Pontificia Universidad Católica del Ecuador

Facultad de Ingeniería

Carrera de Ingeniería en Sistemas de Información

TEMA:

PROPUESTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001. CASO DE ESTUDIO: EMPRESA ALTAC

AUTOR:

Fabricio Mera Amores

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

Quito, noviembre 2022

DEDICATORIA

Dedico este trabajo de investigación a todas las que han dejado una enseñanza en mí.

AGRADECIMIENTO

Agradezco a mi madre Nancy, quien siempre ha guiado mi camino con tanto amor y por su ejemplo de fortaleza y resiliencia que ha formado a la persona que soy hoy.

A mis hermanos María Sol y Carlos, por siempre estar a mi lado bridándome su apoyo incondicional en cada paso, proyecto y aventura que hemos vivido.

Al Dr. Henry Roa y a la Ing. Suyana Arcos por todas sus enseñanzas y su apoyo en este trabajo de titulación

A todos quienes conforman la empresa ALTAC por su colaboración para realizar este trabajo de investigación.

RESUMEN

ALTAC es una empresa que se ubica en la ciudad de Quito y su giro de negocio es la contabilidad y auditoría. Para este trabajo de titulación se realizó una evaluación de la Seguridad de la Información en la empresa basándose en el estándar de la norma ISO/IEC 27001. Para esto, se clasificó los activos de los que la empresa dispone y fueron agrupados en cuatro categorías: Activos de Información, Talento Humano, Hardware y Sistemas de Información.

Se analizó las amenazas y vulnerabilidades que estos activos podrían enfrentar para de esta manera calcular el riesgo y priorizar las actividades necesarias para la remediación. Adicionalmente, se seleccionaron ciertos controles establecidos en el Anexo A de la norma ISO 27001 y se verificó su cumplimiento con el fin de establecer posteriormente recomendaciones acerca de cómo mejorar la seguridad en la empresa.

ÍNDICE

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. Justificación

Una filtración ocurrida por un manejo no adecuado de la información puede ser extremadamente perjudicial para una empresa. Es por esta razón que este trabajo de titulación pretende dar lineamientos para mejorar la seguridad de la información dentro de la empresa, con base en la norma ISO 27001.

El estar alineados con esta norma traerá como beneficio adicional una mayor competitividad, permitiendo que realizar negocios más lucrativos con empresas que exigen los más altos estándares acerca del manejo de la información.

1.2. Planteamiento del problema

Dentro de la empresa ALTAC se observan ciertas debilidades en el manejo de la información como falta de estrategia de respaldos, almacenamiento sin cifrar, manejo de contraseñas y credenciales, etc. Subsanar dichas debilidades representa una oportunidad de mejora de procesos internos y crecimiento empresarial, evitando potenciales desastres y aumentando la competitividad de la empresa. como reutilización de contraseñas, envíos de credenciales en texto plano, falta de estrategia de respaldos, almacenamiento sin cifrar, etc.

1.3. Objetivo General

Realizar una propuesta de gestión de la Seguridad de la Información para la empresa ALTAC basado en la norma ISO 27001.

1.4. Objetivos Específicos

- Identificar fortalezas y debilidades en el manejo de la información en la empresa.
- Definir las oportunidades para el manejo de la información relacionado con la norma ISO 27001.
- Formular un documento con las acciones a ser tomadas por la empresa para mejorar la seguridad.

1.5. Antecedentes

La empresa ALTAC, ubicada en el Distrito Metropolitano de Quito, tiene como giro de negocio principal la actividad de Auditoria y Contabilidad. La empresa maneja información sensible de sus clientes, por lo que es indispensable contar con procedimientos y mecanismos que aseguren que dicha información se mantenga segura en reposo, tránsito y en uso.

1.6. Alcance

En este trabajo de titulación se pretende identificar debilidades y oportunidades de mejora de la seguridad de la información en la empresa ALTAC, para finalmente realizar un documento con recomendaciones basadas en la norma ISO 27001:2013. Es importante clarificar que con este proyecto no se obtendrá la certificación en dicha norma.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. Marco Teórico

2.1. Seguridad de la Información

La seguridad de la Información es la disciplina que busca evitar amenazas a la privacidad de los sistemas de información. Por medio de la aplicación de políticas, procedimientos y controles se busca garantizar la confidencialidad, integridad y la disponibilidad de la información que almacenan las empresas.

La seguridad de la información hace mucho más que evitar las intrusiones a sistemas informáticos. Se debe tratar más bien a la Seguridad de la Información con una perspectiva más amplia en la que se protejan todos los activos que podrían ser vulnerables dentro de una organización.

Para tener un correcto manejo de la Seguridad de la Información se debe evaluar qué peligros corren, por ejemplo, los documentos físicos que tiene la empresa, o los riesgos a los cuales se podría enfrentar uno de los activos más importantes, sus empleados, tambien llamados el recurso humano.

En el pasado, la responsabilidad sobre la seguridad recaía únicamente sobre el departamento de sistemas de la empresa, sin embargo, hoy en día es una responsabilidad compartida entre todos los actores de una organización.

2.1.1. Confidencialidad

La confidencialidad de la información es la característica que esta tiene de que solo las personas autorizadas puedan acceder a ella para leerla o modificarla. Las organizaciones poseen información que podría afectar sus operaciones o la competitividad en el mercado en caso de ser publicada, por lo que mantener la

confidencialidad de los activos de información de la empresa es imperativo. Las violaciones a la confidencialidad pueden ocurrir por omisión de los operadores humanos, por ejemplo, al ser víctima de un ataque de suplantación o robo de contraseñas. (Fortinet, 2022).

2.1.2. Integridad

La integridad significa que se garantiza la autenticidad y exactitud de la información. También se garantiza que la información no ha sido alterada por un agente externo durante el tránsito. Para poder confirmar la integridad de la información es posible utilizar certificados y firmas digitales, así como checksums calculados tras crear el archivo, y que deben ser validados por los destinatarios de la información. Generalmente, para que la integridad se vea comprometida debe existir una acción intencional.

2.1.3. Disponibilidad

La disponibilidad de la información es que esta se encuentre lista para ser utilizada por los usuarios autorizados que la requieren, en el momento en que estos la requieran. Cualquier interrupción en la transferencia, la comunicación de un sistema o el acceso a la información representa una amenaza al principio de disponibilidad (Mejía Medina, 2019). Un claro ejemplo de un ataque contra la disponibilidad de un sistema de información son los ataques distribuidos de denegación del servicio (DDoS, por sus siglas en inglés). En esta clase de ataques se envía solicitudes de manera masiva desde distintos hosts comprometidos, de manera sincronizada hacia el sistema atacado hasta sobrecargarlo, produciendo que no pueda responder a solicitudes legítimas, degradando la disponibilidad (Hoque et al., 2015).

2.2. Conjunto de Normas ISO 27000

La serie de normas de la familia ISO 27000 son normas que destinadas a la implementación de un Sistema de Gestión de la Seguridad de la Información mediante buenas prácticas y están orientadas a la mejora continua. Dentro de este conjunto existen 19 normas. A pesar de que todas las normas de esta familia se relacionan con la creación e implementación de un SGSI, existen normas más específicas según el giro de negocios de una organización, por ejemplo, la norma ISO 27011 es para organizaciones de telecomunicación, mientras que la norma 27015 se utiliza en organizaciones financieras. Existen otras normas utilizadas para la integración con otras familias como la ISO 27013, que indica como integrar los SGSI con las Sistemas de Gestión de Servicios, que son manejan con la familia de la ISO 20000. (International Organization for Standarization, 2018)

2.2.1. Norma ISO 27001

Es un conjunto de políticas y estandarizaciones para aplicación y administración de la seguridad de la información de una organización, sin importar el tipo de organización, su tamaño, o el giro del negocio, utilizando un Sistema de Gestión de la Seguridad de la Información. (International Organization for Standarization, 2013)

Fue creada en el año 2005 de manera conjunta por la Organización Internacional de Estandarización (ISO, International Organization for Standarization, por sus siglas en inglés) y la Comisión Internacional Electrotécnica (IEC. International Electrotechnical Commision, por sus siglas en inglés), con una revisión en 2013, y su última versión fue liberada a finales del mes de octubre de 2022.

La última revisión de la norma trae cambios principalmente de cambio de nombres de cláusulas y en el Anexo A, en conformidad con la última versión de la norma ISO 27002:2022. (Hyseni, 2022)

Esta norma es parte de la familia de normas ISO 27000, que detalla técnicas para seguridad de la información.

La norma ISO 27001 ofrece una estructura para evaluar y garantizar la Seguridad de la Información, la ciberseguridad y la protección de la privacidad.

El proceso que se sigue para obtener una certificación en esta norma comienza con la identificación de vulnerabilidades dentro de la organización. En este paso se determina que acciones se identifican los activos que la organización requiere proteger, los recursos con los que se cuenta y las acciones que se están llevando a cabo para resguardar la seguridad de la información.

A continuación, se estable el alcance que tendrá el Sistema de Gestión de la Seguridad de la Información. Este alcance depende de las necesidades y el contexto de la empresa.

Una vez determinado el alcance, se procede a realizar la evaluación del riesgo que corren los activos, valorando que tan probable es que un evento adverso ocurra y cuál sería el impacto que tendría sobre las operaciones de la organización. Con esta información se pueden seleccionar los controles del Anexo A de la norma que serán aplicados.

La norma ISO 27001:2013 cuenta con 114 controles y 35 objetivos de control que se agrupan en 14 dominios. Se requiere evaluar los controles de la empresa para determinar si es aplicable según el contexto y las necesidades de la empresa.

Tras aplicar los controles, la organización debe crear una declaración de aplicabilidad SoA, por sus siglas en inglés, “Statement of Aplicabilty” (International Organization for

Standarization, 2013). En este documento se enlistan todos los controles del Anexo A y se registra si el control se ha aplicado o no junto con una justificación.

Una vez que la organización cuenta con el SoA, se debe establecer un Plan de Tratamiento de Riesgos (PTR), que es un documento en el que se indica como va a proceder la organización para mitigar, reducir o eliminar los riesgos identificados previamente.

La organización debe documentar todos los componentes de su SGSI y socializar la información obtenida sobre seguridad con todos los empleados. Así mismo se debe realizar pruebas regularmente para comprobar la efectividad de los controles empleados. Al haber completado este proceso, la empresa puede contratar una auditoría externa que le permita certificarse con la norma ISO:27001.

2.2.2. Norma ISO 27002

La norma ISO 27002 provee una guía sobre la implementación de los controles establecidos en el Anexo A de la norma ISO 27001. Es importante destacar que no es posible que una organización se certifique en ISO 27002, únicamente en ISO 27001. Esta norma sirve de apoyo acerca del cómo utilizar los controles, mientras que la ISO 27001 provee la estructura para el SGSI. (International Organization for Standarization, 2022)

2.2.3. Norma ISO 27005

La norma ISO 27005 es la norma que se encarga de la gestión de riesgos de seguridad de la información dentro de una organización, apoyando a en la implementación de la norma ISO 27001. ISO 27005 provee de un marco para realizar actividades como la evaluación y tratamiento de riesgos en los activos de la empresa, tomando en cuenta

factores como el alcance del Sistema de Gestión de la Información. Su última versión fue publicada en octubre del 2022. (International Organization for Standardization, 2022)

2.3. Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) se encarga de gestionar los riesgos y la seguridad de una organización, concentrándose principalmente en la evaluación y mitigación de estos.

Un SGSI sigue el modelo PDCA (Plan-Do-Check-Act):

- Plan: Se identifican debilidades e información que podría resultar útil para definir controles y mejorar la seguridad. Posteriormente se desarrollan los procesos que solucionarán las debilidades encontradas.
- Do: En esta fase se implementan los procesos desarrollados en la fase anterior, considerando los recursos de la empresa.
- Check: Se hace una valoración de los resultados arrojados por la aplicación de los procesos y se verifica que tan eficaces fueron.
- Act: Se levanta documentación con respecto a los resultados, buscando una mejora continua con las lecciones aprendidas que serán aplicadas en las siguientes versiones del SGSI.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA

3.1. Situación actual de la empresa

Se ha realizado una evaluación de la situación actual de la empresa a nivel de seguridad de la información y se han encontrado oportunidades de mejora en el manejo de la información, por ejemplo, en el control de contraseñas y acceso a los servicios. Se identifica que la empresa cuenta con procedimientos de respaldo de la información y restricción de accesos a archivos físicos. Sin embargo, existen procesos que pueden ser automatizados y sometidos a pruebas para validar su eficacia.

3.2. Identificación de activos de la empresa

Para realizar una evaluación de seguridad de los activos que posee una empresa, es posible agruparlos según las necesidades del negocio o los proyectos. (Government of the UK, 2017).

Para este caso de estudio se han agrupado los activos de la empresa en cuatro grupos, y cada grupo será tratado como un único activo.

- Activos de Información
    - Base de datos de clientes de la empresa
    - Documentos internos de la empresa
    - Libro diario
    - Estado de situación inicial/final
    - Estado de resultados
    - Balance financiero
    - Documentos físicos y digitales de cada cliente.

- Talento Humano
- Hardware
    - Servidor de la empresa
    - Computadores de escritorio y computadores portátiles
    - Equipos de red
- Sistemas de Información
    - Software contable

3.3. Identificación de amenazas a los activos

Al realizar la identificación de las amenazas hacia los activos de la empresa se plantearon casos hipotéticos basados en escenarios comunes, artículos disponibles en la red y experiencia del investigador. (Kosustic, 2021)

Activos de información:

- Pérdida de archivos físicos
- Eliminación de archivos digitales
- Desastres naturales (incendio, terremotos, inundaciones)
- Delincuencia
- Vandalismo
- Sabotaje

Talento Humano

- Debilidades en la revisión de antecedentes de los empleados
- Phishing
- Ataques de ingeniería social

Hardware

- Corrupción de datos
- Fallas de energía
- Delincuencia
- Vandalismo
- Sabotaje

Sistemas de Información

- Uso inadecuado de la información de la empresa
- Accesos no autorizados a sistemas
- Interceptación de datos

3.4. Identificación de vulnerabilidades de los activos

En el reconocimiento de las vulnerabilidades en los activos de la empresa se evaluaron los riesgos determinados previamente, se propusieron escenarios hipotéticos comunes y se utilizó artículos disponibles en la red. (Kosustic, 2021)

Activos de Información:

- Sistemas de respaldo de información inadecuados
- Falta de controles en copia y eliminación de archivos

Talento Humano:

- Entrenamiento de seguridad deficiente para empleados
- Falta de supervisión de los empleados
- Desconocimiento de procesos de seguridad

Hardware:

- Dispositivos que alcancen el final de su soporte (EOL)

- Daño físico a los equipos
- Configuraciones incorrectas en los equipos
- Exposición de servicios inseguros o no necesarios en los equipos

Sistemas de Información:

- Falta de capacitación a empleados
- Malware y Ransomware
- Falta de políticas de contraseña

Accesos no autorizados

CAPÍTULO IV: PROPUESTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4. Propuesta de Gestión de la Seguridad de la Información

4.1. Cálculo del riesgo

Se ha evaluado que tan probable es que una amenaza o evento adverso suceda y el impacto que este tendría sobre la normal operación del negocio, y en base a dichas calificaciones se calculará posteriormente el riesgo y se plantearan procedimientos para mitigarlo, reducirlo o asumirlo de ser el caso. Al conocer el riesgo se puede priorizar que procedimientos son más urgentes para la empresa.

Para la calificación de probabilidad se ha definido una escala de 1 a 5, donde uno es una probabilidad baja de ocurrencia y cinco indica que es muy probable que ocurra.

Para la calificación del impacto se determinó la escala de 1 a 5, donde uno es un inconveniente menor, que no representa un impacto real a la normal operación de la empresa, mientras que cinco representa el impacto de un evento adverso en el que la empresa debe detener su operación.

La fórmula con la que se calculará el riesgo es la siguiente:

$$RIESGO = PROBABILIDAD \times IMPACTO$$ (Curtis & Carey, 2012)

Activo:	Activos de información			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Pérdida o deterioro de archivos físicos	3	4	12	Los documentos físicos pueden perderse durante el transporte o deteriorarse si no son almacenados correctamente.
Eliminación de archivos digitales	4	4	16	La operación o manipulación incorrecta de los documentos digitales podría producir una eliminación o sobre escritura de los mismos.

Desastres naturales	3	3	9	Es posible que existan terremotos o incendios que comprometan este activo. El edificio cuenta con sistemas de detección de incendios y su estructura es antisísmica. Al encontrarse las oficinas en el décimo segundo piso, las probabilidades de que exista afectación por una inundación son prácticamente nulas.
Robos	2	4	8	El riesgo de robo es bajo debido a factores como que las instalaciones de la empresa se encuentran en un sector de la ciudad considerado como seguro y se cuenta con personal de seguridad resguardando el acceso. Adicionalmente, existen activos que tendrían mayor valor para un delincuente, por ejemplo, un computador.
Vandalismo	2	4	8	Al igual que con los robos, la empresa cuenta con seguridad para evitar este tipo de amenaza. Sin embargo, fue considerada debido a las protestas que se dieron durante este año y se pudieron observar actos vandálicos durante las mismas
Sabotaje	1	5	5	Se podría sufrir de sabotaje por parte de la competencia o de un exempleado cuya relación laboral no terminó en buenos términos.

Tabla 1. Amenazas de los Activos de Información

*Probabilidad: 1=Muy baja, 5=Muy alta

*Impacto: 1=Molestia menor, 5=Destrucción total

Activo:	Talento Humano			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Debilidades en la revisión de antecedentes de los empleados	3	4	12	Un empleado podría mentir sobre sus credenciales y calificaciones para realizar ciertas funciones
Phishing	4	5	20	Los empleados podrían recibir correos electrónicos o mensajes instantáneos que simulen ser de una fuente de confianza para convencerlos de entregar sus credenciales de accesos a sistemas.
Ataques de ingeniería social	4	5	20	Los empleados podrían ser convencidos de conectar dispositivos removibles, por ejemplo, discos compactos o dispositivos USB a sus equipos y otorgar así acceso a un atacante.

Tabla 2. Amenazas de Talento Humano

*Probabilidad: 1=Muy baja, 5=Muy alta

*Impacto: 1=Molestia menor, 5=Destrucción total

Activo:	Hardware			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Fallas en componentes internos	4	3	12	Los componentes como los discos duros son susceptibles a fallas debido a golpes o a su desgaste esperado. Para contrarrestar esta amenaza es necesario contar con copias de seguridad.
Fallas de energía	4	3	12	Un corte en la energía eléctrica o cambios en la tensión podrían producir pérdida de información o que los equipos dejen de funcionar.
Pérdida de servicios de comunicación	2	3	6	Fallo en procesos normales de la empresa, perdida de acceso a internet y servicio de telefonía fija.
Robos	4	4	16	Se cuenta con seguridades para evitar el robo de equipos dentro de las instalaciones de la empresa. Sin embargo, es posible que los empleados que tienen equipos portátiles pueden llegar a ser víctimas de robos al trasladarse desde y hacia sus domicilios
Vandalismo	2	4	8	Las instalaciones están resguardadas por personal de seguridad, pero se tiene antecedentes de protestas que han terminado en actos vandálicos.
Sabotaje	1	3	3	Un tercero, un empleado actual de la empresa o un exempleado podrían destruir o dañar equipos de la organización para afectar el normal desarrollo de las actividades de negocio.

Tabla 3. Amenazas del Hardware

*Probabilidad: 1=Muy baja, 5=Muy alta

*Impacto: 1=Molestia menor, 5=Destrucción total

Activo:	Sistemas de Información

Amenaza	Probabilidad	Impacto	Riesgo	Descripción
Uso inadecuado de información de la empresa	3	3	9	Un uso no adecuado de la información podría poner en riesgo la reputación y operaciones de la empresa o de sus clientes.
Accesos no autorizados a sistemas	4	5	20	Un atacante podría ingresar a sistemas de la empresa que no se encuentran correctamente configurados y filtrar información sensible o afectar la integridad de los datos almacenados.
Interceptación de datos	3	4	12	La transmisión de información por medio de protocolos inseguros como HTTP o FTP podría permitir que un atacante intercepte la comunicación y obtenga información sensible.

Tabla 4. Amenazas a los Sistemas de Información

*Probabilidad: 1=Muy baja, 5=Muy alta

*Impacto: 1=Molestia menor, 5=Destrucción total

4.2. Controles aplicables a los activos de la empresa

La norma ISO 27001 en su anexo A presenta 14 dominios para controles de seguridad de los cuales se han escogido 5 para este caso de estudio, de los cuales se evaluarán todos los objetivos de controles:

- A.5 Políticas de Seguridad de la Información
- A.7 Seguridad de Recursos Humanos
- A.8 Control de Activos
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Operaciones de Seguridad
- A.13 Seguridad de las Comunicaciones

En la siguiente tabla se presenta una descripción de cada control.

A.5 Políticas de Seguridad de la Información		
A.5.1 Directivas para Seguridad de la Información		
A.5.1.1	Políticas para Seguridad de Información	Un conjunto de políticas para la Seguridad de la Información debe ser definida, aprobada por la gerencia y socializada con los empleados y partes externas relevantes
A.5.1.2	Revisión de políticas para Seguridad de la Información	Las políticas para la Seguridad de la Información deben ser revisadas en intervalos planificados o cuando ocurran cambios para asegurar que son adecuadas y efectivas.
A.7 Seguridad de Recursos Humanos		
A.7.1 Previo a la contratación		
A.7.1.1	Screening	Verificación de antecedentes penales de todos los candidatos al empleo según las leyes y regulaciones vigentes y proporcional a la información con la que el empleado trabajará.
A.7.1.2	Términos y condiciones del empleo	Se debe indicar por escrito las responsabilidades del empleado con la Seguridad de la Información
A.7.2 Durante la relación laboral		
A.7.2.1	Manejo de Responsabilidades	La Gerencia requiere que todos los empleados apliquen seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización
A.7.2.2	Concientización, educación y entrenamiento en Seguridad de la Información	Todos los empleados deben recibir capacitaciones y entrenamientos según sea relevante para las funciones que el empleado desempeña
A.7.2.3	Procesos disciplinarios	Debe existir una proceso formal y documentado para tomar acciones en contra de un empleado que haya cometido una falta contra la Seguridad de la Información
A.7.3 Terminación y cambio de empleo		

A.7.3.1	Terminación de empleo o cambio de responsabilidades	Se debe definir y comunicar responsabilidades y deberes que el empleado tiene con la Seguridad de la Información de la empresa tras la finalización de la relación laboral.
A.8 Control de Activos		
A.8.1 Responsabilidad con los activos		
A.8.1.1	Inventario de activos	Los activos asociados con la información y su procesamiento deben ser identificados y se debe mantener un inventario de los mismos.
A.8.1.2	Propiedad de activos	Todos los activos deben tener un propietario.
A.8.1.3	Uso aceptable de activos	Reglas documentadas para uso aceptable de la información y los activos asociados.
A.8.1.4	Devolución de activos	Todos los empleados deben regresar los activos de la empresa al terminar su relación laboral.
A.8.2 Clasificación de la Información		
A.8.2.1	Clasificación de información	La información debe ser clasificada en términos de requerimientos legales, valor, criticidad y sensibilidad a exposición no autorizada o modificación.
A.8.2.2	Etiquetado de información	Se deben adoptar procedimientos para etiquetar la información de acuerdo con un esquema adoptado por la empresa.
A.8.2.3	Manipulación de los activos	Se deben adoptar procedimientos para manipular la información de acuerdo con un esquema adoptado por la empresa.
A.8.3 Manejo de medios		
A.8.3.1	Manejo de medios extraíbles	Se deben adoptar procedimientos para manejo de medios extraíbles de acuerdo con un esquema adoptado por la empresa.
A.8.3.2	Descarte de medios	Una vez que los medios ya no sean requeridos se deben descartar

		utilizando procedimientos formales.
A.8.3.3	Transferencia física de medios	Los medios que contengan información deben ser protegidos contra uso no autorizado y corrupción durante el transporte.
A.10 Criptografía		
A.10.1 Controles criptográficos		
A.10.1.1	Política de uso de controles criptográficos	Se debe desarrollar una política de uso de criptografía para protección de la información.
A.10.1.2	Manejo de llaves	Una política de uso, protección y ciclo de vida de llaves criptográficas debe ser desarrollada e implementada.
A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		
A.11.1.1	Seguridad física del perímetro	Se debe definir y proteger áreas de las instalaciones en las que se trabaje o procese información crítica o sensible.
A.11.1.2	Controles físicos de entrada	Las áreas deben protegerse con controles de ingreso apropiados para asegurar que únicamente personal autorizado pueda acceder.
A.11.1.3	Aseguramiento de oficinas, habitaciones e instalaciones	Se debe designar y aplicar seguridad física para oficinas, habitaciones e instalaciones.
A.11.1.4	Protección contra amenazas externas y del ambiente	Se debe designar y aplicar protecciones contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Se debe designar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de entrega y carga	Se debe controlar puntos de acceso como áreas de entregas y carga donde personas no autorizadas puedan entrar a las instalaciones. Si es posible, estos puntos de acceso deben estar

		aislados de lugares donde se procesa información.
A.11.2 Equipos		
A.11.2.1	Ubicación y protección de equipos	Los equipos deben ser protegidos para reducir los riesgos de amenazas ambientales y oportunidades de accesos no autorizados.
A.11.2.2	Soporte de servicios básicos	Los equipos deben estar protegidos de fallos de energía y otras interrupciones causadas por servicios básicos.
A.11.2.3	Seguridad de cableado	Cables que transmitan datos y energía eléctrica deben ser protegidos de ser interceptados, de interferencias y daños.
A.11.2.4	Mantenimiento de equipos	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
A.11.2.5	Remoción de activos	Equipos, información o software no deben ser llevados fuera de las instalaciones sin autorización.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar seguridades a activos que pueden ser llevados fuera de las instalaciones considerando los diferentes riesgos que puedan existir fuera de las instalaciones de la organización.
A.11.2.7	Eliminación segura de equipos	Todos los equipos que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier información sensible o software con licencias haya sido removido y sobre escrito de manera segura antes de ser desechado o reutilizado.
A.11.2.8	Equipos de usuarios desatendidos	Los usuarios deben asegurarse de que los equipos desatendidos tengan protecciones apropiadas.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para papeles y

		soportes de almacenamiento, y una política de pantalla limpia para lugares en los que se procese información.
A.12 Operaciones de Seguridad		
A.12.1 Procedimientos operacionales y responsabilidades		
A.12.1.1	Documentación de procedimientos operativos	Los procedimientos operativos deben estar documentados y disponibles para todos los usuarios que los necesiten.
A.12.1.2	Administración de cambios	Cambios realizados a la organización, procesos de negocios, procesamiento de información y sistemas que afectan la seguridad de la información deben ser controlados.
A.12.1.3	Administración de capacidad	El uso de recursos debe ser monitorizado, ajustado, y deben hacerse proyecciones de requerimientos de capacidad futuros para asegurar el desempeño de los sistemas.
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	Los ambientes de desarrollo, prueba, y los operacionales deben ser separados para reducir los riesgos de accesos no autorizados o cambios a los ambientes de producción.
A.12.2 Protección contra el malware		
A.12.2.1	Controles contra el malware	Controles de detección, prevención y recuperación contra el malware deben ser implementados en combinación de concientización y capacitación al usuario.
A.12.3 Respaldos		
A.12.3.1	Respaldos de información	Copias de seguridad de la información, software e imágenes del sistema deben ser realizadas y probadas regularmente de acuerdo con la política de respaldos de la organización.

A.12.4 Registro de eventos y monitoreo		
A.12.4.1	Registro de eventos	Registros de eventos en los que se graben actividades de los usuarios, excepciones, fallas e información de eventos de seguridad deben producirse, mantenerse y revisarse. regularmente.
A.12.4.2	Protección de la información de registros	La información de los registros debe ser protegida contra alteraciones y accesos no autorizados.
A.12.4.3	Registro de eventos de administradores y operadores	Las actividades de administradores y operadores del sistema deben ser registradas y los registros deben ser protegidos y revisados constantemente.
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de información relevantes dentro de la organización deben ser sincronizados con una única fuente de referencia.
A.12.5 Control de Software operacional		
A.12.5.1	Instalación de software en sistemas operacionales	Se debe implementar procedimientos para controlar la instalación de software en los sistemas operacionales
A.12.6 Administración de vulnerabilidades técnicas		
A.12.6.1	Administración de vulnerabilidades técnicas	Información sobre vulnerabilidades técnicas de sistemas de información debe ser obtenida de manera oportuna. La exposición de la organización a dichas vulnerabilidades debe ser evaluada y medidas adecuadas deben ser tomadas según el riesgo.
A.12.6.2	Restricción de la instalación de software	Reglas para normar la instalación de software por parte de los usuarios deben ser establecidas e implementadas.
A.12.7 Consideraciones de auditoría de Sistemas de Información		
A.12.7.1	Controles de auditoría de Sistemas de la Información	Requerimientos y actividades de auditoría que involucran la verificación de sistemas

		operacionales deben ser planificadas cuidadosamente y acordadas para minimizar la interrupción de los procesos de negocios.
A.13 Seguridad de las Comunicaciones		
A.13.1 Administración de la Seguridad de Red		
A.13.1.1	Controles de Red	Las redes deben ser administradas y controladas para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de servicios de red	Mecanismos de seguridad, niveles de servicio y requerimientos de servicios de red deben ser identificados e incluidos en acuerdos de servicios, tanto si son internos o externalizados.
A.13.1.3	Segregación de redes	Grupos, usuarios y sistemas de información deben estar segregados en la red.
A.13.2 Transferencia de Información		
A.13.2.1	Políticas y procedimientos de transferencia de información	Políticas formales de transferencia, procedimientos y controles deben determinados para proteger la transferencia de información.
A.13.2.2	Acuerdos de transferencia de información	Acuerdos para la transferencia segura de información del negocio entre la organización y terceros.
A.13.2.3	Mensajería electrónica	La información involucrada en mensajería electrónica debe ser protegida apropiadamente.
A.13.2.4	Confidencialidad y acuerdos de no divulgación	Requerimientos de confidencialidad y acuerdos de no divulgación que reflejen las necesidades de protección de información de la organización deben ser identificados, documentados y revisados regularmente.

Tabla 5. Controles del Anexo A de la Norma ISO 27001 (ISO, 2022)

4.3. Evaluación de Controles

A continuación, se presenta un resumen de la evaluación realizada en base a los controles que establece el Anexo A de la norma ISO 27001. Para realizar esta evaluación se tomó en consideración el texto del control y se determinó si la empresa actualmente lo cumple, no lo cumple o si el control no aplica para el activo junto con un comentario.

CONTROL		CUMPLE			COMENTARIO
		SI	NO	N/A	
A.5 Políticas de Seguridad de la Información					
A.5.1 Directivas para Seguridad de la Información					
A.5.1.1	Políticas para Seguridad de Información		X		La empresa no cuenta con documentación acerca de la Seguridad de la Información del activo
A.5.1.2	Revisión de políticas para Seguridad de la Información		X		Debido a que no se cuenta con documentación específica sobre S.I, no es posible realizar una revisión constante.
A.7 Seguridad de Recursos Humanos					
A.7.1 Previo a la contratación					
A.7.1.1	Screening	X			Se realiza una investigación dentro de los límites permitidos por la legislación ecuatoriana.
A.7.1.2	Términos y condiciones del empleo	X			Se menciona en el contrato que el empleado tiene responsabilidades con la seguridad de la información de la empresa, sin embargo, se podría ser más específicos.
A.7.2 Durante la relación laboral					
A.7.2.1	Manejo de Responsabilidades		X		Se cuenta con documentación sobre las responsabilidades de los empleados, sin embargo, se requiere algo más específico sobre seguridad de la información.
A.7.2.2	Concientización, educación y entrenamiento		X		Los empleados no están recibiendo entrenamientos o

	en Seguridad de la Información				capacitaciones sobre Seguridad de la Información
A.7.2.3	Procesos disciplinarios		X		Se menciona en el contrato de los empleados que existen procesos disciplinarios mas no son específicos para un caso de una brecha de seguridad.
A.7.3 Terminación y cambio de empleo					
A.7.3.1	Terminación de empleo o cambio de responsabilidades	X			Existe documentación, pero se debe profundizar en las responsabilidades que conciernen específicamente} a la Seguridad de la Información.
A.8 Control de Activos					
A.8.1 Responsabilidad con los activos					
A.8.1.1	Inventario de activos	X			La empresa cuenta con un inventario de activos, sin embargo, se podría mejorar el registro de activos como documentos físicos.
A.8.1.2	Propiedad de activos	X			Este proceso se encuentra detallado para activos de hardware como servidores, computadores y equipos de redes. Los empleados conocen con claridad cuales dispositivos se encuentran a su cargo. Se puede mejorar este proceso para activos de información como documentos físicos.
A.8.1.3	Uso aceptable de activos		X		Se requiere documentar políticas de uso aceptable para todos los activos.
A.8.1.4	Devolución de activos	X			Para los activos como computadoras, se cuenta con un proceso en el que el empleado al ser desvinculado devuelve el equipo y recibe una constancia por escrito de la devolución. Se requiere implementar un proceso para activos de información.
A.8.2 Clasificación de la Información					

A.8.2.1	Clasificación de información	X			La información de la empresa se encuentra clasificada correctamente según criterios establecidos por las áreas de la empresa.
A.8.2.2	Etiquetado de información	X			La información de la empresa se encuentra etiquetada correctamente según criterios establecidos por las áreas de la empresa.
A.8.2.3	Manipulación de los activos		X		Existen expectativas para los empleados sobre cómo manejar correctamente los activos, sin embargo, no existe un documento formal en el que se indique los correctos procedimientos.
A.8.3 Manejo de medios					
A.8.3.1	Manejo de medios extraíbles		X		La empresa no cuenta con procedimientos para el manejo de medios extraíbles.
A.8.3.2	Descarte de medios		X		La empresa no cuenta con procedimientos para el descarte de medios.
A.8.3.3	Transferencia física de medios		X		La empresa no cuenta con procedimientos para la transferencia física de medios extraíbles.
A.10 Criptografía					
A.10.1 Controles criptográficos					
A.10.1.1	Política de uso de controles criptográficos		X		La empresa no cuenta con una política que rija el uso de controles criptográficos.
A.10.1.2	Manejo de llaves	X			Se cumple parcialmente. Los empleados utilizan ciertas claves criptográficas. En general se intenta utilizar contraseñas robustas. No se realizan respaldos de las claves.
A.11 Seguridad física y del entorno					
A.11.1 Áreas seguras					
A.11.1.1	Seguridad física del perímetro	X			Las instalaciones de la empresa se encuentran en un sector

					considerado como seguro en la ciudad. Las puertas de las oficinas cuentan con cerraduras. El servidor de la empresa y ciertos equipos de red se encuentran en un rack con cerradura y con acceso restringido.
A.11.1.2	Controles físicos de entrada	X			El edificio cuenta con un punto de control en la entrada protegido por personal de seguridad y video vigilancia.
A.11.1.3	Aseguramiento de oficinas, habitaciones e instalaciones	X			Las instalaciones cuentan con medidas de seguridad para evitar accesos no permitidos.
A.11.1.4	Protección contra amenazas externas y del ambiente	X			El edificio cuenta con un sistema contra incendios, escaleras de emergencia y su estructura es antisísmica.
A.11.1.5	Trabajo en áreas seguras	X			No se identifican potenciales peligros en las áreas de trabajo.
A.11.1.6	Áreas de entrega y carga	X			Las entregas y descargas se realizan en la recepción del edificio y en el parqueadero. Ambos lugares se encuentran custodiados por personal de seguridad.
A.11.2 Equipos					
A.11.2.1	Ubicación y protección de equipos	X			La ubicación de equipos es adecuada para evitar daños por amenazas física y desastres naturales.
A.11.2.2	Soporte de servicios básicos y suministro	X			Los equipos tecnológicos de la empresa cuentan con UPS y existe suministro de equipos para garantizar cierto nivel de redundancia en las operaciones.
A.11.2.3	Seguridad de cableado	X			El manejo de cables en las oficinas es adecuado. No existen cables expuestos que transporten datos y/o electricidad.
A.11.2.4	Mantenimiento de equipos	X			Se realizan mantenimientos a los equipos. Algunos equipos se encuentran asegurados.

A.11.2.5	Remoción de activos		X		No se cuenta con documentación sobre procedimientos de traslado de activos de la empresa. Se deben establecer políticas y procedimientos.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		X		Se requiere definir una política sobre la utilización de equipos fuera de la empresa.
A.11.2.7	Eliminación segura de equipos	X			La información de los equipos es borrada antes de ser descartados o reutilizados por otro empleado.
A.11.2.8	Equipos de usuarios desatendidos	X			Los equipos como computadoras se encuentran configurados para bloquearse después de cierto periodo de inactividad. Se solicita a los empleados que bloqueen sus terminales, o cierren la tapa al tratarse de computadoras portátiles, antes de abandonar temporalmente su puesto de trabajo.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	X			Se observa que los empleados cumplen con no dejar información que podría ser sensible en sus escritorios. Sin embargo, este proceso debe ser documentado. Se debe designar un triturador de papeles específico para la destrucción de documentos con información confidencial.
A.12 Operaciones de Seguridad					
A.12.1 Procedimientos operacionales y responsabilidades					
A.12.1.1	Documentación de procedimientos operativos	X			Existe documentación y manuales con respecto a procedimientos del servidor y a documentos físicos de la empresa. Se recomienda ampliar esta documentación.
A.12.1.2	Administración de cambios	X			Este control se cumple parcialmente pues se controlan cambios al servidor y a los sistemas de información.

A.12.1.3	Administración de capacidad	X			Se cuentan con métricas sobre los recursos de los activos informáticos. Como mejora, se podría centralizar esta información.
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción			X	Control no aplicable debido al giro del negocio de la empresa.
A.12.2 Protección contra el malware					
A.12.2.1	Controles contra el malware	X			Los equipos informáticos como el servidor y computadoras de empleados cuentan con software antivirus actualizado.
A.12.3 Respaldos					
A.12.3.1	Respaldos de información	X			En el caso de los activos como el servidor y computadoras se realizan copias de seguridad, sin embargo, este proceso es manual. Se debe levantar un proceso para realizar copias de seguridad de la información de manera automatizada.
A.12.4 Registro de eventos y monitoreo					
A.12.4.1	Registro de eventos	X			Existe un control de logs producidos en por los activos informáticos de la empresa.
A.12.4.2	Protección de la información de registros		X		No se cuenta con un mecanismo que garantice la integridad de los registros.
A.12.4.3	Registro de eventos de administradores y operadores	X			La actividad de todos los usuarios en el servidor se encuentra registrada y es monitorizada.
A.12.4.4	Sincronización de relojes	X			Los relojes de los equipos se encuentran sincronizado con servidores NTP corporativos de los proveedores.
A.12.5 Control de Software operacional					

A.12.5.1	Instalación de software en sistemas operacionales	X			Únicamente usuarios con privilegios administrativos pueden instalar software en los equipos.
A.12.6 Administración de vulnerabilidades técnicas					
A.12.6.1	Administración de vulnerabilidades técnicas		X		No se cuenta con información sobre vulnerabilidades técnicas.
A.12.6.2	Restricción de la instalación de software	X			Únicamente usuarios con privilegios administrativos pueden instalar software en los equipos. Los usuarios pueden instalar aplicativos que no requieran permisos administrativos.
A.12.7 Consideraciones de auditoría de Sistemas de Información					
A.12.7.1	Controles de auditoría de Sistemas de la Información		X		No existen procedimientos sobre auditoría a Sistemas de Información.
A.13 Seguridad de las Comunicaciones					
A.13.1 Administración de la Seguridad de Red					
A.13.1.1	Controles de Red	X			Existen controles para la red a la que se encuentra conectado este activo
A.13.1.2	Seguridad de servicios de red		X		Se requiere definir y documentar niveles de servicio y requerimientos administrativos.
A.13.1.3	Segregación de redes	X			El activo se encuentra en una red segregada.
A.13.2 Transferencia de Información					
A.13.2.1	Políticas y procedimientos de transferencia de información		X		Se requiere definir y documentar procedimientos de transferencia de información para este activo.
A.13.2.2	Acuerdos de transferencia de información		X		Se requiere definir y documentar acuerdos de transferencia de información para este activo.
A.13.2.3	Mensajería electrónica		X		

A.13.2.4	Confidencialidad y acuerdos de no divulgación	X			Los empleados firman un acuerdo de no divulgación durante su contratación

Tabla 6. Evaluación de Controles del Anexo A de la Norma ISO 27001

4.4 Acciones a ser tomadas por la empresa para el tratamiento del riesgo

Tratamiento del riesgo

Tras haber realizado la evaluación del riesgo se presenta a continuación acciones que la empresa necesita tomar para reducir la posibilidad de un evento adverso. La empresa debe priorizar las amenazas que tienen el número de riesgo más alto.

Activos de Información

Activo:	Activos de información			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Eliminación de archivos digitales	4	4	16	La operación o manipulación incorrecta de los documentos digitales podría producir una eliminación o sobre escritura de los mismos.
Pérdida o deterioro de archivos físicos	3	3	9	Los documentos físicos pueden perderse durante el transporte o deteriorarse si no son almacenados correctamente.
Desastres naturales	3	3	9	Es posible que existan terremotos o incendios que comprometan este activo. El edificio cuenta con sistemas de detección de incendios y su estructura es antisísmica. Al encontrarse las oficinas en el decimo segundo piso, las probabilidades de que exista afectación por una inundación son prácticamente nulas.
Robos	2	4	8	El riesgo de robo es bajo debido a factores como que las instalaciones de la empresa se encuentran en un sector de la ciudad considerado como seguro y se cuenta con personal de seguridad resguardando el acceso. Adicionalmente, existen activos que tendrian mayor valor para un delincuente, por ejemplo un computador.
Vandalismo	2	4	8	Al igual que con los robos, la empresa cuenta con seguridad para evitar este tipo de amenza. Sin embargo, fue considerada debido a las protestas que se dieron durante este año y se pudieron observar actos vandálicos durante las mismas

Sabotaje	1	5	5	Se podría sufrir de sabotaje por parte de la competencia o de un ex empleado cuya relación laboral no terminó en buenos términos.

Tabla 7. Riesgos prioritarios para los Activos de Información

Para eliminar los riesgos con mayor calificación del activo es necesario contar con procedimientos de respaldo de la información

Copias de Seguridad y redundancia:

Es necesario crear una política de copias de seguridad, definiendo qué información es crítica para la operación del negocio y almacenarla en un repositorio centralizado del cual se creen copias automáticas de seguridad, tanto locales como off-site, con una frecuencia razonable de acuerdo con la necesidad de la empresa. Se debe validar que las copias de seguridad se creen correctamente. Es posible contratar servicios de respaldos de terceros.

Documentos físicos:

Se debe evaluar de que documentos físicos se pueden realizar copias, y cuáles pueden ser digitalizados para tener un respaldo. Es importante tener en cuenta que las copias simples de ciertos documentos no tienen validez legal, por lo que se requiere asesoría en el tema para definir una estrategia de respaldo.

Talento Humano

Activo:	Talento Humano			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Phishing	4	5	20	Los empleados podrían recibir correos electrónicos o mensajes instantaneos que simulen ser de una fuente de confianza para convencerlos de entregar sus credenciales de accesos a sistemas.
Ataques de ingeniería social	4	5	20	Los empleados podrian ser convencidos de conectar dispositivos removibles, por ejemplo, discos compactos o dispositivos USB a sus equipos y otorgar así acceso a un atacante.

Debilidades en la revisión de antecedentes de los empleados	3	4	12	Un empleado podría mentir sobre sus credenciales y calificaciones para realizar ciertas funciones

Tabla 8. Riesgos prioritarios para Talento Humano

Para el activo de Talento Humano se identificaron dos riesgos con mayor calificación: Ataques de Phishing y Ataques de Ingeniería Social.

La manera de reducir estos riesgos es mediante la capacitación del talento humano. Uno de los casos más relevantes en el presente año fue el hackeo a la empresa Uber. El atacante habría obtenido acceso a los sistemas enviando un mensaje de texto a un empleado en el que se le solicitaba su contraseña.

Es importante prevenir a los usuarios para que puedan reconocer la legitimidad de un mensaje.

Hardware:

Activo:	Hardware			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Robos	4	4	16	Se cuenta con seguridades para evitar el robo de equipos dentro de las instalaciones de la empresa. Sin embargo, es posible que los empleados que tienen equipos portatiles pueden llegar a ser víctimas de robos al trasladarse desde y hacia sus domicilios
Fallas en componentes internos	4	3	12	Los componentes como los discos duros son suceptibles a fallas debido a golpes o a su desgaste esperado. Para contrarestar esta amenza es necesario contar con copias de seguridad.
Fallas de energía	4	3	12	Un corte en la energía electrica o cambios en la tensión podrian producir pérdida de información o que los equipos dejen de funcionar.
Vandalismo	2	4	8	Las instalaciones está resguardadas por personal de seguridad pero se tiene antecendentes de protestas que han terminado en actos vandálicos.

Pérdida de servicios de comunicación	2	3	6	Fallo en procesos normales de la empresa, perdida de acceso a internet y servicio de telefonía fija.
Sabotaje	1	3	3	Un tercero, un empleado actual de la empresa o un ex-empleado podrian destruir o dañar equipos de la organización para afectar el normal desarrollo de las actividades de negocio.

Tabla 9. Riesgos prioritarios para activos de Hardware

Para los activos de hardware se consideró el robo como la mayor amenaza. Se recomienda asegurar los equipos portátiles que los empleados llevan a casa para trabajar. Para las fallas en componentes internos se recomienda establecer un plan de mantenimiento preventivo y mantener copias de seguridad de la información almacenada en los computadores.

Sistemas de Información

Activo:	Sistemas de Información			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Descripción**
Accesos no autorizados a sistemas	4	5	20	Un atacante podría ingresar a sistemas de la empresa que no se encuentran correctamente configurados y filtrar información sensible o afectar la integridad de los datos almacenados.
Interceptación de datos	3	4	12	La transmisión de información por medio de protocolos inseguros como HTTP o FTP, podria permitir que un atacante intercepte la comunicación y obtenga información sensible.
Uso inadecuado de información de la empresa	3	3	9	Un uso no adecuado de la información podría poner en riesgo la reputación y operaciones de la empresa o de sus clientes.

Tabla 10. Riesgos prioritarios para los Sistemas de Información

Se observa que la amenaza con mayor riesgo es el acceso no autorizado a los sistemas. Para evitar la materialización de esta amenaza se requiere definir una política de uso de contraseñas, con longitudes mínimas y complejidad establecida, así como definir el uso de gestores de contraseñas y autenticación de múltiple factor para los servicios que soportan esta tecnología.
Se recomienda establecer una política de auditoría a Sistemas de Información en la que se establezca criterios que deben ser evaluados y la frecuencia con la que se debe hacerlo.

Recomendaciones adicionales

Se recomienda principalmente documentar por escrito todos los procesos de la empresa de manera clara y precisa. Existen controles con los que la empresa está cumpliendo, pero se requiere un sustento escrito de estos controles.

Control de Activos:

Se debe redactar una política de uso aceptable de cada activo para que los empleados puedan tener una constancia de que actividades puede realizar con los activos y qué expectativas tiene el empleador con respecto a la seguridad de la información cuando el empleado maneja estos activos.
Se requiere implementar una política de relacionada a medios extraíbles (CD, memorias flash, discos duros externos, etc.) para indicar que tienen permitido realizar los empleados con estos dispositivos y cuáles son sus responsabilidades al utilizarlos.
Se debe definir una política y procedimientos para transportar información de la empresa, no solo digital, si no tambien física. Por ejemplo, definir una empresa de transporte con la que se enviarán todos los documentos que se requieran.

Criptografía:

Todos los equipos informáticos deben tener su unidad principal de almacenamiento cifrada. Es necesario definir una política con respecto al uso de firmas electrónicas.

Políticas de escritorio y pantalla limpios:

A pesar de que se puede apreciar un cumplimiento de estas políticas en la empresa, es necesario contar con una política documentada de escritorio y pantalla limpia para que los empleados conozcan su responsabilidad sobre no dejar documentos que contienen información sensible a vista otras personas.

Logs y métricas:

Se presenta como oportunidad de mejora la centralización de registros (logs) y métricas producidas por los sistemas informáticos para facilitar su monitorización y auditoria, estableciendo la frecuencia con la que se revisarán. Así mismo, se debe definir periodos de retención y métodos para garantizar la integridad de esta información.

Mensajería electrónica

Se requiere crear una política de seguridad de correo electrónico en la que se defina que comunicaciones son aceptables por este medio y periodos de retención de los mensajes de correo electrónico según una categorización.

Se requiere adoptar una solución de mensajería instantánea corporativa que maneje estándares de seguridad, por ejemplo, Microsoft Teams, Slack, Cisco Webex, etc.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5. Conclusiones y recomendaciones

5.1 Conclusiones

- Se concluye que tras haber realizado una evaluación de la situación de la empresa con respecto a la Seguridad de la Información que la empresa tiene ciertas prácticas acertadas al manejar información, sin embargo, existen debilidades que necesitan ser corregidas para evitar el impacto de la materialización de las amenazas identificadas.
- Fue posible identificar oportunidades de mejora en los procesos internos de manejo de la información de la empresa, por ejemplo, definiendo políticas que deben ser socializadas con los empleados de la empresa con la finalidad de que conozcan sus responsabilidades con respecto a la seguridad de la información.
- Tras la realización de este trabajo de investigación se determinó que existen amenazas a los activos de la empresa cuyo riesgo debe ser reducido o mitigado para prevenir afectación a la normal operación del negocio.

5.2 Recomendaciones

- Se recomienda revisar los procesos de la empresa y redactar documentación clara y precisa sobre los mismos.
- Se recomienda analizar los controles restantes del anexo A de la norma ISO/IEC 27001 para encontrar nuevas oportunidades de mejora con respecto a la Seguridad de la Información.
- Se recomienda a la empresa realizar una evaluación más exhaustiva que permita en un futuro obtener la certificación ISO 27001.

BIBLIOGRFÍA

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case. *Journal of Cybersecurity and Privacy*, 219-238.

Fortinet. (2022). *What is the Information Security Triad?* Fortinet: https://www.fortinet.com/resources/cyberglossary/cia-triad

Government of the UK. (2017). Information Asset factsheet. *The National Archives* .

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials, 17*(4), 2242.

Mejía Medina, M. (2019). Implementación de Técnicas de Seguridad Informática para garantizar los prinicipios de Integridadd, Confidencialidad y Disponibilidad de la iInformacion a un Sistema de Radiolocalización Híbrido. Universidad Pontificia Bolivariana.

International Organization for Standardization. (Octubre de 2022). ISO/IEC 27005:2022. *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

International Organization for Standarization. (01 de octubre de 2013). ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*.

International Organization for Standarization. (Febrero de 2018). ISO/IEC 27000:2018. *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

Hyseni, V. (25 de Octubre de 2022). *ISO/IEC 27001 - What are the main changes in 2022?* PECB University.

International Organization for Standarization. (Febrero de 2022). ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*.

Kosustic, D. (2021). *Catalogue of threats & vulnerabilities*. 27001 Academy - Advisera.