posteriormente determinar el cumplimiento con las políticas y normas de seguridad de la información en la empresa.

Tabla 35: Declaración de Aplicabilidad

Elaborado por: Investigador

3.2.4.8 Análisis del cumplimiento de los controles

La presente valoración porcentual del cumplimiento de cada uno de los controles se realiza conjuntamente con el Ing. Carlos López Jefe del Departamento de TIC's de la empresa EPC COMPU.

Para lo cual se elaboró una gráfica con el cumplimiento para cada una de las áreas, las cuales detallan porcentajes de los resultados obtenidos, además se detalla cada control, y a su vez como están establecidos en el momento de la revisión.

A.5 Políticas de seguridad de la información

A.5.1 Directrices establecidas por la dirección para la seguridad de la información

A.5.1.1 Políticas para la seguridad de la información

EPC COMPU no cuenta con documentación de políticas de seguridad. Los procesos que se llevan a cabo no se los realiza en base a lineamientos, únicamente se aplican ciertas normativas para gestionar la información, pero éstas son básicas las cuales no garantizan que la información esté protegida.

Es necesario que la dirección establezca políticas de seguridad y de carácter obligatorio. Las mismas deben ser documentadas y socializadas a todo el personal de EPC COMPU.

A.5.1.2 Revisión de las políticas para seguridad de la información

Como se mencionó EPC COMPU no cuenta con un documento con políticas de seguridad, como ya se lo menciono anteriormente, por tal motivo no podemos obtener una revisión de políticas de seguridad dentro de la empresa.

Ahora, ya definidas y documentadas las políticas de seguridad, en conjunto con el Departamento de TIC's y la gerencia se deben comprometer con la revisión periódica permanente de las políticas de seguridad, para garantizar la efectividad de dichas políticas

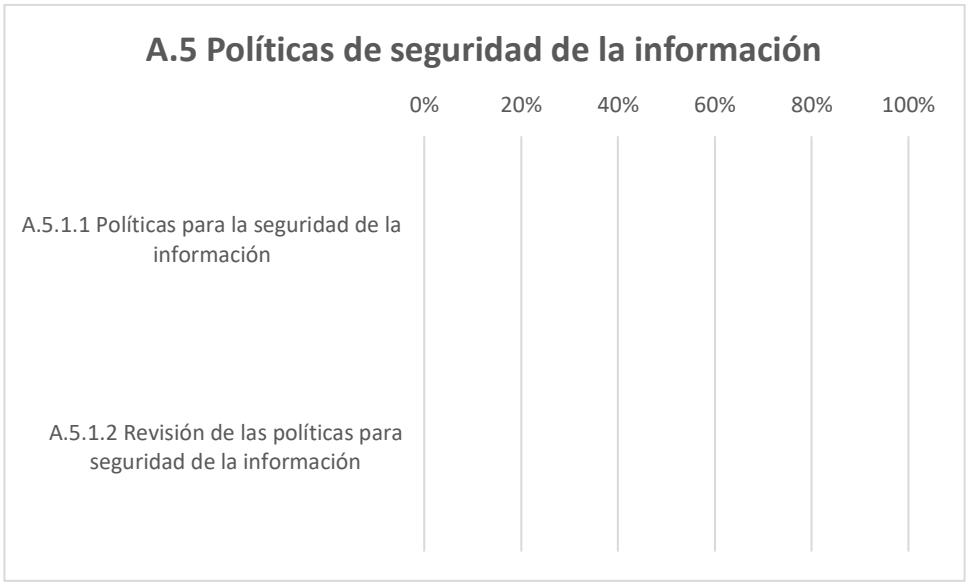


Figura 13. Análisis porcentual- políticas de seguridad de la información.

Elaborado por: Investigador

Como se puede observar en la figura 13, no se cumple ninguno de los controles relacionados con el dominio de las políticas de seguridad. Es decir, no se lleva a cabo ninguna documentación ni revisión periódica.

A.6: Organización de la Seguridad de la información Seguridad de la información

A 6.1 Organización Interna

A.6.1.1 Funciones y responsabilidades de la Seguridad de la información

La coordinación de la seguridad es uno de los principales puntos en los que se debe delegar a los responsables de cada área los cuales deben estar comprometidos en analizar situaciones potenciales y actuar con rapidez, además, cada acción que se realice facilitará la actuación del responsable cuando se presenten situaciones similares en el futuro.

A.6.1.2 Separación de deberes

Es importante evitar el uso o acceso indebido a la información, a las aplicaciones o sistemas, es decir se debe conservar la integridad de la información, separando funciones en tareas asignando diferentes perfiles o responsabilidades.

A.6.1.3 Contacto con las autoridades

EPC COMPU actualmente sigue este control de acuerdo con la estructura organizativa de la empresa. el área de TIC cumple con su cometido, hasta un cierto punto. En caso de surgir un problema se comunica de inmediato al Jefe de Sistemas y al Gerente.

A.6.1.4 Contacto con grupos de interés especial

Se recomienda mantener conexiones adecuadas con los grupos de intereses especiales u otros foros y asociaciones profesionales expertos en seguridad.

A.6.1.5 Seguridad de la información en la gestión de proyectos

La seguridad de la información debe ser considerada durante la gestión. independientemente del tipo de proyecto.

A 6.2 Dispositivos Móviles y Teletrabajo

A 6.2.1 Política para dispositivos móviles

Es necesario establecer políticas y salvaguardas para apoyar la seguridad y gestiona los riesgos asociados con el uso de dispositivos móviles

A 6.2.2 Teletrabajo

No aplicable debido a que las actividades se realizan netamente presenciales

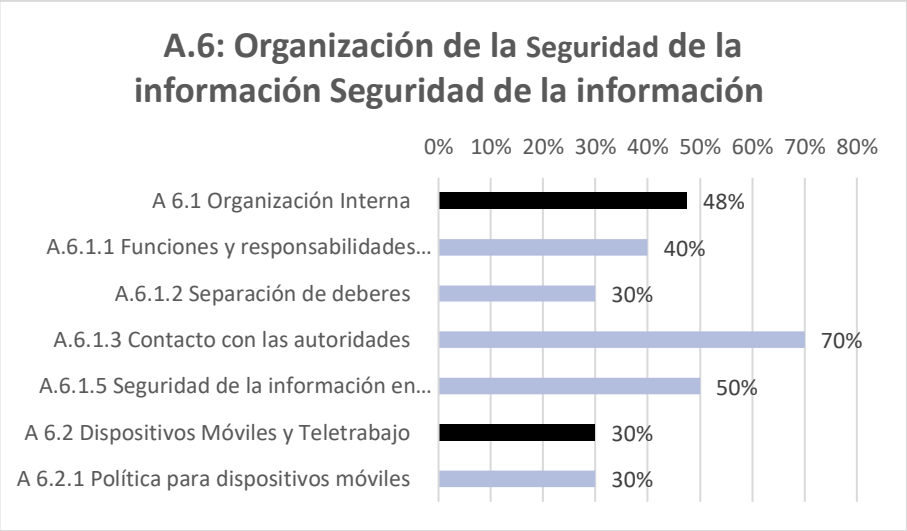


Figura 14.Análisis porcentual - Organización de la Seguridad de la información Seguridad de la información.

Elaborado por: Investigador

De acuerdo con la figura 14 presentado anteriormente se tiene un nivel regular en cuanto a cumplimiento del control de Organización de la Seguridad de la información por lo que se deberán tomar las medidas correctivas apropiadas

A 7 Seguridad de los recursos humanos

A 7.1 Antes de asumir el empleo

A 7.1.1 Selección

La verificación de antecedentes para todos los solicitantes del empleo debe comportarse de acuerdo con las leyes y reglamentos pertinentes y la ética profesional, y estar en términos razonables con las necesidades de negocio, clasificación de la información disponible y riesgo percibido.

A 7.1.2 Términos y condiciones del empleo

Los términos y contratos solo se realizan de acuerdo a sus funciones y no con respecto a la seguridad de la información. Por tal motivo los contratos con empleados y contratistas deben especificar sus responsabilidades y las de la organización sobre seguridad de la información.

A 7.2 Durante la ejecución del empleo

A 7.2.1 Responsabilidades de la dirección

La gerencia debe hace cumplir a los empleados sobre sus funciones, y con respecto a la seguridad de la información. Por tal razón la gerencia debe exigir a todos los empleados y contratistas aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

A 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Todos los empleados de la organización, así como los contratistas relevantes, deben recibir capacitación de concientización adecuadas y actualizar periódicamente las políticas y los procedimientos relevantes para sus responsabilidades.

A 7.2.3 Proceso disciplinario

Debe haber un proceso disciplinario formal que debe ser notificado para tomar medidas contra los empleados que violen las reglas de seguridad de la información.

7.3 Terminación o cambio de empleo

7.3.1 Terminación o cambio de responsabilidades de empleo

Existe un acuerdo después de la terminación de las responsabilidades del empleado, pero no de la seguridad de la información. Los deberes y obligaciones de seguridad de la información que permanezcan en vigencia a la terminación o modificación del contrato deben definirse, comunicarse a los empleados o contratistas y hacerse cumplir.

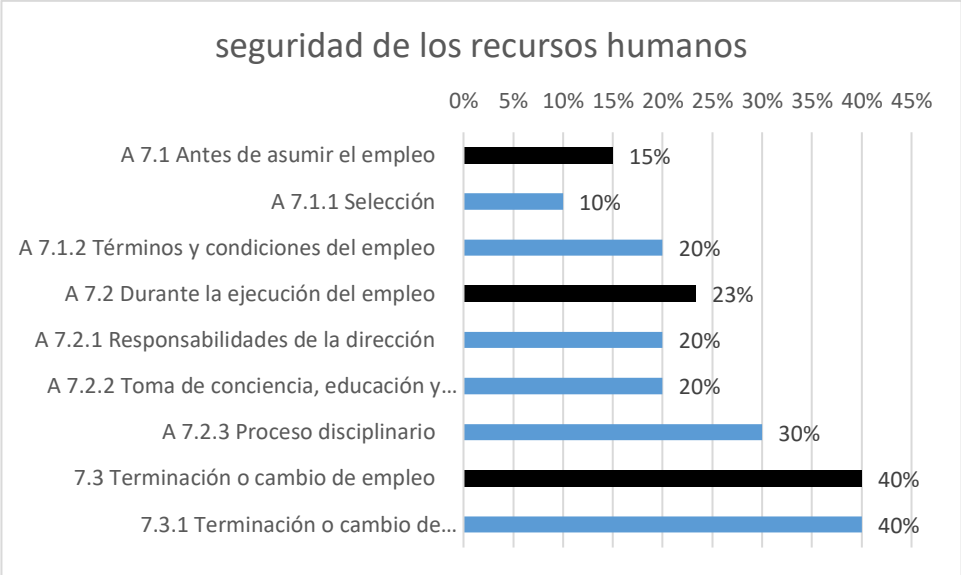


Figura 15.Análisis porcentual - seguridad de los recursos humanos.

Elaborado por: Investigador

De acuerdo con la figura 15 presentado anteriormente se tiene un nivel muy bajo en cuanto a cumplimiento del control de seguridad de los recursos humanos por lo que se deberán tomar las medidas correctivas apropiadas.

A.8 Gestión de Activos

A 8.1 Responsabilidad por los activos

8.1.1 Inventario de Activos

La parte administrativa se encarga de mantener el inventario total de la institución, este departamento se encarga de distribuir los fondos a quienes ingresan. Cabe mencionar que el departamento de TI no es responsable de todos los activos de TI de la institución. el empleado es responsable de los bienes que se le asignan para el desempeño de diversas funciones.

8.1.2 Propiedad de Los Activos

Estos bienes son propiedad de EPC COMPU ya que fueron comprados en base a las necesidades institucionales con el presupuesto asignado. Existe una clara responsabilidad por su cuidado.

Este proceso es realizado por unidades de personal y administrativas, las cuales designan a diversos funcionarios con documentos legales como custodios de los bienes que utilizarán al ingresar a la empresa. Por lo tanto, la empresa está sujeto a las reglas generales que rigen el manejo, uso y control de la propiedad pública.

8.1.3 Uso Aceptable de los Activos

Se han identificado casos en los que se puede demostrar el uso incorrecto o inadecuado de los recursos tecnológicos. Por ejemplo, el acceso a Internet y la forma en que se utilizan las computadoras asignadas a cada empleado es algo irresponsable. En ocasiones desperdician energía dejando las computadoras encendidas, mientras que en otros casos, los usuarios individuales las utilizan para uso personal o entretenimiento, provocando retrasos en las actividades laborales.

Por lo tanto, es importante que los funcionarios que tienen acceso a los activos de TI comprendan los parámetros y las limitaciones de su uso. Adicionalmente, deben ser conscientes de que además de los bienes de los que son responsables, también lo son de la información que manejan.

8.1.4 Devolución de Activos

Cuando finaliza un contrato o acuerdo de trabajo, todos los empleados o contratistas serán evaluados para la devolución de los activos de información. El proceso se formaliza con documentación que verifica el cumplimiento de las condiciones para la devolución de activos físicos y/o electrónicos y, en su caso, establece procedimientos para la transferencia y eliminación de información de forma segura.

8.2 Clasificación de la Información

8.2.1 Clasificación de la Información

La clasificación de la información ya sea física o digital está clasificada de acuerdo al área correspondiente y de manera restringida, todos los departamentos cuentan con procedimientos para acceder a la información relevante, pero no existen controles para garantizar que la información no se altere o elimine de manera malintencionada o accidental**.**

8.2.2 Etiquetado de la Información

Toda la información de la empresa esta identificada digital o físicamente según el departamento que la administra, de manera física mediante sellos y rótulos en las carpetas y de manera digital mediante colores, nombres y descripciones en las carpetas en el computador, cabe mencionar que solo se tiene etiquetada la información crítica de la empresa por tal razón se debe considerar etiquetar toda la información y los activos del sistema para clasificar la información como crítica, valiosa y sensible.

8.2.3 Manejo de activos

Para un adecuado procesamiento, procesamiento y almacenamiento efectivo de la información, se clasifican por área y se configuran de acuerdo a las restricciones de acceso, debido a que un departamento no puede acceder a la información de otro departamento, por lo que también es importante etiquetar la información.

8.3 Manipulación de Soportes

8.3.1 Gestión de medios removibles

Se informa a los empleados sobre el uso de medios de almacenamiento extraíbles, si el empleado necesita usar algún medio removible ya sea alguna Unidad USB, disco duro externo, o CD en el equipo informático solicita permiso al departamento de TIC’s, su respectivo uso requiere la aprobación del departamento de TIC’s, que es responsable de la confidencialidad de los datos recopilados en las computadoras y los medios extraíbles.

8.3.2 Disposición de los medios

No se tienen en consideración ningún procedimiento para eliminar la información, lo que genera un riesgo a la información. A medida que se eliminan los activos sin valor agregado, los miembros de la empresa o terceros pueden descubrir el programa de recuperación de datos existente. información

8.3.3 Transferencia de medios físicos

Se establecen registros y permisos para trasladar los medios físicos como Unidades USB, discos duros externos, o CDs, a otros departamentos de la empresa.

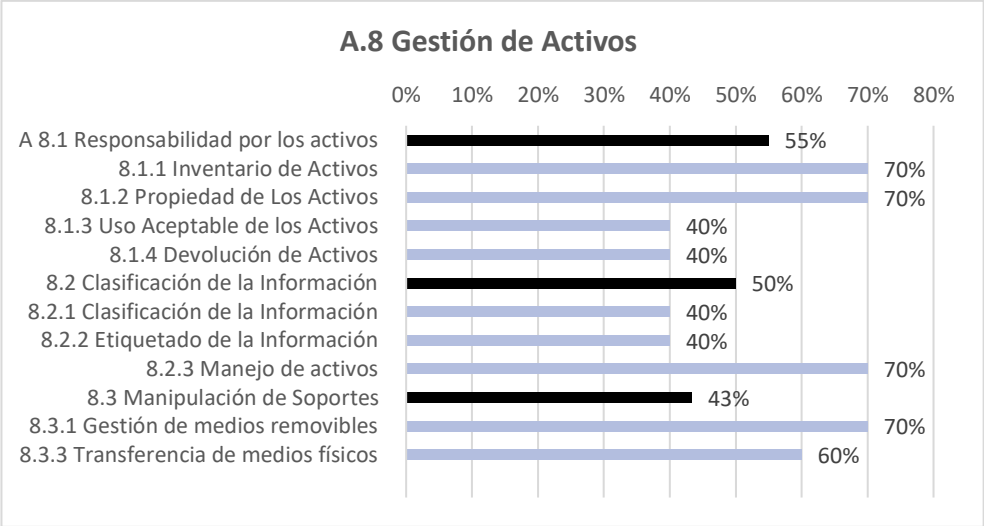


Figura 16.Análisis porcentual - Gestión de Activos.

Elaborado por: Investigador

De acuerdo con la figura 16 presentado anteriormente se tiene un nivel regular en cuanto a cumplimiento del control de Gestión de activos por lo que se deberán tomar las medidas correctivas apropiadas.

A.9 Control de acceso

A.9.1 Requisitos del negocio para control de acceso

A.9.1.1 Política de control de acceso

No tienen una política de control de acceso definida, pero cuentan con ciertos procedimientos para ayudar a hacer cumplir estos controles

A.9.1.2 Política sobre el uso de los servicios de red

El departamento de TIC's restringe el acceso de los empleados a sitios no autorizados e inseguros y mantiene requisitos de autenticación para el acceso a la red, además de servicios que no son necesarios para realizar y completar actividades laborales.

El Personal del Departamento de sistemas de información tienen acceso a la configuración de la red, por tal motivo evita que las personas no autorizadas usen el Wi-Fi, pero aquellos que tienen acceso no son supervisados

A.9.2 Gestión de acceso de usuarios

A.9.2.1 Registro y cancelación del registro de usuarios

El personal del departamento de TIC's es responsable de asignar y eliminar las cuentas y las contraseñas de los usuarios a los equipos y sistemas de información, dichas contraseñas no son gestionadas correctamente, ni documentadas.

A.9.2.2 Suministro de acceso de usuarios

No disponen un control adecuado donde garanticen que se asignen permisos conforme a las necesidades que el usuario, solo se le crea el usuario en el sistema sin aplicar controles que gestionen la cuenta.

A.9.2.3 Gestión de derechos de acceso privilegiado

Este control no se aplica de manera efectiva porque no hay una política de acceso definida con privilegios especiales, solo otorgan privilegios de acuerdo a sus intereses, pero debido a la falta de documentación de acceso, no saben si algunos usuarios tienen derechos de acceso privilegiado.

A.9.2.4 Gestión de información de autenticación secreta de usuarios

En el departamento de TIC se menciona de manera verbal la confidencialidad de las contraseñas de autenticación de usuarios dentro de la empresa y se advierte que es importante resguardar la contraseña después de que se le haya asignado.

Uno de los problemas encontrados fue que los usuarios no estaban capacitados o instruidos para crear contraseñas, poniendo en riesgo su seguridad de la información**.**

A.9.2.5 Revisión de los derechos de acceso de usuarios

El acceso de usuarios regulares o privilegiados no se revisa ni documenta en los sistemas y aplicaciones, por lo que los usuarios regulares tienen acceso a privilegios que solo deberían estar disponibles para el personal autorizado. Es importante contar con procedimientos para llevar a cabo esta revisión de forma regular.

A.9.2.6 Retiro o ajuste de los derechos de acceso

Dicho control ocurre cuando hay un cambio de trabajo o un miembro subordinado de la empresa renuncia a su cargo o empleo, no existe un proceso escrito para hacerlo y

el cumplimiento de esta sección es ineficaz, debido a que existen inconvenientes en administrar las cuentas de los empleados.

A.9.3 Responsabilidades de los usuarios

A.9.3.1 Uso de la información de autenticación secreta

No existen controles formales para garantizar la confidencialidad de la información de autenticación, por lo que los departamentos de TI intentan garantizar esto proporcionando avisos informativos a todos los usuarios que muestran los siguientes puntos de seguridad para la información confidencial**.**

A.9.4 Control de acceso a sistemas y aplicaciones

A.9.4.1 Restricción de acceso Información

La información de los sistemas y aplicaciones de la empresa tiene restricciones de escritura y lectura basadas en las actividades de desarrollo requeridas, son asignadas a los usuarios y la información es oculta para los usuarios regulares a través de la administración del sistema.

A.9.4.2 Procedimiento de ingreso seguro

Los inicios de sesión en los sistemas y aplicaciones existentes se crean con el nombre inicial seguido de un punto y el apellido, el sistema tiene advertencias para ayudar a iniciar sesión, cuando el sistema ha verificado las credenciales, debe ingresarlas al sistema o serán bloqueadas, en estos casos, el usuario debe acudir al departamento de TIC's para desbloquear.

A.9.4.3 Sistema de gestión de contraseñas

Los sistemas y aplicaciones no se gestionan con contraseñas definidas en las políticas y estándares de la empresa, ya que estos controles aún no se han generado.

A.9.4.4 Uso de programas utilitarios privilegiados

El departamento de TIC's se divide en tareas, donde existe un responsable del control de los servicios privilegiados en el sistema, los cuales se prestan únicamente de acuerdo a su rol y responsabilidades en las condiciones de trabajo.

A.9.4.5 Control de acceso a códigos fuente de programas

El software desarrollado es fundamentalmente de uso exclusivo de la empresa. El código fuente de los programas se encuentran protegidos con acceso restringido solo el personal de desarrollo de software tiene acceso al mismo, pero no se tiene un control del uso de un controlador de versiones ni tampoco se tiene un entorno de compilación seguro para pruebas.

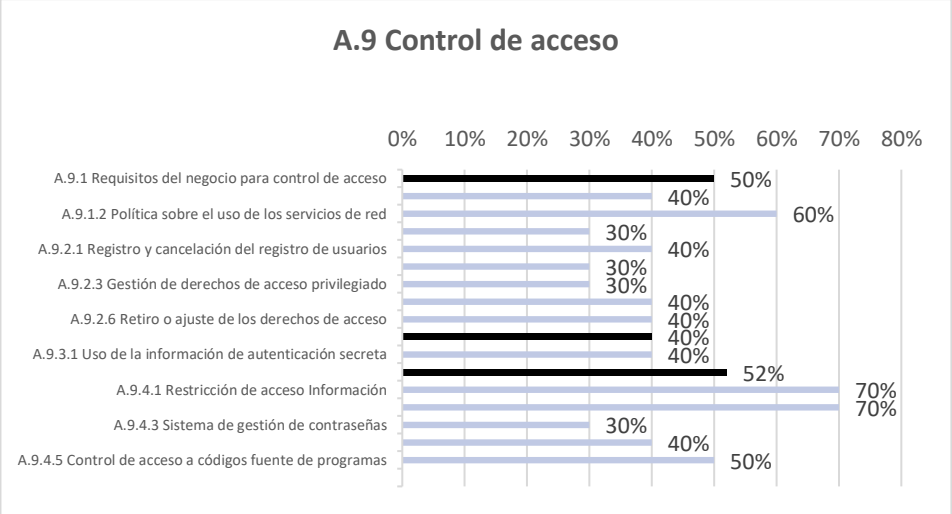


Figura 17.Análisis porcentual - Control de acceso.

Elaborado por: Investigador

De acuerdo con la figura 17 presentado anteriormente se tiene un nivel bajo en cuanto a cumplimiento del control de acceso por lo que se deberán tomar las medidas correctivas apropiadas.

A.10 Criptografía

A.10.1 Controles criptográficos

A.10.1.1 Política sobre el uso de controles criptográficos

La empresa no ha establecido una política para el uso de controles criptográficos.

A.10.1.2 Gestión de llaves

Debido a que no tiene una política de control de contraseñas, no se puede crear un método de gestión de llaves.

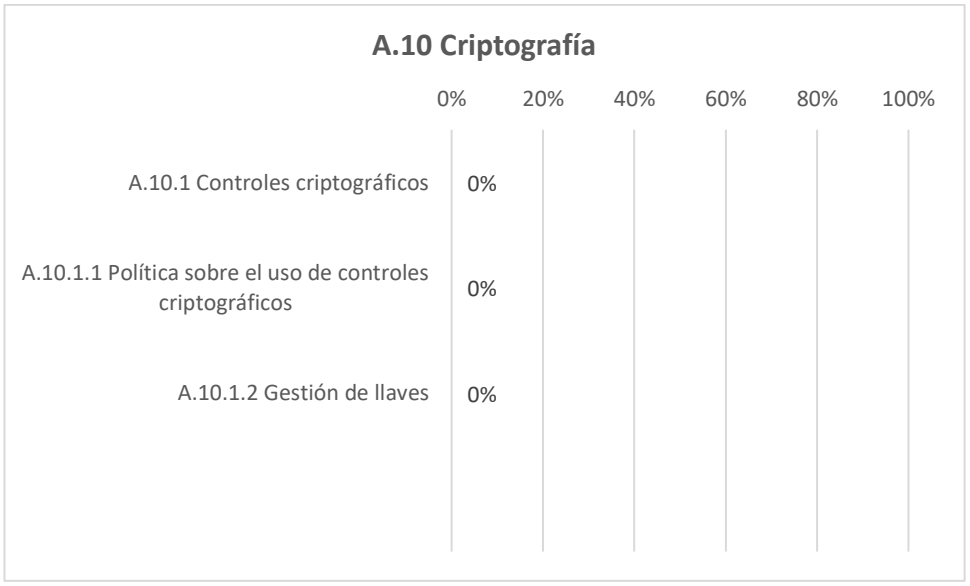


Figura 18.Análisis porcentual - Criptografía.

Elaborado por: Investigador

Como se puede observar en la figura 18, no se cumple ninguno de los controles relacionados con el dominio de Criptografía.

A.11 Seguridad física y del entorno

A.11.1 Áreas seguras

A.11.1.1 Perímetro de seguridad física

Se evidenció que las oficinas, las redes informáticas, los archivos… no tienen un límite de seguridad claro, un factor favorable que **s**e limita el acceso a personas de la empresa**.**

A.11.1.2 Controles físicos de entrada

No se tiene ningún control físico de entrada de los empleados, simplemente los empleados llegan a la empresa y avisan que llegaron a laborar.

A.11.1.3 Seguridad de oficinas, recintos e instalaciones

Las oficinas que tienen la información tienen seguridad de llaves para evitar que cualquier persona ingrese, pero no se tienen ningún otro método de seguridad lo cual es recomendable establecerlo tal como un lector biométrico.

A.11.1.4 Protección contra amenazas externas y ambientales

Para las protecciones en caso de un incendio se tienen extintores ubicadas en zonas estratégicas de la empresa, no existen facilidades de evacuación en caso de un sismo, para detectar intrusos no se tiene de cámaras de seguridad ni de sensores de movimientos y alarmas.

A.11.1.5 Trabajo en áreas seguras

Para promover la seguridad de la información, el departamento de TIC's menciono que eventualmente se inspeccionan oficinas de los departamentos de la empresa.

A.11.1.6 Áreas de despacho y carga

La carga y descarga de los equipos se realiza a través de la puerta principal donde se controla el acceso y solo se permite el acceso al personal autorizado estableciendo horarios de apertura y cierre.

A.11.2 Equipos

A.11.2.1 Ubicación y protección de los equipos

Tienen en cuenta controles ambientales para proteger los equipos y evitar daños, tiene a su disposición los UPS diseñados para ahorrar energía, pero se debe realización un mantenimiento a dichos dispositivos.

A.11.2.2 Servicios de suministro

En la empresa se encuentra establecido medidas de control para el sistema UPS necesario y potencia adecuada para mantener operativos todos los equipos informáticos, cabe mencionar que existen algunos equipos no cuentan con UPS lo cual pueden generar afectación a la integridad física de los equipos.

A.11.2.3 Seguridad del cableado

Los cables de potencia no se encuentran separados de los cables de red. No se tiene el uso de canaletas evitar daños al cableado de la red.

A.11.2.4 Mantenimiento de equipos

Se tiene conocimiento de que no existe un plan programático de mantenimiento de los equipos informáticos, el mantenimiento ocurre cuando una computadora se estropea

por cualquier motivo o no funciona correctamente y/o no se le da mantenimiento desde hace mucho tiempo, cuando se realiza un mantenimiento global de todas las computadoras existentes. requerido.

A.11.2.5 Retiro de activos

Este control es necesario ya que se requiere documentar los bienes y activos que salen de la empresa, y debe contar con actas de entrega y recepción.

A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Control no aplicable debido a que todas las actividades se realizan en los equipos dentro de la empresa.

A.11.2.7 Disposición segura o reutilización de equipos

Los equipos informáticos que van a ser reutilizados o eliminados se encuentran establecidos bajo las siguientes normas:

- La información almacenada en el equipo es eliminado o transferido a otro equipo según la importancia antes de su debida reutilización.
- Se asegura que la información del equipo sea eliminada completamente
- Se evalúa el riesgo antes de proceder a una reparación del equipo que se encuentre dañado.
- Se lleva un registro de los equipos informáticos reutilizados o eliminados

A.11.2.8 Equipos de usuario desatendidos

El proceso para que los equipos que no estén en uso se lo hacen mediante un tiempo de 10 minutos dado ese intervalo la maquina es bloqueada con contraseña que sabe solo el propietario de ese equipo, pero no se tiene un seguimiento de este control.

A.11.2.9 Política de escritorio limpio y pantalla limpia

No se tiene un control, lo que puede generar la visualización de la información en pantalla que se maneja en el área de trabajo.

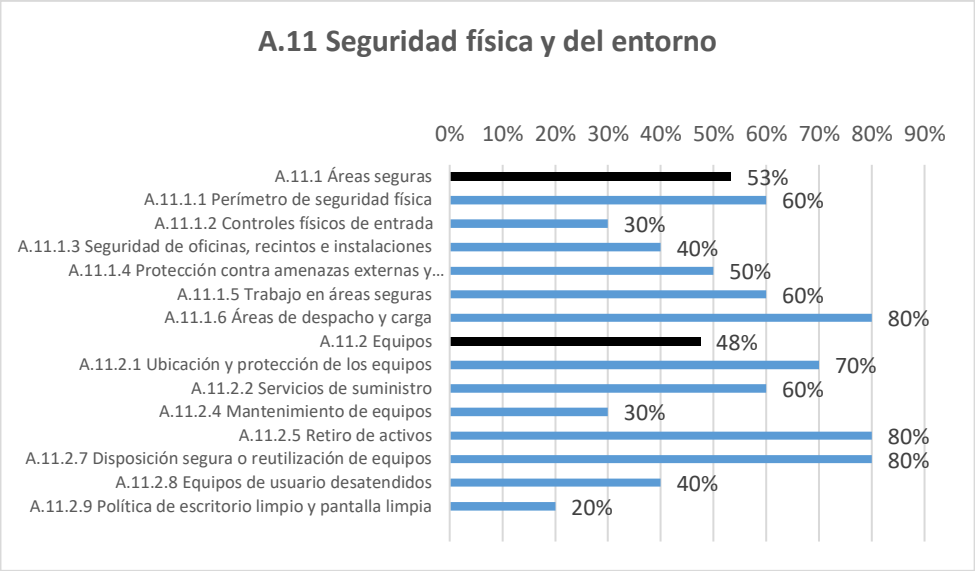


Figura 19.Análisis porcentual - Seguridad física y del entorno.

Elaborado por: Investigador

De acuerdo con la figura 19 presentado anteriormente se tiene un nivel bajo en cuanto a cumplimiento de la seguridad física y del entorno por lo que se deberán tomar las medidas correctivas apropiadas

A.12 Seguridad de las operaciones

A.12.1 Procedimientos operacionales y responsabilidades

A.12.1.1 Procedimientos de operación documentados

Uno de los problemas es que los procesos relacionados con la seguridad de la información no están documentados y solo son socializados para que los empleados involucrados en ciertos procesos sepan cómo se llevan a cabo estos procesos.

A.12.1.2 Gestión de cambios

No se establece una política de gestión de cambios el proceso se lo realiza informalmente con medidas de precaución y verificando el control de cambios en la infraestructura de la empresa.

A.12.1.3 Gestión de capacidad

La gestión de la capacidad de las tecnologías de la información se aplica mediante el seguimiento del uso de recursos.

El problema detectado es que no se realizan registros de la gestión de capacidades, ya que no cuentan con el establecimiento de políticas eficientes que ayuden a que se aplique correctamente este control.

A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación

No se cuenta con entornos de desarrollo separados de los entornos de producción o prueba, lo cual es necesario para evitar problemas de indisponibilidad o fallas en el servicio.

A.12.2 Protección contra códigos maliciosos

A.12.2.1 Controles contra códigos maliciosos

Este control se aplica por medio de un antivirus que se usa para contrarrestar los códigos maliciosos, el antivirus que se usa en la empresa es el Avast Free Antivirus sin licencia. Además, no existen controles establecidos para que los usuarios que utilizan los equipos informáticos utilicen el antivirus al momento de introducir los dispositivos de almacenamiento extraíbles.

A.12.3 Copias de respaldo

A.12.3.1 Respaldo de información

El respaldo de la información se la llevada a cabo, pero no en base a una política de seguridad para que se realicen backups de la información importante, dicho respaldo se lo hace semanalmente.

Especialmente las copias se hacen de los archivos que maneja la empresa tales como: Las bases de datos de los clientes y los Informes de reparación de los equipos, las copias de respaldo se almacenan discos duros en ubicaciones inadecuadas, en la misma empresa generando riesgos de acceso.

A.12.4 Registro y seguimiento

A.12.4.1 Registro de eventos

Este tipo de control no tiene políticas ni procedimientos establecidos para cubrir lo que sucede en el sistema de información, por lo que, si algo sale mal, el Departamento de TIC's brinda una solución en base a las herramientas disponibles, una de las cuales es la revisión, donde se puede ver lo que salió mal. en el registro.

A.12.4.2 Protección de la información de registro

No se aplican controles, tampoco se aplican procedimientos para resguardar la información por lo que es necesario brindar protección de los registros del sistema para evitar pérdidas, o cambios no autorizados.

A.12.4.3 Registros del administrador y del operador

No están documentados los registros para los responsables pongan en marcha el control y administración de usuarios comunes y privilegiados.

A.12.4.4 sincronización de relojes

Se ejecuta procedimientos relativos a la sincronización del reloj, pero no mediante referencias como reloj automático, GPS, NTP …, por consiguiente, no se tiene un cumplimiento de este control.

A.12.5 Control de software operacional

A.12.5.1 Instalación de software en sistemas operativos

Se realizan instalaciones de software en cualquier equipo informático de la empresa, cabe recalcar que el software solo está permitido su instalación por el departamento de sistemas, además no se tiene un control para realizar una correcta instalación del software.

A.12.6 Gestión de la vulnerabilidad técnica

A.12.6.1 Gestión de las vulnerabilidades técnicas

Este control no se aplica debidamente en la empresa ya que no tienen políticas ni procedimientos donde se realicen escaneos periódicos de vulnerabilidades técnicas en los equipos informáticos.

A.12.6.2 Restricciones sobre la instalación de software

La Instalación de software en los equipos informáticos es limitado solo el personal autorizado con privilegios de administrador lo realiza.

A.12.7 Consideraciones sobre auditorias de sistemas de información

A.12.7.1 Información controles de auditoría de sistemas

Este control no se cumple porque la empresa no tiene una auditoria de seguridad en los sistemas.

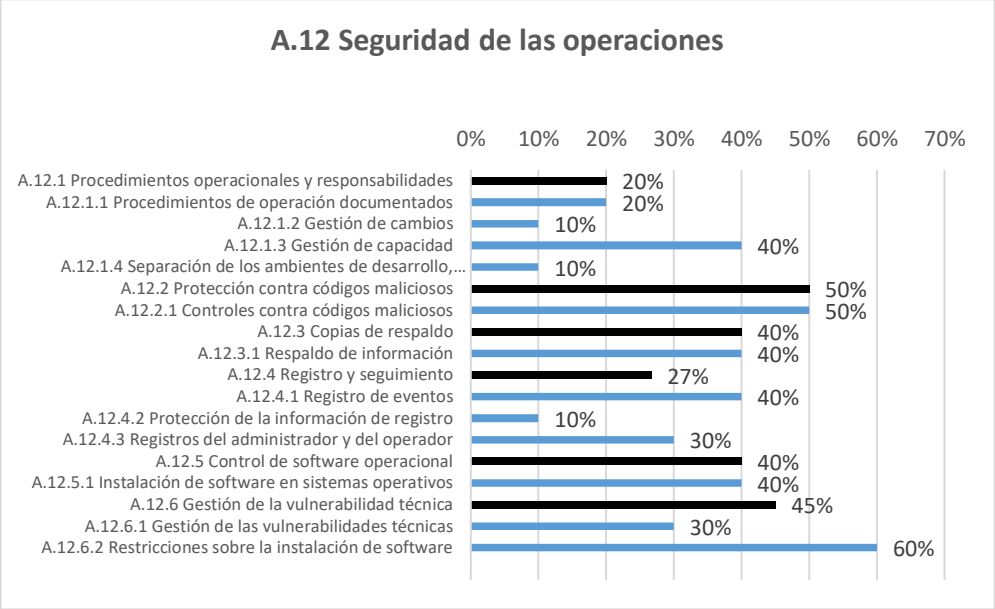


Figura 20.Análisis porcentual - Seguridad de las operaciones.

Elaborado por: Investigador

De acuerdo con la figura 20 presentado se tiene un nivel sumamente bajo en cuanto a cumplimiento de la seguridad de las operaciones por lo que se deberán tomar las medidas correctivas apropiadas

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

A.13.1.1 Controles de redes

No se lleva a cabo controles adecuados en la red, como consecuencia está expuesto a sufrir ataques y robo de la información, existen un control de autentificación para todos los que requieran acceder a la red.

A.13.1.2 Seguridad de los servicios de red

Este control se cumple indebidamente ya que no clasifican y protegen los servicios de red de forma adecuada, tampoco existe un monitoreo de los servicios de red, tampoco mantienen una auditoria. Solamente existen ciertos procedimientos como la autentificación en la red, revisiones de las configuraciones de la red, etc.

A.13.1.3 Separación en las redes

No existe un control para segmentar la red, pero su distribución está ordenada de acuerdo a los requerimientos de la empresa. Sin embargo, no se lleva a cabo la segmentación de red lógica en la empresa.

A.13.2 Transferencia de información

A.13.2.1 Políticas y procedimientos de transferencia de información

No existe un control que permita el cumplimiento del mismo.

A.13.2.2 Acuerdos sobre transferencia de información

No se ha establecido acuerdos de transferencia de la información, lo cual conlleva a ser un riesgo perjudicial para quienes intercambian datos de la empresa.

A.13.2.3 Mensajería electrónica

Se administra mediante controles que no son eficientes al no poseen una política segura de mensajería que cubra los intercambios de datos por comunicación en la red.

A.13.2.4 Acuerdos de confidencialidad o de no divulgación

Este control no se aplica correctamente debido a que no se tienen establecidos acuerdos de confidencialidad de intercambio de la información.

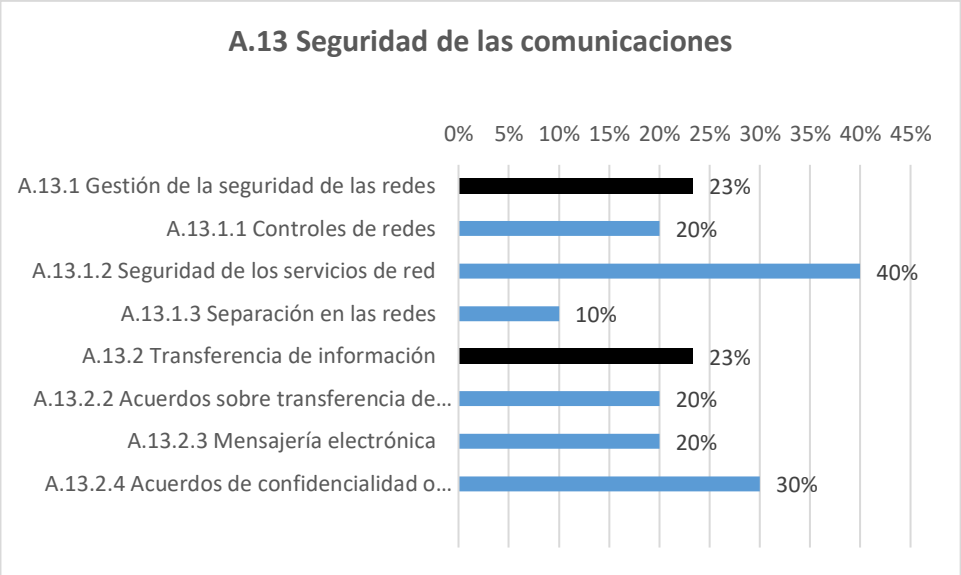


Figura 21. Análisis porcentual - Seguridad de las comunicaciones.

Elaborado por: Investigador

Con respecto a la figura 21 presentado se tiene un nivel sumamente bajo en cuanto a cumplimiento de la seguridad de las comunicaciones por lo que se deberán tomar las medidas correctivas apropiadas.

A.14 Adquisición, desarrollo y mantenimientos de sistemas

A.14.1 Requisitos de seguridad de los sistemas de información

A.14.1.1 Análisis y especificación de requisitos de seguridad de la información

Al momento de adquirir un software se tienen en cuenta los requisitos tales como: accesos al sistema, características y funcionalidades que se pueda mantener a largo plazo.

A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas

No se establece un control para resguardar la seguridad de los servicios de las aplicaciones solamente se establece un control para mantener las aplicaciones.

A.14.1.3 Protección de transacciones de los servicios de las aplicaciones

No se cuenta con un control apropiado para brindar protección a los servicios de las aplicaciones.

A.14.2 Seguridad en los procesos de desarrollo y soporte

A.14.2.1 Política de desarrollo seguro

Después de desarrollar un software se ejecutan los nuevos sistemas en producción, y no se efectúan pruebas de seguridad.

A.14.2.2 Procedimientos de control de cambios en sistemas

No existe un control para gestionar los cambios en los sistemas, solamente se lo realiza en base a los riesgos de información.

A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

No se establecen revisiones técnicas de las aplicaciones después de aplicado los cambios.

A.14.2.4 Restricciones en los cambios a los paquetes de software

No se limita los cambios en los paquetes de software.

A.14.2.5 Principios de construcción de sistemas seguros

Se sigue un procedimiento por etapas para el diseño y codificación del software, también para mecanismos de autenticación.

A.14.2.6 Ambiente de desarrollo seguro

No se controla el ambiente de desarrollo, solamente de confía en el desarrollo del software con informes.

A.14.2.7 Desarrollo contratado externamente

No se tiene control de una externalización del desarrollo del software.

A.14.2.8 Pruebas de seguridad de sistemas

Se encuentran establecido un control para llevar a cabo procedimientos de pruebas y verificación para los nuevos sistemas o actualizados.

A.14.2.9 Prueba de aceptación de sistemas

No existe un control para analizar la seguridad de los sistemas antes de ser llevados en producción.

A.14.3 Datos de prueba

A.14.3.1 Protección de datos de prueba

No se dispone de un control para llevar a cabo controles de seguridad de los sistemas que se desarrollan.

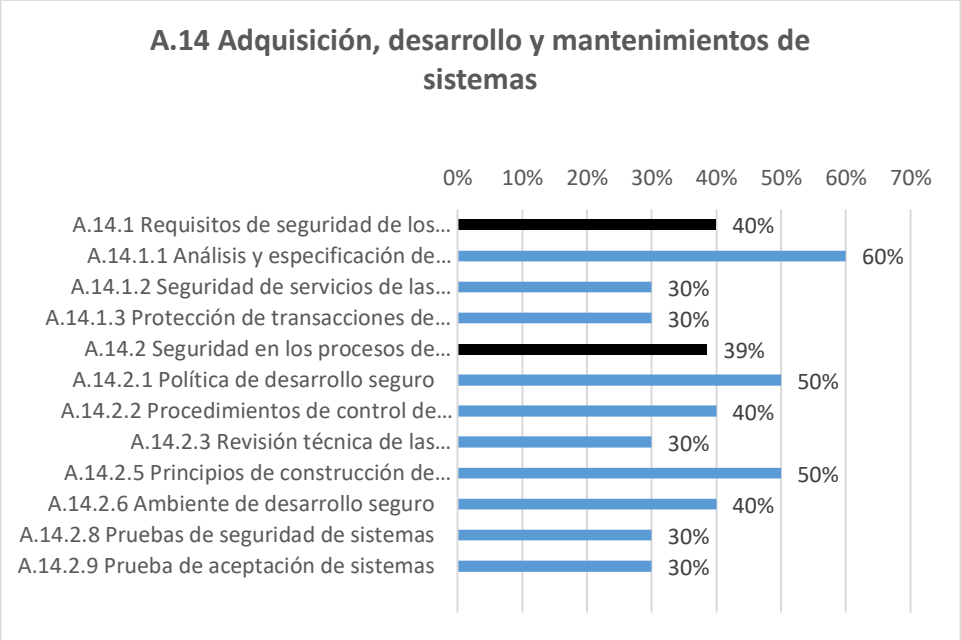


Figura 22. Análisis porcentual - Adquisición, desarrollo y mantenimientos de sistemas.

Elaborado por: Investigador

Una vez analizada la figura 22 se tiene un nivel sumamente bajo en cuanto a cumplimiento de la seguridad de las comunicaciones por lo que se deberán tomar las medidas correctivas apropiadas.

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

A.16.1.1 Responsabilidad y procedimientos

No se tiene establecido un control para llevar a cabo procedimientos y responsables del Departamento de TIC’s para aplicar medidas de seguridad.

A.16.1.2 Reporte de eventos de seguridad de la información

No existe un control para la notificación de los eventos de seguridad de la información, únicamente se socializa por parte del departamento de TIC’s

A.16.1.3 Reporte de debilidades de seguridad de la información

No se cuenta con un control que ayude a notificar la seguridad de la información, por tal motivo los empleados no tienen una obligación para informar cualquier incidente en la empresa.

A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Para la evaluación de los eventos de seguridad, se socializa a todo el personal que notifiquen incidentes sobre la seguridad de la información, después se realiza una evaluación dependiendo del tipo de incidente por parte del departamento de TIC’s.

A.16.1.5 Respuesta a incidentes de seguridad de la información

El personal del departamento de TICS es el encargado de dar respuesta y solución a los incidentes de seguridad.

A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

No se tienen registrados los incidentes suscitados y pese a ello no se concientiza sobre lo importante que es tener una gestión de riesgos.

A.16.1.7 Recolección de evidencia

Con respecto a este control el personal del departamento de TIC’s intervienen al momento de solucionar los ataques informáticos y ejecutan conocimientos.

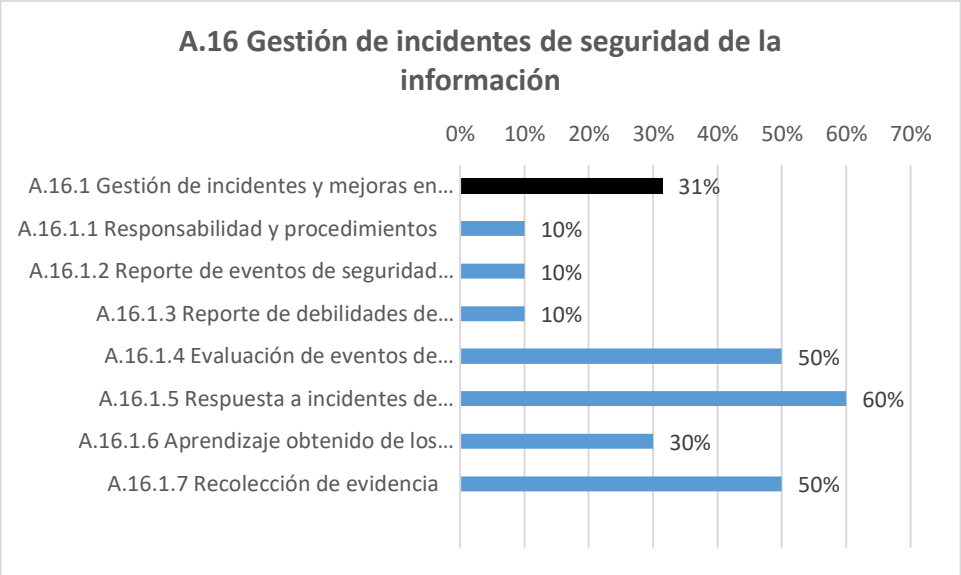


Figura 23. Análisis porcentual - Gestión de incidentes de seguridad de la información.

Elaborado por: Investigador

Analizada la figura 23 se tiene un nivel bajo en cuanto a cumplimiento de la Gestión de incidentes de seguridad de la información por lo que se deberán tomar las medidas correctivas apropiadas.

A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

A.17.1 Continuidad de seguridad de la información

A.17.1.1 Planificación de la continuidad de la seguridad de la información

Se cuenta con un plan de contingencia para la continuidad de negocio, pero no está establecida por la criticidad de los equipos tecnológicos ni para la seguridad de la información.

A.17.1.2 Implementación de la continuidad de la seguridad de la información

No se tiene cumplimiento debido a que no tienen planificado la continuidad con respecto a la seguridad de la información

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

No existe una gestión para la continuidad con respecto a la seguridad de la información, por consiguiente, no se puede verificar, revisar y evaluar.

A.17.2 Redundancias

A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Se dispone de un control para poner a disposición procedimientos de instalación de software definiendo la capacidad del rendimiento del equipo informático.

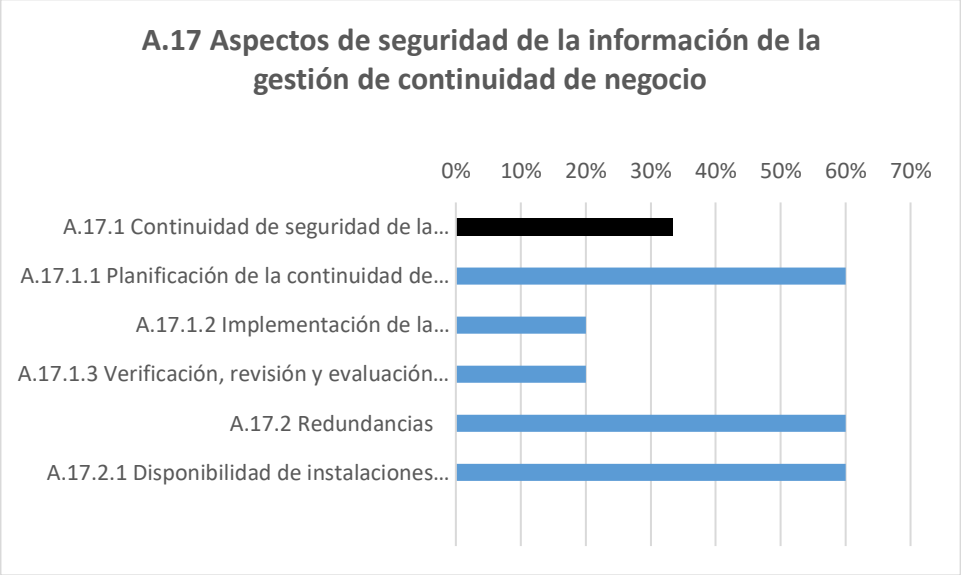


Figura 24. Análisis porcentual - Aspectos de seguridad de la información de la gestión de continuidad de negocio.

Elaborado por: Investigador

Como se puede observar en la figura 24 se tiene un nivel regular en cuanto a cumplimiento de la seguridad de la información y de la gestión de continuidad del negocio por lo que se deberán tomar las medidas correctivas apropiadas.

A.18 Cumplimiento

A.18.1 Cumplimiento de requisitos legales y contractuales

A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

La empresa no tiene controles sobre el cumplimiento de requisitos legales como la Ley Orgánica de Protección de Datos (LOPD)

A.18.1.2 Derechos de propiedad intelectual

El uso del software está basado en los derechos de propiedad intelectual mediante procedimientos en la adquisición.

A.18.1.3 Protección de registros

El departamento de TIC's es el encargado de evitar el robo de información, falsificación o el acceso no autorizado, pero no se tiene en cuenta los requisitos legales.

A.18.1.4 Privacidad y protección de datos personales

El departamento de TIC's socializa a todo el personal de la empresa que la información de cada usuario debe ser resguardada de manera segura con la finalidad de mantener la confidencialidad e integridad de su información.

A.18.1.5 Reglamentación de controles criptográficos

No se dispone de un control para tener controles criptográficos de la información en la empresa.

A.18.2 Revisiones de seguridad de la información

A.18.2.1 Revisión independiente de la seguridad de la información

No se toma en consideración la elaboración de la gestión de riesgos para detectar vulnerabilidades en los activos de información, en consecuencia, no se tienen revisiones de seguridad de la información.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad

El cumplimiento de las políticas de seguridad está encargado de los responsables de cada departamento de la empresa con el departamento de TIC's

A.18.2.3 Revisión del cumplimiento técnico

No existe una revisión periódica para realizar escaneos de vulnerabilidades en la red y en los equipos informáticos.

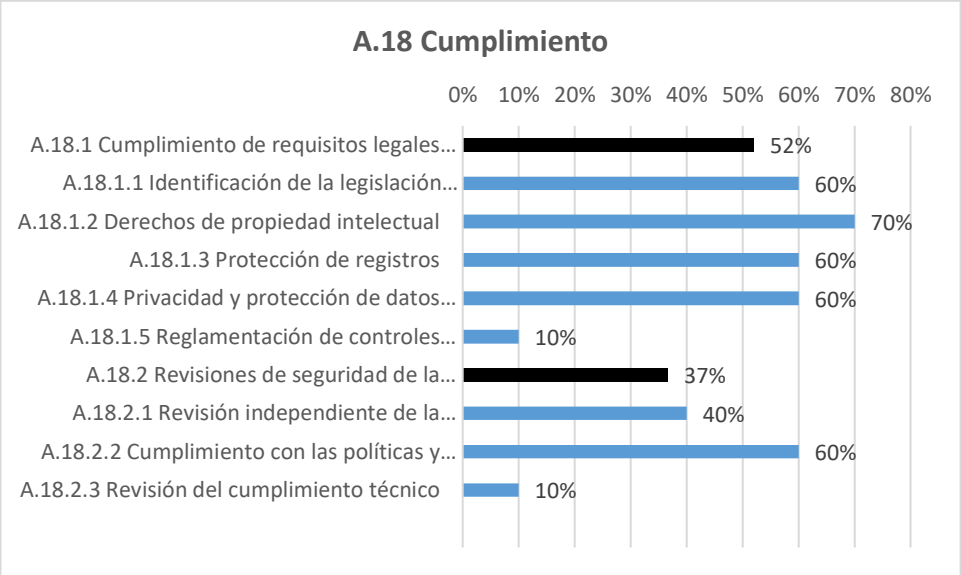


Figura 25.Análisis porcentual - Cumplimiento.

Elaborado por: Investigador

Como se puede identificar en el grafico presentado se tiene un nivel regular en cuanto al cumplimiento por lo que se deberán tomar las medidas correctivas apropiadas.

3.2.4.8 Políticas y controles para la seguridad de la información para la empresa EPC COMPU

A través de la implementación de la Norma ISO 27001:2013, se realizó un análisis de la seguridad de la información en EPC COMPU en base a los procedimientos tales como la evaluación de riesgos, declaración de aplicabilidad, porcentaje de cumplimiento de los controles al momento de la revisión, permitiendo establecer las nuevas Políticas y controles para la seguridad de la información

A continuación, se definirán políticas que satisfagan las necesidades requeridas en las diferentes áreas de la empresa, tanto: organizacional, física, lógica y legal de EPC COMPU en lo referente al manejo adecuado de la seguridad de la información.

Seguridad Organizacional

Se establecerá una estructura formal para administrar la empresa, incluidos los aspectos relacionados con los servicios, la gestión de activos, los recursos humanos y materiales, las responsabilidades y las actividades de apoyo en situaciones o incidentes de seguridad de la información.

Seguridad Lógica

Se desarrollarán lineamientos y reglamentos para gestionar el control de acceso de los usuarios a los sistemas y equipos de EPC COMPU para evitar cambios o modificaciones en sus configuraciones. Además, se definen reglas para controlar vulnerabilidades creadas por malware.

Seguridad Física

Se establecerán controles relacionados con el mantenimiento y soporte de los equipos y se establecerán restricciones adicionales con referencia a la seguridad perimetral de EPC COMPU.

Seguridad Legal

Las políticas y estándares de seguridad se definirán de acuerdo con el reglamento interno de EPC COMPU para asegurar el cumplimiento de este reglamento. Además, se impondrán las sanciones correspondientes a quienes no cumplan a cabalidad con las normas mencionadas y pongan en peligro la seguridad de la información.

3.2.4.9. Aplicación de las Normas ISO 27001 a la empresa EPC COMPU

I. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En vista de que no tienen definidos los roles y responsables (Ver **ANEXO 9**) para la seguridad de la información fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsables: Jefe de Mantenimiento de Informática, Asistente de Tecnologías

I.I Roles y responsabilidades para la seguridad de información

- Se debe definir un equipo de seguridad mediante la elaboración de un documento en el que se definan los roles, responsabilidades y actividades a

realizar para solucionar el incidente de la seguridad de la información por parte del encargado.

A continuación, se designan los roles del equipo de seguridad del Departamento de TIC's

- **Rol: Jefe del Departamento de TIC's**

  Responsabilidades

  - Liderar y controlar la seguridad en la Empresa
  - Asignar responsabilidades.
  - Supervisión de las actividades del Departamento de TIC's
  - Implementar programas de capacitaciones a todo el personal.
  - Recurrir a medidas de sanción en caso de incumplimiento de los controles de seguridad.
  - Proporcionar recursos informáticos.
  - Revisión de las políticas de seguridad.

- **Rol: Asistente de Tecnologías**

  Responsabilidades

  - Análisis y Elaboración de informes.
  - Pruebas de seguridad en la red

- **Rol: Jefe de Mantenimiento de informática**

  Responsabilidades

  - Examinar y diagnosticar el estado de los equipos informáticos y de los sistemas de información.
  - Instalación y configuración del software
  - Reparación y sustitución de equipos informáticos.
  - Soporte Técnico

- **Rol: Desarrollador de Software**

  Responsabilidades

  - Documentación y Manual del Software
  - Pruebas e Implementación del Software

- Los roles y responsabilidades del equipo de seguridad deben estar claramente definidas para que los empleados tengan claro las actividades que deben realizar ante un incidente de seguridad informático.

- Comunicar de manera clara a cada empleado a través de sesiones informativas generales distribuyendo el documento que detalle los roles y responsabilidades.
- Elaborar un documento en el que se detallen los roles y responsabilidades asignar anteriormente para solucionar los incidentes de seguridad de la información.
- Reportar los incidentes de seguridad o riesgos que podrían afectar la seguridad de la información y posterior a eso comunicar al jefe del departamento de TIC.

II. GESTIÓN DE ACTIVOS

Como se observó no tienen definido una adecuada Gestión de Activos para la seguridad de la información y fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Jefe de Mantenimiento de Informática

II.I Clasificación de la información

- Se deberá clasificar debidamente toda la información que se maneja en la empresa, para resguardar la seguridad al acceso de la misma por parte de los empleados.
- Se elaborará un documento en el que se registre si la información del activo que se maneja en la empresa es pública o privada, además se deberá registrar el activo de acuerdo con los siguientes criterios de clasificación:
    a. Critica: Información indispensable para el funcionamiento de la empresa, debe ser manejada con extrema precaución y solo los más altos directivos de la empresa tendrán acceso a la misma. De acuerdo a este argumento la información crítica de la empresa son las bases de datos de los clientes.
    b. Valiosa: Es la información muy importante para la empresa por lo que debe ser manejada con cuidado. la información valiosa de la empresa son todos los archivos de bienes, recursos e información de la empresa de la empresa.

c. Sensible: Información que solo debe ser conocida por el personal autorizado dentro de la empresa. La información sensible dentro de la empresa son los archivos como datos personales de los empleados.

- Diferentes tipos de respaldos:
    a. Respaldo completo: Este tipo de respaldo copia todos los archivos y datos seleccionados en su totalidad.
    b. Respaldo incremental: Solo se respaldas los archivos que han cambiado o han sido modificados desde el último respaldo, ya sea este completo o incremental.
    c. Respaldo continuo: Realiza copias de seguridad constantes y en tiempo real de los archivos a medida que se van modificando.

- Identificar los directorios o servidores que contienen los archivos críticos para respaldar es decir el directorio de documentos compartidos, la base de datos, correos electrónicos, sacar un respaldo completo una vez a la semana y respaldos incrementales diarios.
- En caso de optar por un respaldo manual se debe verificar que los archivos se hayan copiado correctamente y que puedan ser accesibles y restaurados. Es importante realizar pruebas de recuperación para asegurar que los respaldos sean válidos.
- Guardar el disco duro de respaldo en un lugar seguro como un Data center externo estos centros de datos especializados ofrecen servicios de almacenamiento seguro y protección de datos incluyendo sistemas de respaldo y protección.

II.II Etiquetado de la información

Se diseñará un sistema de etiquetado claro y consistente para indicar el nivel de confidencialidad o de clasificación. A continuación, se presenta la manera del etiquetado si se utiliza información física se deberá utilizar sellos y rótulos en las carpetas y archivadores para identificarlos correctamente, y para la información digital se utilizará colores de identificación en las carpetas de archivos.

II.III Manejo de activos

Se deberá tener un control eficiente de la clasificación y del etiquetado de la información.

III. SEGURIDAD DE LOS RECURSOS HUMANOS

Como se pudo observar se presentan falencias en la seguridad de los recursos humanos y fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Jefe de Mantenimiento de Informática

III.I Durante la ejecución del empleo

- El personal que ingrese a la empresa a laborar deberá recibir capacitación en el uso adecuado de la seguridad de la información para mantener la integridad, disponibilidad y confidencialidad de la información, según el área en la que se encuentre y las funciones que desempeñe.
- La información procesada en la empresa es propiedad exclusiva de EPC COMPU, y los empleados tienen prohibido alterar o eliminar información sin su permiso.
- Los empleados deben comprometerse y firmar un acuerdo de confidencialidad con respecto a la información con la que trabajarán mientras estén en las instalaciones.

III.II Terminación o cambio de empleo

- A la terminación de su relación laboral con la empresa, los empleados que se retiren deberán devolver los bienes que les hayan sido asignados para el desarrollo de sus actividades.
- Al finalizar la relación laboral con el empleado, se deberá cerrar y eliminar cada una de las cuentas asignadas a éste, este proceso garantizará la seguridad de la información institucional.

III.III. Gestión De Medios Removibles

- Se debe requerir la utilización de los medios removibles con autorización del Jefe del Departamento de TIC's.
- Encriptar los medios removibles los cuales contengan información crítica, valiosa, y sensible.
- Mantener bajo control la transferencia de información hacia los medios removibles.
- Documentar todos los procedimientos de autorización.

IV. CONTROL DE ACCESO

Como se pudo observar se presentan falencias en el control de acceso por tal motivo fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Jefe de Mantenimiento de Informática

IV.I. Registro y cancelación del registro de usuarios

- Elaborar un registro de las cuentas de usuarios para identificar al usuario correspondiente.
- Asignar la cuenta de usuario de acuerdo con el rol y responsabilidad dentro de la empresa.
- Desactivar la cuenta de usuario inmediatamente cuando el usuario abandona la empresa.

IV.II. Gestión de derechos de acceso privilegiado

- Identificar los accesos privilegiados para acceder al equipo informático o al sistema de información.
- Establecer un periodo de caducidad de los permisos privilegiados.
- Forzar el cambio de contraseñas cuando un usuario cambia o abandona el puesto de trabajo.
- Elaborar un documento en el que se detallen una lista de los equipos, dirección ip, el usuario y la contraseña para gestionar los accesos privilegiados.

IV.III. Responsabilidades de los usuarios

- Las contraseñas asignadas no deben ser divulgadas
- Evitar escribir las contraseñas en notas, papel etc.
- El único medio de acceso al equipo será mediante la contraseña asignada por el jefe del departamento de TIC's.
- El único medio de acceso al sistema de información será mediante el usuario y contraseña asignada por el jefe del departamento de TIC's.

IV.VI. Control de acceso a sistemas y aplicaciones

- Elaborar un documento para restringir derechos de lectura, escritura, eliminación, modificación etc.

IV.VII. Procedimiento de ingreso seguro

- El proceso de inicio de sesión de validar la identidad del usuario.
- Implementar el sistema de doble factor de autenticación.
- No se deberá mostrar la contraseña de inicio de sesión al equipo informático o al sistema de información.
- Se debe registrar el número de intentos fallidos de inicio de sesión.
- Las contraseñas del sistema de información deberán permanecer encriptadas.
- Las sesiones inactivas deben ser cerradas durante un tiempo determinado.
- Limitar horas del día para acceder al sistema de información.

IV.VIII. Sistema de gestión de contraseñas

- Se deberá usar un gestor de contraseñas para generar contraseñas robustas y seguras para acceder a los equipos informáticos y a los sistemas de información.
- Las contraseñas asignadas a los usuarios deberán ser administradas y gestionadas.
- Queda totalmente prohibida la divulgación de las contraseñas asignadas a los empleados de la empresa.
- En caso de pérdida de contraseñas por parte del empleado, se deberá presentar una justificación formal para que el personal del departamento de TIC's habilite una contraseña temporal.

V. SEGURIDAD DE LAS OPERACIONES

Como se pudo evidenciar se presentan falencias en la seguridad de las operaciones por tal razón fue necesario crear una política y controles para llevar a cabo este procedimiento bajo los siguientes controles:

Responsables: Jefe del Departamento de TIC's, Asistente de Tecnologías

V.I. Separación de los ambientes de desarrollo, pruebas y operación

- Los sistemas que se desarrollan deberán pasar por escenarios de pruebas para posteriormente ser puesto en producción.
- Toda la información de código fuente o base de datos deberá tener acceso únicamente el desarrollador de software bajo un acuerdo de confidencialidad**.**
- Cada ambiente debe tener su propia infraestructura evitando así que los cambios afecten a otros ambientes.
- Los accesos y permisos deben estar bien configurados para cada ambiente, limitando el acceso según el rol.

V.II. Protección contra códigos maliciosos

- Se deberá adquirir un antivirus con licencia de paga como el McAfee y se deberá mantenerlo actualizado en todos los equipos de cada empleado perteneciente a la empresa.
- Actualizar los sistemas operativos de todos los equipos a la última versión para optimizar la seguridad de la información analizando que la actualización no genere cambios en los programas del equipo y no afecte a la información.
- Analizar con el antivirus todos los dispositivos de almacenamiento extraíbles que se conecten en los equipos informáticos.
- Capacitar a los empleados sobre los distintos tipos de ataques de Ingeniería social como por ejemplo formas para evitar el Phishing en correo electrónicos con archivos adjuntos y enlaces no confiables en internet.

V.III. Copias de respaldo

- Definir los medios de almacenamientos para realizar las copias de seguridad tales como Unidades de disco duro externo y en la nube.

- Utilizar el tipo de respaldo completo ya que es el más utilizado para realizar copias de seguridad de todos los archivos y carpetas.
- Se deberán realizar los respaldos necesarios cada semana.
- Cifrar las copias de seguridad utilizando el administrador de BitLocker de Windows.
- Guardar las copias de seguridad en lugares estratégicos y seguros bajo llave.
- Se verifica la integridad de las copias de respaldo para asegurarse de que no haya errores de corrupción o pérdida de datos durante el proceso de respaldo.
- Elaborar un informe en el que se establezca el proceso de copias de seguridad.

V.VI. Gestión de la vulnerabilidad técnica

- Realizar ataques de simulación de Hacking ético.
- Monitorear todos los puertos de los equipos informáticos para identificar puertos abiertos con la utilización de Nmap
- Elaborar un registro de los eventos ocurridos en los sistemas de información.

V.VII. Instalación de software en sistemas operativos

- Los empleados, independientemente de su área de trabajo, tienen prohibido instalar software externo. Deberán presentar una solicitud al departamento de TIC's detallando las razones por las cuales los programas anteriores deben ser instalados en sus estaciones de trabajo.
- Se implementará un procedimiento adecuado para aplicar reglas de instalación de software seguro en los equipos informáticos de EPC COMPU.
- Llevar un control adecuado de las instalaciones de software en los equipos por parte del Departamento de TIC's.
- Antes de realizar cualquier actualización de sistemas operativos verificar si la actualización es compatible con el resto del sistema y de los programas o dispositivos que se tenga en el equipo.
- Realizar copias de seguridad completas de los datos importantes ante de realizar cualquier actualización.

VI. SEGURIDAD DE LAS COMUNICACIONES

Como se pudo evidenciar no se aplica ningún control de seguridad de las comunicaciones por tal razón fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Asistente de Tecnología

VI.I. Controles de redes

- Estará terminantemente prohibido el acceso de terceros a la red de la empresa, considerando terceros a todas las entidades que mantengan relaciones laborales con la empresa, así como a las personas naturales que ingresen a la entidad.
- Para obtener el acceso a la red se deberá presentar una solicitud dirigida al jefe departamento de TIC's con los datos de la persona solicitante, luego este deberá ser aprobado.
- Sera necesario la adquisición y utilización de un dispositivo firewall el cual deberá estar debidamente configurado determinando los servicios de la red a los cuales pueden ser accedidos.
- Se debe monitorear los accesos de los usuarios a la red y a los sistemas de información mediante la implementación de sistemas de detección de intrusos tales como Snort o suricata.

VI.II. Separación en las redes

- Dividir la red en subredes en distintos dominios para una mayor seguridad.
- Verificar que el tráfico entre las diferentes redes esté adecuadamente segmentado y controlado.
- Utilizar técnicas como VLAN, ACL para asegurarte que el tráfico se dirija correctamente.

VI.III. Mensajería electrónica

- Encriptar la información confidencial a ser enviada por correo electrónico.
- Utilizar firmas digitales.
- Instalar filtros de spam y protección contra malware en los servidores de correo electrónico.
- Aplicar medidas de múltiple factor de autenticación.

VII. CRIPTOGRAFÍA

Como se pudo evidenciar no se aplica ningún control de criptografía por tal razón fue necesario crear una política y un control para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Asistente de Tecnología

VII.I Controles criptográficos

- Si la información confidencial se transfiere a medios legibles por computadora (DVD, CD, unidades USB), la información debe cifrarse siempre que el destinatario acepte el intercambio de datos cifrados. Para las computadoras portátiles, esta información se almacena mediante aplicaciones encriptadas

VIII. SEGURIDAD FÍSICA

Como se pudo notar se presentan falencia de seguridad física por tal motivo fue necesario crear una política y controles para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Jefe de Mantenimiento de Informática

VIII.I. Perímetro de seguridad física

- La empresa deberá estar equipada con herramientas auxiliares, como, extintores, alarmas, sensores y luces de emergencia, para proteger la seguridad física de los funcionarios y recursos en caso de un incidente físico o ambiental.
- Implementar señalización de advertencias en los distintos puntos del área de trabajo.
- Los muros, puertas y cerraduras deben estar en perfecto estado.
- Establecer un perímetro de seguridad para proteger las áreas con cables, equipos eléctricos, etc

VIII.II. Controles físicos de entrada

- Todos los empleados de EPC COMPU deberán contar con una credencial identificación para el ingreso a la empresa con el propósito de evitar acceso de personas no autorizadas.

- Contar con un registro para que los visitantes detallen la fecha y la hora de entrada y salida.

VIII.III. Mantenimiento de equipos

- Es importante contar con sistemas de refrigeración en las estaciones de trabajo.
- Para evitar interferencias, los cables de red deben estar separados físicamente de otro tipo de cables, especialmente de los cables de alimentación o alimentación.
- Para mantener la integridad de los equipos y la información, las estaciones de trabajo deberán tener fuentes de alimentación adecuadas alimentadas por una fuente de alimentación ininterrumpida o UPS.
- Implementar un plan trimestral de mantenimiento preventivo y correctivo de los equipos informáticos para prevenir daños y problemas futuros.
- El mantenimiento de los equipos estará a cargo del personal del departamento de TIC's, está prohibido la manipulación por parte de los empleados sin ninguna autorización.

VIII.IV. Política de escritorio limpio y pantalla limpia

- Las pantallas no deben mostrar ningún tipo de información cuando el equipo no esté en uso.
- Se deberá bloquear la sesión cuando el equipo este en estado de inactividad

IX. DESARROLLO Y MANTENIMIENTOS DE SISTEMAS

Como se pudo evidenciar no se aplica ningún control para el desarrollo y mantenimiento de los Sistemas por lo cual fue necesario crear una política y controles para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Asistente de Tecnologías

IX.I. Análisis y especificación de requisitos de seguridad de la información

- Al momento de integrar un software en los sistemas considerar su configuración al momento de implantar la seguridad.

- Aplicar criterios de aceptación en relación con la seguridad en actuaciones del software.

IX.II. Seguridad de servicios de las aplicaciones en redes publicas

- Implementar el cifrado en las comunicaciones.
- Utilizar sistemas de múltiple autenticación.
- Aplicar certificados digitales.

IX.III. Protección de transacciones de los servicios de las aplicaciones

- Usar firmas digitales para resguardar las comunicaciones de extremo a extremo.
- Validar y verificar la autenticación en el canal de transmisión.
- Se deberá utilizar protocolos de comunicación seguros.
- La información de las transacciones se guardará en lugares no accesibles desde la intranet.

IX.IV. Ambiente de desarrollo seguro

- Se debe tener total confianza en el desarrollador de software con un acuerdo de confidencialidad.
- Establecer metodologías de desarrollo optimas y elegir la que mejor se adapte a los requerimientos.
- Detallar todas etapas por las cuales va a pasar el desarrollo de software.
- Definir estándares de seguridad y calidad del software.

IX.V. Prueba de aceptación de sistemas

- Implementar entornos de prueba los cuales deben ser distintos a los entornos de operación para evitar fallos.
- Realizar pruebas de funcionalidad y de seguridad.

X. CUMPLIMIENTO

Como se pudo observar no se aplica ningún control para el llevar a cabo el cumplimiento de las políticas de seguridad por tal razón fue necesario crear una política y controles para llevar a cabo este procedimiento bajo los siguientes controles:

Responsable: Jefe de Mantenimiento de Informática

X.I. Cumplimiento con las políticas y normas de seguridad

- Revisar el cumplimiento de los requisitos de seguridad definidos en las políticas, normas y regulaciones legales.
- El Departamento de TIC's realizará el monitoreo y revisión periódica del cumplimiento de las políticas y controles establecidos anteriormente.
- El incumplimiento de las políticas y controles será motivo de sanciones de acuerdo con la ley establecida.

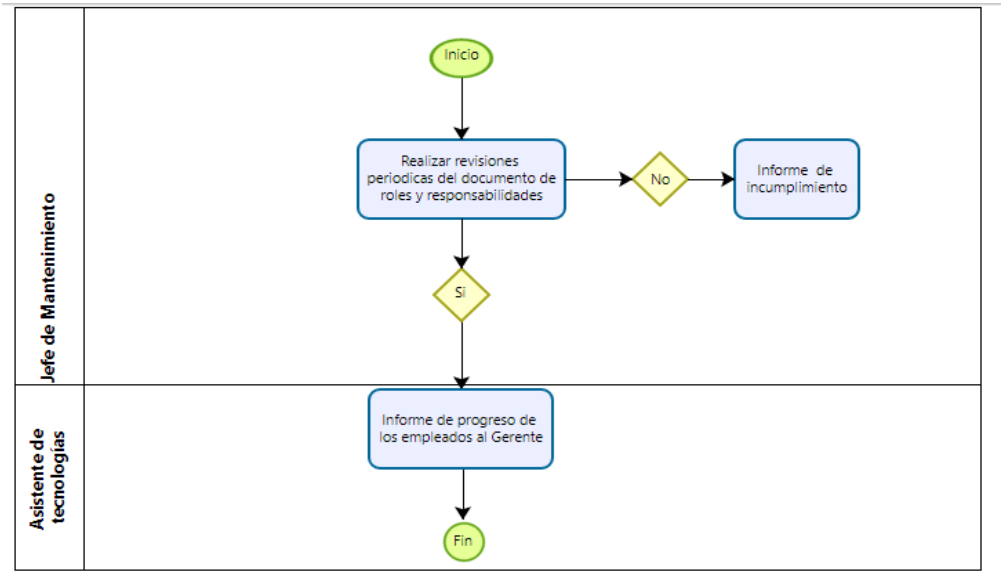
X.II. Revisión del cumplimiento técnico

- Identificar falencias en las actualizaciones de los sistemas.
- Se establecerá medidas correctivas antes de que dichas falencias puedan representar una amenaza para el sistema.

3.2.4.9 Procesos de seguimiento de las políticas establecidas

Para verificar el cumplimiento se establecieron los siguientes procesos:

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

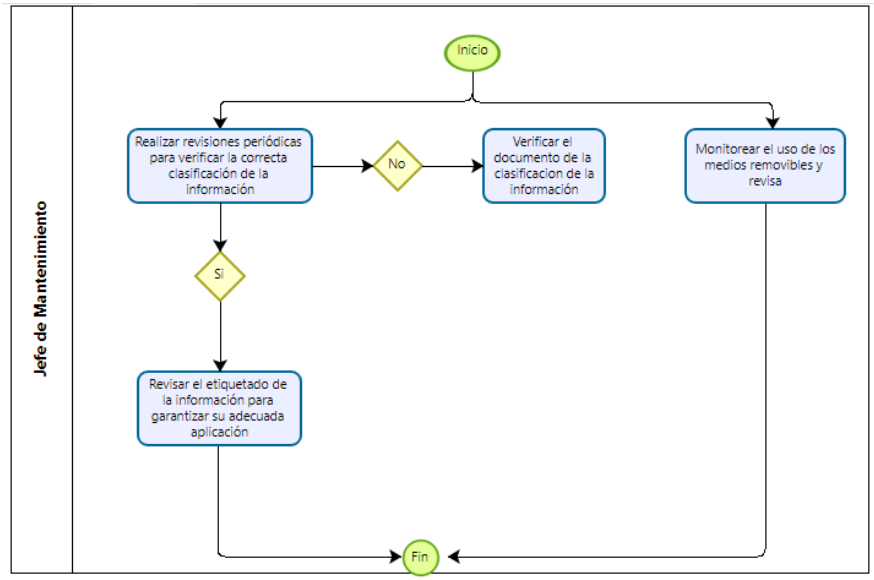


Tiempo: Este proceso se realiza cada 6 meses

Figura 26. Proceso de seguimiento - Organización de la Seguridad de la Información.

Elaborado por: Investigador

GESTIÓN DE ACTIVOS

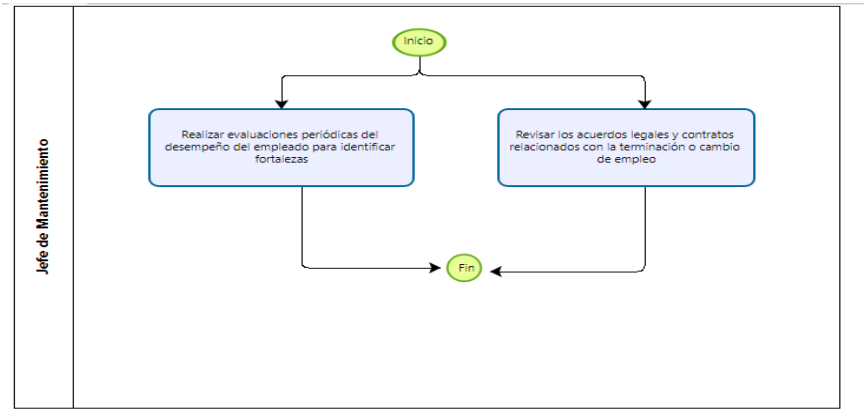


Tiempo: Este proceso se realiza todos los días

Figura 27. Proceso de seguimiento - gestión de activos.

Elaborado por: Investigador

SEGURIDAD DE LOS RECURSOS HUMANOS

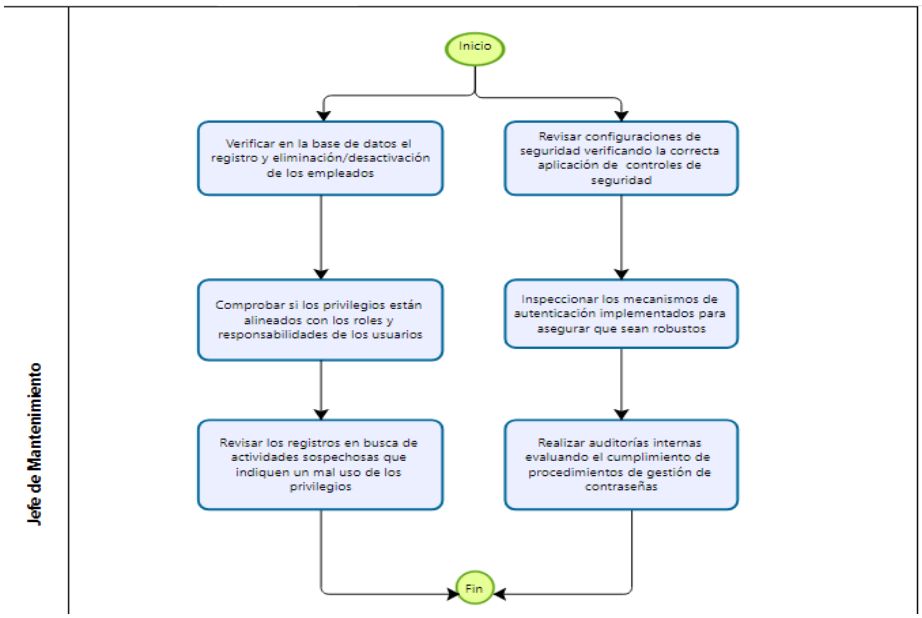


Tiempo: Este proceso se realiza cada semana

Figura 28.Proceso de seguimiento - Seguridad de los recursos humanos.

Elaborado por: Investigador

CONTROL DE ACCESO

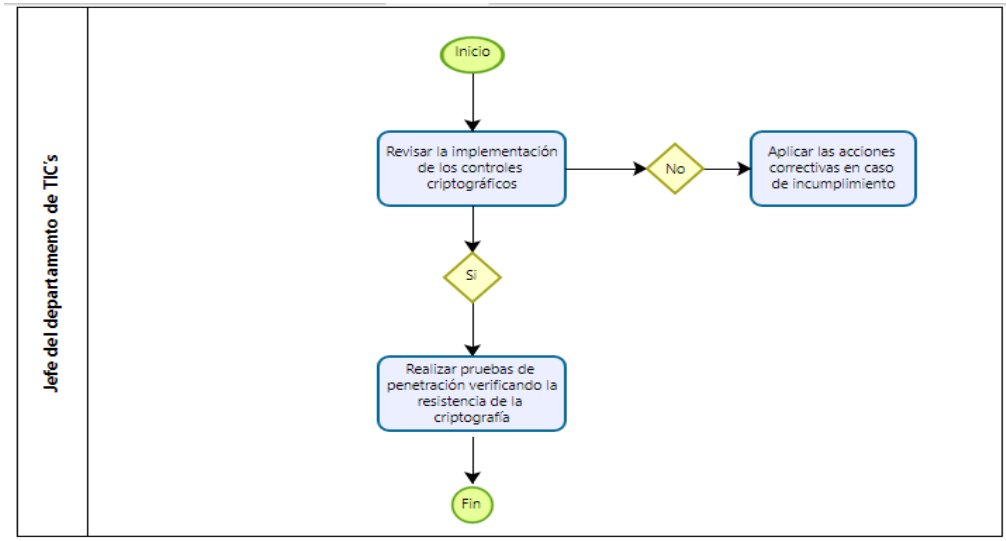


Tiempo: Este proceso se realiza todos los días

Figura 29.Proceso de seguimiento – Control de acceso.

Elaborado por: Investigador

CRIPTOGRAFÍA

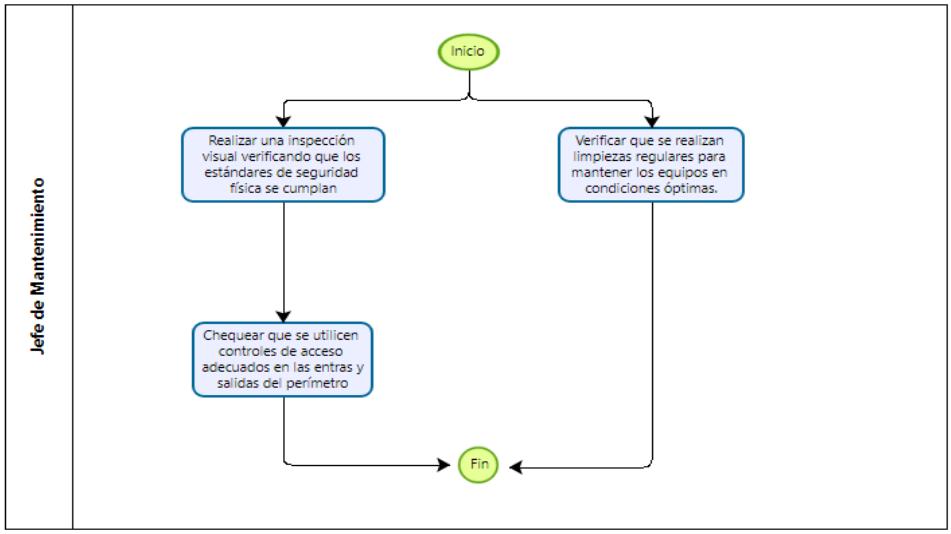


Tiempo: Este proceso se realiza cada mes

Figura 30.Proceso de seguimiento – Criptografía.

Elaborado por: Investigador

SEGURIDAD FÍSICA

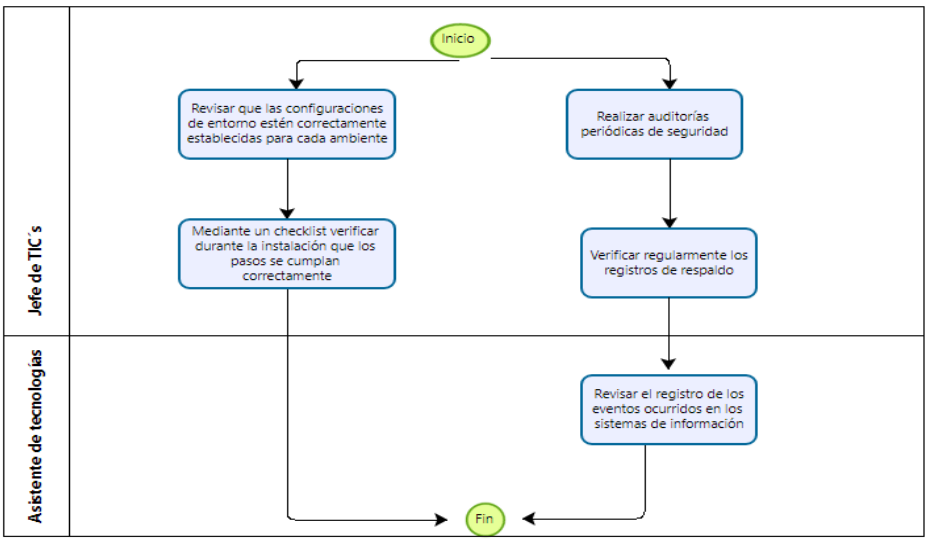


Tiempo: Este proceso se realiza cada 6 meses

Figura 31.Proceso de seguimiento - Seguridad Física.

Elaborado por: Investigador

SEGURIDAD DE LAS OPERACIONES

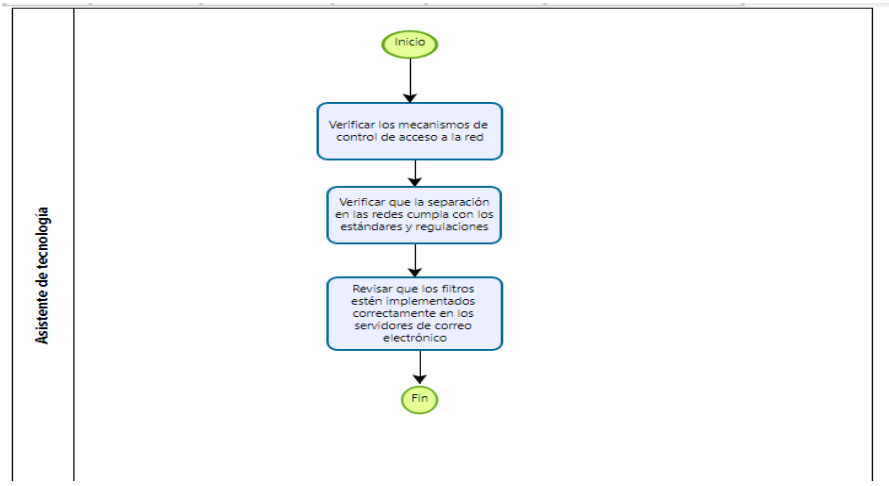


Tiempo: Este proceso se realiza cada semana

Figura 32.Proceso de seguimiento - Seguridad de las operaciones.

Elaborado por: Investigador

SEGURIDAD DE LAS COMUNICACIONES

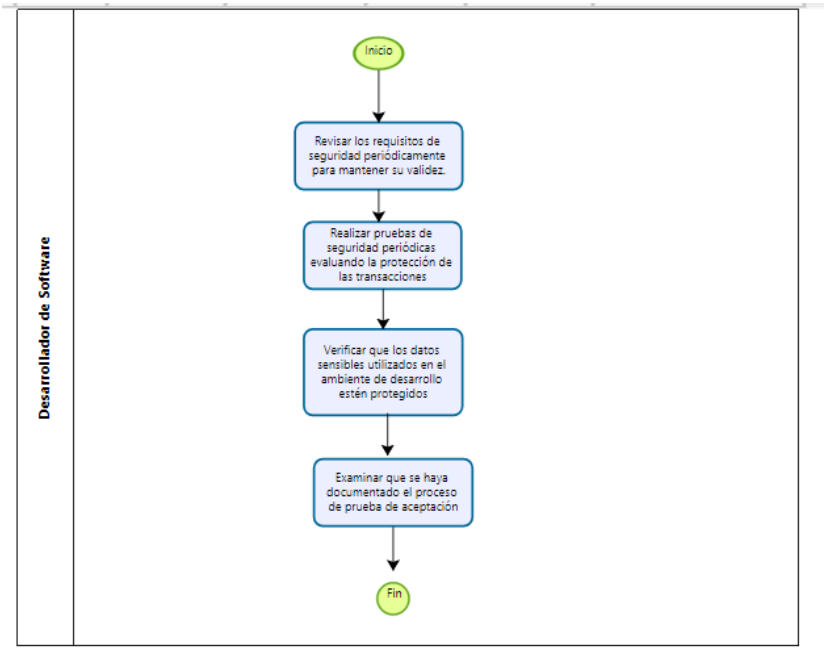


Tiempo: Este proceso se realiza todos los días

Figura 33.Proceso de seguimiento - Seguridad de las comunicaciones.

Elaborado por: Investigador

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

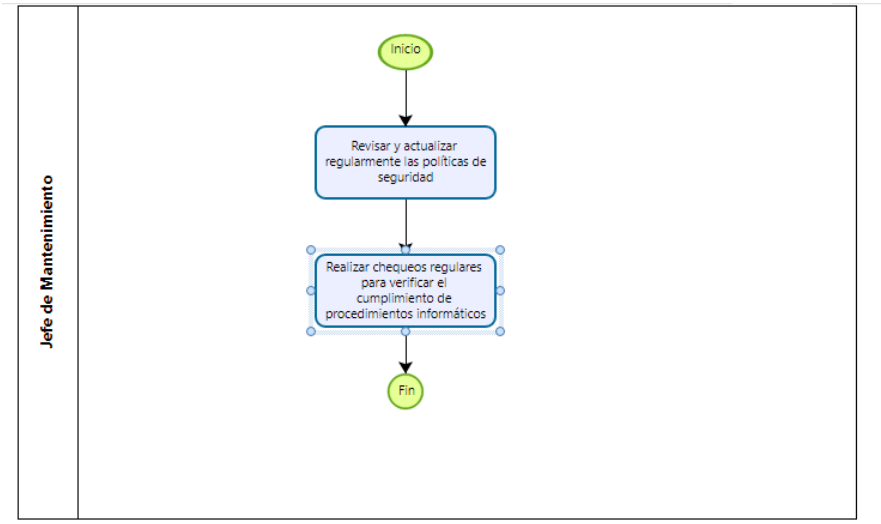


Tiempo: Este proceso se realiza cada mes

Figura 34.Proceso de seguimiento - Desarrollo y mantenimiento de sistemas.

Elaborado por: Investigador

CUMPLIMIENTO



Tiempo: Este proceso se realiza cada 6 meses

Figura 35.Proceso de seguimiento - Cumplimiento.

Elaborado por: Investigador

Se presenta la bitácora para registrar los eventos suscitados al momento de ejecutar la política y control de seguridad

BITÁCORA PARA LA GESTIÓN DE EVENTO EN EPC COMPU					
	Fecha de Inicio del Periodo				
	Duración del Periodo:				
Fecha/Hora	Responsable	Incidentes	Tiempo	Consecuencias	Solución

Firma Responsable Firma Asistente de Tecnologías

Firma Jefe del Dep. de Sistemas

Tabla 36: Bitácora

Elaborado por Investigador

3.2.5.0 Manual del Plan de Contingencia

Identificación de riesgos

A continuación, se detallan los riesgos más importantes identificados en los activos, ver Tabla 31: Identificación de Amenazas

N.º	**Riesgo**
R1	Hurto de información
R2	Sniffing
R3	Phishing
R4	Exceso de privilegios de ingresos
R5	Alteración o eliminación de cuentas
R6	Licencias Vencidas y desactualizadas
R7	Falla en el disco duro
R8	Daños en la fuente de poder
R9	Daños en los ventiladores
R10	Malware
R11	Sismos
R12	Incendio

R13	Robo
R14	Falla en la tarjeta de red
R15	Falla de cableado y conectores
R16	Falla en la BIOS
R17	Fallas de Hardware
R18	Errores de arranque
R19	Fallas en la memoria RAM
R20	Fallas del procesador
R21	Pésima Resolución de pantalla
R22	Sustracción de documentos
R23	Daño en los cartuchos y cabezales
R24	Agotamiento de tinta
R25	Atascamiento de papel
R26	Errores humanos
R27	Corte de servicio eléctrico
R28	Filtración de Agua
R29	Spoffing de ARP
R30	Intrusión de dispositivos ilegítimos en la red
R31	Puertos abiertos y mal configurados
R32	Acceso no autorizado
R33	Sobrecalentamiento
R34	Conexión intermitente
R35	Denegación de servicio distribuido
R36	Envenenamiento de DNS

Tabla 37: Identificación de Riesgos

Elaborado por: Investigador

Identificación de los Elementos Afectados de los riesgos priorizados

R1: Hurto de información

- Datos confidenciales
- Integridad de los datos
- Continuidad del negocio

- Propiedad Intelectual
- Privacidad y cumplimiento normativo
- Costos financieros

R2: Sniffing

- Datos confidenciales
- Privacidad de la Información
- Integridad de los datos
- Seguridad de la red
- Reputación y confianza
- Cumplimiento normativo

R3: Phishing

- Datos confidenciales
- Cuentas de usuarios
- Robo de identidades
- Reputación y confianza
- Seguridad de la red y sistemas
- Cumplimiento normativo

R4: Alteración de privilegios

- Usuarios
- Sistema Operativo
- Registros

R5: Alteración o eliminación de cuentas

- Acceso a servicios y datos
- Información personal y privacidad

- Actividades en línea y reputación
- Servicios y transacciones
- Perdida de datos y respaldo
- Reputación y confianza

R6: Malware

- Seguridad de la información
- Rendimiento de los equipos y sistemas
- Privacidad y robo de identidad
- Productividad y continuidad del negocio
- Reputación y confianza
- Costos financieros

R8: Daños en la fuente de poder

- CPU
- Monitor.
- Teclado
- Mouse-
- Componentes Internos

R9: Daños en los ventiladores

- Procesador
- Tarjeta Madre
- Memorias RAM
- Disco Duro

R30: Intrusión de dispositivos ilegítimos en la red

- Equipos Informáticos
- Información sensible

R33: Sobrecalentamiento

- Rendimiento del sistema
- Vida útil de los componentes
- Estabilidad del equipo
- Seguridad de los datos
- Consumo de energía

R35: Denegación de servicio distribuido

- Acceso al router
- Comunicación en red
- Trafico de la red

R36: Envenenamiento de DNS

- Acceso al router
- Comunicación en red
- Trafico de la red

R14: Falla en la tarjeta de red

- Comunicaciones en red
- Transferencia de información

R15: Falla de cableado y conectores

- Equipos informáticos
- Equipos de red

R16: Falla en la BIOS

- Equipo informático
- Configuración del hardware

R17: Fallas de Hardware

- Funcionalidad de los equipos informáticos
- Integridad de los datos
- Productividad y eficiencia
- Costos financieros
- Continuidad del negocio
- Seguridad de la información

R18: Errores de arranque

- Equipo informático
- Configuración del hardware
- Disponibilidad de la información

R7: Falla en el disco duro

- Disponibilidad de la información
- Funcionamiento del equipo

R19: Fallas en la memoria RAM

- Rendimiento del equipo informático
- Disponibilidad de la información
- Funcionamiento del equipo

R20: Fallas del procesador

- Rendimiento del equipo informático
- Disponibilidad de la información
- Funcionamiento del equipo

R31: Puertos abiertos y mal configurados

- Switches
- Acceso a la red
- Seguridad de la información

R16: Acceso no autorizado

- Activos Informáticos
- Activos de Información
- Personal de la empresa

R11: Sismos

- Infraestructura física
- Recursos humanos
- Tecnología y comunicaciones
- Datos y sistemas
- Cadena de suministros
- Reputación y relaciones con los clientes

R12: Incendio

- Equipos Informáticos
- Infraestructura física
- Personal

R13: Robo

- Equipos informáticos
- Integridad de la empresa
- Seguridad de la empresa

R26: Errores Humanos

- Sistemas Operativos
- Sistemas de información
- Equipos Informáticos

R28: filtración de Agua

- Equipos informáticos
- Disponibilidad de la información

R22: Sustracción de documentos

- Seguridad de la información
- Integridad de la empresa

R34: Conexión intermitente

- Conectividad a internet
- Comunicación de los equipos de trabajo
- Transferencia de datos
- Acceso a recursos de sistemas
- Seguridad de la red
- Experiencia del usuario

R11: Corte de servicio eléctrico

- Equipos informáticos
- Disponibilidad de la información

R29: Spoffing de ARP

- Switches
- Comunicación en red
- Acceso a la red
- Trafico de la red

R23: Daño en los cartuchos y cabezales

- Disponibilidad de la información

R24: Agotamiento de tinta

- Disponibilidad de la información

R25: Atascamiento de papel

- Disponibilidad de la información

R21: Pésima Resolución de pantalla

- Visualización de la información

Identificación de Consecuencias de los riesgos

R1: Hurto de información

- Perdida de información confidencial
- Suspensión de las operaciones laborales
- Suspensión de los principales servicios

R2: Sniffing

- Robo de información confidencial
- Violación de la privacidad
- Suspensión de los principales servicios

R3: Phishing

- Robo de información

- Cuentas de correo comprometidas
- Fraude y suplantación de identidad
- Propagación de malware

R4: Alteración de privilegios

- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R5: Alteración o eliminación de cuentas

- Perdida de información personal
- Robo de información confidencial.
- Interrupción de servicios y operaciones

R6: Malware

- Perdida de información
- Errores en los sistemas operativos
- Bajo rendimiento de los equipos informáticos

R8: Daños en la fuente de poder

- La computadora no enciende
- Reinicios o apagados inesperados
- Bajo rendimiento de los equipos informáticos.
- Cortocircuitos.
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R9: Daños en los ventiladores

- La computadora no enciende

- Reinicios o apagados inesperados
- Bajo rendimiento de los equipos informáticos.
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R9: Daños en los ventiladores

- La computadora no enciende
- Reinicios o apagados inesperados
- Bajo rendimiento de los equipos informáticos.
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R30: Intrusión de dispositivos ilegítimos en la red

- Sobrecarga de la red.
- Pérdidas económicas.
- Perdida de información.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R33: Sobrecalentamiento

- Daños a los componentes físicos
- Perdida de información
- Aumento del consumo de energía
- Reinicios inesperados
- Pérdidas económicas
- Bajo rendimiento del equipo informático

R35: Denegación de servicio distribuido

- Ruptura de la comunicación en red.
- Pérdidas económicas.
- Perdida de información.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R21: Envenenamiento de DNS

- Suplantación de identidad de los usuarios en red
- Intercepción de información
- Perdida de información
- Ruptura de la comunicación en red.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R14: Falla en la tarjeta de red

- Problemas al detectar comunicaciones
- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R15: Falla de cableado y conectores

- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R16: Falla en la BIOS

- La computadora no enciende.
- Pérdidas económicas.
- Interrupción de las operaciones laborales.

- Interrupción de los principales servicios.

R17: Fallas de Hardware

- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R18: Errores de arranque

- Perdida de información.
- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R7: Falla en el disco duro

- Perdida de información.
- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R19: Fallas en la memoria RAM

- Perdida de información.
- Pérdidas económicas.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R20: Fallas del procesador

- Perdida de información.
- Pérdidas económicas.
- Interrupción de las operaciones laborales.

- Interrupción de los principales servicios.

R31: Puertos abiertos y mal configurados

- Sobrecarga de la red.
- Perdida de información.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R16: Acceso no autorizado

- Perdida de información.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R11: Sismos

- Daños en la infraestructura física
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios
- Perdida de información
- Pérdidas económicas

R12: Incendio

- Pérdidas económicas
- Daños en los equipos informáticos
- Perdida de información
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R13: Robo

- Pérdidas económicas

- Perdida de información
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R26: Errores humanos

- Daños a los equipos informáticos
- Pérdidas económicas
- Perdida de información
- Interrupción de las operaciones laborales

R28: Filtración de Agua

- Daños a los equipos informáticos
- Pérdidas económicas
- Perdida de información
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R22: Sustracción de documentos

- Pérdidas económicas
- Perdida de información
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios

R34: Conexión intermitente

- Interrupción de los servicios
- Interrupción de las operaciones laborales
- Perdida de información
- Dificultades en la comunicación en red

R11: Corte de servicio eléctrico

- Daños en el cableado eléctrico
- Daños en la infraestructura de red
- Interrupción de las operaciones laborales
- Interrupción de los principales servicios
- Perdida de información

R23: Daño en los cartuchos y cabezales

- Pérdidas económicas
- Interrupción de las operaciones laborales

R24: Agotamiento de tinta

- Pérdidas económicas
- Interrupción de las operaciones laborales

R25: Atascamiento de papel

- Pérdidas económicas
- Interrupción de las operaciones laborales

R29: Spoffing de ARP

- Falsificación de la tabla ARP del swich.
- Ruptura de la comunicación en red.
- Pérdidas económicas.
- Perdida de información.
- Interrupción de las operaciones laborales.
- Interrupción de los principales servicios.

R21: Pésima Resolución de pantalla

- Problemas de visualización de la información

Gestión de riesgos por consecuencia

Consecuencia	Perdida de información confidencial
Prevención	• Realizar capacitaciones a los empleados sobre las buenas prácticas en seguridad de la información. • Realizar copias de seguridad continua de toda la información. • Disponer con un respaldo del sistema operativo, de los sistemas desarrollados, lenguajes de programación y base de datos. • Al momento de realizar las copias de seguridad utilizar herramientas de encriptación para que la información pueda ser recuperada por quien generó dicho respaldo.
Detección	• Monitorización de registros y actividad de red mediante la utilización de sistemas IDS. • Revisar regularmente los registros de acceso y actividad de los usuarios en los sistemas y aplicaciones de la empresa.
Corrección	• Determinar cómo se produjo la perdida de información. • Informar a las partes interesadas internas y externas, como empleados, clientes y socios comerciales, sobre la pérdida de información confidencial. • Si existe la posibilidad de recuperar la información perdida, trabajar con profesionales de TI o expertos en seguridad para intentar recuperar los datos. • Realizar una evaluación exhaustiva del alcance del incidente para determinar qué información se ha visto comprometida y qué riesgos potenciales existen.

	• Identificar las brechas de seguridad o las debilidades que permitieron la pérdida de información confidencial y tomar medidas correctivas para evitar futuros incidentes. • En casos de pérdida de información confidencial, es posible que sea necesario comunicarse con las autoridades competentes, como las agencias de protección de datos. • Evaluar y actualizar las políticas y procedimientos de seguridad de la empresa para asegurarse de que sean adecuados y estén actualizados. • Realizar una auditoría interna de seguridad para identificar posibles brechas adicionales y asegurarse de que se están siguiendo las mejores prácticas de seguridad. • Proporcionar capacitación y concienciación periódica sobre seguridad de la información a todo el personal de la empresa. • Evaluar la efectividad de las medidas implementadas

Tabla 38:Consecuencia - Perdida de información confidencial

Elaborado por: Investigador

Consecuencia	Suspensión de las operaciones laborales
Prevención	• Realizar una evaluación exhaustiva de los riesgos y vulnerabilidades que pueden afectar las operaciones de la empresa • Mantener adecuadamente la infraestructura y los equipos necesarios para las operaciones de la empresa. • Implementar sistemas de respaldo y recuperación de datos para asegurar que la información crítica esté protegida y disponible en caso de interrupción. • Monitorear de forma continua los riesgos y las condiciones que puedan afectar las operaciones de la empresa.

Detección	Rendimiento de la red.
Corrección	• Determinar la causa exacta de la suspensión de las operaciones laborales. • Desarrollar un plan de recuperación detallado que aborde los aspectos clave para restablecer las operaciones • Identificar y asignar los recursos necesarios para corregir la suspensión de las operaciones. • Si la suspensión está relacionada con problemas técnicos o de infraestructura, tomar medidas para reparar y restablecer la infraestructura afectada. • Mantener una comunicación clara y constante con los empleados, clientes, proveedores y otras partes interesadas para informarles sobre el proceso de recuperación y los plazos esperados. Evaluar la implementación de medidas de contingencia para minimizar el impacto de futuras interrupciones • Revisar y actualizar los planes de continuidad del negocio. • Proporcionar capacitación y preparación adecuada al personal para hacer frente a situaciones de suspensión y recuperación de operaciones. • Evaluar el impacto de la suspensión en el negocio y revisar la estrategia empresarial para adaptarse a los cambios resultantes.

Tabla 39: Consecuencia - Suspensión de las operaciones laborales

Elaborador por: Investigador

Consecuencia	Suspensión de los principales servicios
Prevención	• Realiza una evaluación exhaustiva de los riesgos que podrían afectar los servicios principales de la empresa. • Realiza mantenimiento preventivo regularmente en los equipos y sistemas que son vitales para los servicios principales de la empresa.

	• Mantener la infraestructura tecnológica actualizada y con capacidades adecuadas para soportar la demanda de los servicios principales. • Establecer sistemas de respaldo y recuperación de datos robustos para garantizar la disponibilidad de la información crítica en caso de interrupciones.
Detección	Falencias en los sistemas de información
Corrección	• Determina la causa exacta de la suspensión de los servicios informáticos. • Reunión con un equipo de expertos en tecnología y sistemas informáticos para abordar la suspensión de los servicios. • Identifica los servicios informáticos críticos que deben restablecerse de manera prioritaria. • Crear un plan detallado que describa las acciones específicas que se deben tomar para corregir la suspensión de los servicios. • Realiza las acciones necesarias para solucionar la causa raíz del problema. Esto puede implicar reemplazar hardware defectuoso, aplicar parches de software, restablecer configuraciones de red, recuperar datos, entre otras acciones técnicas específicas. • Informa a los empleados, clientes y otras partes interesadas sobre la situación y las medidas que se están tomando para corregir la suspensión de los servicios. • Durante el proceso de corrección, considerar la implementación de medidas de contingencia temporales para minimizar el impacto en las operaciones de la empresa. • Una vez que se haya corregido la suspensión de los servicios, realizar pruebas exhaustivas para verificar que los servicios se hayan restaurado correctamente.

	• Establecer un sistema de monitoreo continuo para supervisar la estabilidad y el rendimiento de los servicios restaurados.

Tabla 40: Consecuencia - Suspensión de los principales servicios

Elaborado por: Investigador

Consecuencia	Violación de la privacidad
Prevención	• Brindar capacitación regular a todos los empleados sobre la importancia de la privacidad de la información y las mejores prácticas para protegerla. • Implementar medidas de gestión de accesos adecuadas para garantizar que solo las personas autorizadas tengan acceso a la información confidencial. • Tener sistemas de seguridad sólidos, como firewalls, sistemas de detección de intrusiones, cifrado de datos y software antivirus/antimalware actualizados.
Detección	Alertas de seguridad en la red
Corrección	• Tan pronto como se descubra la violación de privacidad, identificar la causa y detén cualquier actividad no autorizada. • Evaluar la gravedad de la violación y determina si es necesario notificar a las partes afectadas, como clientes, empleados u otras entidades. • Informar a los miembros clave de la organización sobre la violación de privacidad. • Realizar una investigación interna para comprender completamente la causa y el alcance de la violación de privacidad. • Desarrollar e implementar medidas correctivas para fortalecer la seguridad y prevenir futuras violaciones de privacidad.

Tabla 41: Consecuencia - Violación de la privacidad

Elaborado por: Investigador

Consecuencia	Cuentas de correo comprometidas
Prevención	• Establece políticas de contraseñas fuertes para las cuentas de correo. • Implementar la autenticación de dos factores para las cuentas de correo. • Mantener actualizado el software de gestión de correo y los clientes de correo electrónico. • Capacitar a los usuarios sobre las mejores prácticas de seguridad y la importancia de proteger sus cuentas de correo. • Realiza copias de seguridad regulares de los correos electrónicos importantes y otros datos relacionados con las cuentas de correo.
Detección	Revisión y monitoreo de las cuentas de usuarios.
Corrección	• Cambiar la contraseña de la cuenta comprometida. • Al cambiar la contraseña, revoca cualquier sesión activa que pueda estar abierta en otros dispositivos. • Revisar y actualizar la información de seguridad asociada a la cuenta comprometida. • Realizar un escaneo completo de malware y antivirus en los dispositivos que hayan tenido acceso a la cuenta comprometida. • Verificar si se han configurado reenvíos no autorizados o cambios en los filtros de correo electrónico en la cuenta comprometida. • Revisar la actividad reciente de la cuenta comprometida para identificar cualquier actividad inusual o no autorizada. • Si la cuenta comprometida ha enviado correos electrónicos o mensajes sospechosos a tus contactos,

	informar a esas personas sobre la situación para que estén alerta y eviten interactuar con mensajes fraudulentos. • Si se utiliza la misma dirección de correo electrónico comprometida en otros servicios en línea, cambia las contraseñas y revisa la seguridad de esos servicios para prevenir cualquier compromiso adicional. • Mantener un monitoreo continuo de la cuenta comprometida y sus actividades.

Tabla 42: Consecuencia - Cuentas de correo comprometidas

Elaborado por: Investigador

Consecuencia	Propagación de malware
Prevención	• Instalar y mantener actualizado un antivirus con licenciamiento en todos los equipos informáticos. • Mantener actualizados los sistemas operativos y aplicaciones instaladas en los equipos con los últimos parches de seguridad. • Descargar archivos y software de fuentes seguras y confiables. • Evitar abrir y descargar archivos con correo electrónicos de remitentes desconocidos.
Detección	Revisión de las Alertas de malware
Corrección	• Identificar los sistemas comprometidos y aíslalos de la red para evitar que el malware se propague aún más y desconectarlos de Internet y de otros dispositivos en la red. • Utilizar software antivirus y antimalware actualizados para realizar un análisis completo de todos los sistemas afectados. • Utilizar las herramientas de seguridad adecuadas para eliminar el malware de los sistemas afectados y restaurar

	los sistemas a un estado seguro utilizando copias de seguridad limpias y confiables. • Aplicar las actualizaciones de seguridad y los parches correspondientes en todos los sistemas de la empresa para cerrar las vulnerabilidades que pudieron haber sido explotadas por el malware. • Recomendar a todos los empleados que cambien sus contraseñas y credenciales de acceso, especialmente si existe la posibilidad de que hayan sido comprometidas. • Considerar la implementación de soluciones de seguridad adicionales, como firewalls mejorados.

Tabla 43: Consecuencia - Propagación de malware

Elaborado por: Investigador

Consecuencia	Daños en la infraestructura física
Prevención	• Realizar convenios con proveedores. • Contratación de seguros.
Detección	Deterioro de la infraestructura de la empresa
Corrección	• Realizar una evaluación completa de los daños en la infraestructura física. Identifica los componentes afectados, como cables, equipos, estructuras, sistemas de energía, sistemas de refrigeración, entre otros. • Determinar la prioridad de los elementos dañados en función de su importancia para las operaciones comerciales. • Si es necesario, tomar medidas para garantizar la seguridad, como desconectar la energía o cerrar áreas afectadas. • Comunicarse con los proveedores de servicios necesarios, como electricistas, plomeros o especialistas en infraestructura, para que te brinden asistencia en la reparación y solución de los daños.

	• Realizar las reparaciones necesarias o reemplaza los equipos dañados. • Si los daños afectaron la infraestructura de red y comunicaciones, trabajar en la restauración de estos sistemas. • Si hubo interrupciones en el suministro de energía u otros servicios, coordinar con los proveedores de servicios públicos para restablecerlos lo antes posible. • Una vez completadas las reparaciones, realizar pruebas y verificaciones exhaustivas para asegurarte de que los sistemas y equipos afectados funcionen correctamente.

Tabla 44: Consecuencia - Daños en la infraestructura física

Elaborado por: Investigador

Consecuencia	Dificultades en la comunicación en red
Prevención	• Disponer de proveedores de servicio de internet que cumplan con los estándares mínimos de seguridad y calidad. • Contar con un diagrama de toda la infraestructura de red
Detección	• Consumo de ancho de banda. • Falta de acceso a internet.
Corrección	• Asegurarse de que todos los cables de red estén correctamente conectados y en buen estado. • Apagar y volver a encender los dispositivos de red, como routers, switches y puntos de acceso. • Revisar la configuración de red en los dispositivos y asegúrate de que estén correctamente configurados y verificar las direcciones IP, la configuración de DNS, la configuración de puertos y cualquier otra configuración relevante. • Utilizar herramientas de diagnóstico de red para identificar problemas de conectividad.

	• Asegurarse de que las reglas de firewall no estén bloqueando la comunicación en red. • Verificar si hay actualizaciones de firmware y controladores disponibles para tus dispositivos de red. • Si hay un uso intensivo de la red o una congestión de tráfico, considera implementar medidas para optimizar el uso del ancho de banda, como la priorización de tráfico o la limitación del ancho de banda para aplicaciones no críticas. • Utilizar herramientas de prueba de rendimiento de red para evaluar la velocidad y latencia de la red.

Tabla 45: Consecuencia -Dificultades en la comunicación en red

Elaborado por: Investigador

Consecuencia	Falsificación de la tabla ARP del switch.
Prevención	• Utilización de un firewall para interceptar el tráfico. • Segmentar la red. • Implementación de listas de control de acceso. • Utilización del protocolo IPSec.
Detección	• Anomalías del tráfico ARP. • Duplicación de direcciones IP.
Corrección	• Aislar el dispositivo comprometido. • Actualizar contraseñas y credenciales. • Restablecer la tabla ARP. • Verificar la configuración del swich. • Actualizar el firmware del swich. • Monitoreo continuo del dispositivo.

Tabla 46:Consecuencia- Falsificación de la tabla ARP del switch.

Elaborado por: Investigador

Priorización de Riesgos

Probabilidad \ Impacto		1	2	3	4	5
		Insignificante	Menor	Crítico	Mayor	Catastrófico
Constante	5			R1, R2	R3, R4	R5, R6
Moderado	4			R34	R8, R9, R30,	R33, R35, R36
Ocasional	3			R27, R29	R14, R15, R16, R17, R18, R36, R37	R7, R19, R20, R31, R32
Posible	2		R21		R23, R24, R25	R10, R11, R12, R13, R26, R28, R22
Improbable	1					

Tabla 47: Matriz de Priorización de riesgos

Elaborado por: Investigador

Lista de Prioridades.

<u>Prioridad 1:</u>

- R1: Hurto de información
- R2: Sniffing
- R3: Phishing
- R4: Alteración de privilegios
- R5: Alteración o eliminación de cuentas
- R6: Malware
- R8: Daños en la fuente de poder
- R9: Daños en los ventiladores
- R30: Intrusión de dispositivos ilegítimos en la red
- R33: Sobrecalentamiento.
- R35: Denegación de servicio distribuido.
- R36: Envenenamiento de DNS
- R14: Falla en la tarjeta de red

- R15: Falla de cableado y conectores
- R16: Falla en la BIOS
- R17: Fallas de Hardware
- R18: Errores de arranque
- R7: Falla en el disco duro
- R19: Fallas en la memoria RAM
- R20: Fallas del procesador
- R31: Puertos abiertos y mal configurados
- R32: Acceso no autorizado
- R11: Sismos
- R12: Incendio
- R13: Robo
- R26: Errores humanos
- R28: Filtración de Agua.
- R22: Sustracción de documentos

Prioridad 2:

- R34: Conexión intermitente
- R27: Corte de servicio eléctrico
- R29: Spoffing de ARP
- R23: Daño en los cartuchos y cabezales
- R24: Agotamiento de tinta
- R25: Atascamiento de papel

Prioridad 3:

- R21: Pésima Resolución de pantalla

En vista a lo analizado anteriormente se va a plantear políticas que son los elementos de prevención que se puede ver en el **ANEXO 2,** los elementos de detección que se puede ver en el **ANEXO 3** y los elementos de corrección que es el Plan de Contingencia como se observa en el **ANEXO 4.**

Plan de Contingencia

Se generó el presente Plan de Contingencia para identificar los riesgos a los sistemas y recursos informáticos que posee la organización para mantener la continuidad del negocio en el caso de surgir alguna falla, interrupción o desastre natural en el área informática

Riesgo	Hurto de información
Evento	Perdida de información confidencial por ataques informáticos
Responsable	Asistente de Tecnologías
Actividades 1) Informar la pérdida de información confidencial a las partes interesadas internas y externas, como empleados, clientes y socios comerciales. 2) Contratar y trabajar con profesionales de TI o expertos en seguridad para intentar recuperar los datos. 3) Determinar qué información está en riesgo y cuáles son los riesgos potenciales. 4) Identificar las brechas de seguridad o las debilidades. **5)** Brindar capacitación y concientización periódicas sobre seguridad de la información para todos los empleados de la empresa. 6) Implementar y revisar las políticas la seguridad de la información	

Tabla 48: Riesgo - Hurto de información

Elaborado por: Investigador

Riesgo	Sniffing
Evento	Suspensión de las operaciones laborales por intrusiones en la red
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Detectar todos los dispositivos conectados a la red **2)** Aislar el dispositivo infectado. **3)** Cambiar contraseñas y credenciales del router 4) Actualizar el sistema operativo y aplicaciones. 5) Monitoreo de la red.	

6) Implementar y revisar los controles de red

Tabla 49: Riesgo – Sniffing

Elaborado por: Investigador

Riesgo	Phishing
Evento	Robo de credenciales de cuentas de correo electrónico por técnicas de ingeniería social
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Revisar los registros e incidentes de correo electrónico. 2) Bloquear el enlace o correo malicioso. 3) Cambiar contraseñas comprometidas 4) Capacitación a los empleados sobre las técnicas de phishing. 5) Monitoreo de la red con sistemas IDS y firewall. 6) Implementar y revisar el control de mensajería electrónica.	

Tabla 50: Riesgo – Phishing

Elaborado por: Investigador

Riesgo	Alteración de privilegios
Evento	Acceso no autorizado a los sistemas de información por falta de monitoreo.
Responsable	Asistente de Tecnologías
Actividades: 1) Identificar el sistema alterado 2) Aislar el sistema de la red 3) Cambiar contraseñas de las cuentas 4) Restablecer los privilegios. 5) Actualizar el sistema operativo y aplicaciones. 6) Realizar evaluaciones de seguridad de los sistemas. 7) Implementar y revisar el control de Gestión de derechos de acceso privilegiado.	

Tabla 51:Riesgo - Alteración de privilegios

Elaborado por: Investigador

Riesgo	Alteración o eliminación de cuentas
Evento	Acceso no autorizado a las cuentas de correo electrónico y del sistema de información.
Responsable	Asistente de Tecnologías

Actividades:

1) Identificar la cuenta de usuario alterada
2) Aislar la cuenta afectada.
3) Cambiar las cuentas y credenciales
4) Restaurar las configuraciones de las cuentas.
5) Eliminar cualquier acceso no autorizado de la cuenta
6) Identificar la brecha de seguridad.
7) Monitorear la seguridad de las cuentas de usuarios
8) Implementar y revisar el control de registro y cancelación del registro de usuarios

Tabla 52: Riesgo - Alteración o eliminación de cuentas

Elaborado por: Investigador

Riesgo	Licencias Vencidas y desactualizadas
Evento	Licencia de algunas aplicaciones sin actualizar.
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Identificar que aplicaciones requieren actualización con licencia
2) Revisar los términos de licencias.
3) Contactar con los proveedores de licencias.
4) Implementar la actualización de las licencias.
5) Establecer proceso de seguimiento periódico de las licencias.
6) Implementar y revisar el control de mantenimiento de equipos.

Tabla 53: Riesgo - Licencias Vencidas y desactualizadas

Elaborado por: Investigador

Riesgo	Falla en el disco duro
Evento	Pantallazo azul y sonidos extraños
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Detener el uso del disco duro. 2) Realizar una copia de seguridad de la información en otro equipo. 3) Determinar la gravedad del daño en disco duro. 4) Considerar opciones de reparación o reemplazo. 5) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 54: Riesgo - Falla en el disco duro

Elaborado por: Investigador

Riesgo	Daños en los ventiladores
Evento	Ruido excesivo y vibraciones anormales.
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Detener el uso del equipo. 2) Reemplazar los ventiladores dañados. 3) Verificar la temperatura del procesador. 4) Realizar pruebas de rendimiento 5) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 55: Riesgo - Daños en los ventiladores

Elaborado por: Investigador

Riesgo	Malware
Evento	Infección de malware den los equipos por ataques de pishing
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Desconectar el equipo infectado de la red 2) Realizar un escaneo completo con un antimalware de confianza 3) Actualizar el sistema operativo y de todas las aplicaciones instaladas en el equipo.	

4) Reiniciar del equipo en modo seguro.
5) Escaneo adicional con unas herramientas de antimalware.
6) Eliminar archivos y programas sospechosos.
7) Restauración del sistema operativo y de los archivos.
8) Actualizar las contraseñas en el equipo como el correo electrónico y de acceso a los sistemas de información
9) Implementar y revisar controles contra código maliciosos

Tabla 56:Riesgo – Malware

Elaborado por: Investigador

Riesgo	Sismos
Evento	Sismo por causa natural
Responsable	Gerente

Actividades:

1) Mantener la calma.
2) Evaluar la seguridad del personal.
3) Alejarse de ventanas, vidrios, y estructuras que puedan colapsar.
4) Evaluación de los daños
5) Contactar con alguna empresa aseguradora
6) Actualizar el plan de evacuación del edificio.
7) Inspección de daños estructurales.
8) Determinar alguna forma de reanudar las operaciones
9) Implementar y revisar el control de Protección contra amenazas externas y ambientales

Tabla 57: Riesgo – Sismos

Elaborado por: Investigador

Riesgo	Incendio
Evento	Incendio por malas instalaciones eléctricas
Responsable	Gerente

Actividades:

1) Evaluar la seguridad del personal

2) Comunicar y notificar a todo el personal sobre el incendio. 3) Realizar una evaluación exhaustiva de los daños. 4) Contactar con alguna empresa aseguradora 5) Reemplazo de equipos y sistemas dañados. 6) Determinar si es posible reanudar las operaciones 7) Investigar la causa del incendio. 8) Revisar el plan de emergencia. 9) Implementar y revisar el control de Protección contra amenazas externas y ambientales,

Tabla 58: Riesgo – Incendio

Elaborado por: Investigador

Riesgo	Robo
Evento	Robo de un equipo informático debido a la falta de sistemas de seguridad
Responsable	Gerente
Actividades: 1) Informar a las autoridades sobre el robo. 2) Verificar las instalaciones de la empresa. 3) Notificar a los proveedores de servicios. 4) Cambiar las contraseñas de los sistemas de información. 5) Notificar a los clientes y socios 6) Recuperar la información de las copias de seguridad 7) Implementar y revisar el control de Ubicación y protección de los equipos	

Tabla 59: Riesgo – Robo

Elaborado por: Investigador

Riesgo	Falla en la tarjeta de red
Evento	Sin acceso a internet
Responsable	Jefe de Mantenimiento de Informática
Actividades:	

1) Asegurar que los cables estén correctamente conectados a la tarjeta de red o al router o switch.
2) Reiniciar el equipo o el router.
3) Actualizar los controladores de la tarjeta de red.
4) Verificar la configuración de la red en la computadora.
5) Realizar pruebas de conectividad.
6) Si el problema persiste reemplazar la tarjeta de red y realizar pruebas de conectividad.
7) Implementar y revisar el control de Mantenimiento de equipos.

Tabla 60: Riesgo - Falla en la tarjeta de red

Elaborado por: Investigador

Riesgo	Falla de cableado y conectores
Evento	El equipo no enciende
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Revisar el cableado de red.
2) Revisar el cableado del regulador de voltaje.
3) Identificar posibles daños en los componentes del hardware.
4) Implementar y revisar el control de Seguridad del cableado

Tabla 61: Riesgo - Falla de cableado y conectores

Elaborado por: Investigador

Riesgo	Falla en la BIOS
Evento	El sistema operativo no puede inicializarse
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Acceder a la configuración de la BIOS con una tecla en específico F2, Sup, etc.
2) Restaurar los ajustes predeterminados.
3) Actualizar la versión de la BIOS.
4) Restablecer la configuración del CMOS.

5) Verificar la integridad del hardware. 6) Implementar y revisar el control de Mantenimiento de equipos.

Tabla 62: Riesgo - Falla en la BIOS

Elaborado por: Investigador

Riesgo	Fallas de Hardware
Evento	Daños de los componentes de hardware por falta de mantenimiento
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Aislar el componente dañado. 2) Evaluar el alcance del daño. 3) Notificar el daño 4) Reemplazar el componente dañado. 5) Monitorear y realizar mantenimientos preventivos y correctivos a los equipos informáticos.	

Tabla 63: Riesgo - Fallas de Hardware

Elaborado por: Investigador

Riesgo	Errores de arranque
Evento	Problemas al iniciar el sistema operativo.
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Reiniciar al equipo 2) Verificar los cables y conexiones 3) Arrancar el equipo en modo seguro. 4) Utilizar las opciones de reparación del sistema. 5) Verificar la configuración de la BIOS. 6) Restaurar el sistema. 7) Reinstalar el sistema operativo. 8) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 64: Riesgo - Errores de arranque

Elaborado por: Investigador

Riesgo	Fallas en la memoria RAM
Evento	Bajo rendimiento del equipo.
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Verificar la compatibilidad de las memorias RAM 2) Limpiar los módulos de memoria RAM 3) Limpiar las memorias RAM. 4) Ejecutar un diagnóstico de memoria RAM. 5) Actualizar el firmware de la tarjeta madre. 6) Si no son compatibles o sufrieron un daño irreversible remplazar las memorias RAM. 7) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 65: Riesgo - Fallas en la memoria RAM

Elaborado por: Investigador

Riesgo	Fallas del procesador
Evento	El equipo no inicia.
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Verificar la temperatura del procesador. 2) Verificar que el procesador este correctamente colocado en el zócalo. 3) Verificar la compatibilidad del procesador. 4) Actualizar el firmware del procesador. 5) Realizar pruebas de estabilidad. 6) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 66: Riesgo - Fallas del procesador

Elaborado por: Investigador

Riesgo	Pésima Resolución de pantalla

Evento	Problemas de visualización de la información en pantalla
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Iniciar y configurar correctamente la resolución de pantalla. 2) Actualizar los controladores de video. 3) Implementar y revisar el control de Mantenimiento de equipos.	

Tabla 67: Riesgo - Pésima Resolución de pantalla

Elaborado por: Investigador

Riesgo	Sustracción de documentos
Evento	Perdida de documentación física
Responsable	Asistente de Tecnologías
Actividades: 1) Evaluar el alcance de la perdida. 2) Informar a los responsables. 3) Recuperar copias de seguridad. 4) Recopilar información de respaldo. 5) Revisar contratos y acuerdos. 6) Implementar medidas preventivas. 7) Implementar y revisar el control de Seguridad de Oficinas, recintos e instalaciones.	

Tabla 68: Riesgo - Sustracción de documentos

Elaborado por: Investigador

Riesgo	Daño en los cartuchos y cabezales
Evento	Impresora con problemas mecánicos
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Verificar los mensajes de error. 2) Retirar y limpiar los cartuchos. 3) Limpiar los cabezales de impresión.	

4) Realizar una alienación de los cabezales. 5) Actualizar los controladores de la impresora. 6) Realizar pruebas de impresión. 7) Implementar y revisar el control de Mantenimiento de equipos.

Tabla 69: Riesgo - Daño en los cartuchos y cabezales

Elaborado por: Investigador

Riesgo	Agotamiento de tinta
Evento	Impresora con baja calidad de impresión
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Realizar cambios de cartuchos de impresión, 2) Recargar la tinta en caso de tener una impresora de tinta continua. 3) Revisión y limpieza interna de la impresora. 4) Implementar y revisar el control de Mantenimiento de equipos	

Tabla 70: Riesgo - Agotamiento de tinta

Elaborado por: Investigador

Riesgo	Atascamiento de papel
Evento	Problemas mecánicos
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Apagar la impresora 2) Abrir las cubiertas 3) Retirar el papel atascado. 4) Verificar los rodillos. 5) Revisar los trayectos del papel. 6) Asegurarse de que el papel este correctamente colocado. 7) Reiniciar la impresora. 8) Implementar y revisar el control de Mantenimiento de equipos.	

Tabla 71: Riesgo - Atascamiento de papel

Elaborado por: Investigador

Riesgo	Errores humanos
Evento	Negligencia en la utilización de los equipos y sistemas de información
Responsable	Jefe del Departamento de TIC's

Actividades:

1) Realizar sesiones de capacitaciones periódicas en la utilización correcta de un equipo informático también protección de contraseñas.
2) Limitar privilegios de acceso a los empleados a los sistemas de información.
3) Monitoreo del registro de actividades en los equipos informáticos.
4) Realizar un reporte de incidentes
5) Implementar y revisar el control de Toma de conciencia, educación y formación en la seguridad de la información.

Tabla 72: Riesgo - Errores humanos

Elaborado por: Investigador

Riesgo	Corte de servicio eléctrico
Evento	Fallas en el consumo de energía por malas instalaciones eléctricas
Responsable	Jefe del Departamento de TIC's

Actividades:

1) Verificar el entorno del personal.
2) Verificar el estado de los equipos informáticos.
3) Restaurar los sistemas críticos.
4) Realizar copias de seguridad de la información.
5) Evaluar si hay equipos o sistemas afectados.
6) Tratar de reanudar las operaciones
7) Implementar y revisar el control de Servicios de suministro.

Tabla 73: Riesgo - Corte de servicio eléctrico

Elaborado por: Investigador

Riesgo	Filtración de Agua
Evento	Deterioros de las paredes y techo por humedad
Responsable	Jefe del Departamento de TIC's

Actividades:

1) Identificar la fuente de filtración de agua.
2) Evaluar el alcance del daño por la filtración de agua.
3) Verificar la seguridad de los dispositivos eléctricos.
4) Limpiar y secar las áreas afectadas.
5) Reparar o reemplazar los equipos dañados.
6) Revisar los sistemas de tubería.
7) Si es posible tratar de reanudar las operaciones.
8) Implementar y revisar el control de Perímetro de seguridad física.

Tabla 74: Riesgo- Filtración de Agua

Elaborado por: Investigador

Riesgo	Spoffing de ARP
Evento	Intrusión de dispositivos en la red
Responsable	Asistente de Tecnologías

Actividades:

1) Identificar los dispositivos desconocidos en la red.
2) Aislarlos de la red.
3) Crear una lista de negra de esos dispositivos.
4) Monitorear el tráfico del switch
5) Implementar y revisar los controles de redes

Tabla 75: Riesgo - Spoffing de ARP

Elaborado por: Investigador

Riesgo	Intrusión de dispositivos ilegítimos en la red
Evento	Robo de información
Responsable	Asistente de Tecnologías

Actividades:

1) Identificar el dispositivo conectado a la red

2) Bloquear su dirección ip
3) Cambiar las contraseñas del router
4) Configurar filtros de acceso.
5) Revisar la comunicación encriptada WPA2, WPA3.
6) Monitorear el tráfico de la red.
7) Implementar y revisar el control de Gestión de derechos de acceso privilegiado.

Tabla 76: Riesgo - Intrusión de dispositivos ilegítimos en la red

Elaborado por: Investigador

Riesgo	Puertos abiertos y mal configurados
Evento	Acceso no autorizado a la red
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Verificar la legitimidad de los puertos en el switch.
2) Desactivar o cerrar los puertos que no sean necesarios.
3) Actualizar el firmware del switch.
4) Establecer listas de control de acceso.
5) Fortalecer las contraseñas del switch.
6) Implementar y revisar los controles de redes

Tabla 77: Riesgo - Puertos abiertos y mal configurados

Elaborado por: Investigador

Riesgo	Acceso no autorizado
Evento	Robo de equipos por falta de sistemas de seguridad
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Informar del incidente
2) Realizar una evaluación de daños
3) Cambiar cerraduras y puertas de acceso.
4) Implementar y revisar los controles físicos de entrada.

Tabla 78:Riesgo - Acceso no autorizado

Elaborado por: Investigador

Riesgo	Sobrecalentamiento
Evento	Bajo rendimiento del equipo informático
Responsable	Jefe de Mantenimiento de Informática
Actividades: 1) Apagar inmediatamente el equipo. 2) Permitir que el equipo se enfrié. 3) Verificar la ventilación del equipo esté libre de obstrucciones 4) Verificar que el equipo este en un lugar ventilado. 5) Limpiar los componentes internos. 6) Utilizar herramientas de monitoreo de temperatura. 7) Instalar ventiladores adicionales. 8) Realizar pruebas de rendimiento. 9) Implementar y revisar el control de Mantenimiento de equipos.	

Tabla 79: Riesgo – Sobrecalentamiento

Elaborado por: Investigador

Riesgo	Conexión intermitente
Evento	Congestión de la red por interferencias
Responsable	Asistente de Tecnologías
Actividades: 1) Asegurarse que los cables estén correctamente conectados. 2) Reiniciar el router. 3) Verificar que el router no tenga interferencias alrededor como dispositivos inalámbricos o electrónicos. 4) Verificar la configuración de red. 5) Realizar pruebas de velocidad. 6) Implementar y revisar los controles de redes.	

Tabla 80: Riesgo - Conexión intermitente

Elaborado por: Investigador

Riesgo	Denegación de servicio distribuido
Evento	Bajo rendimiento de la red por interrupciones frecuentes
Responsable	Asistente de Tecnologías

Actividades:

1) Identificar el rendimiento de la red.
2) Notificar el ataque al proveedor de internet
3) Bloquear las direcciones ip atacantes.
4) Actualizar el firmware del router.
5) Configurar las reglas de filtrado del router.
6) Monitorear el tráfico de red.
7) Cambiar la contraseña del router.
8) Utilizar el cifrado WPA2 o WPA3 en redes inalámbricas.
9) Implementar y revisar los controles de redes.

Tabla 81: Riesgo - Denegación de servicio distribuido

Elaborado por: Investigador

Riesgo	Envenenamiento de DNS
Evento	Redirección de los usuarios a sitios web equivocados
Responsable	Asistente de Tecnologías

Actividades:

1) Determinar el alcance del envenenamiento DNS
2) Verificar la configuración DNS en los dispositivos.
3) Limpiar la cache DNS en los dispositivos.
4) Actualizar el firmware del router.
5) Utilizar DNSSEC para proteger la falsificación de respuestas DNS.
6) Restringir el acceso a la red.
7) Monitorear y supervisar el tráfico de red.
8) Implementar y revisar los controles de redes.

Tabla 82: Riesgo - Envenenamiento de DNS

Elaborado por: Investigador

Dar a conocer el SGSI a la dirección

Una vez que se dé por terminado el diseño del SGSI se dará a conocer a la gerencia o dirección principal para su revisión y aprobación.

Capacitación al personal para conocer el Sistema de Gestión de Seguridad de la información y el manual de contingencias

Se llevará a cabo una capacitación integral dirigida al personal de EPC COMPU sobre la importancia del Sistema de Gestión de la Seguridad de la Información y el manual de contingencia se puede visualizar en el **ANEXO 5.**

Durante esta capacitación, se proporcionará a los participantes un mejor entendimiento de cómo opera el SGSI y cómo se relaciona con la seguridad informática de la empresa. Además, se presentará detalladamente el Plan de Contingencia que es una parte esencial del SGSI esto será de ayuda para que los empleados aprendan como se desarrolla y se implementa este plan para enfrentar situaciones de emergencia o incidentes de seguridad informática.

3.3 Establecer un proceso de evaluación y mejoramiento continuo del SGSI lo cual garantice un adecuado tratamiento de la información.

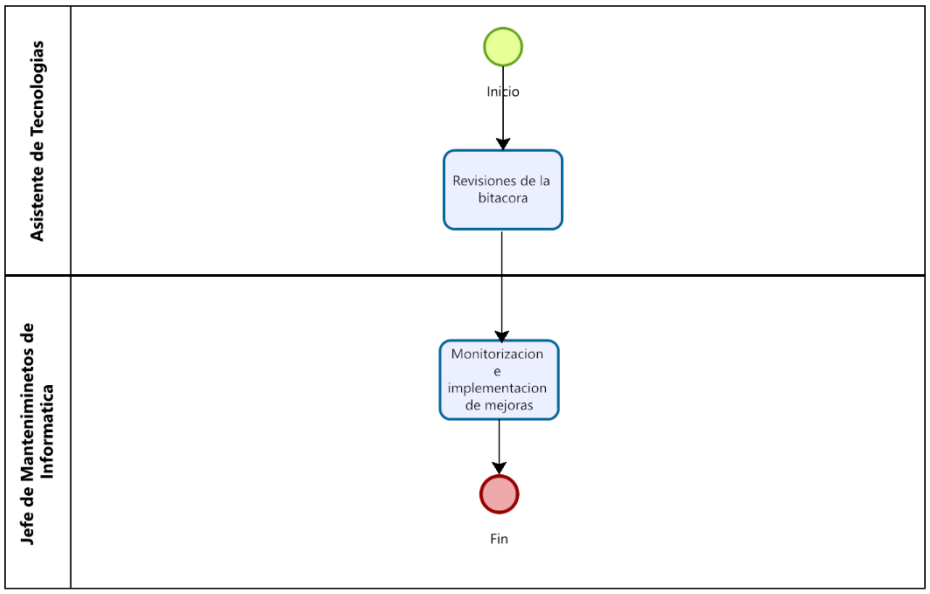


Figura 36.Proceso de evaluación y mejoramiento continuo del SGSI.

Elaborado por: Investigador

CAPITULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se evidenció falencias de Seguridad Informática en la empresa EPC COMPU lo que implica que los equipos informáticos se encuentran expuestos a vulnerabilidades y amenazas, poniendo en riesgo la seguridad de la información.
- Se encontró que la empresa no cuenta con políticas para proteger la información que utiliza cotidianamente, solo cuenta con controles básicos que no están alineados con una política y no garantizan la integridad, disponibilidad y confiabilidad de la información.
- Se diseñó un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo a la norma ISO 27001 y a las necesidades de la empresa el cual ayudará a tener un mejor control en el manejo de la seguridad de la información y de los activos informáticos.
- Se ha identificado una deficiencia en la correcta administración de los activos informáticos, lo que ha resultado que la información este expuesta a amenazas y vulnerabilidades.
- La implementación del sistema de gestión de seguridad de la información contribuirá a un mejor control de la seguridad de la información y la gestión de activos.
- Se ha desarrollado un manual que proporciona directrices claras sobre la correcta aplicación de políticas de seguridad de la información, tomando como base la norma internacional ISO/IEC 27001:2013.

4.2 Recomendaciones

- Se recomienda implementar cada una de las políticas y controles establecidos y mantener revisiones periódicas sobre el cumplimiento de estas para garantizar la seguridad de la información en la empresa.

- Se recomienda revisar continua o periódicamente cada 6 meses el Sistema de Gestión de Seguridad de la Información (SGSI) para proponer mejoras en un futuro de acuerdo con las necesidades de la empresa
- Se sugiere que las empresas capaciten al personal sobre la seguridad informática concientizando al mismo acerca de la importancia de proteger la información, considerando esta acción como una inversión en lugar de un gasto.
- Se recomienda asignar correctamente los roles y responsabilidades para llevar a cabo el cumplimento de las políticas de seguridad establecidas para EPC COMPU.
- Se sugiere verificar la efectividad de las actividades del plan de contingencia en el caso de ocurrir algún riesgo para que de esta manera se pueda mitigar en lo posible dicho riesgo.
- Implementar una metodología que permita mantener y fortalecer constantemente la seguridad de la información.
- Con el fin de reducir la posibilidad de que ocurran incidencias y minimizar su impacto, es recomendable implementar medidas preventivas y proactivas. Además, resulta fundamental contar con acciones correctivas eficaces para resolver cualquier inconveniente que pudiera surgir.

MATERIALES DE REFERENCIA

Bibliografía

[1] G. Vicente Salgado Andrade and W. Ruiz Buchelli, "Universidad Politécnica Salesiana Sede Guayaquil DIRECTOR," *Rev. EIA, ISSN 1794-1237*, vol. Volumen 17, pp. 1–323, 2015, [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/10070-. (TESIS)

[2] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez, and D. Lévano Rodríguez, "Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú," *Enfoque UTE*, vol. 12, no. 2, pp. 69–79, 2021, doi: 10.29019/enfoqueute.743. (REVISTA)

[3] E. Vega Briceño, *Seguridad de la información*. 2021. doi: 10.17993/tics.2021.4.

(LIBRO)

[4] M. I. Romero *et al.*, *Mecanismo Correctivos en seguridad informática*. 2018. (LIBRO)

[5] B. En, L. A. S. Normas, I. S. O. Iec, and E. N. E. L. D. De, "FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL INFORMÁTICOS Tema : SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍAS DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC . Trabajo de Titulación Modalidad : Proyec," 2020. (TESIS)

[6] R. A. Guevara, "Sistema de gestión de seguridad de información basado en la norma ISO 27001 para el departamento de tecnologías de la información y comunicación del distrito 18D01 de educación," p. 104, 2017, [Online]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339si. (TESIS)

[7] G. T. R. Alejandro, "Sistema de gestión de seguridad de la información basado en la norma iso/iec 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de educación", 2017, [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339si.pdf. (TESIS)

[8] R. L. C. Pomaquero, "Auditoría informática aplicando la norma iso 27001 para optimizar la seguridad de la información en el departamento de tic's del centro de investigación y desarrollo fae," 2022, [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/35566/1/t2039si.pdf (TESIS)

[9] J. Vásquez, "Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI," *Univ. Nac. Mayor San Marcos*, pp. 32–65, 2018, [Online]. Available: https://cybertesis.unmsm.edu.pe/handle/20.500.12672/8436 (TESIS)

[10] J. G. Arévalo Ascanio, R. A. Bayona Trillos, and D. W. Rico Bautista,

"Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información," *Rev. Tecnura*, vol. 19, no. 46, p. 123, 2015, doi: 10.14483/udistrital.jour.tecnura.2015.4.a10. (REVISTA)

[11] R. A. Guerra Mantilla, "Gestión de seguridad de la información con la norma ISO 27001:2013 Information security management with ISO 27001: 2013 standard," *Espacios*, vol. 39, p. 7, 2018, [Online]. Available: https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf (REVISTA)

[12] H. Vite Cevallos, B. Molina Montero, and J. Dávila Cuesta, "Gestión de la Información en las Instituciones de Educación Superior (IES) con base a la norma ISO 27001," *Informática y Sist. Rev. Tecnol. la Informática y las Comun.*, vol. 2, no. 2, p. 28, 2018, doi: 10.33936/isrtic.v2i2.1434. (REVISTA)

[13] J. I. Monsalve-Maldonado and A. E. Merchán-De Monsalve, "El uso de las Tecnologías de la Información y la Comunicación (TIC)," *Sostenibilidad, Tecnol. y Humanismo*, vol. 11, no. 2, pp. 74–86, 2020, doi: 10.25213/2216-1872.97. (LIBRO)

[14] G. Barvo and F. Barrera, "Utilizando Como Mecanismo De Hacking Ético El Sistema Operativo Kali Linux Previo a La Propuesta De Implementación Del Firewall Pfsense Y Correlacionador De," 2020. (TESIS)

[15] M. A. ORELLANA TOLEDO, "Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA," 2022. (TESIS)

[16] N. Iso and C. Tecnolog, "Información Application of the ISO 27001 Standard for the security of Information Systems Aplicação da Norma ISO 27001 para a segurança de Sistemas de Informação," vol. 8, pp. 1025–1041, 2022. (LIBRO)

[17] M. D. E. L. Proceso, "Gestión de seguridad informática," pp. 1–26, 2017. (LIBRO)

[18] INCIBE, "PROTEGE TU EMPRESA Colección PROTECCIÓN DE LA INFORMACIÓN," 2019. (LIBRO)

[19] OSRI, "Metodología para la gestión de la seguridad informática," *Of. Segur.*

para las Redes Informaticas, pp. 1–68, 2018, [Online]. Available: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf (LIBRO)

[20] B. J. F. Roa, *Seguridad informática - Ciclo formativo grado medio*. 2015. [Online]. Available: www.mhe.es/cf/informatica (LIBRO)

[21] R. Adriano, "Aprendijzaje .NET Framework," pp. 1–228, 2020, [Online]. Available:https://manual-informatica.com/download-file.html#google_vignette (LIBRO)

[22] Avast, "Avast Free Antivirus," *Avast*, vol. 2019, pp. 1–29, 2021, [Online]. Available:https://www.avast.com/en-my/free-antivirus-download#pc (LIBRO)

[23] Universidad del Pacífico, "Manual de uso de Zoom Meeting," *Gestión La Inf. E Innovación Tecnológica – Giit*, p. 11, 2020, [Online]. Available: https://www.up.edu.pe/pie/SiteAssets/Manual de acceso y uso de Zoom (2).pdf (LIBRO)

[24] E. S. Anydesk, "Instructivo Para La Instalación Y Uso De Anydesk ¿Qué Es Anydesk?," pp. 1–9, [Online]. Available: http://entsys.ceip.edu.uy/entsysevo/servlet/mainlogin•SIAP:http://siap.ceip.edu.uy/SIAP_CEIP•GRP:https://odoo.ceip.edu.uy/•CorreoCEIP:https://correo.ceip.edu.uy/•Guri:https://guri.ceip.edu.uy/ (LIBRO)

[25] A. Office, I. Outlook, G. P. Store, and O. Empresarial, "Manual-office-365-utn," pp. 66–81, [Online]. Available:https://www.utn.edu.ec/wp-content/uploads/2021/09/Manual-office-365-utn.pdf (LIBRO)

[26] C. De Virtualbox and N. F. Jesús, "UT01 : Manual de Instalación y". (LIBRO)

[27] D. D. V. Studio, "¿ Qué es Visual Studio ? ¿ Por qué usar Visual Studio ? Descubra Visual Studio Desarrolle su código," 2023. (LIBRO)

[28] S. Darias Pérez, "¿ Qué es Microsoft SQL Server ? ¿ Para qué sirve exactamente Microsoft SQL Server ? Funciones y Características de Microsoft SQL Server : ¿ Qué ediciones existen de Microsoft SQL Server ?," pp. 1–4, 2021, [Online]. Available:https://intelequia.com/blog/post/2948/qué-es-microsoft-sql-server-

y-para-qué-sirve (LIBRO)

[29] HostGator Mexico, “PuTTY en programación, aprende qué es y cómo utilizarlo,” 2022, [Online]. Available: https://www.hostgator.mx/blog/putty-en-programacion-aprende-que-es/ (LIBRO)

[30] A. Friends, “XAMPP,” vol. 4, pp. 0–2. (LIBRO)

[31] J. Gomar, “CPU-Z : Qué es y para qué sirve CPU-Z es la herramienta de detección de hardware que estabas buscando , todo lo que necesitas saber Descarga la versión portátil de CPU-Z,” 2018. (LIBRO)

[32] Solé Roberto, “¿ Qué es Adobe Reader ? - Características y alternativas - HardwarEsfera,” 2019, [Online].Available: https://hardwaresfera.com/articulos/que-es-adobe-reader/ (LIBRO)

Anexos

ANEXO 1

Tabla 2 – Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

Núm.	Nombre	Selección / Exención	Descripción / Justificación
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información		Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información		Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información		Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información		Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial		Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles		Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1.1	Selección		Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo		Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección		Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario		Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo		Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos		Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos		Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos		Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos		Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información		Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información		Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información		Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos		Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles		Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios		Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos		Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso		Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red		Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información		Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro		Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas		Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados		Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía		
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos		Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves		Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno		

A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física		Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada		Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales		Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos		Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro		Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado		Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos		Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos		Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos		Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados		Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios		Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos		Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo		Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información		Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes		Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos		Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas		Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software		Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas		Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes		Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red		Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información		Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información		Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

A.13.2.2	Acuerdos sobre transferencia de información		Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica		Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas		Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro		Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas		Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros		Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro		Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente		Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas		Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba		Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba		Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.

A.15	Relación con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores		Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos		Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información		Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información		Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información		Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia		Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

A.17.1.1	Planificación de la continuidad de la seguridad de la información		Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información		Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
A.17.2	Redundancias		Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual		Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros		Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales		Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos		Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información		Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico		Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

ANEXO 2

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA EPC COMPU

POLITICAS DEL SGSI
ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION
Elaborar un documento en el que se detallen los roles y responsabilidades asignar anteriormente para solucionar los incidentes de seguridad de la información.
GESTION DE ACTIVOS
Se elaborará un documento en el que se registre si la información del activo que se maneja en la empresa es pública o privada, además se deberá registrar el activo de acuerdo con los siguientes criterios: critica, valiosa y sensible.
Guardar el disco duro de respaldo en un lugar seguro como un Data center externo.
Cifrar las copias de seguridad utilizando el administrador de BitLocker de Windows.
Realiza copias de seguridad regulares de los correos electrónicos importantes y otros datos relacionados con las cuentas de correo.
Se deberá utilizar sellos y rótulos en las carpetas y archivadores para identificarlos correctamente, y para la información digital se utilizará colores de identificación en las carpetas de archivos.
SEGURIDAD DE LOS RECURSOS HUMANOS
El personal que ingrese a la empresa a laborar deberá recibir capacitación en el uso adecuado de la seguridad de la información para mantener la integridad, disponibilidad y confidencialidad de la información, según el área en la que se encuentre y las funciones que desempeñe.
Los empleados deben comprometerse y firmar un acuerdo de confidencialidad con respecto a la información con la que trabajarán mientras estén en las instalaciones.
Al finalizar la relación laboral con el empleado, se deberá cerrar y eliminar cada una de las cuentas asignadas a éste, tanto en las plataformas institucionales como en las computadoras, este proceso garantizará la seguridad de la información institucional.
Encriptar los medios removibles los cuales contengan información critica, valiosa, y sensible.

CONTROL DE ACCESO
Asignar la cuenta de usuario de acuerdo con el rol y responsabilidad dentro de la empresa.
Desactivar la cuenta de usuario inmediatamente cuando el usuario abandona la empresa.
Establecer un periodo de caducidad de los permisos privilegiados.
Forzar el cambio de contraseñas cuando un usuario cambia o abandona el puesto de trabajo.
Las contraseñas del sistema de información deberán permanecer encriptadas.
Implementar el sistema de doble factor de autenticación.
Brindar capacitación regular a todos los empleados sobre la importancia de la privacidad de la información y las mejores prácticas para protegerla.
Implementación de listas de control de acceso.
Utilización de un firewall para interceptar el tráfico.
SEGURIDAD DE LAS OPERACIONES
Los sistemas que se desarrollan deberán pasar por escenarios de pruebas para posteriormente ser puesto en producción.
Se deberá capacitar a los empleados sobre los distintos tipos de ataques de Ingeniería social.
Se deberá adquirir un antivirus con licencia de paga.
Se deberá llevar un control adecuado de las instalaciones de software en los equipos.
Mantener actualizado el software de gestión de correo y los clientes de correo electrónico.
Descargar archivos y software de fuentes seguras y confiables.
SEGURIDAD DE LAS COMUNICACIONES
Estará terminantemente prohibido el acceso de terceros a la red de la empresa, considerando terceros a todas las entidades que mantengan relaciones laborales con la empresa.
Se debe monitorear los accesos de los usuarios a la red y a los sistemas de información mediante la implementación de sistemas de detección de intrusos.
Utilizar firmas digitales.
Encriptar la información confidencial a ser enviada por correo electrónico.
Contar con un diagrama de toda la infraestructura de red.

CRIPTOGRAFIA
La información debe cifrarse siempre que el destinatario acepte el intercambio de datos cifrados
SEGURIDAD FISICA
Implementar señalización de advertencias en los distintos puntos del área de trabajo.
Contar con sistemas de refrigeración en las estaciones de trabajo.
Implementar un plan trimestral de mantenimiento preventivo y correctivo de los equipos informáticos para prevenir daños y problemas futuros.
Las pantallas no deben mostrar ningún tipo de información cuando el equipo no esté en uso.
Realizar convenios con proveedores.
Contratación de seguros.
DESARROLLO Y MANTENIMIENTOS DE SISTEMAS
Aplicar certificados digitales.
Implementar el cifrado en las comunicaciones.
Establecer metodologías de desarrollo optimas y elegir la que mejor se adapte a los requerimientos.
CUMPLIMIENTO
Realizará el monitoreo y revisión periódica del cumplimiento de las políticas y controles.

ANEXO 3

PLAN DE CONTINGENCIA

Riesgo	Sustracción de documentos
Evento	Perdida de documentación física
Responsable	Asistente de Tecnologías
Actividades:	
1) Evaluar el alcance de la perdida. 2) Informar a los responsables. 3) Recuperar copias de seguridad. 4) Recopilar información de respaldo. 5) Revisar contratos y acuerdos. 6) Implementar medidas preventivas.	

Riesgo	Hurto de información
Evento	Perdida de información confidencial por ataques informáticos
Responsable	Asistente de Tecnologías
Actividades	
1) Informar la pérdida de información confidencial a las partes interesadas internas y externas, como empleados, clientes y socios comerciales. 2) Contratar y trabajar con profesionales de TI o expertos en seguridad para intentar recuperar los datos. 3) Determinar qué información está en riesgo y cuáles son los riesgos potenciales. 4) Identificar las brechas de seguridad o las debilidades. **5)** Brindar capacitación y concientización periódicas sobre seguridad de la información para todos los empleados de la empresa. 6) Implementar y revisar las políticas la seguridad de la información	

Riesgo	Phishing
Evento	Robo de credenciales de cuentas de correo electrónico por técnicas de ingeniería social
Responsable	Jefe de Mantenimiento de Informática
Actividades:	
1) Revisar los registros e incidentes de correo electrónico. 2) Bloquear el enlace o correo malicioso. 3) Cambiar contraseñas comprometidas 4) Capacitación a los empleados sobre las técnicas de phishing. 5) Monitoreo de la red con sistemas IDS y firewall. 6) Implementar y revisar el control de mensajería electrónica.	

Riesgo	Alteración de privilegios
Evento	Acceso no autorizado a los sistemas de información por falta de monitoreo.
Responsable	Asistente de Tecnologías
Actividades:	
1) Identificar el sistema alterado 2) Aislar el sistema de la red 3) Cambiar contraseñas de las cuentas 4) Restablecer los privilegios. 5) Actualizar el sistema operativo y aplicaciones. 6) Realizar evaluaciones de seguridad de los sistemas. 7) Implementar y revisar el control de Gestión de derechos de acceso privilegiado.	

Riesgo	Alteración o eliminación de cuentas
Evento	Acceso no autorizado a las cuentas de correo electrónico y del sistema de información.
Responsable	Asistente de Tecnologías

Actividades:

1) Identificar la cuenta de usuario alterada
2) Aislar la cuenta afectada.
3) Cambiar las cuentas y credenciales
4) Restaurar las configuraciones de las cuentas.
5) Eliminar cualquier acceso no autorizado de la cuenta
6) Identificar la brecha de seguridad.
7) Monitorear la seguridad de las cuentas de usuarios
8) Implementar y revisar el control de registro y cancelación del registro de usuarios

Riesgo	Licencias Vencidas y desactualizadas
Evento	Licencia de algunas aplicaciones sin actualizar.
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Identificar que aplicaciones requieren actualización con licencia
2) Revisar los términos de licencias.
3) Contactar con los proveedores de licencias.
4) Implementar la actualización de las licencias.
5) Establecer proceso de seguimiento periódico de las licencias.
6) Implementar y revisar el control de mantenimiento de equipos.

Riesgo	Sniffing
Evento	Suspensión de las operaciones laborales por intrusiones en la red
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Detectar todos los dispositivos conectados a la red
2) Aislar el dispositivo infectado.
3) Cambiar contraseñas y credenciales del router
4) Actualizar el sistema operativo y aplicaciones.
5) Monitoreo de la red.
6) Implementar y revisar los controles de red

Riesgo	Falla en el disco duro
Evento	Pantallazo azul y sonidos extraños
Responsable	Jefe de Mantenimiento de Informática

Actividades:

1) Detener el uso del disco duro.
2) Realizar una copia de seguridad de la información en otro equipo.
3) Determinar la gravedad del daño en disco duro.
4) Considerar opciones de reparación o reemplazo.
5) Implementar y revisar el control de Mantenimiento de equipos

Riesgo	Incendio
Evento	Incendio por malas instalaciones eléctricas
Responsable	Gerente

Actividades:

1) Evaluar la seguridad del personal
2) Comunicar y notificar a todo el personal sobre el incendio.
3) Realizar una evaluación exhaustiva de los daños.
4) Contactar con alguna empresa aseguradora
5) Reemplazo de equipos y sistemas dañados.
6) Determinar si es posible reanudar las operaciones
7) Investigar la causa del incendio.
8) Revisar el plan de emergencia.
9) Implementar y revisar el control de Protección contra amenazas externas y ambientales,

Riesgo	Robo
Evento	Robo de un equipo informático debido a la falta de sistemas de seguridad
Responsable	Gerente

Actividades:

1) Informar a las autoridades sobre el robo.
2) Verificar las instalaciones de la empresa.
3) Notificar a los proveedores de servicios.
4) Cambiar las contraseñas de los sistemas de información.
5) Notificar a los clientes y socios
6) Recuperar la información de las copias de seguridad
7) Implementar y revisar el control de Ubicación y protección de los equipos

ANEXO 4

ELEMENTOS DE DETECCIÓN

ELEMENTOS DE DETECCIÓN
• Monitorización de registros y actividad de red mediante la utilización de sistemas IDS.
• Revisar regularmente los registros de acceso y actividad de los usuarios en los sistemas y aplicaciones de la empresa.
• Rendimiento de la red
• Alertas de seguridad en la red
• Revisión y monitoreo de las cuentas de usuarios
• Revisión de las Alertas de malware
• Deterioro de la infraestructura de la empresa
• Consumo de ancho de banda
• Falta de acceso a internet
• Anomalías del tráfico ARP.
• Duplicación de direcciones IP

ANEXO 5

PLAN DE CAPACITACIÓN

Capacitación sobre el SGSI:

- Objetivo: Familiarizar al personal con los conceptos y requisitos del SGSI.
- Actividades:
  - Sesión de capacitación introductoria sobre la norma ISO 27001 y los requisitos del SGSI.
  - Capacitación específica sobre los procedimientos y controles de seguridad de la información.
- Responsables: Equipo de proyecto del SGSI.
- Fecha: 17 de julio (sesión 1-2)
- Evidencia: Asistencia de los empleados a la capacitación, evaluaciones de conocimientos.

Capacitación sobre el Plan de Contingencia:

- Objetivo: Entrenar al personal en la respuesta a incidentes y la implementación del Plan de Contingencia.
- Actividades:
  - Sesión de capacitación sobre los procedimientos de respuesta a incidentes y las medidas de contingencia.
  - Ejercicios prácticos para simular escenarios de incidentes y practicar la ejecución del Plan de Contingencia.
- Responsables: Cristina Sailema
- Fecha: 18 de julio (sesión 3-4)
- Evidencia: Asistencia de los empleados a la capacitación, registro de los ejercicios prácticos.

Seguimiento y refuerzo:

- Objetivo: Realizar sesiones de seguimiento para reforzar los conocimientos adquiridos.
- Actividades:
  - Sesiones de revisión periódicas para aclarar dudas y brindar orientación adicional.
  - Sesiones de actualización sobre cambios en el SGSI y el Plan de Contingencia.
- Responsables: Cristina Sailema
- Fecha: Sesiones mensuales a partir de julio de 2023.
- Evidencia: Registro de asistencia a las sesiones de seguimiento.

Cronograma de Capacitación

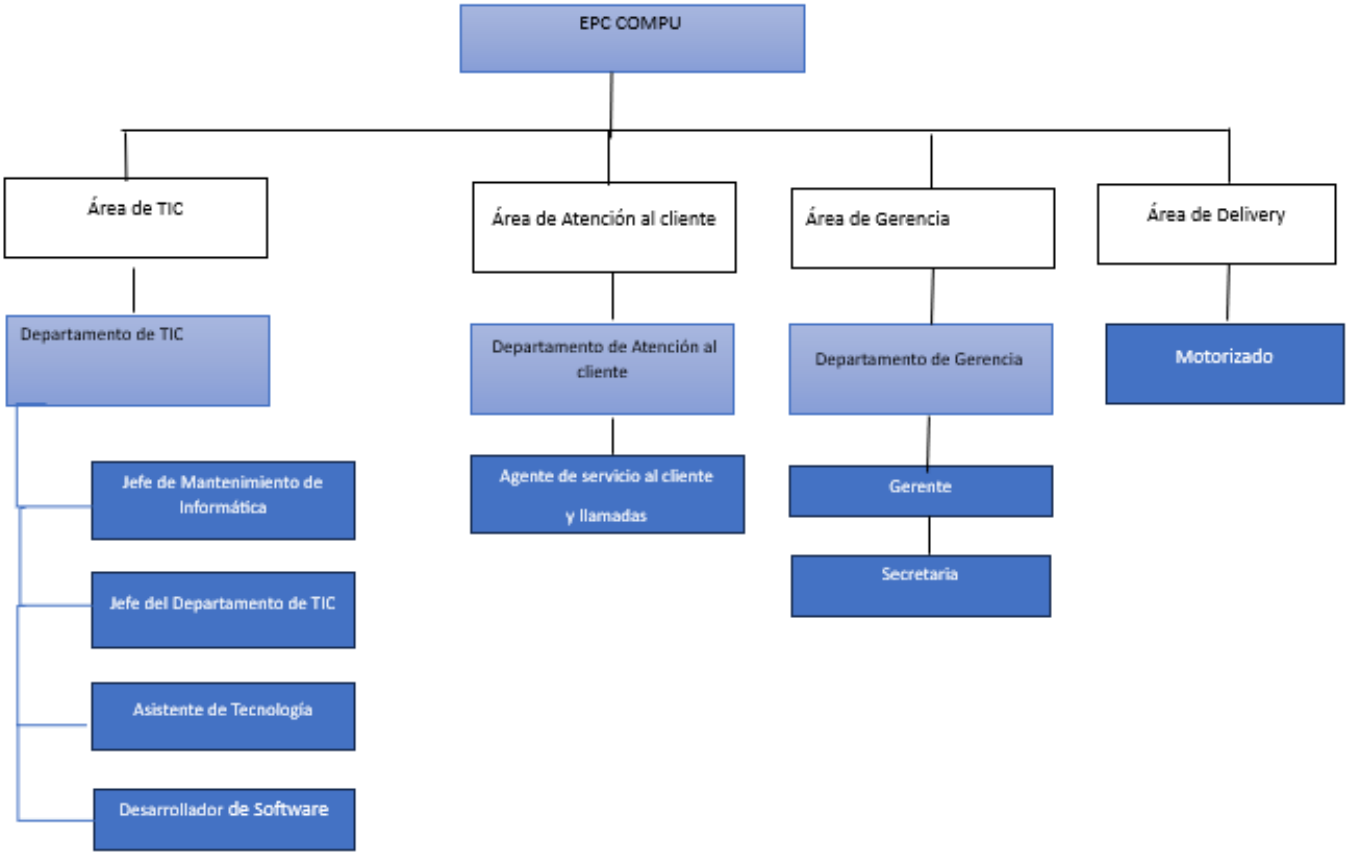
Actividad	Responsables	Fecha	Evidencia
Sesión de capacitación introductoria SGSI	Cristina Sailema	17 de julio (Sesión 1)	Asistencia, evaluaciones de conocimientos
Capacitación específica sobre procedimientos y controles	Cristina Sailema	17 de julio (Sesión 2)	Asistencia, evaluaciones de conocimientos
Sesión de capacitación Plan de Contingencia	Cristina Sailema	18 de julio (Sesión 3)	Asistencia
Ejercicios prácticos de respuesta a incidentes	Cristina Sailema	18 de julio (Sesión 4)	Registro de ejercicios prácticos
Sesiones de seguimiento y refuerzo	Cristina Sailema	Mensualmente	Registro de asistencia

Formato de Asistencia a Capacitaciones

Cargo	Sesión 1	Sesión 2	Sesión 3	Sesión 4	Sesión 5
Gerente	X	X	X	X	X
Jefe del Departamento de TICS	X	X	X	X	X
Desarrollador de Software	X	X	X	X	X
Asistente de Tecnología	X	X	X	X	X
Jefe de Mantenimiento de Informática	X	X	X	X	X

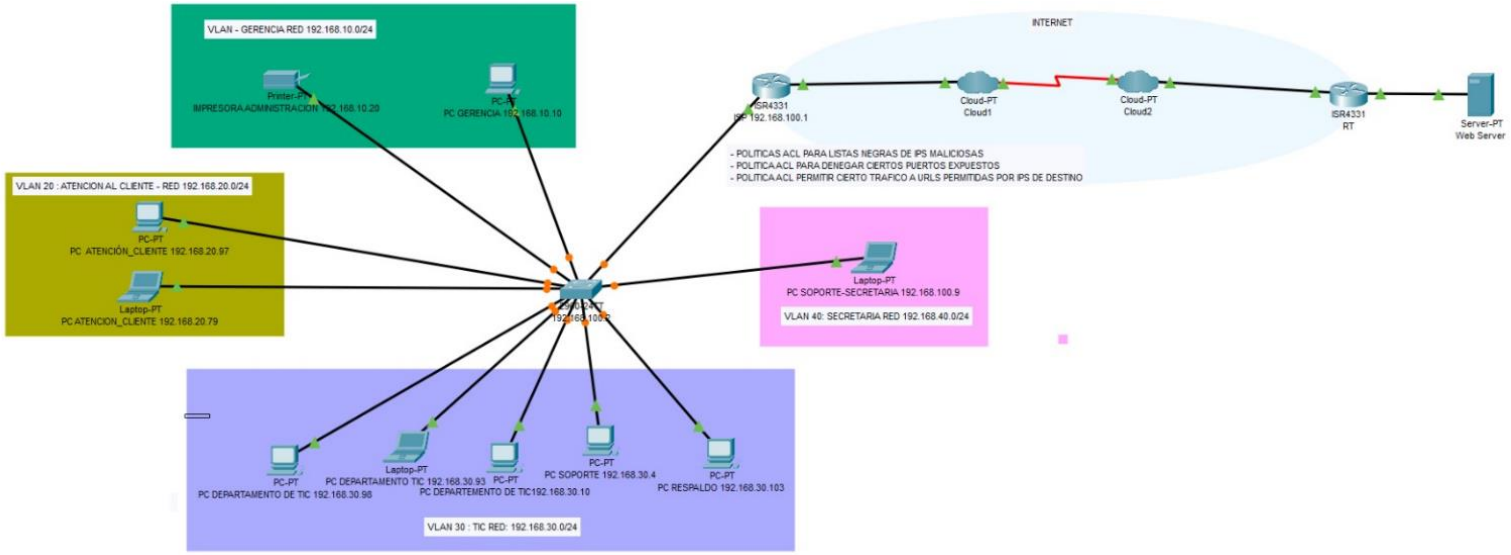
ANEXO 6

ORGANIGRAMA



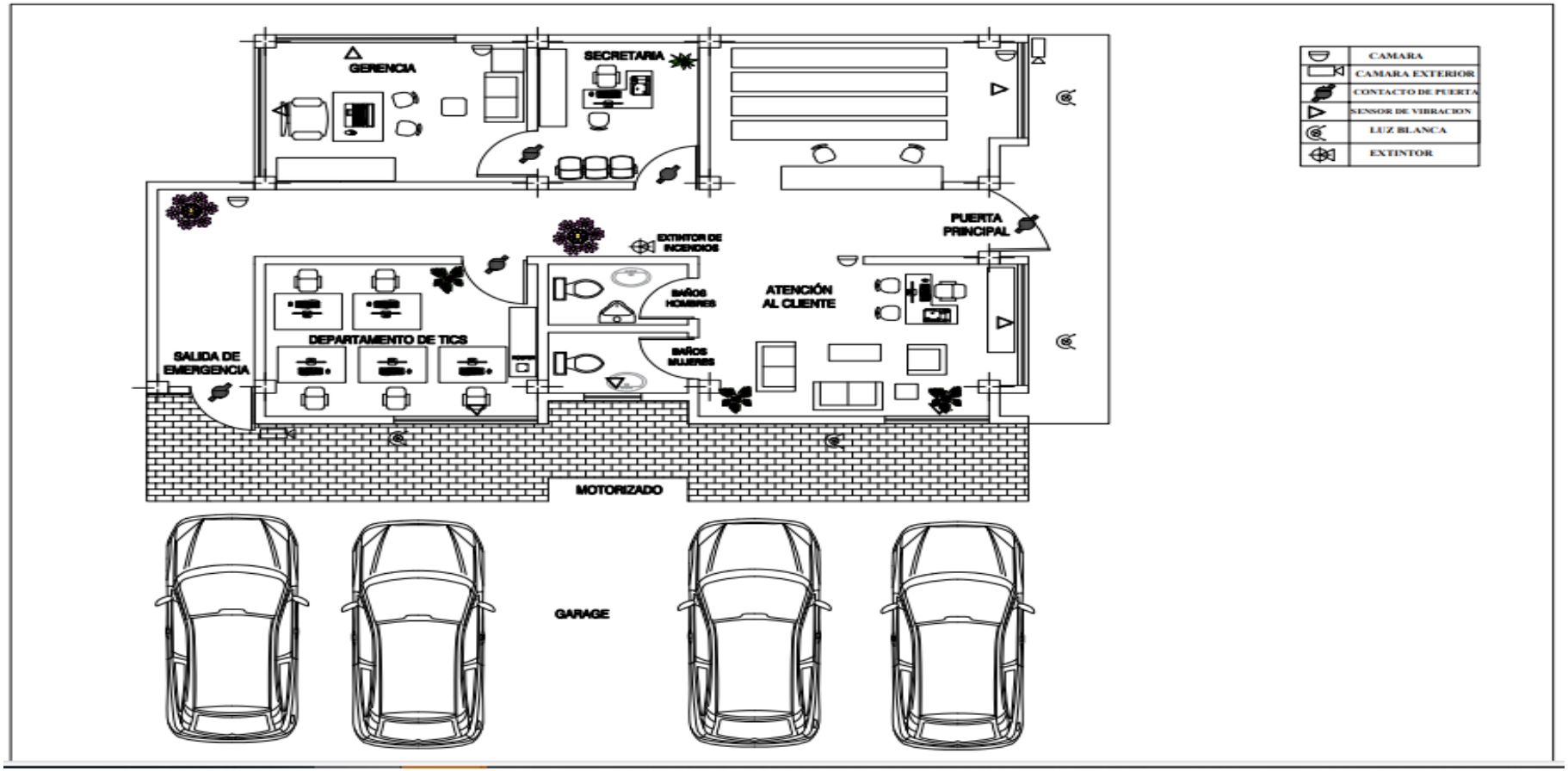
ANEXO 7

ESTRUCTURA DEL DIAGRAMA DE RED



ANEXO 8

ESTRUCTURA FÍSICA



ANEXO 9

FUNCIONES DE LOS EMPLEADOS

N°	Área	Cargo	Funciones
1	GERENCIA	GERENTE GENERAL	Supervisión del personal, Relaciones con Clientes y Socios, Resolución de problemas, Toma de desiciones.
2	TIC	JEFE DE DEPARTAMENTO DE TICS	Asignar responsabilidades, Supervisar a los empleados.
3	TIC	JEFE DE MANTENIMIENTO DE INFORMÁTICA	Soporte Técnico, Elaboración de informes, Configuración de dispositivos.
4	TIC	DESARROLLADOR DE SOFTWARE	Soporte Técnico del sistema web.
5	TIC	ASISTENTE DE TECNOLOGÍA	Ayuda en el proceso de adquisición de nuevo hadware y software, Mantenimiento de equipos.
6	SECRETARÍA	SECRETARIA	Redactar documentos, Desarrollar presentaciones, Organizar eventos, Gestión de nóminas, Asigna ingresos a los motorizados, Validar pagos.
7	ATENCIÓN AL CLIENTE	ASESOR DE VENTAS 1	Informar sobre productos y servicios, Brindar asistencia técnica especializada, Orientar en el uso de productos y servicios.
8	ATENCIÓN AL CLIENTE	ASESOR DE VENTAS 2	Informar sobre productos y servicios, Brindar asistencia técnica especializada, Orientar en el uso de productos y servicios.
9	DELIVERY	MOTORIZADO	Tiene acceso a ver los retiros, Realiza los retiros de equipos que requieran un servcio y entrega de los mismos.