UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

AUDITORIA INFORMÁTICA PARA EL ANÁLISIS DE LA SEGURIDAD EN LOS RECURSOS INFORMÁTICOS UTILIZANDO NORMAS ISO 27001 EN MEGAKONS S.A.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en tecnologías de la información.

ÁREA: Gestión de tecnologías de la información.

LÍNEA DE INVESTIGACIÓN: Tecnologías de la información y Sistemas de control.

AUTOR: Marco Orlando Tenezaca Caizabanda

TUTOR: Ing. Julio Enrique Balarezo López, PhD.

Ambato - Ecuador

febrero – 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: AUDITORIA INFORMÁTICA PARA EL ANÁLISIS DE LA SEGURIDAD EN LOS RECURSOS INFORMÁTICOS UTILIZANDO NORMAS ISO 27001 EN MEGAKONS S.A. desarrollado bajo la modalidad Proyecto de Investigación por el señor Marco Orlando Tenezaca Caizabanda, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado 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, febrero 2024

Ing. Julio Enrique Balarezo López, PhD.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: AUDITORIA INFORMÁTICA PARA EL ANÁLISIS DE LA SEGURIDAD EN LOS RECURSOS INFORMÁTICOS UTILIZANDO NORMAS ISO 27001 EN MEGAKONS S.A. 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, febrero 2024

Marco Orlando Tenezaca Caizabanda

C.C. 1804143681

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, febrero 2024

Marco Orlando Tenezaca Caizabanda

C.C. 1804143681

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Marco Orlando Tenezaca Caizabanda estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado AUDITORIA INFORMÁTICA PARA EL ANÁLISIS DE LA SEGURIDAD EN LOS RECURSOS INFORMÁTICOS UTILIZANDO NORMAS ISO 27001 EN MEGAKONS S.A., 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, febrero 2024

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

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

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Chicaiza Castillo, Mg
PROFESOR CALIFICADOR

Firmado electrónicamente por:
VICTOR HUGO GUACHIMBOSA VILLALBA

Ing. Victor Guachimbosa Villalba, PhD
PROFESOR CALIFICADOR

DEDICATORIA

A mi madre por su apoyo incondicional en cada etapa de mi vida, su amor comprensión y su esfuerzo que me han hecho llegar hasta esta etapa de mi vida, a mi padre por ser un guía en mi vida personal y académica, a mi hermana por siempre estar en los momentos más difíciles de mi vida, a mi hija que desde el cielo ha sido una motivación para seguir adelante, a Tinna por estar a mi lado y ser un apoyo emocional a diario y a mis amigos por su aliento constante durante esta travesía académica. Esta tesis está dedicada a ustedes, como un sincero agradecimiento por formar parte de mi viaje académico y personal.

AGRADECIMIENTO

Agradezco sinceramente a mi tutor de proyecto de titulación por su guía a lo largo de este proceso, a mis padres por el esfuerzo durante todos estos años de estudio.

.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

En la actualidad la seguridad de la información es un campo fundamental dentro de toda organización, por lo cual su tratamiento necesita tener un análisis profundo para poder garantizar su uso de una forma óptima y segura. En la empresa MEGAKONS S.A. existe un deficiente control y seguimiento de seguridad de la información dentro de sus equipos informáticos, por lo cual pueden existir varias brechas de seguridad las cuales provocaría robo o perdida de los activos informáticos. El siguiente proyecto tiene como finalidad evaluar el sistema de gestión de seguridad de la empresa MEGAKONS S.A. basándose en los controles que posee la norma ISO (Organización Internacional de Normalización) 27001 y todas las políticas a cumplir. Para lo cual se inició analizando los requerimientos de un buen sistema de gestión de seguridad de la información (SGSI), para así obtener mejores resultados dentro de la evaluación. Luego se recolecto información necesaria mediante dos instrumentos de recolección de la información para analizar el estado actual en conocimiento de la seguridad de la información por parte de los empleados y encargados del área de TI (tecnologías de la información). Se utilizo la metodología PDCA (Plan, Do, Check, Act), basada en el ciclo de Deming que se construye de 4 fases (Planear, Hacer, Verificar, Actuar), la cual ayuda a tener una mejor organización al momento de evaluar los diferentes controles de la norma, en la planificación se desarrolla el alcance y las actividades a desarrollar dentro de la evaluación, en la segunda fase se desarrollan las actividades planificadas, en la tercera fase se evalúa los resultados de las actividades. Después de la evaluación de todos los controles del ANEXO A de la norma ISO 27001, se generó un informe en el cual se detalla todos los hallazgos encontrados y emitir conclusiones y recomendaciones. las cuales ayudaran a una mejora continua dentro de la empresa.

Palabras clave: SGSI, Sistema de gestión de seguridad de la información, auditoria informática, ISO 27001, TI.

ABSTRACT

Currently, information security is a fundamental field within every organization, requiring a thorough analysis to ensure its optimal and secure use. MEGAKONS S.A. lacks effective control and monitoring of information security within its computer systems, potentially leading to various security breaches that could result in theft or loss of IT assets. The objective of the following project is to evaluate the security management system of MEGAKONS S.A., based on the controls outlined in the ISO (International Organization for Standardization) 27001 standard and all associated policies. The project began by analyzing the requirements of a robust Information Security Management System (ISMS) to achieve better results in the evaluation. Information was gathered using two data collection instruments to analyze the current level of awareness regarding information security among employees and IT personnel. The PDCA methodology (Plan, Do, Check, Act), based on the Deming cycle consisting of four phases (Plan, Do, Check, Act), was employed. This methodology aids in better organization when assessing different standard controls. The planning phase involves defining the scope and activities for the evaluation, the second phase involves executing the planned activities, and the third phase assesses the results of these activities. Following the evaluation of all controls in Annex A of the ISO 27001 standard, a report was generated detailing all findings and issuing conclusions and recommendations. These findings and recommendations will contribute to continuous improvement within the company.

Keywords: SGSI, Information Security Management System, IT audit, ISO 27001, TI.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

AUDITORIA INFORMÁTICA PARA EL ANÁLISIS DE LA SEGURIDAD EN LOS RECURSOS INFORMÁTICOS UTILIZANDO NORMAS ISO 27001 EN MEGAKONS S.A.

1.1.1 Planteamiento del problema

El uso de las TIC (Las Tecnologías de la Información y las Comunicaciones) a nivel mundial se ha convertido en parte importante de las empresas, los procesos que llevan a cabo las Tecnologías de la Información y las Comunicaciones buscan lograr eficacia y eficiencia en los procesos que con llevan recursos informáticos y así mejorar la calidad de vida y a su vez lograr cumplir los objetivos de la organización donde se está aplicando. [1]

En los últimos años la seguridad informática ha comenzado a ganar importancia y popularidad, es así como dejo de ser vista como un gasto extra a ser vista como una inversión por parte de las grandes y pequeñas empresas. Lamentablemente a nivel mundial son pocos los países que implementaron esta seguridad en sus empresas, sin embargo, debido al nuevo mundo digital es casi una obligación el contar con normativas y procedimientos que ayuden a las empresas a mejorar su seguridad informática.[2]

En Ecuador a raíz de la emergencia sanitaria mundial del Covid-19, las empresas comenzaron a utilizar las TIC para así mejorar sus procesos y evitar el trabajo presencial, lo cual logró ser de ayuda para empleados, porque por medio de estos cambios las personas adaptaron una nueva forma de pensar y así evolucionan tecnológicamente y para los empleadores el saber que el mejorar los recursos y procesos tecnológicos le reduce muchos gastos a corto o largo tiempo. Uno de los ejemplos más claros son los servicios en línea que hoy en día se ofrecen en la mayoría de las entidades públicas y privadas del Ecuador.[3]

A nivel de Ambato son pocas las empresas que tienen incorporado las TIC vinculados a la seguridad de la información. Si bien se tiene conocimiento de ciertas maneras de resguardar la información estas no están documentadas o asignadas de la mejor manera, esto hace que tengan problemas en seguridad y también gastos innecesarios los cuales muchas veces el estado no puede sustentar. No utilizar los procesos y metodologías que nos ofrece las TIC nos genera un retraso a nivel tecnológico porque no se aprovecha ni se asegura la información al 100%.

En la empresa MEGAKONS S.A. existen ciertos protocolos de seguridad de la información sin embargo existen ciertos controles que no se aplican o que no existen dentro del SGSI y del cual es importante llevar un control y mantenimiento y tener una mejora para no tener futuros problemas de un ataque cibernético o perdida de información importante, por lo cual una auditoria informática seria esencial para identificar las falencias y las brechas de seguridad que existen.

1.2 Antecedentes investigativos

Según Z. Wendy Gabriela [4] .Su objetivo es verificar la calidad de los procesos de la Gestión Financiera y económica de la organización y a su vez evaluar la entrega de los servicios requeridos desde dicha gestión y que interfieran directamente con las TI todo esto utilizando las normas COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas).

Una vez realizado el análisis de todos los procesos se concluyó que dicho GAD (Gobierno Autónomo Descentralizado) no aprovecha todos los recursos informáticos ni tampoco integra las estrategias de negocios y de TI. Si la organización implementara las TI en sus departamentos podría sacar un gran beneficio y a su vez menorar costos adicionales que pueden verse reflejados en compras de implementos informáticos.

Según R. Carlos [5]. Su objetivo principal fue realizar una auditoria informática la cual ayudaría a evaluar la situación actual del GAD de Ambato y así proponer un plan para mejorar las prácticas y obtener una mayor integridad, confidencialidad y confiablidad de la información lo cual se dio con existo y se utilizó la metodología COBIT 5.0. El analizar la situación de una organización mediante una auditoria informática ayuda a la empresa a tener más credibilidad y mejorar en sus procesos.

Según T. Moposita Jorge Luis[6]. Elaboro un plan de gestión de seguridad informática el cual ayuda a mejorar el control de la información y la seguridad de cada sistema de la empresa, en este documento se basa en las normas ISO 27001 las cuales según el análisis del investigador son las que más se ajustan para dicha empresa, el proceso con el que el investigador comienza es analizando el estado de la empresa a nivel de seguridad informática después realizado ciertas evaluaciones en cada departamento y por ultimo genera un plan estratégico adecuado para mejorar la seguridad.

Según B. Christian Andres [7]. Analizo las vulnerabilidades que existen en toda la infraestructura tecnológica de dicha institución una vez que se analice se propuso un plan de contingencia informática basado en la norma ISO 27001:2013 el cual según el investigador es el que más se ajusta a dicha institución. Con esto el investigador busca disminuir los riesgos y gastos asociados y también que dicha institución aumente su competitividad y confianza entre las demás instituciones.

Según B. Jefersson Vinicio [8].El tener un mejor control de seguridad ayuda a salvaguardar la disponibilidad, integridad y confidencialidad de la información a su vez en caso de no tener un mejor control existirían brechas de seguridad las cuales provocarían gastos innecesarios y desprestigio de dicha empresa. El utiliza la metodología NIST (Instituto Nacional de Estándares y Tecnología) 800-115 ayuda a diseñar un buen proceso de gestión de

vulnerabilidades técnicas las cuales son responsabilidad de las personas que están involucradas en el área de TI.

1.3 Fundamentación teórica

1.3.1 Normas ISO 27001

Las normas ISO 27001 son normas que ayudan a mantener un sistema de gestión de seguridad de la información, el cual fue publicado por primera vez en el año 2005 por la International Organization for Standardization y por la International Electrotechnical Commission. Esta norma se trataba de una serie de mejores prácticas para ayudar a las empresas británicas a administrar mejor la seguridad de la información.[9]

Estas normas auxilian a las empresas a cumplir los requerimientos legales para su funcionamiento y así eludir la vulneración de la legislación o el incumplimiento de toda obligación legal de las entidades de cualquier requisito de seguridad. [10]

1.3.2 Leyes de propiedad intelectual

Según el Art.1. de la Ley de propiedad intelectual el estado reconoce, regula y garantiza la propiedad intelectual que comprende a: los derechos de autor y derechos anexos. Con esto se prohíbe la copia, duplicado o transformación de algún documento sin consentimiento del autor. Entonces si se utiliza algún tipo de software y no esta licenciada estaríamos incumpliendo dicha norma.

La ley orgánica de protección de datos personales estipulada en el 2021 hace referencia a la garantía que ofrece el país sobre el uso indebido de los datos personales es decir ofrece protección de estos.[11]

Estas leyes aprobadas en Ecuador tienen el propósito de generar tranquilidad tanto a las empresas como a los usuarios al momento de manipular o dar algún tipo de información personal, también permite que las empresas que utilizan software pagado cumplan con pagar los servicios prestados y así no exista un plagio de ningún tipo, con esto las empresas también se aseguran de que la información que tiene no sea robada o mal manipulada.

1.3.3 Auditoria informática con Normas ISO 27001

Segundo ISO 2700, una auditoria es un proceso sistemático independiente y documentado para poder obtener las evidencias de auditoría y evaluar objetivamente con el fin de determinar el grado en el que se cumplen algunos procesos. [12]

La utilidad de estas auditorias es incuestionable, a través de estas se puede comprobar si el SGSI es eficaz. Esta auditoria se puede realizar por un miembro de la misma empresa siempre y cuando este cualificado para esta actividad.[13]

1.3.4 Auditoria TI

Una auditoria informática tiene como objetivo valorizar los sistemas informáticos de alguna organización en particular, el resultado de una auditoria es un informe el cual detalla en qué nivel se encuentra la organización. En otras palabras, toda la informática que existe en la organización debe cumplir ciertos estándares de eficiencia.[14]

Entre las características que debe tener una auditoria informática son:

- Una auditoria informática debe ser realizada por profesional capacitado.
- La evaluación debe ir más allá que el estudio de los activos informáticos físicos debe abarcar la práctica y el uso de las plantillas.
- Debe existir un constante seguimiento en las actualizaciones informáticas del mercado y su aplicación empresarial.

1.3.5 Auditoría externa

Para este tipo de auditoria se necesita una persona ajena a la empresa (Auditor Externo), el cual verificara el cumplimiento de los requisitos legales establecidos. El beneficio principal de esta auditoria es tener un resultado imparcial, objetivo y crítico.[15]

Entre sus características importantes tenemos:

- Los auditores se mantienen independientes de la empresa para preventivamente evitar conflictos de interés.
- Las compañías acceden a una perspectiva externa y profesionalizada sobre sus finanzas mediante este servicio.
- La función del auditor incluye la identificación de áreas de mejora, lo que permite una mayor eficiencia y optimización de los procesos empresariales.
- Los auditores tienen la obligación de reportar cualquier negligencia o incumplimiento de normativas que detecten.[16]

1.3.6 Seguridad Informática

La seguridad informática puede definirse como un proceso para prevenir y detectar el uso no autorizado de un sistema informático, esto implica proteger a los sistemas o recursos informáticos de terceros que quieran hacer uso inapropiado del mismo. Abarca una seri de medidas como software de antivirus, firewalls y otras medidas que depende del usuario tales como activaciones de ciertas funciones en el software.[17]

Las áreas que debe cubrir la seguridad informática son:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación

1.3.7 Tecnologías de la información

Las tecnologías de la información engloban todo el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos. Las TI están conformada por software, apoyo organizativo y metodológico y de hardware informático.[18]

1.3.8 Gestión empresarial

Se define como el proceso que dirige y guía las operaciones de una organización para hacer realidad los objetivos establecidos. En otras palabras, en un área que se encarga de organizar los recursos que tiene una empresa para poder sacarle el mejor provecho posible y así llegar a los objetivos que tiene dicha empresa. Esta gestión pasa por un proceso de planeación, organización, integración, direccionamiento para así controlar los recursos tanto humanos, materiales, financieros entre otro.[19]

1.3.9 Gestión de proyectos de tecnología de la información

Se llama gestión de proyectos de TI a el proceso de gestionar, planificar y desarrollar proyectos relacionados con la tecnología de la información. Esto se divide en los desarrolladores de proyectos TI y los gerentes. Los desarrolladores se encargan de ofrecer un producto o servicios mientras que los gerentes de la gestión de proyectos de TI estos son responsables se dirigir el proyecto y hacer que se cumpla en el tiempo establecido.[19]

Las fases para una gestión de proyectos de TI son:

- Fase de iniciación.
- Fase de Planificación.
- Fase de ejecución.
- Fase de supervisión y control.

- Fase de cierre[19]

Funciones de un gerente de proyectos TI

- Asegurar la funcionalidad del producto
- Asignar tareas a los mientras del equipo
- Dar seguimiento al progreso y al desempeño
- Organizar reuniones agiles con los participantes [19]

1.3.10 Planificación estratégica de tecnología de la información

Es un modo de identificar un futuro planificado que permite mejorar los procesos de TI, la estructura informática, alineándose con los objetivos Estratégicos de la organización. Esto quiere decir que la persona encargada se proyecta al que puede suceder dentro de un proyecto de TI, asumiendo los riesgos y los gastos que este podría tener.[20]

1.3.11 Sistema de gestión de seguridad de la información (SGSI)

Es un conjunto de políticas, procedimientos y controles asociados a la seguridad de la información que se deben implementar en una organización y están vinculados a las normas ISO 27001.[21]

Para lograr proteger estos activos vinculados a la seguridad de la información se necesita seguir una serie de pasos que están implementados en base al Ciclo de Deming.

- Planificar.
- Hacer.
- Verificar.
- Actuar.

1.3.12 Elementos de un Sistema de Gestión de Seguridad de la Información

Existen varios elementos importantes para poder garantizar la seguridad de la información de una organización entre los elementos más importantes tenemos:

- Evaluación de riesgos.
- Políticas de seguridad de la información.
- Plan de seguridad de la información.
- Controles de seguridad.
- Auditoria y monitorización.[22]

1.3.13 Pasos para implementar un SGSI

1. Identificar los activos de información.
2. Realizar una evaluación de riesgos.
3. Implementar medidas de seguridad.
4. Monitorizar y revisar el SGSI.
5. Mejora continua.[22]

1.4 Objetivos

1.4.1 Objetivo general

Realizar una auditoria informática a la gestión de las normas ISO 27001 en la empresa MEGAKONS S.A.

1.4.2 Objetivos específicos

- Analizar las normas ISO 27001 a fin de realizar una correcta evaluación del sistema de gestión de seguridad.
- Planificar la auditoria informática en la empresa MEGAKONS S.A.
- Evaluar y emitir un informe sobre los procesos, políticas y controles de recursos de TI en la empresa MEGAKONS S.A.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Como materiales para la investigación científica para el presente proyecto, se utilizó una entrevista y la encuesta detallada a continuación.

Tabla 1.Formato de entrevista.

FORMULARIO DE LA ENTREVISTA

Entrevista		
Entrevistado:		
Cargo:	Jefe de área de TI	
Entrevistador:	Marco Orlando Tenezaca Caizabanda	
Objetivo:	Conocer el nivel de seguridad de la información que tiene la empresa.	
Pregunta	**Respuesta**	**Conclusión**
1. ¿Cuáles son los principales riesgos de seguridad de la información que enfrenta la empresa?		
2. ¿Qué tipos de archivos son parte de los activos informáticos de la empresa?		
3. ¿Como se asegura la empresa de que su información es segura?		
4. ¿Cómo se comunica la seguridad de la información a los empleados?		
5. ¿Los controles que se emplean en la empresa son los adecuados para asegurar el buen uso de la información en la empresa por parte de los empleados?		
6. ¿Qué persona esta designada en el proceso de seguimiento y control de la seguridad de la información?	.	
7. ¿Con que frecuencia se realiza una actualización del análisis de riesgo en la empresa?		
8. ¿Cómo se gestiona el acceso a la información sensible en los recursos informáticos de la empresa?		

Pregunta	Respuesta	Conclusión
9. ¿Cómo se documenta y mantiene el SGSI?		
10. ¿Cuáles son los desafíos más importantes que enfrenta la empresa en materia de seguridad de la información?		
11. ¿Tienen respaldos de la base de datos y donde se almacenan los mismos?		

Tabla 2.Formato de Encuesta para los empleados.

FORMULARIO DE LA ENCUESTA

	ENCUESTA
Dirigido a:	Personal de TI y jefes de cada departamento de la empresa.
Encuestador:	Marco Orlando Tenezaca Caizabanda
Objetivo:	Medir el conocimiento sobre la seguridad de la información que poseen los diferentes departamentos de la empresa.
Indicaciones:	Leer detenidamente cada pregunta y seleccionar una sola opción

Preguntas:

1.- ¿Con que frecuencia se han presentado fallos en los recursos informáticos que comprometan la integridad de los datos de la empresa?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

2.- ¿Se realiza un monitoreo de la seguridad de los equipos informáticos?

a) Si ( )

b) No ( )

3.- ¿Con que frecuencia se realiza mantenimiento preventivo/correctivo a los recursos informáticos?

a) 1 vez al mes ( )

b) cada 2 meses ( )

b) cada 3 meses ( )

c) cada 6 meses ( )

d) cada año ( )

4.- ¿Con que frecuencia el personal de TI realiza capacitaciones sobre la seguridad de la información de la empresa?

a) 1 vez al mes ( )

b) cada 2 meses ( )

b) cada 3 meses ( )

c) cada 6 meses ( )

d) cada año ( )

5.- ¿Con que frecuencia se realiza una actualización de los recursos informáticos?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

6.- ¿Los archivos de uso individual de la empresa son respaldados?

a) Si ( )

b) No ( )

7.- ¿Cada que tiempo se realiza un respaldo de la información en la empresa?

a) 1 vez al mes ( )

b) cada 2 meses ( )

b) cada 3 meses ( )

c) cada 6 meses ( )

8.- ¿Alguna vez ha tenido que recuperar datos con los respaldos que se realiza en la empresa?

a) Si ( )

b) No ( )

Indicaciones: Leer detenidamente cada pregunta y seleccionar una o varias opciones.

9.- ¿Qué políticas para la seguridad de la información conoce que tiene la empresa?

a) Control de acceso ( )

b) Cifrado de archivos ( )

c) Respaldos ( )

d) Ninguna ( )

10. ¿Con que métodos usted protege la seguridad de su computador?

a) Contraseña ( )

b) Huella dactilar ()

b) Reconocimiento Facial ( )

c) Ninguno ( )

11. ¿Qué sitios web usted frecuenta en los dispositivos de la empresa?

a) Redes Sociales ( )

b) YouTube ( )

b) Paginas de compras en línea ( )

2.2 Métodos

En la presente investigación se utilizó un enfoque cuantitativo y cualitativo, para lo cual se realizó una recolección de datos relacionados a la seguridad de la información mediante una entrevista al jefe del área de TI y varias encuestas a todos los empleados que utilizan algún recurso informático dentro de la empresa.

2.2.1 Modalidad de la investigación

Investigación de campo

La Investigación fue de campo debido a que se analizó la problemática en el mismo sitio donde se produjo, es decir, la empresa MEGAKONS S.A. para poder determinar el nivel de la problemática y también sus causas y consecuencias.

Investigación bibliográfica – documental

La Investigación fue Bibliográfica – Documental por que se analizó problemáticas similares en diferentes documentos y a su vez se analizó las diferentes soluciones que se puede tener para la problemática en tesis, artículos científicos.

2.2.2 Población y muestra

En este trabajo investigativo se trabajó con el total de la población conformada por grupos del área administrativa y los empleados de MEGAKONS S.A., con un total de 22 personas por lo que no es necesario calcular muestra estadística debido a que no es una población extensa.

Tabla 3. Población de la empresa.

Área	Población	Porcentaje
Área de TI	3	13.63%
Empleados	19	86.37%
Total	22	100%

2.2.3 Recolección de información

Se aplico una encuesta a un total de 21 personas, que están divididas en empleados del departamento de TI, Gerencia, Diseño gráfico, Contabilidad, Recursos humanos, Facturación. La encuesta tuvo un total de 12 preguntas y los resultados se presentan en forma de tablas y gráficos estadísticos.

Pregunta 1: ¿Con que frecuencia se han presentado fallos en los recursos informáticos que comprometan la integridad de los datos de la empresa?

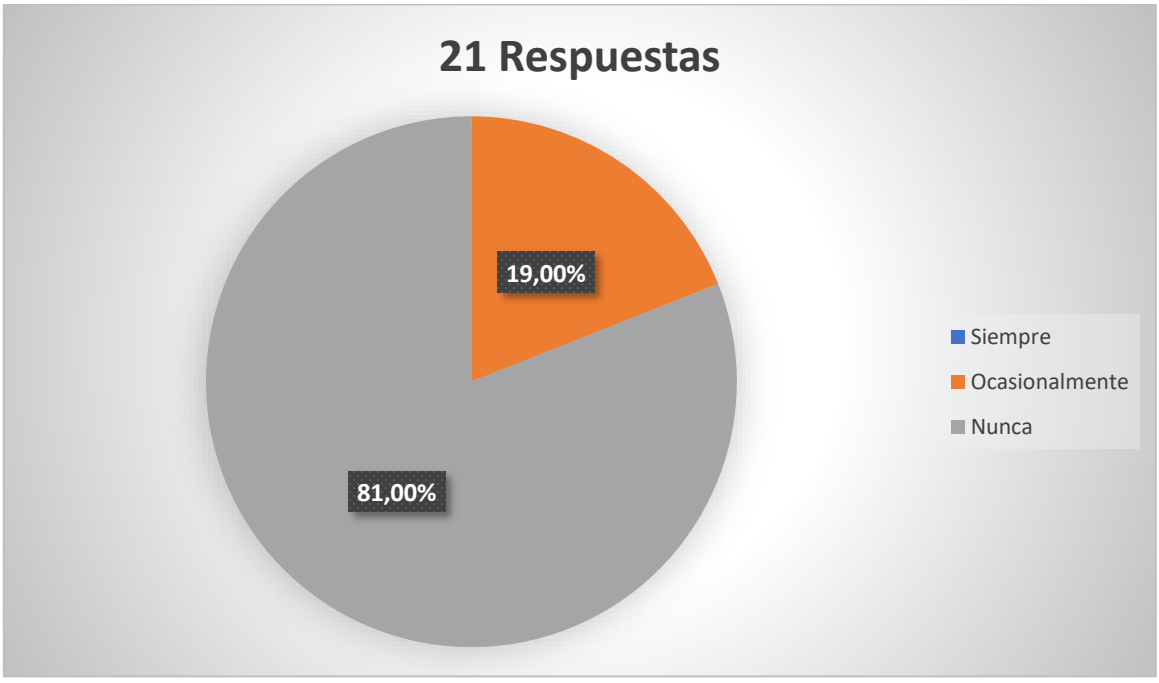


Figura. 1 Resultado de Pregunta 1.

Análisis e interpretación

Según los datos representados en la Figura 1, en la empresa MEGAKONS S.A. el 81% de las personas encuestadas nunca ha tenido un fallo en su computador o recurso informático que ocupa para cumplir su función, de lo contrario el 19% ha tenido algún inconveniente con su computador y se ha visto comprometida la seguridad de la información de su trabajo. A pesar de no existir un porcentaje muy alto de inconvenientes en el funcionamiento de los recursos informáticos, el fallo de alguno puede inferir en que exista vulnerabilidad en la información de la empresa.

Pregunta 2: ¿Se realiza un monitoreo de la seguridad de los equipos informáticos?

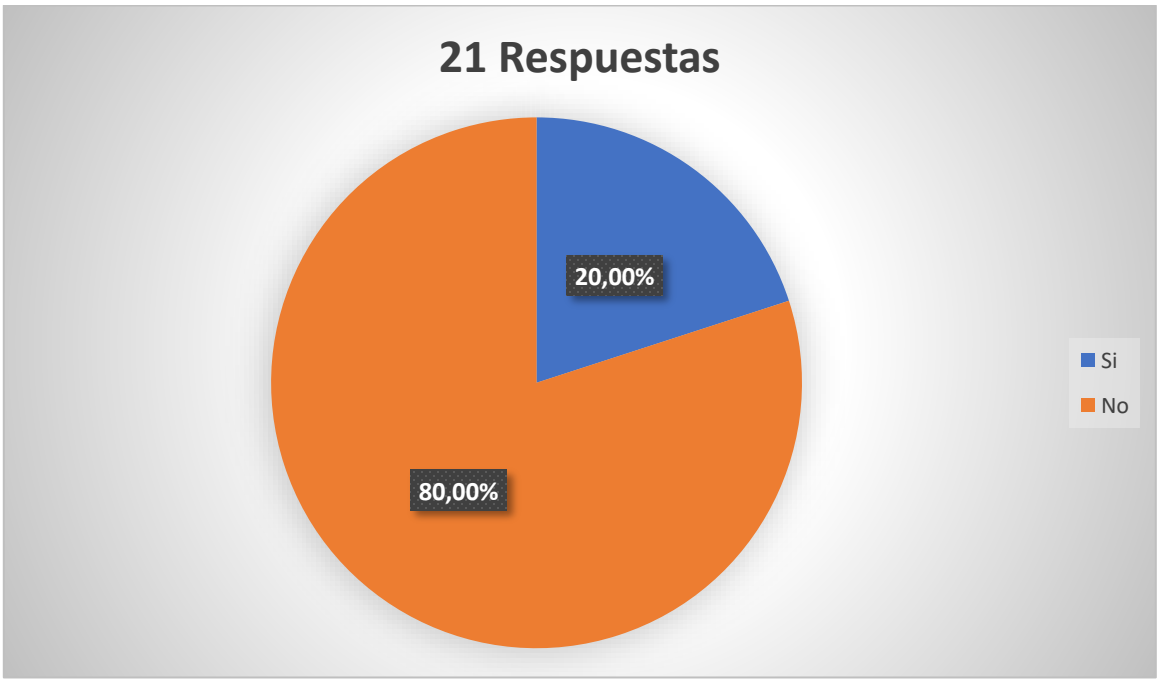


Figura. 2 Resultado de Pregunta 2.

Análisis e interpretación

Según los datos representados en la Figura 2, la empresa MEGAKONS S.A. el 20% de los empleados han tenido un monitoreo en sus computadores referente a la seguridad de la información, de lo contrario el 80% de los empleados nunca ha recibido un monitoreo de su instrumento de trabajo, a lo que se concluye que la empresa no tiene un monitoreo adecuado y esto puede permitir que se tenga intrusos en los computadores y por ende un robo de información sensible para la empresa.

Pregunta 3: ¿Con que frecuencia se realiza mantenimiento preventivo/correctivo a los recursos informáticos?

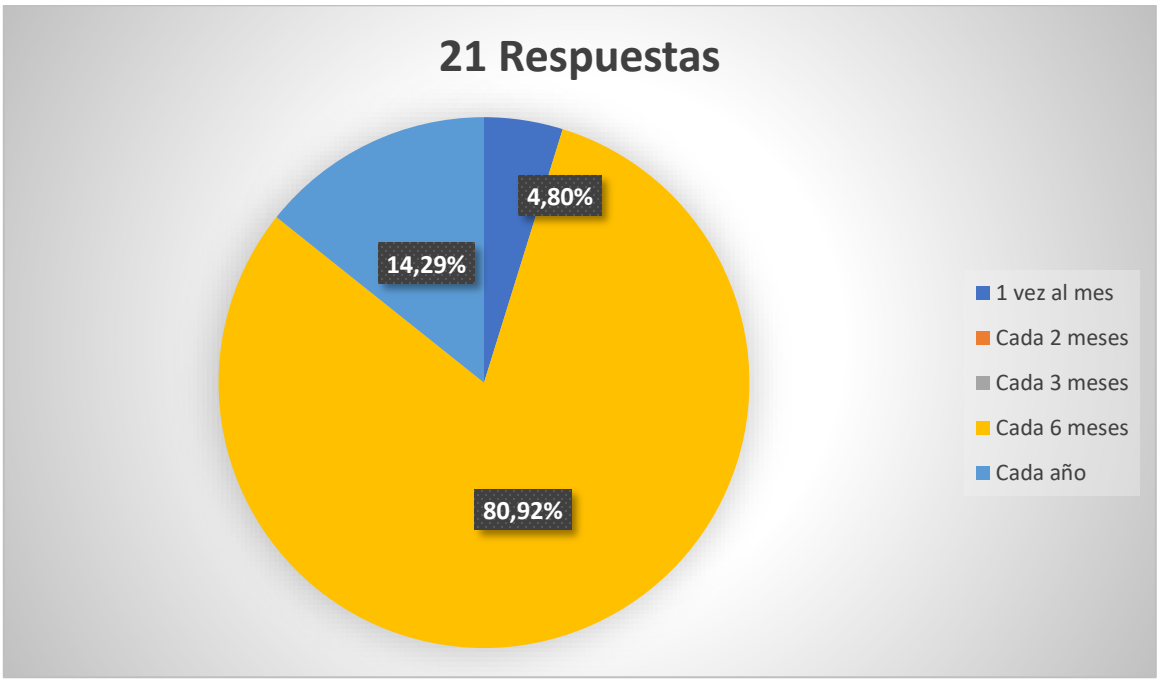


Figura. 3 Resultado de Pregunta 3.

Análisis e interpretación

Según los datos representados en la Figura 3. En la empresa MEGAKONS S.A. el 80% de los recursos informáticos tiene un mantenimiento cada 6 meses, el 14.29% tiene un

mantenimiento cada año y 4.80% tiene un mantenimiento cada mes, estos valores se deben a que en algunas áreas de la empresa no se requiere un mantenimiento muy seguido de los recursos informáticos, sin embargo si existe un mantenimiento continuo en los recursos mas vulnerables de la empresa y se puede verificar que si se trata de mantener a los equipos informáticos en buen estado.

Pregunta 4: ¿Con que frecuencia el personal de TI realiza capacitaciones sobre la seguridad de la información de la empresa?

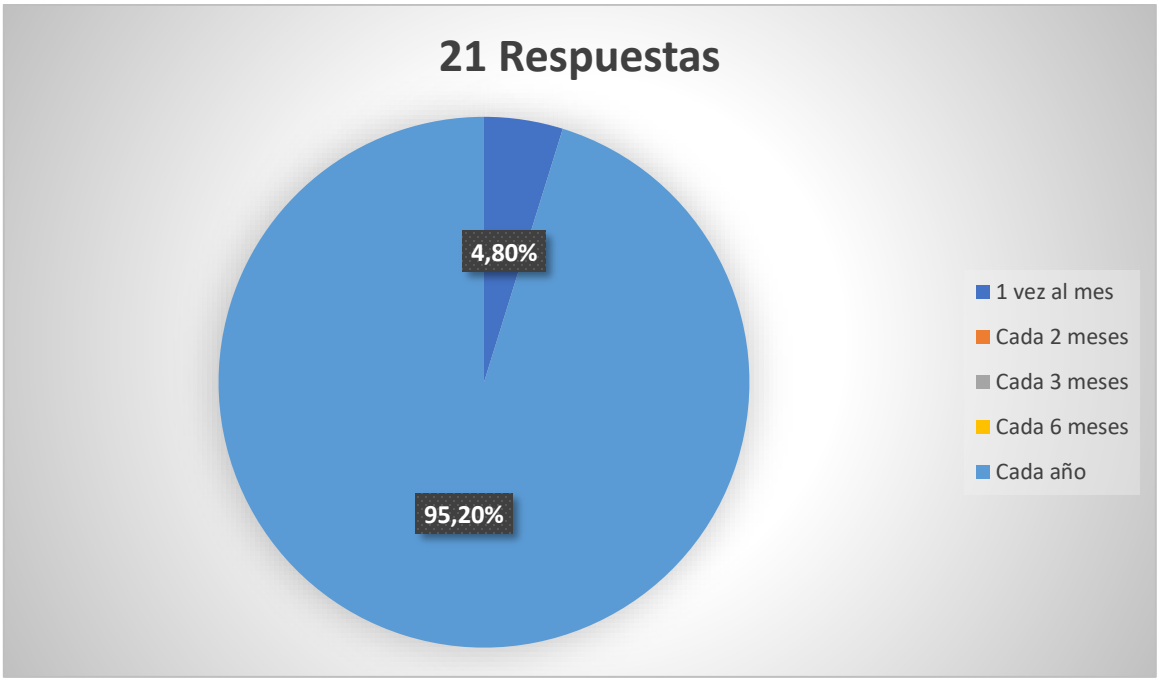


Figura. 4 Resultado de Pregunta 4.

Análisis e interpretación

Según los datos representados en la Figura 4, el 95.20% de la empresa es capacitada por lo menos 1 vez al año sobre la importancia de la seguridad de la información, por otro lado el 4.80% de la empresa se capacita por lo menos 1 vez al mes en temas referentes a la seguridad de la información, esto quiere decir que a las personas con menos riesgos se les capacidad

con menos intensidad, sin embargo dentro del área de TI de la empresa se necesita estar siempre informado sobre nuevos ataques informáticos que puedan afectar en la empresa por lo cual están capacitándose cada mes.

Pregunta 5: ¿Con que frecuencia se realiza una actualización de los recursos informáticos?

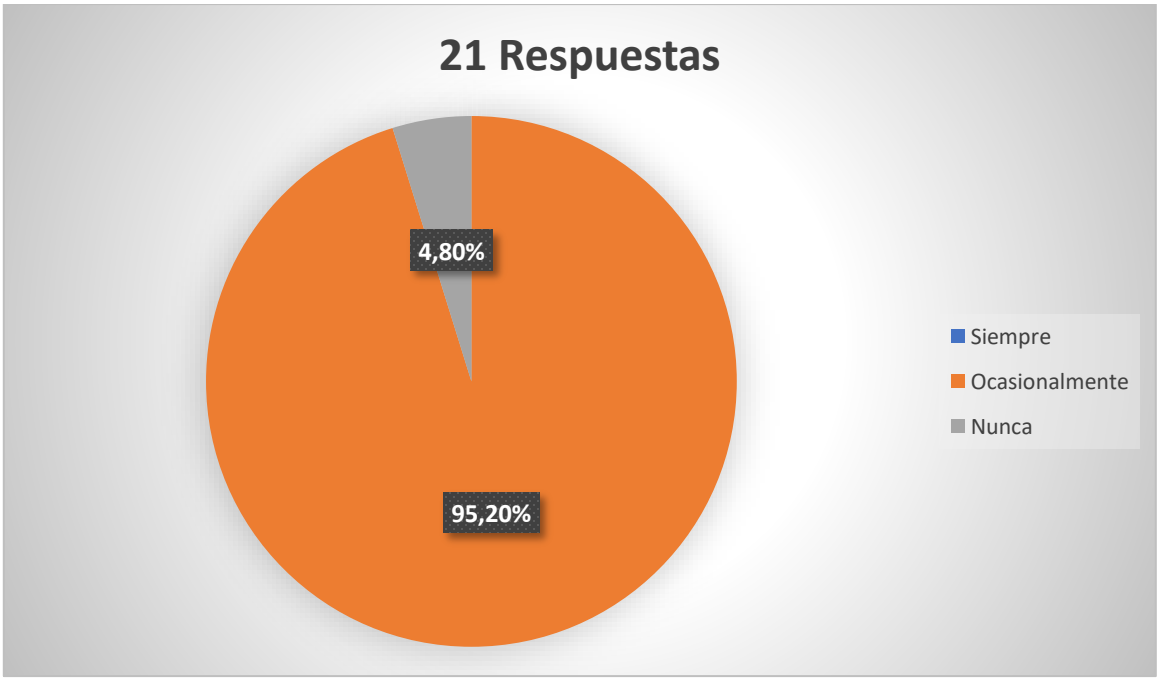


Figura. 5 Resultado de Pregunta 5.

Análisis e interpretación

Según los datos representados en la Figura 5. En la empresa MEGAKONS S.A. el 4.80% de los empleados no ha recibido una actualización de los recursos informáticos con los que trabajan de lo contrario el 95.20% afirma que ocasionalmente existe una actualización en sus recursos informáticos de trabajo. Para lo cual podemos analizar que la empresa si bien no mantiene una actualización continua de sus recursos, cuando es necesario los cambia o actualiza para así tratar de evitar algún fallo referente a la seguridad de la información.

Pregunta 6: ¿Los archivos de uso individual de la empresa son respaldados?

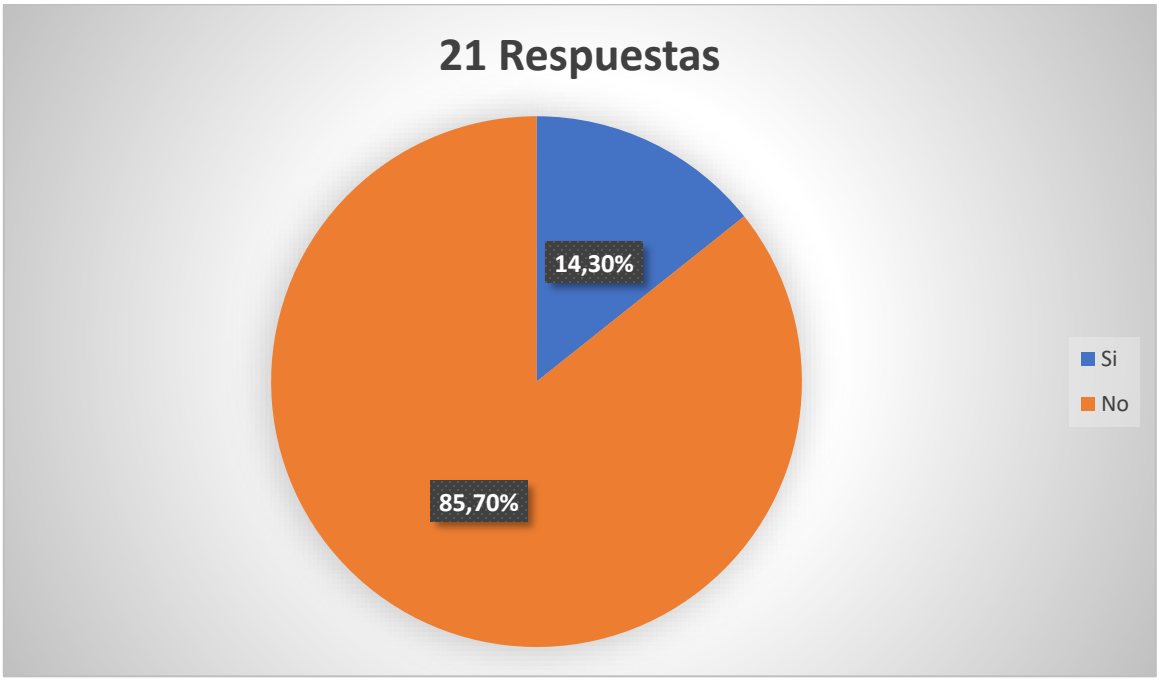


Figura. 6 Resultado de Pregunta 6.

Análisis e interpretación

Según los datos representados en la Figura 6. En la empresa MEGAKONS S.A. EL 85.70% de los empleados no respalda sus datos individuales referentes a la empresa y el 14.30% de los empleados si saca un respaldo de sus datos individuales. Según lo analizado se puede verificar que los únicos que respaldan sus datos son el área de TI, mientras que los demás departamentos no tienen un respaldo en caso de algún fallo en sus recursos informáticos lo que podría llevar a un caos total si se llega a perder o robar esa información.

Pregunta 7: ¿Cada que tiempo se realiza un respaldo de la información en la empresa?

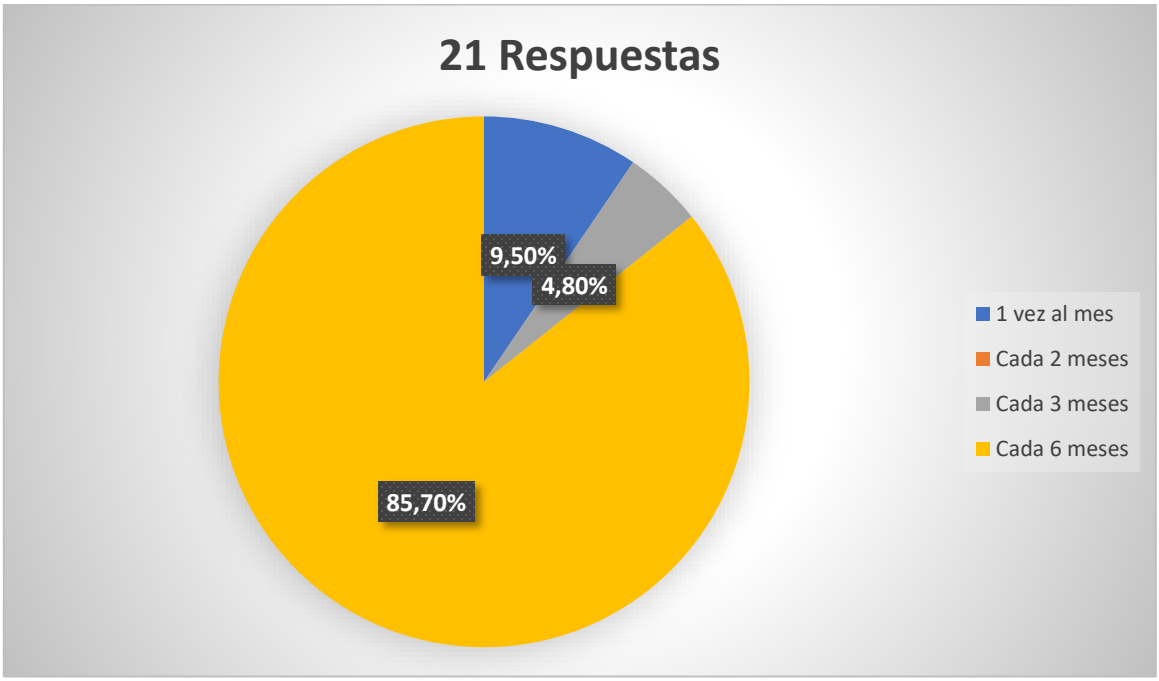


Figura. 7 Resultado de Pregunta 7.

Análisis e interpretación

Según los datos representados en la Figura 7. En la empresa MEGAKONS S.A. EL 85.70% de la empresa respalda su información cada 6 meses, el 4.80% de la empresa respalda su información cada 3 meses y tan solo el 9.50% de la empresa respalda su información 1 vez al mes. Una vez analizado estos resultados podemos verificar que la poca información de la cual se saca un respaldo no se lo hace muy frecuentemente, la empresa dentro del área de TI analiza cual es la información que necesita respaldos y cada que tiempo.

Pregunta 8: ¿Alguna vez ha tenido que recuperar datos con los respaldos que se realiza en la empresa?

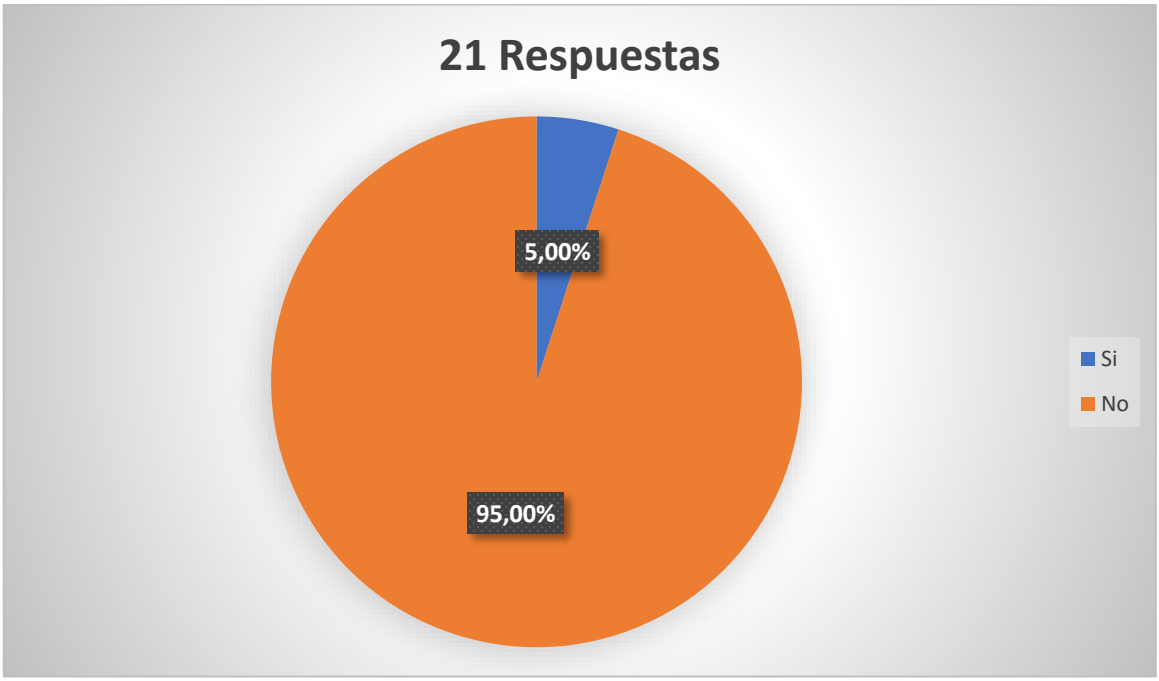


Figura. 8 Resultado de Pregunta 8.

Análisis e interpretación

Según los datos representados en la Figura 8. En la empresa MEGAKONS S.A. solo el 5% de los empleados a tenido que recuperar información de algún respaldo obtenido con anterioridad y el 95% de los empleados no ha tenido que recuperar sus datos de respaldos, por lo cual se puede verificar que los empleados al no tener respaldos de su información no van a tener como recuperarla en caso de perdida y eso es una gran desventaja para la empresa porque parte de esa información puede ser sensible.

Pregunta 9: ¿Qué políticas para la seguridad de la información conoce que tiene la empresa?

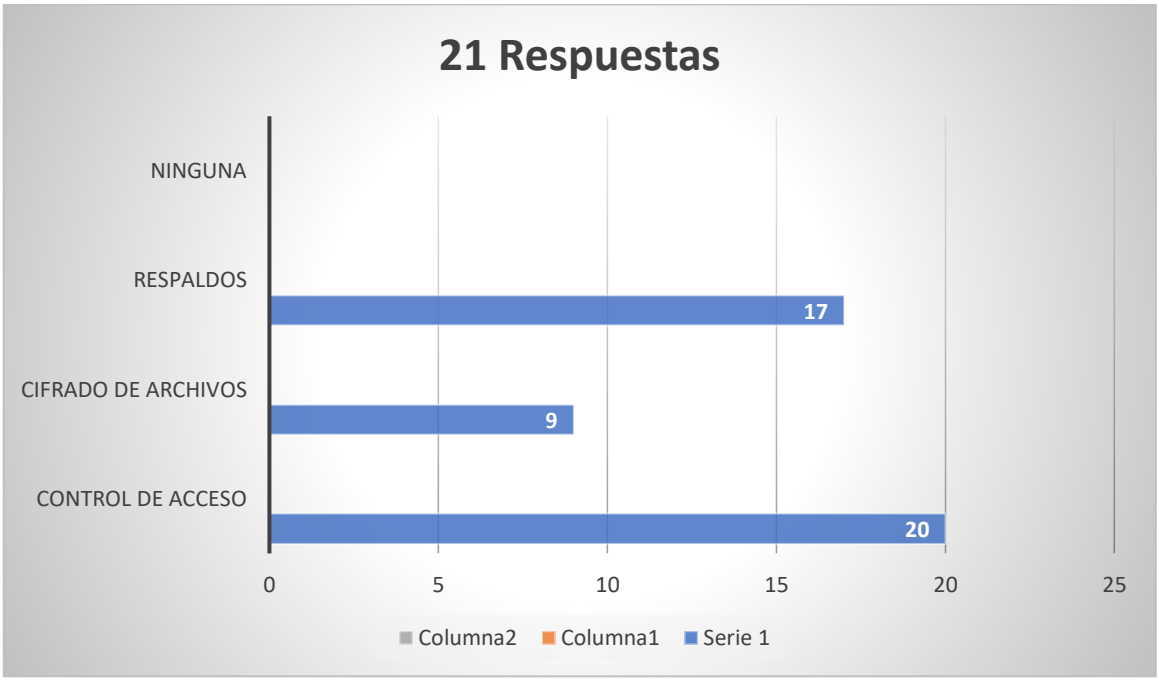


Figura. 9 Resultado de Pregunta 9.

Análisis e interpretación

Según los datos representados en la Figura 9. En la empresa MEGAKONS S.A. el 95.20% (20) de los empleados conoce que la empresa tiene un control de acceso a la información, el 42.9% (9) conoce sobre el cifrado de los archivos en la empresa, el 81% (17) de los empleados conoce que se debería tener respaldos de la información sensible de la empresa. Entonces se concluye que los empleados conoces sobre las políticas básicas de seguridad que debería tener la empresa referente a la seguridad de la información que se maneja en la misma.

Pregunta 10: ¿Con que métodos usted protege la seguridad de su computador?

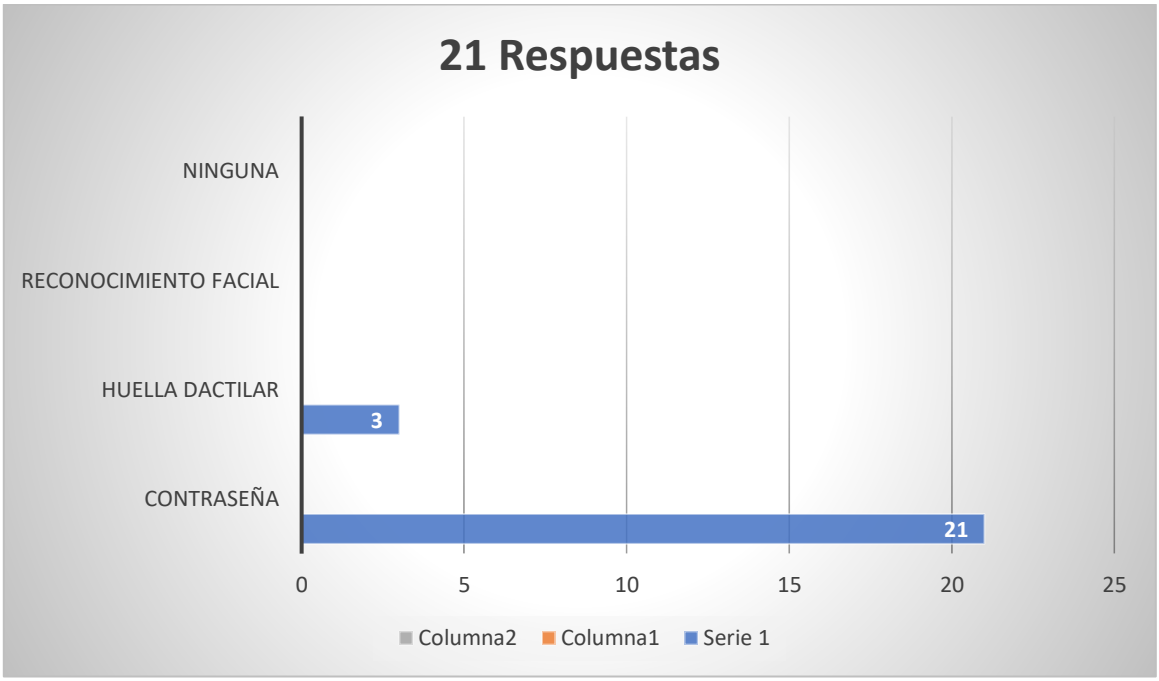


Figura. 10 Resultado de Pregunta 10.

Análisis e interpretación

Según los datos representados en la Figura 10. En la empresa MEGAKONS S.A. el 100% (21) de los empleados protege su computador o dispositivo con una contraseña y tan solo el 14.3% (3) utiliza como método de protección la huella dactilar. Para lo cual podemos observar que en la empresa no existe ningún empleado que no tenga su recurso informático sin ninguna seguridad, sin embargo, se debería analizar qué tan segura es la contraseña y verificar si cumple con el requisito mínimo de una contraseña segura.

Pregunta 11: ¿Qué dispositivos informáticos ocupa dentro de la empresa?

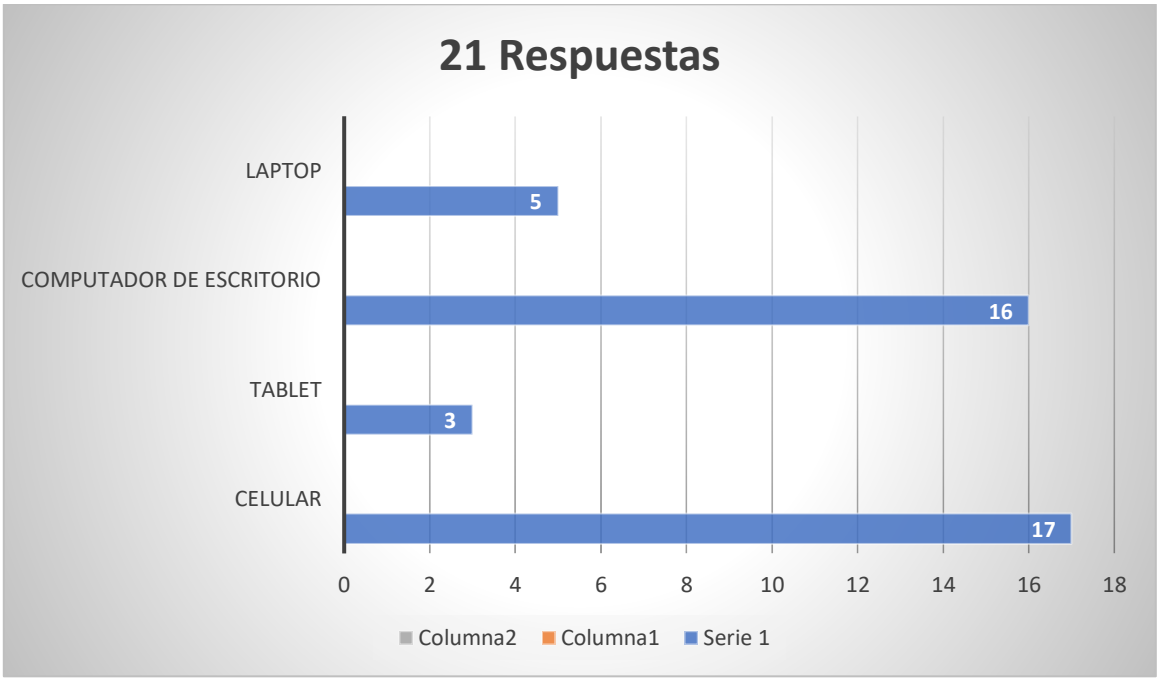


Figura. 11 Resultado de Pregunta 11.

Análisis e interpretación

Según los datos representados en la Figura 11. En la empresa MEGAKONS S.A. el 81% (17) de los empleados utilizan su teléfono dentro de la empresa, el 76.2% (16) de los empleados utiliza computador de escritorio, el 23.8% (5) utiliza laptop y el 14.3% (3) de los empleados utiliza una Tablet dentro de la empresa. Para lo cual podemos verificar que todos los empleados utilizan un computador (escritorio o portátil) y ciertos empleados manejan celulares para poder comunicarse entre departamentos o llamadas a clientes y esos teléfonos o tabletas están conectados a la red de la empresa para lo cual se debe tener un acceso limitado dentro de la red y así evitar fuga de información.

Pregunta 12: ¿Qué sitios web usted frecuenta en los dispositivos de la empresa?

Figura. 12 Resultado de Pregunta 12.

Análisis e interpretación

Según los datos representados en la Figura 12. En la empresa MEGAKONS S.A. todos los empleados utilizan redes sociales dentro de la misma y la red social más utilizada en WhatsApp móvil y web, ese es el medio por el cual por lo general se envían archivos de trabajo entre empleados o se comunican con los clientes.

Se aplico una entrevista para el jefe del área de TI de la empresa y se obtuvo los siguientes resultados.

Tabla 4. Resultado de entrevista al área de TI.

Pregunta	**Respuesta**	**Conclusión**
1. ¿Cuáles son los principales riesgos de seguridad de la información que enfrenta la empresa?	La fuga de información interna, no se tiene un control de los empleados para verificar que se lleven cierta información a la casa, tampoco se tiene bloqueos en los computadores para no ingresar dispositivos de almacenamiento.	No existen controles para mitigar la fuga de información entre los empleados, aunque no haya existido ningún inconveniente.
2. ¿Qué tipos de archivos son parte de los activos informáticos de la empresa?	Entre los archivos más importantes de la empresa esa la base de datos y los archivos de Excel que manejan contabilidad y recursos humanos.	Entre los archivos que son importantes en la empresa, existe algunos que no tiene ninguna seguridad en caso de robo o perdida.
3. ¿Como se asegura la empresa de que su información es segura?	Externamente se trabaja con MikroTik para asegurar la información, internamente se maneja según las políticas establecidas	Los controles no están bien establecidos en el margen de seguridad de la información.
4. ¿Cómo se comunica la seguridad de la información a los empleados?	Anualmente se realiza una reunión en la cual se concientiza a los empleados sobre la seguridad de la información además se realiza un ataque mediante phishing para saber que tan informados están los empleados.	La capacitación que reciben los empleados sobre la seguridad de la información es la adecuada para poder concientizar a todos sobre el buen manejo de la información sensible de la empresa.
5. ¿Los controles que se emplean en la empresa son los adecuados para asegurar el buen uso de la información en la empresa por parte de los empleados?	En los diferentes sistemas se tiene diferentes roles y usuarios para que cada persona solo obtenga la información que necesita para realizar su trabajo, además existen datos que solo tienen acceso gerencia y el área de ti.	Los roles y usuarios que manejan la empresa permiten que no todos tengan acceso a toda la información por lo cual se está manejando de una manera adecuada.
6. ¿Qué persona esta designada en el proceso de seguimiento y control de la seguridad de la información?	En la actualidad no existe ninguna persona encargada del control de la seguridad de la información.	Se debería asignar a una persona del área de TI, para verificar los controles de seguridad de la información de la empresa.
7. ¿Con que frecuencia se realiza una actualización del análisis de riesgo en la empresa?	Cada año.	Este punto se maneja de una manera adecuada ya que cada año existen diferentes fenómenos que pueden afectar a la empresa.
8. ¿Cómo se gestiona el acceso a la información sensible en los recursos informáticos de la empresa?	El sistema tiene gestión de usuarios y roles que están definidos según el cargo y la necesidad de cada empleado.	La forma en la que cada empleado tiene acceso a la información es la adecuada.
9. ¿Cómo se documenta y mantiene el SGSI?	Solo se tiene ciertos datos que cumplen con el SGSI y las normas ISO 27001, por el momento falta algunos detalles para poder tener un SGSI completo.	Se debe analizar toda la documentación que existe en la empresa referente a la seguridad de la información.

Pregunta	Respuesta	Conclusión
10. ¿Cuáles son los desafíos más importantes que enfrenta la empresa en materia de seguridad de la información?	La seguridad interna y el manejo de la información que tiene cada uno de los empleados, se busca implementar un bloqueo y escaneo de los dispositivos que se ingresan a los computadores, así como un escaneo de los sitios a los que acceden los empleados dentro de la red de la empresa.	La empresa está consciente de todos los puntos débiles que tiene a nivel de seguridad de la información, para lo cual se está intentando capacitar y mejorar los puntos débiles.
11. ¿Tienen respaldos de la base de datos y donde se almacenan los mismos?	Si se realiza un respaldo de la base de datos y el mismo se lo guarda en un disco externo.	Los respaldos deberían implementarse también en la nube debido a que los dispositivos externos también pueden sufrir algún daño o robo

Conclusión: La empresa MEGAKONS S.A. ha implementado ciertos protocolos de seguridad según las normas ISO 27001 sin embargo existe muchos huecos de seguridad que pueden llevar a un robo o perdida de la información, el personal de la empresa está capacitado sobre la seguridad de la información sin embargo se necesita implementar algunos controles para no permitir la fuga de información.

2.2.4 Procesamiento y análisis de datos

Con toda la información recolectada en encuestas y entrevistas y después de analizar debidamente la información se llega a la conclusión que:

Existen varios controles y procesos referente a la seguridad de la información en la empresa, sin embargo, no todos los empleados están debidamente capacitados sobre el manejo de los activos informáticos y de los controles que existen para poder resguardar la información valiosa de la empresa.
Existen algunas brechas de seguridad por las cuales podría existir algún tipo de ataque o robo de información de la empresa y el área de TI aun no soluciona ese tipo de errores.

Si bien se tiene una idea de los activos informáticos más importantes de la empresa estos no están debidamente clasificados ni tienen un seguimiento correcto lo que lleva a no tener

copias de seguridad y por lo tanto la empresa al perder esta información no podría recuperarla de ninguna manera.

El personal del área de TI de la empresa necesita indagar más sobre la seguridad de la información y así poder implementar ciertos controles y procesos que ayudarán a que no exista fuga interna de información entre los empleados.

La comunicación sobre la seguridad de la información a los empleados no es la correcta, se debería tener más capacitaciones referentes al tema y así evitar que los empleados caigan en algún tipo de ataque como phishing.

Existen ciertos documentos que sustentan la seguridad de la información de la empresa sin embargo no existe una persona encargada de un control y seguimiento de esta documentación lo que con lleva a no tener una buena seguridad en la empresa.

Una auditoria informática ayudaría a verificar que tipo de archivos son los que cumplen con la seguridad de la información y se basan en las normas ISO 27001 y saber si los mismos se están implementando y llevan con seguimiento continuo dentro de la empresa.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1.Análisis y discusión de los resultados.

3.1.1 Auditorias informáticas con normas ISO 27001

Una auditoria informática con normas ISO 27001 nos ayuda a verificar posibles errores y malas prácticas referentes a la seguridad de la información. Existen dos tipos de auditorías informáticas, la externa y la interna.

a. Auditoría Interna

Se define como auditoría interna al proceso de revisión, análisis y corrección de los procesos y controles de una empresa, el cual está a cargo por uno o varios miembros de la misma organización y así buscar mejoras en diferentes áreas como, servidores, equipos de red, seguridad de la información entre otros. La finalidad de esta auditoria es corregir y subsanar los errores y brechas de seguridad existentes.[23]

b. Auditoría Externa

Llamada también auditoria perimetral, consta de un análisis detallado y critico por parte de una persona ajena a la organización y que tenga un criterio profesional. En este tipo de auditoria no existe una mejora por parte del auditor externo, solo se analiza los datos, evalúa y se emite un informe de los hallazgos encontrados.[24]

Tabla 5. Comparativa de auditoria informática externa e interna.

Comparativa de auditoría interna y auditoría externa		
Aspecto	**Auditoría Interna**	**Auditoría Externa**
Relación con la empresa	Realizada por los empleados de la empresa	Realizada por un personal externo debidamente capacitado.
Objetivo	Evaluar los controles y procesos internos específicos de la empresa y mejorarlos.	Revisar la existencia y cumplimiento de controles, riesgos.
Independencia	Se puede dudar de una imparcialidad debido a que se realiza por el personal de la empresa	Sus resultados son imparciales y veraces.
Implicaciones Legal	Puede ser de utilidad como evidencia legal.	Sus informes tienen una validez legal para uso de terceros.

Una vez analizado los dos tipos de auditorías, la auditoria para el presente proyecto es la auditoría externa debido a que el autor no tiene ningún vínculo con la empresa MEGAKONS S.A. y su objetivo es revisar, analizar y emitir un informe de los hallazgos.

3.1.2 Metodologías para el desarrollo de una auditoria informática con normas ISO 27001.

Existen varias metodologías aplicables en una auditoria informática entre las más importantes y utilizadas tenemos a Metodología PDCA, basada en riesgos, basada en procesos. Estas metodologías se aplican en la norma establecida debido a que se ajustan a los requerimientos y análisis de la seguridad de la información.

a. Metodología PDCA

Es un modelo de calidad circular (siglas en ingles de Plan, Do, Check y Act), es uno de los métodos más eficaces para realizar una auditoria informática externa debido a su conjunto de etapas las cuales se alinean a tener un buen resultado en la auditoria.[25]

- Planificar
- Hacer
- Verificar
- Actuar

b. Metodología basada en riesgos

La metodología basada en riesgos analiza cada uno de los riesgos existentes en la empresa, así como su plan de contingencia y demás archivos, sin embargo, deja a un lado las políticas de seguridad y los procesos que deben estar establecidos dentro del SGSI. Para esta metodología existe un análisis profundo de los riesgos establecidos y también de los riesgos que pueden existir.[26]

c. Metodología basada en procesos.

Se evalúa los procesos de una organización, así como su eficacia, eficiencia y cumplimiento, una vez evaluado se emite un informe de recomendaciones las cuales ayudaran a mejorar y aumentar la calidad de estos procesos. En este tipo de metodología se evita analizar los riesgos y políticas ya que se encuentra centrado en los procesos.[27]

Tabla 6. Comparativa entre metodologías para una auditoria informática.

Comparativa de Metodologías para una auditoría informática con normas ISO 27001			
Aspecto	Metodología PDCA	Metodología Basada en Riesgos	Metodología Basada en Procesos
Enfoque principal	Se enfoca tanto en los riesgos, procesos y controles de una empresa. Es más general y ayuda a mejorar los resultados.	Se enfoca solo en la identificación y mitigación de riesgos.	Se enfoca solo en la evaluación y mejora de los procesos.
Fases	Planificar. Hacer. Verificar. Actuar.	Identificación de riesgos Evaluación de riesgos Mitigación de riesgos Monitoreo y revisión.	Evaluación de procesos de SGSI Revisión de implementación y mantenimiento de controles. Mejora continua de procesos.
Objetivo principal	Evaluar la mejora continua de la eficiencia y eficacia de los procesos y controles del SGSI.	Identificar y gestionar los riesgos vinculados con la seguridad de la información.	Evaluar la eficiencia de los procesos del SGSI.
Enfoque en Riesgos	Centrado en todos los aspectos del SGSI, incluyendo riesgos y procesos.	Centrado en los riesgos y hace menos énfasis en los procesos.	Centrado en la eficiencia de los procesos relacionados con la seguridad con poco énfasis en los riesgos.
Enfoque en Procesos	Enfocado en evaluar todos los aspectos del SGSI, incluyendo los procesos.	Enfoque en la gestión de riesgos, sin énfasis a los procesos.	Enfoque en los procesos relacionados con la seguridad de la información.
Aplicación	Esta metodología no está limitada a un sector en específico, es recomendable en cualquier aspecto.	Esta metodología no está limitada sin embargo su enfoque principal es el análisis de riesgo, dejando a un lado los controles y procesos.	Esta metodología se limita al análisis de los procesos vinculados con la seguridad de la información.
Resultado esperado	Mejora y eficiencia en la evaluación de controles y procesos vinculados con la seguridad de la información.	Mejora en el análisis de riesgos de la seguridad de la información.	Mejora en el análisis de los procesos vinculados con la seguridad de la información.

3.2 Metodología aplicable para la auditoria informática en MEGAKONS S.A.

Entre las metodologías analizadas, la que mejor se ajusta a las necesidades de la empresa MEGAKONS S.A. es la metodología PDCA basada en el ciclo deming, ya que abarca tanto a los controles y procesos de la seguridad de la información. Con esta metodología las actividades a seguir serían las siguientes:

1. Planificación (Plan): Definimos el alcance, limites, objetivos y criterios de la auditoria informática externa.

2. Hacer (Do): Llevar a cabo las actividades que se planificaron para la obtención de documentos que ayuden al análisis de la auditoria informática externa.

3. Verificar (Check): Se evalúa la evidencia recopilada en la empresa para determinar si cumple con los estándares de la ISO 27001.

4. Actuar (Act): emisión de informe y hallazgos de la auditoria, así como recomendaciones y acciones correctivas.

3.3 Desarrollo de la auditoria informática externa con normas ISO 27001 en MEGAKONS S.A.

3.3.1 Planificación de la auditoria informática (Plan).

1. Definición del Alcance:

La empresa MEGAKONS S.A. desea someterse a una auditoria informática externa con normas ISO 27001 las cuales están vinculadas con la seguridad de la información, para lo

cual se analizará su Sistemas de Gestión de Seguridad de la Información (SGSI), con el objetivo de evaluar si cumple con los requisitos establecidos en la norma.

2. Límites y Extensión:

La auditoría se centrará en los controles y procesos definidos por la empresa, y se analizará los dispositivos informáticos que existen en la empresa y se verificara su correcto funcionamiento en base a la seguridad de la información.

3. Objetivos de la auditoría:
    - Evaluar la Conformidad con ISO 27001.
    - Revisión del análisis de seguridad.
    - Revisar la Implementación de Controles de Seguridad definidos como aplicables.
    - Verificar el Cumplimiento de los procesos de seguimiento y control.

4. Criterios de la auditoria.

Normas ISO 27001:2013

Todo lo evaluado se basó en los requisitos establecidos en la norma ISO 27001:2013.

Políticas y procedimientos

Se utilizó la documentación que posee la empresa como, plan de contingencia, análisis de riesgos, bitácoras, plan estratégico.

Los controles para auditar de la empresa MEGAKONS S.A. deben estar alineados a los controles que existen en las normas ISO 27001. El anexo A detalla los controles y objetivos

a través de los 18 dominios que tiene la norma, para aplicar la auditoria informática en la empresa se tomó en cuenta los siguientes controles.

- A.5. Políticas de seguridad.

Importante para establecer los lineamientos y principios generales por parte de la seguridad de la información orientados a las normativas correspondientes.

- A.6. Aspectos organizativos de la seguridad de la información.

Esencial para establecer una estructura organizada y efectiva para la gestión de la seguridad de la información en la empresa.

- A.8. Gestión de activos.

Destinado a la seguridad de los activos informáticos de la empresa, reconociendo y clasificando la información sensible, así como establecer el ciclo de vida de estos.

- A.9. Control de accesos.

Establecer restricciones al acceso de la información según los roles de usuarios.

- A.10. Cifrado.

Asegurar el buen uso de claves y criptografía en los datos de la empresa.

- A.11. Seguridad física y ambiental.

Establecer restricciones y verificar el acceso no autorizado a las diferentes instalaciones de la empresa donde se tiene información delicada.

- A.12. Seguridad en la operativa.

Proteger el correcto uso y funcionamiento de los equipos informáticos de la empresa.

- A.13. Seguridad en las telecomunicaciones.

Protección de la información que se encuentra en la web y soporte de esta información.

- A.15. Relaciones con suministradores.

Protección a los activos de información que tengan relación con los diferentes proveedores de la empresa.

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

Coordinación de la gestión de los problemas de seguridad de la información, así como la comunicación y planes antes algún riesgo.

- A.18. Cumplimiento.

Comprobar el cumplimiento de las políticas y controles que exige la norma ISO 27001.

Actividades de la auditoria informática para la empresa MEGAKONS S.A.

Las actividades que se definen en la auditoria para la empresa MEGAKONS S.A. deben estar alineadas a las políticas establecidas por las normas ISO 27001, para lo cual se determinó las siguientes actividades:

Tabla 7. Actividades de la auditoria informática en MEGAKONS S.A.

ACTIVIDADES DE AUDITORIA		
CÓDIGO	**ACTIVIDAD**	**CONTROL POR REVISAR.**
5. POLÍTICAS DE SEGURIDAD.		
CAU01	Verificar las políticas de seguridad.	5.1.1
CAU02	Examinar la existencia de un control de seguimiento de las políticas de seguridad.	5.1.2
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.		
CAU03	Inspeccionar si existe una persona encargada de la seguridad de la información de la empresa.	6.1.1
CAU04	Examinar si la persona encargada tiene definidas tareas y responsabilidades.	6.1.2
CAU05	Verificar si existe seguridad de la información para nuevos proyectos.	6.1.5
8. GESTIÓN DE ACTIVOS.		
CAU06	Revisar si existe un inventario de activos de información.	8.1.1

CÓDIGO	ACTIVIDAD	CONTROL POR REVISAR.
CAU07	Inspeccionar como se garantiza el buen uso de los activos de información.	8.1.3
CAU08	Revisar si existe una clasificación de los activos de la empresa.	8.2.1
CAU09	Como se maneja el acceso a la información confidencial de la empresa.	8.2.3
CAU10	Verificar como se maneja el soporte de almacenamiento.	8.3.1
9. CONTROL DE ACCESOS.		
CAU11	Revisión del acceso físico a la zona de servidores.	9.1.1
CAU12	Revisión del acceso a redes inalámbricas.	9.1.2
10. CIFRADO.		
CAU13	Revisar las políticas de claves seguras.	10.1.2
11. SEGURIDAD FÍSICA Y AMBIENTAL.		
CAU14	Revisión física de las oficinas vinculado con la seguridad de los equipos de TI.	11.1.3
CAU15	Comprobar si existe documentación de los mantenimientos de los equipos informáticos.	11.2.4
12. SEGURIDAD EN LA OPERATIVA.		
CAU16	Revisión de procedimiento de operación.	12.1.1
CAU17	Revisión de controles para el código malicioso.	12.2.1
CAU18	Verificación de la gestión de las copias de seguridad.	12.3.1
CAU19	Revisión de los registros de eventos de actividad.	12.4.1
CAU20	Verificación de instalación de software en el sistema operativo.	12.5.1
CAU21	Verificación de las vulnerabilidades del software instalado en el sistema.	12.6.1
CAU22	Revisión de restricciones de usuarios en la instalación de software.	12.6.2
CAU23	Comprobación de controles de auditoría de los sistemas.	12.7.1

CÓDIGO	ACTIVIDAD	CONTROL POR REVISAR.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.		
CAU24	Verificación de la segmentación de redes.	13.1.3
CAU25	Revisión de las políticas y procedimientos de intercambio de información.	13.2.1
15. RELACIONES CON SUMINISTRADORES.		
CAU26	Revisión de las políticas de seguridad de la información para suministradores.	15.1.1
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.		
CAU27	Verificación de las responsabilidades y procedimientos en los incidentes de la seguridad de la información.	16.1.1
CAU28	Análisis de las notificaciones de los eventos de seguridad de la información.	16.1.2
18. CUMPLIMIENTO.		
CAU29	Revisión de protección de datos y privacidad de la información personal	18.1.4

3.3.2 Desarrollo del plan de auditoría (Do).

Descripción de las actividades

Las actividades definidas en la Tabla 7 se desarrollarán de la siguiente manera.

Tabla 8. Actividad 1 de auditoria informática en MEGAKONS S.A.

Actividad 1	
Código	CAU01
Actividad	Verificar las políticas de seguridad.
Descripción	Confirmar la existencia de las políticas de seguridad de la empresa. Analizar si cumple con las normas ISO 27001.
Requisitos	Documento de políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 9 Actividad 2 de auditoria informática en MEGAKONS S.A.

Actividad 2	
Código	CAU02
Actividad	Examinar la existencia de un control de seguimiento de las políticas de seguridad.
Descripción	Confirmar la existencia del documento de seguimiento de las políticas de seguridad. Analizar si cumple con las normas ISO 27001.
Requisitos	Documento de seguimiento de políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 10 Actividad 3 de auditoria informática en MEGAKONS S.A.

Actividad 3	
Código	CAU03
Actividad	Inspeccionar si existe una persona encargada de la seguridad de la información de la empresa.
Descripción	Revisar en la documentación si existe una persona encargada de la documentación y seguimiento de la seguridad de la información.
Requisitos	Documentación de roles y usuarios.
Responsable	Marco Tenezaca

Tabla 11 Actividad 4 de auditoria informática en MEGAKONS S.A.

Actividad 4	
Código	CAU04
Actividad	Examinar si la persona encargada tiene definidas tareas y responsabilidades.
Descripción	Verificar en el documento pertinente si la persona responsable tiene asignado responsabilidades.
Requisitos	Documentación sobre funciones de los empleados.
Responsable	Marco Tenezaca

Tabla 12 Actividad 5 de auditoria informática en MEGAKONS S.A.

Actividad 5	
Código	CAU05
Actividad	Verificar si existe seguridad de la información para nuevos proyectos.
Descripción	Verificar si existe documentación que evalué y garanticé la seguridad de la información en nuevos proyectos.
Requisitos	Documentación de seguridad de la información para proyectos nuevos.
Responsable	Marco Tenezaca

Tabla 13 Actividad 6 de auditoria informática en MEGAKONS S.A.

Actividad 6	
Código	CAU06
Actividad	Revisar si existe un inventario de activos de información.
Descripción	Confirmar la existencia de documentación sobre los activos de información de la empresa.
Requisitos	Documento de inventario informático de la empresa.
Responsable	Marco Tenezaca

Tabla 14 Actividad 7 de auditoria informática en MEGAKONS S.A.

Actividad 7	
Código	CAU07
Actividad	Inspeccionar como se garantiza el buen uso de los activos de información.
Descripción	Revisa si existe una documentación sobre políticas del buen uso de los activos de información dentro de los recursos informáticos.
Requisitos	Políticas de uso de los recursos informáticos.
Responsable	Marco Tenezaca

Tabla 15 Actividad 8 de auditoria informática en MEGAKONS S.A.

Actividad 8	
Código	CAU08
Actividad	Revisar si existe una clasificación de los activos de la empresa.
Descripción	Confirmar la existencia de una clasificación de la información por importancia.
Requisitos	Archivos de la empresa.
Responsable	Marco Tenezaca

Tabla 16 Actividad 9 de auditoria informática en MEGAKONS S.A.

Actividad 9	
Código	CAU09
Actividad	Como se maneja el acceso a la información confidencial de la empresa.
Descripción	Verificar la existencia de un documento de políticas de seguridad donde especifique el control al acceso a la información sensible de la empresa.
Requisitos	Documento de políticas de la seguridad de la información.
Responsable	Marco Tenezaca

Tabla 17 Actividad 10 de auditoria informática en MEGAKONS S.A.

Actividad 10	
Código	CAU10
Actividad	Verificar como se maneja el soporte de almacenamiento.
Descripción	Verificar si existe una política donde se especifique el uso de los dispositivos de almacenamiento externos.
Requisitos	Documento de políticas de seguridad
Responsable	Marco Tenezaca

Tabla 18 Actividad 11 de auditoria informática en MEGAKONS S.A.

Actividad 11	
Código	CAU11
Actividad	Revisión del acceso físico a la zona de servidores.
Descripción	Revisar controles de seguridad del acceso al área de servidores.
Requisitos	Documento de políticas de control de acceso.
Responsable	Marco Tenezaca

Tabla 19 Actividad 12 de auditoria informática en MEGAKONS S.A.

Actividad 12	
Código	CAU12
Actividad	Revisión del acceso a redes inalámbricas.
Descripción	Confirmar que existe un documento donde se especifique las personas que tienen acceso al área de redes de la empresa.
Requisitos	Documento de políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 20 Actividad 13 de auditoria informática en MEGAKONS S.A.

Actividad 13	
Código	CAU13
Actividad	Revisar las políticas de claves seguras.
Descripción	Confirmar la existencia del documento de políticas de seguridad vinculado con claves seguras y criptografía.
Requisitos	Documento de políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 21 Actividad 14 de auditoria informática en MEGAKONS S.A.

Actividad 14	
Código	CAU14
Actividad	Revisión física de las oficinas vinculado con la seguridad de los equipos de TI.
Descripción	Revisar si existe protección de los equipos informáticos y si se encuentran en un área segura.
Requisitos	Documento de políticas de seguridad física.
Responsable	Marco Tenezaca

Tabla 22 Actividad 15 de auditoria informática en MEGAKONS S.A.

Actividad 15	
Código	CAU015
Actividad	Comprobar si existe documentación de los mantenimientos de los equipos informáticos.
Descripción	Confirmar la existencia de un documento que registre los mantenimientos que se realizan en la empresa.
Requisitos	Documento de seguimiento a los mantenimientos de la empresa.
Responsable	Marco Tenezaca

Tabla 23 Actividad 16 de auditoria informática en MEGAKONS S.A.

Actividad 16	
Código	CAU16
Actividad	Revisión de procedimiento de operación.
Descripción	Revisar que existan procedimiento alineados a los requerimientos de la empresa.
Requisitos	Documento de procedimientos vinculados a la seguridad de la información.
Responsable	Marco Tenezaca

Tabla 24 Actividad 17 de auditoria informática en MEGAKONS S.A.

Actividad 17	
Código	CAU17
Actividad	Revisión de controles para el código malicioso.
Descripción	Confirmar la existencia de un documento donde existan controles y reglamentos de código de programación para evitar que existan brechas de seguridad.
Requisitos	Documento de políticas sobre el desarrollo de programación.
Responsable	Marco Tenezaca

Tabla 25 Actividad 18 de auditoria informática en MEGAKONS S.A.

Actividad 18	
Código	CAU18
Actividad	Verificación de la gestión de las copias de seguridad.
Descripción	Confirmar la existencia de un documento que sustente los activos a los que se deben hacer copias de seguridad, así como el tiempo y responsables.
Requisitos	Políticas de seguridad vinculadas a las copias de seguridad.
Responsable	Marco Tenezaca

Tabla 26 Actividad 19 de auditoria informática en MEGAKONS S.A.

Actividad 19	
Código	CAU19
Actividad	Revisión de los registros de eventos de actividad.
Descripción	Confirmar la existencia y el formato de la bitácora de sucesos de la empresa.
Requisitos	Bitácora de eventos.
Responsable	Marco Tenezaca

Tabla 27 Actividad 20 de auditoria informática en MEGAKONS S.A.

Actividad 20	
Código	CAU20
Actividad	Verificación de instalación de software en el sistema operativo.
Descripción	Confirmar si existe un documento de políticas de software que se puede instalar en el SO de los equipos informáticos.
Requisitos	Políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 28 Actividad 21 de auditoria informática en MEGAKONS S.A.

Actividad 21	
Código	CAU21
Actividad	Verificación de las vulnerabilidades del software instalado en el sistema.
Descripción	Confirmar la existencia del análisis de las vulnerabilidades del software y sistema operativo instalado en los equipos informáticos de la empresa.
Requisitos	Análisis de riesgo.
Responsable	Marco Tenezaca

Tabla 29 Actividad 22 de auditoria informática en MEGAKONS S.A.

Actividad 22	
Código	CAU22
Actividad	Revisión de restricciones de usuarios en la instalación de software.
Descripción	Confirmar la existencia de políticas vinculadas a la restricción de los usuarios al manejo o instalación de otros programas dentro de los computadores de la empresa.
Requisitos	Políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 30 Actividad 23 de auditoria informática en MEGAKONS S.A.

Actividad 23	
Código	CAU23
Actividad	Comprobación de controles de auditoría de los sistemas.
Descripción	Confirmar la existencia de registros de actividades de la base de datos de la empresa.
Requisitos	Documentación de cambios en la base de datos.
Responsable	Marco Tenezaca

Tabla 31 Actividad 24 de auditoria informática en MEGAKONS S.A.

Actividad 24	
Código	CAU24
Actividad	Verificación de la segmentación de redes.
Descripción	Confirmar si existe un documento donde especifique la estructura de la red.
Requisitos	Documento de estructura de la red.
Responsable	Marco Tenezaca

Tabla 32 Actividad 25 de auditoria informática en MEGAKONS S.A.

Actividad 25	
Código	CAU25
Actividad	Revisión de las políticas y procedimientos de intercambio de información.
Descripción	Confirmar la existencia de políticas que ayuden a el manejo del intercambio de información dentro de la empresa por parte de los empleados.
Requisitos	Políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 33 Actividad 26 de auditoria informática en MEGAKONS S.A.

Actividad 26	
Código	CAU26
Actividad	Revisión de las políticas de seguridad de la información para suministradores.
Descripción	Revisar la existencia de política de seguridad vinculadas a los proveedores de la empresa para resguardar la seguridad de la información.
Requisitos	Políticas de seguridad.
Responsable	Marco Tenezaca

Tabla 34 Actividad 27 de auditoria informática en MEGAKONS S.A.

Actividad 27	
Código	CAU27
Actividad	Verificación de las responsabilidades y procedimientos en los incidentes de la seguridad de la información.
Descripción	Confirmar la existencia de documentos de funciones de los empleados referente a la seguridad de la información.
Requisitos	Documento de funciones de los empleados.
Responsable	Marco Tenezaca

Tabla 35 Actividad 28 de auditoria informática en MEGAKONS S.A.

Actividad 28	
Código	CAU28
Actividad	Análisis de las notificaciones de los eventos de seguridad de la información.
Descripción	Confirmar la existencia y el seguimiento de la documentación de notificaciones ante algún suceso de la empresa referente a la seguridad de la información.
Requisitos	Documentación de notificaciones sobre eventos.
Responsable	Marco Tenezaca

Tabla 36 Actividad 29 de auditoria informática en MEGAKONS S.A.

Actividad 29	
Código	CAU29
Actividad	Revisión de protección de datos y privacidad de la información personal
Descripción	Confirmar si se cumple la ley de protección de datos establecida por el estado.
Requisitos	Ley de protección de datos.
Responsable	Marco Tenezaca

3.3.3 Ejecución de la auditoria informática en MEGAKONS S.A. (Check).

Una vez definidas las actividades de la auditoria informática, se procede a analizar cada una de las actividades y realizar una valoración de cumplimiento.

Tabla 37. Calificación de actividades según su cumplimiento

Calificación de las actividades		
CALIFICACIÓN	**DESCRIPCIÓN**	**COLOR**
APROBADO	Valida que la actividad o componente a evaluar cumpla con la norma ISO 27001 plenamente y que no se ha detectado ningún incumplimiento de los estándares de seguridad de la información.	
APROBADO CON OBSERVACIONES	Implica que la actividad o componente a evaluar se ajusta en su mayor parte a las normas ISO 27001 y que se han encontrado cosas que pueden mejorar para lograr tu cumplimiento pleno.	
NEGADO CON OBSERVACIONES	Implica que la actividad o componente a evaluar tiene deficiencias significativas por lo cual no cumple con los criterios de la norma ISO 27001. Pero aun así se puede hacer mejoras para asegurar su cumplimiento.	
NEGADO	Indica que la actividad o elemento a evaluar no cumple con los requisitos de la norma ISO 27001 y no hay indicios de mejoras para su cumplimiento.	

Tabla 38. Ejecución de actividad 1.

Ejecución de actividad 1 **Fecha: 13/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU01
Resultados	Las políticas de seguridad que tiene definido la empresa están incompletas como se puede observar en el **ANEXO B**, debido a que existen algunos puntos dentro de las políticas que no están tomadas en cuenta como: • Política de escritorio y pantalla limpios. • Política de Transferencia de la información. • Políticas de Teletrabajo. • Políticas de instalaciones y uso del software.
Calificación	**NEGADO CON OBSERVACIONES**
Observación	Se necesita actualizar las políticas de seguridad de la empresa.

Tabla 39.Ejecución de actividad 2.

Ejecución de actividad 2 **Fecha: 15/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU02
Resultados	Las políticas de seguridad de la empresa están definidas en base a un análisis que tiene correcciones por hacer, un documento que sustente el seguimiento de estas políticas no existe.
Calificación	**NEGADO**
Observación	Se necesita un documento donde se detalle el seguimiento del análisis de las políticas de seguridad.

Tabla 40. Ejecución de actividad 3.

Ejecución de actividad 3 **Fecha: 14/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU03
Resultados	No existe un documento que designe como encargado a un empleado de la empresa como el encargado de la seguridad de la información.
Calificación	**NEGADO**
Observación	Se necesita un documento donde se asigne roles y responsabilidades a los empleados del área de TI

Tabla 41.Ejecución de actividad 4.

Ejecución de actividad 4 **Fecha: 16/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU04
Resultados	Si no existe un documento con roles sobre la seguridad de la información como se ve en la **TABLA 40**, podemos verificar que tampoco existe un documento donde se asignen responsabilidades a uno de los empleados del área de TI sobre la seguridad de la información
Calificación	**NEGADO**
Observación	Se necesita un documento con actividades y responsabilidades dentro del documento de roles del área de TI.

Tabla 42.Ejecución de actividad 5.

Ejecución de actividad 5 **Fecha: 17/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU05
Resultados	No existen documentación para validar la seguridad de la información de nuevos proyectos en la empresa.
Calificación	**NEGADO**
Observación	Se necesita una documentación en la cual existan procedimientos y políticas a seguir para nuevos proyectos.

Tabla 43.Ejecución de actividad 6.

Ejecución de actividad 6 **Fecha: 20/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU06
Resultados	La empresa cuenta con un documento de activos definidos referente a la seguridad de la información como se detalla en el **ANEXO A,** sin embargo, el documento se encuentra incompleto debido a que no existe: • Clasificación por su importancia • Clasificación por el tipo de activo • Propietario del activo Además, existen activos informáticos que no están en e documento debido a que no se actualizó este documento desde el 2021.
Calificación	**APROBADO CON OBSERVACIONES**
Observación	Se necesita hacer una actualización de los activos de la empresa y mejorar su documento con lo establecido en los resultados.

Tabla 44.Ejecución de actividad 7.

Ejecución de actividad 7 **Fecha: 21/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU07
Resultados	Según lo analizado en el **ANEXO B** se encontró que: • Existe una política de seguridad de los recursos informáticos donde se detalla cómo debe ser configurado, actualizado y asegurado un dispositivo informático. • Existe una política de uso aceptable de los recursos informáticos donde se detalla algunas reglas que deben cumplir los empleados con respecto a sus recursos informáticos asignados. A demás como se puede observar en el **ANEXO I**, podemos observar que existen configuraciones para evitar la navegación en redes sociales.
Calificación	**APROBADO CON OBSERVACIONES**
Observación	Se necesita un análisis más profundo para poder determinar el buen uso de los recursos informáticos en la empresa.

Tabla 45.Ejecución de actividad 8.

Ejecución de actividad 8 **Fecha: 22/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU08
Resultados	La empresa solo cuenta con una ficha de activos de información ver **ANEXO A** y dentro de ese archivo solo existe una clasificación según su valor dentro de la empresa (alto, medio, bajo), además en las políticas de seguridad ver **ANEXO B**, existe la política de clasificación y etiquetado de datos, pero esta no tiene un documento que sustente su aplicación.
Calificación	**NEGADO CON OBSERVACIONES**
Observación	Se necesita tener una ficha de etiquetado de la información según la importancia de los activos.

Tabla 46.Ejecución de actividad 9.

Ejecución de actividad 9 **Fecha: 23/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU09
Resultados	Según lo analizado en el **ANEXO B** se encontró una política de acceso y control de la información donde se detalla que: • El acceso a la información esta detallada según el rol que cumple cada empleado. • Si se necesita acceso a la información confidencial se debe detallar con un oficio a la persona encargada como se detalla en el **ANEXO C**. Sin embargo, no existen procedimiento que sustenten el manejo de los activos de información en la empresa.
Calificación	**APROBADO CON OBSERVACIONES**
Observación	Se necesita un análisis más profundo para poder determinar el buen uso de los activos en la empresa, además se necesita tener en cuenta la creación de procedimientos que ayuden al buen manejo de estos

Tabla 47.Ejecución de actividad 10.

Ejecución de actividad 10 **Fecha: 24/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU10
Resultados	No existe ninguna política que especifique el uso adecuado de los dispositivos de almacenamiento externo.
Calificación	**NEGADO**
Observación	Generar una política donde especifique el uso de los dispositivos de almacenamiento externos en la empresa y sus penalidades.

Tabla 48.Ejecución de actividad 11.

Ejecución de actividad 11 **Fecha: 27/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU11
Resultados	Como se puede observar en el **ANEXO B**, existe unas políticas de seguridad de acceso donde se detalla el seguimiento al acceso de los servidores de a la empresa. Por otra parte, como se observa en el **ANEXO D**, tenemos un formato de control o seguimiento de las personas que tuvieron acceso al área de servidores.
Calificación	**APROBADO**
Observación	Sin observaciones.

Tabla 49.Ejecución de actividad 12.

Ejecución de actividad 12 **Fecha: 28/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU12
Resultados	Como se puede observar en el **ANEXO B**, existe unas políticas de seguridad de red donde se detalla algunas políticas que se deben seguir para un uso adecuado de las redes, sin embargo, existen algunos puntos a considerar que no están especificados en la política como: • Monitoreo y registro de acceso a redes. • Prueba de penetración para evaluar el control de acceso. • Mejoras en la autenticación para confirmar la identidad de los empleados.
Calificación	**NEGADO CON OBSERVACIONES**
Observación	Se debe implementar ciertas políticas para asegurar el acceso y control de las redes, además debe existir un control de las personas que tiene acceso a la red.

Tabla 50.Ejecución de actividad 13

Ejecución de actividad 13 **Fecha: 29/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU13
Resultados	Como se puede observar en el **ANEXO B**, en la política de Gestión de contraseñas, especifica lo siguiente: • Mínimo de caracteres • Combinaciones entre letras, caracteres y números. • Aviso sobre la no utilización de información personal • Aviso sobre la no utilización de palabras comunes • Tiempo adecuado para cambiar la contraseña A demás tienen un gestor de contraseñas el cual les ayuda a mantener un mejor control de todos los accesos a los diferentes sitios web como se puede observar en el **ANEXO K**.
Calificación	**APROBADO**
Observación	Sin observaciones

Tabla 51.Ejecución de actividad 14.

Ejecución de actividad 14 **Fecha: 30/11/2023** **Encargado:** Marco Tenezaca	
Código	CAU14
Resultados	Como se puede observar en el **ANEXO B**, en la política de seguridad física, especifica lo siguiente: • Control de identificación por parte de todos los empleados • El área de servidores debe estar restringida y debe tener medidas de seguridad. • Se debe tener un sistema de alarma y cámaras de vigilancia en el área de servidores A su vez como se puede observar en el **ANEXO J**, existe cierta señalización dentro del área de sistemas y del servidor.
Calificación	**APROBADO CON OBSERVACIONES**
Observación	Se necesita más señalética de restricciones en el área de sistemas y servidores.

Tabla 52.Ejecución de actividad 15.

Ejecución de actividad 15 **Fecha: 01/12/203** **Encargado:** Marco Tenezaca	
Código	CAU15
Resultados	Como se puede observar en el **ANEXO E** existe un documento de control de mantenimiento de equipos informáticos.
Calificación	**APROBADO**
Observación	Sin observaciones

Tabla 53.Ejecución de actividad 16.

Ejecución de actividad 16 **Fecha: 04/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU16
Resultados	No existe ningún documento donde se encuentren los procedimientos de la empresa, esto quiere decir que no existen instrucciones detalladas de los procesos que se realizan en la empresa.
Calificación	**NEGADO**
Observación	Realizar un documento de procedimientos.

Tabla 54.Ejecución de actividad 17.

Ejecución de actividad 17 **Fecha: 05/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU17
Resultados	No existe una documentación de controles y políticas para la verificación de código malicioso dentro de los sistemas desarrollados de la empresa.
Calificación	**NEGADO**
Observación	Realizar un análisis de las políticas a seguir para asegurar la información dentro del código de programación en los sistemas de la empresa.

Tabla 55.Ejecución de actividad 18.

Ejecución de actividad 18 **Fecha: 06/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU18
Resultados	En el **ANEXO B**, podemos verificar que existe una política de seguridad contra las copias de seguridad y a su vez en el **ANEXO A**, existe un documento que verifica los activos de la empresa sin embargo no existe un documento para poder verificar los activos que se deben someter a una copia de seguridad y cada que tiempo se debe actualizar dicha copia.
Calificación	**NEGADO**
Observación	Generar un documento donde se sustente los activos que necesitan una copia de seguridad.

Tabla 56.Ejecución de actividad 19.

Ejecución de actividad 19 **Fecha: 07/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU19
Resultados	Como se puede observar en el **ANEXO F**, existe un documento donde se registra los eventos que pasan en la empresa.
Calificación	**APROBADO**
Observación	Sin observaciones.

Tabla 57.Ejecución de actividad 20.

Ejecución de actividad 20 **Fecha: 11/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU20
Resultados	No existe un documento donde detallen los procedimientos a seguir sobre la instalación de software en los recursos informáticos de la empresa.
Calificación	**NEGADO**
Observación	Crear documento de procedimientos sobre la instalación de software en la empresa.

Tabla 58.Ejecución de actividad 21.

Ejecución de actividad 21 **Fecha: 12/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU21
Resultados	Como se puede ver en el **ANEXO G**, no existe un análisis de riesgo vinculado a la instalación de software dentro de los computadores de la empresa.
Calificación	**NEGADO**
Observación	Añadir al documento del análisis de riesgo vinculado a la instalación de software en los computadores de la empresa.

Tabla 59.Ejecución de actividad 22.

Ejecución de actividad 22 **Fecha: 13/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU22
Resultados	Como se puede observar en el **ANEXO B**, existe una política de seguridad vinculada con las restricciones a los empleados al momento de instalar software en los computadores de la empresa.
Calificación	**APROBADO CON OBSERVACIONES**
Observación	Se debe implementar un documento que especifique el software que está autorizado a instalarse.

Tabla 60.Ejecución de actividad 23.

Ejecución de actividad 23 **Fecha: 14/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU23
Resultados	Como se puede observar en el **ANEXO D**, existe un documento para el registro de las actividades de la base de datos en la empresa.
Calificación	**APROBADO**
Observación	Sin observaciones.

Tabla 61.Ejecución de actividad 24.

Ejecución de actividad 24 **Fecha: 15/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU24
Resultados	No existe un documento de: • Estructura de cableado de red. • Diagrama de red.
Calificación	**NEGADO**
Observación	Crear un diagrama de red y un documento sobre la estructura del cableado de red.

Tabla 62.Ejecución de actividad 25.

Ejecución de actividad 25 **Fecha: 18/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU25
Resultados	No existen políticas ni procedimientos de intercambio de información entre los empleados.
Calificación	**NEGADO**
Observación	Se necesita un registro del intercambio de información confidencial en la empresa.

Tabla 63.Ejecución de actividad 26.

Ejecución de actividad 26 **Fecha: 19/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU26
Resultados	Como se observa en el **ANEXO B**, existe una política sobre la seguridad de la información para suministradores donde se detalla las reglas que deben cumplir los proveedores de la empresa para asegurar la información de esta.
Calificación	**APROBADO**
Observación	Sin observaciones.

Tabla 64.Ejecución de actividad 27.

Ejecución de actividad 27 **Fecha: 20/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU27
Resultados	No existen procedimientos para los incidentes de la seguridad de la información en la empresa, sin embargo, como se puede observar en el **ANEXO G**, existe un análisis de riesgo de las posibles vulnerabilidades de la empresa y también como se puede observar en el **ANEXO H**, podemos verificar que existe un plan de contingencia de los posibles riesgos de la empresa.
Calificación	**NEGADO CON OBSERVACIONES**
Observación	Se necesita generar procedimientos que establezcan los posibles incidentes sobre la seguridad de la información en la empresa.

Tabla 65.Ejecución de actividad 28.

Ejecución de actividad 28 **Fecha: 21/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU28
Resultados	Al no tener procedimientos definidos sobre los incidentes en la seguridad de la información tampoco se tiene un seguimiento de estos procedimientos, solo te tiene un formato de eventos que se registran en la empresa como podemos observar en el **ANEXO F.**
Calificación	**NEGADO**
Observación	Se necesita cumplir los requerimientos de la **TABLA**, para crear un formato de seguimiento.

Tabla 66.Ejecución de actividad 29.

Ejecución de actividad 29 **Fecha: 26/12/2023** **Encargado:** Marco Tenezaca	
Código	CAU29
Resultados	La empresa cumple con ciertos protocolos de seguridad de la información y a su vez tiene políticas de seguridad que ayudan a que la información de terceros no sea vulnerable a robos, entre estas políticas están: • Buen manejo de los datos por parte de los empleados. • Capacitaciones a los empleados sobre el buen uso de la información. Buen manejo de contraseñas en toda la empresa. • Políticas de seguridad de la información para los proveedores.
Calificación	**NEGADO CON OBSERVACIONES**
Observación	Se necesita una actualización de políticas de seguridad de la información y la creación de ciertos procedimientos que sustenten los procesos que se lleva a cabo en la empresa.

3.3.4 Informe de la Auditoria informática externa (Act).

1. Portada

Título: Informe de auditoría informática externa con normas ISO 27001

Empresa: MEGAKONS S.A.

Dirigido a: Ing. David Parra.

Cargo: Jefe de área de sistemas de la empresa.

Auditor: Marco Orlando Tenezaca Caizabanda

Misión

Generar valor en la comercialización de productos y servicios para la construcción, a través de la innovación de nuestros procesos.

Visión

• En el año 2032 ser uno de los 5 principales importadores y distribuidores en el mercado nacional, diversificando el negocio de forma confiable y sostenible en el tiempo.

• En el año 2025 llegar a comercializar el 20% de producto importado del total de nuestras ventas; reconocidos como una empresa altamente competitiva, ofreciendo productos y servicios de calidad.

• En el año 2023 aspiramos tener un crecimiento del 15% en ventas; apalancándonos en líneas de negocio rentables, manteniendo relaciones confiables con todas nuestras partes interesadas.

Fecha: 22/12/2023

2. Objetivos

- Evaluar la Conformidad con ISO 27001.
- Revisión del análisis de seguridad.
- Revisar la Implementación de Controles de Seguridad definidos como aplicables.
- Verificar el Cumplimiento de los procesos de seguimiento y control.

3. Alcance:

La empresa MEGAKONS S.A. desea someterse a una auditoria informática externa con normas ISO 27001 las cuales están vinculadas con la seguridad de la información, para lo cual se analizará su Sistemas de Gestión de Seguridad de la Información (SGSI), con el objetivo de evaluar si cumple con los requisitos establecidos en la norma.

La auditoría informática estará asociada únicamente al local principal por lo cual se evaluará todo lo obtenido dentro de esta sucursal, además se analizará los puntos que la empresa tiene implementados y que el auditor crea importante se cumpla dentro de la empresa.

4. Límites y Extensión:

La auditoría se centrará en los controles y procesos definidos por la empresa y se analizara los dispositivos informáticos que existen en la empresa y se verificara su correcto funcionamiento en base a la seguridad de la información.

5. Marco Legal

Normas ISO 27001

ANEXO A DE normas ISO 27001

Ley de protección de datos.

6. Criterios

Normas ISO 27001:2013

Todos lo evaluado se basó en los requisitos establecidos en la norma ISO 27001:2013.

Políticas y procedimientos de ISO 27001

Se utilizo la documentación que posee la empresa como, plan de contingencia, análisis de riesgos, bitácoras, plan estratégico.

Los controles para auditar de la empresa MEGAKONS S.A. deben estar alineados a los controles que existen en las normas ISO 27001. El anexo A detalla los controles y objetivos a través de los 18 dominios que tiene la norma, para aplicar la auditoria informática en la empresa se tomó en cuenta los siguientes controles:

- A.5. Políticas de seguridad.
- A.6. Aspectos organizativos de la seguridad de la información.
- A.8. Gestión de activos.
- A.9. Control de accesos.
- A.10. Cifrado.
- A.11. Seguridad física y ambiental.
- A.12. Seguridad en la operativa.
- A.13. Seguridad en las telecomunicaciones.
- A.15. Relaciones con suministradores.

- A.16. Gestión de incidentes en la seguridad de la información.
- A.18. Cumplimiento.

7. Metodología utilizada

Con la finalidad de analizar y evaluar los requerimientos de la norma ISO 27001 el auditor tomo en cuenta la siguiente metodología.

Planificar

El auditor define el alcance de la auditoria, así como sus límites y criterios establecidos según la norma a utilizar. A su vez realiza las actividades que se va a llevar a cabo dentro de la auditoria.

Hacer

El auditor analizo todos los documentos que serán necesarios para realizar la auditoria informática y así proceder a solicitar a la empresa estos documentos como análisis de riesgos, políticas de seguridad, plan de contingencia, procedimientos entre otros documentos importantes, para posteriormente determinar si cumplen con la norma aplicada.

Verificar

El auditor ejecuta la auditoria llevando a cabo cada una de las actividades generadas anteriormente y mediante un rango de valoración da una calificación a cada una de las actividades.

- **Aprobado:** si la actividad cumple plenamente con lo establecido en la norma.
- **Aprobado con observaciones:** Si la actividad cumple en su mayor parte con lo establecido en la norma, pero puede ser sujeta a mejoras.
- **Negado con observaciones:** Si la actividad tiene varias deficiencias en su cumplimiento, pero existen aspectos que si cumplen con lo establecido en la norma.
- **Negado:** Si la actividad no cumple con lo establecido en la norma.

Actuar

El auditor emitirá un informe completo con todos los hallazgos obtenidos dentro de la empresa referente a la seguridad de la información a demás se otorgará diferentes recomendaciones que harán que la empresa mejore su SGSI y así pueda cumplir de mejor manera con la norma ISO 27001.

8. Planificación de actividades.

ACTIVIDADES DE AUDITORIA	
CÓDIGO	**ACTIVIDAD**
CAU01	Verificar las políticas de seguridad.
CAU02	Examinar la existencia de un control de seguimiento de las políticas de seguridad.
CAU03	Inspeccionar si existe una persona encargada de la seguridad de la información de la empresa.
CAU04	Examinar si la persona encargada tiene definidas tareas y responsabilidades.
CAU05	Verificar si existe seguridad de la información para nuevos proyectos.
CAU06	Revisar si existe un inventario de activos de información.
CAU07	Inspeccionar como se garantiza el buen uso de los activos de información.
CAU08	Revisar si existe una clasificación de los activos de la empresa.
CAU09	Como se maneja el acceso a la información confidencial de la empresa.
CAU10	Verificar como se maneja el soporte de almacenamiento.
CAU11	Revisión del acceso físico a la zona de servidores.
CAU12	Revisión del acceso a redes inalámbricas.
CAU13	Revisar las políticas de claves seguras.
CAU14	Revisión física de las oficinas vinculado con la seguridad de los equipos de TI.
CAU15	Comprobar si existe documentación de los mantenimientos de los equipos informáticos.
CAU16	Revisión de procedimiento de operación.
CAU17	Revisión de controles para el código malicioso.
CAU18	Verificación de la gestión de las copias de seguridad.
CAU19	Revisión de los registros de eventos de actividad.
CAU20	Verificación de instalación de software en el sistema operativo.
CAU21	Verificación de las vulnerabilidades del software instalado en el sistema.
CAU22	Revisión de restricciones de usuarios en la instalación de software.
CAU23	Comprobación de controles de auditoría de los sistemas.
CAU24	Verificación de la segmentación de redes.
CAU25	Revisión de las políticas y procedimientos de intercambio de información.
CAU26	Revisión de las políticas de seguridad de la información para suministradores.
CAU27	Verificación de las responsabilidades y procedimientos en los incidentes de la seguridad de la información.
CAU28	Análisis de las notificaciones de los eventos de seguridad de la información.
CAU29	Revisión de protección de datos y privacidad de la información personal

9. Cronograma de actividades

	Nombre de tarea	Fecha de ini	Fecha final
		13/11/202:	26/12/202
1	Verificar la existencia de Políticas de seguridad .	13/11/2023	14/11/202:
2	Examinar documentos de roles del área de TI.	14/11/2023	15/11/202:
3	Verificar el seguimiento de cumplimiento de políticas de seguridad.	15/11/2023	16/11/202:
4	Examinar si la persona encargada tiene definidas tareas y responsabilidades.	16/11/2023	17/11/202:
5	Verificar la existencia de políticas para nuevos proyectos	17/11/2023	17/11/202:
6	Revisar si existe documentación de activos de información.	20/11/2023	21/11/202:
7	Inspeccionar como se garantiza el buen uso de los activos de información.	21/11/2023	22/11/202:
8	Revisar la existencia de una clasificación de activos.	22/11/2023	23/11/202:
9	Como se maneja el acceso de la información en la empresa.	23/11/2023	24/11/202:
10	Verificar como se maneja el soporte de almacenamiento.	24/11/2023	24/11/202:
11	Revisión del acceso físico a la zona del servidor.	27/11/2023	28/11/202:
12	Revisión del acceso a redes inalámbricas.	28/11/2023	29/11/202:
13	Revisar políticas de claves seguras.	29/11/2023	29/11/202:
14	Revisar las oficinas y verificar la seguridad de los equipos de TI.	30/11/2023	01/12/202:
15	Verificar la existencia de documentos de mantenimiento de equipos informáticos.	01/12/2023	01/12/202:
16	Revisar de procedimientos de operación.	04/12/2023	05/12/202:
17	Revisar controles para el código malicioso.	05/12/2023	06/12/202:
18	Verificar la gestión de copias de seguridad.	06/12/2023	07/12/202:
19	Revisar los registros de eventos de actividad.	07/12/2023	08/12/202:
20	Verificar la existencia de documentos para instalación de software en los equipos.	11/12/2023	12/12/202:
21	Revisar el análisis de vulnerabilidades del software instalado.	12/12/2023	13/12/202:
22	Revisión de restricciones al instalar software en los equipos.	13/12/2023	14/12/202:
23	Revisar la existencia de controles de auditoria de los sistemas.	14/12/2023	15/12/202:
24	Verificación de la segmentación de redes.	15/12/2023	15/12/202:
25	Revisar las políticas y procedimientos de intercambio de información.	18/12/2023	19/12/202:
26	Revisión de políticas para proveedores.	19/12/2023	20/12/202:
27	Verificar las responsabilidades y procedimientos en los incidentes.	20/12/2023	21/12/202:
28	Análisis de las notificaciones de eventos ocurridos en la empresa.	21/12/2023	22/12/202:
29	Revisión de documentos de protección de datos y privacidad de la información perso...	26/12/2023	26/12/202:

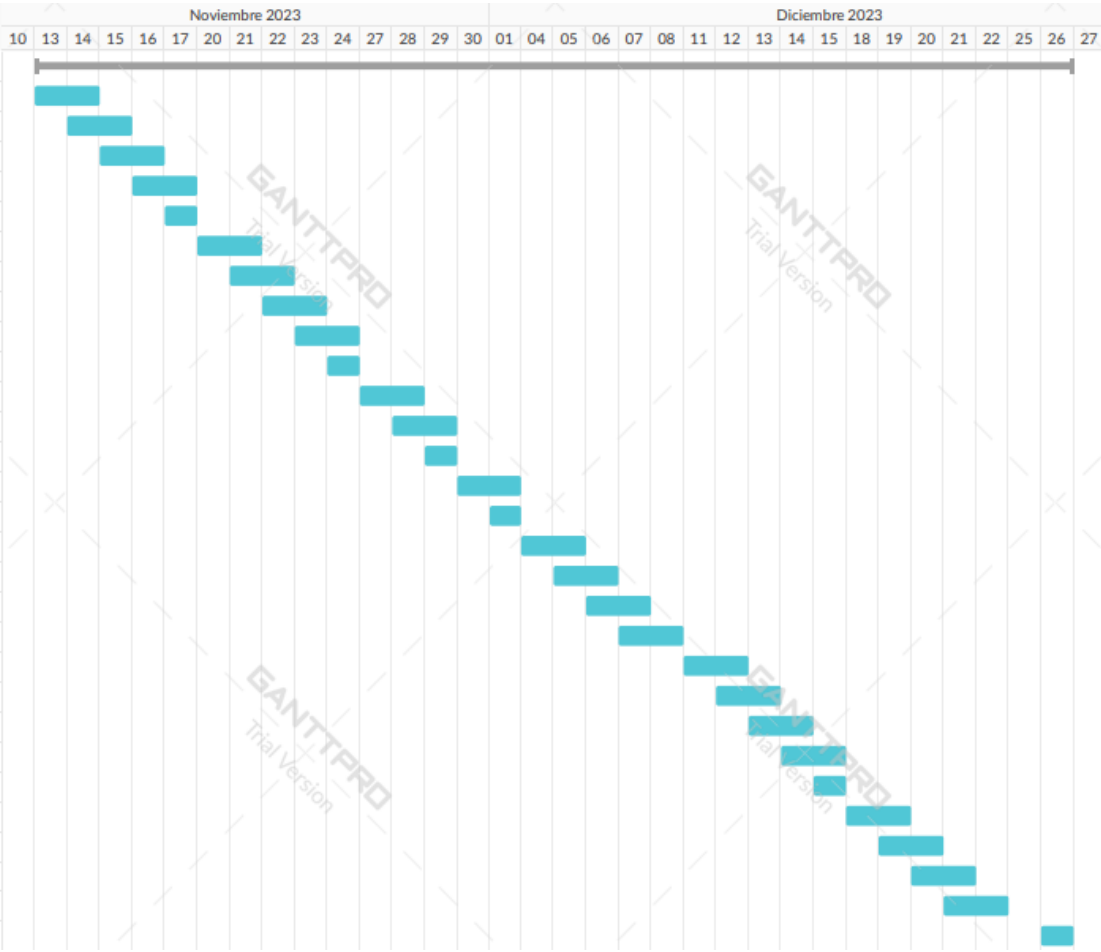


Figura. 13 Cronograma de actividades

10. Resultados de la Auditoria

La auditoría realizada en la empresa MEGAKONS S.A. se divide en 4 resultados según el cumplimiento de cada actividad:

- En conformidad
- En conformidad con observaciones
- No conformidad con observaciones
- No conformidad

Y se obtuvo los siguientes resultados.

10.1. En conformidad

Código: CAU11

Requisito cumplido: Política de control de accesos (A.9.1.1).

Descripción: La empresa tiene políticas de seguridad de acceso donde se puede observar:

- El personal no tiene acceso al servidor al menos que tenga los permisos necesarios.
- El personal que necesite acceso al servidor necesita realizar un oficio

Por lo cual se cumple el requerimiento de la actividad.

Evidencia: Revisar **Anexo B y Anexo D.**

Código: CAU13

Requisito cumplido: Gestión de claves (A.10.1.2).

Descripción: La empresa tiene una política de gestión de contraseñas en la que especifica:

- El mínimo de caracteres que debe tener la contraseña
- La combinación que debe tener entre letras, números y caracteres especiales.
- No utilizar palabras comunes

- Generar contraseñas diferentes para cada plataforma.
- Tiempo estimado de actualización de contraseñas.

Por lo cual se cumple el requerimiento de la actividad

Evidencia: Revisar **Anexo B y Anexo K.**

Código: CAU15

Requisito cumplido: Mantenimiento de los equipos (A.11.2.4).

Descripción: La empresa tiene un formato en el cual lleva un control de los mantenimientos de los equipos informáticos bien detallado el cual ayuda a tener un mejor control y ayuda asegurar la información de la empresa.

Por lo cual se cumple el requerimiento de la actividad.

Evidencia: Revisar el **Anexo E.**

Código: CAU19

Requisito cumplido: Registro y gestión de eventos de actividad (A.12.4.1).

Descripción: La empresa tiene un formato en el cual se lleva un control de los eventos ocurridos a nivel informáticos como:

- Fallas en el sistema
- Daños en los equipos informáticos
- Robo de información

Entre otros.

Por lo cual se cumple el requerimiento de la actividad.

Evidencia: Revisar **Anexo F.**

Código: CAU23

Requisito cumplido: Controles de auditoría de los sistemas de información (A.12.7.1).

Descripción: La empresa tiene un formato donde se puede llevar control de las personas que tienen acceso a la base de datos de tal modo se aseguran de que la información este protegida y en caso de existir un problema se podría llegar al culpable.

Por lo cual se cumple el requerimiento de la actividad.

Evidencia: Revisar **Anexo D.**

Código: CAU26

Requisito cumplido: Política de seguridad de la información para suministradores (A.15.1.1).

Descripción: La empresa cuenta con una política de seguridad de la información para suministradores(proveedores), donde se detalla lo siguiente:

- Acceso que tienen los proveedores a la información de la empresa.
- Reglamentos que deben cumplir los proveedores dentro de su empresa.
- Capacitaciones que deben tener los proveedores con respecto a la seguridad de la información
- Evidencia de capacitaciones y reglamentos.

Por lo cual se cumple el requerimiento de la actividad.

Evidencia: Revisar **Anexo B.**

10.2. En conformidad con observaciones.

Código: CAU06

Requisito cumplido con observación: Inventario de activos (A.8.1.1).

Descripción: La empresa tiene definido un documento de inventario de activos sin embargo se necesita ampliar el documento con detalles importantes que pueden ayudar a mejorar el uso y control de estos activos.

Evidencia: Revisar **Anexo B.**

Impacto: El no tener una clasificación más específica de los activos de información de la empresa puede llevar a dar acceso a quienes no deberían y así se pondría en riesgo a los activos de esta empresa.

Código: CAU07

Requisito cumplido con observación: Uso aceptable de los activos (A.8.1.3).

Descripción: La empresa tiene definidas políticas de seguridad de los recursos humanos donde se puede observar pocas reglas para el buen uso de los recursos informáticos. A demás existe una configuración para que los empleados no hagan un mal uso del internet, restringiendo ciertas páginas que pueden ayudar al robo de información.

Evidencia: Revisar **Anexo B** y **Anexo I.**

Impacto: El no tener bien definidas las políticas de seguridad de los recursos humanos implica mucho riesgo a nivel de los recursos informáticos donde están alojados los activos de información de la empresa.

Código: CAU09

Requisito cumplido con observación: Manipulación de activos (A.8.2.3).

Descripción: En la empresa existen políticas de acceso y control de la información donde se detalla:

- El acceso que se tiene a los activos de información.
- Reglas que debe tener cada empleado con sus contraseñas.
- Permisos de acceso a terceros.
- Permisos de acceso al servidor.

Sin embargo, no existen procedimiento que ayuden a sustentar estas políticas de acceso y algunas de las políticas no se cumplen dentro de la empresa como los roles que desempeña cada persona dentro del área de TI.

Evidencia: Revisar **Anexo B.**

Impacto: El no tener bien definidas las políticas de accesos y control de la información permiten que existan brechas de seguridad por donde podría existir robo de información de personas externas y el no tener procedimientos que avalen estas políticas hace que no se tenga la seguridad de que estas se apliquen.

Código: CAU14

Requisito cumplido con observación: Seguridad de oficinas, despachos y recursos (A.11.1.3).

Descripción: En la empresa existe una política de seguridad física donde se detalla:

- El control de identificación de los empleados en la empresa
- Las medidas y restricciones del área del servidor.
- Control mediante cámaras de seguridad y alarmas.

Además, existe cierta señalética dentro del área de TI, sin embargo, no existe señalética de: Área restringida al servidor.

- Acceso solo a personal autorizado.
- Evacuación en caso de emergencia.
- Instrucciones del buen uso de los recursos informáticos.

Evidencia: Revisar **Anexo B** y **Anexo J**.

Impacto: El no tener una señalética adecuada puede generar que cualquier persona ingrese a las áreas restringidas y pueda hacer un mal uso de los dispositivos que existen ahí, además en caso de un siniestro el personal no sabría por dónde evacuar para ponerse a salvo y eso genera caos que puede tener como consecuencia daños en los equipos.

Código: CAU22

Requisito cumplido con observaciones: Restricciones en la instalación de software (A.12.6.2).

Descripción: La empresa tiene una política de gestión de instalación de software donde se detalla lo siguiente:

- Permisos para instalar software.
- Inventario de software autorizado a instalarse.
- Instalación de software de fuentes confiables.
- Limitaciones por parte del personal para instalar software.

Sin embargo, al verificar dentro de la empresa estas políticas no se cumplen debido a que no existe un documento el cual sustente cual es el software permitido a instalar, además no se tiene un control del software que tiene cada empleado en su computador.

Evidencia: Revisar **Anexo B.**

Impacto: El no cumplir unas políticas establecidas genera un problema dentro de la empresa, el permitir que los empleados instalen cualquier programa dentro de su computador, por lo cual podría ingresar virus que dañe el recurso informático o que robe información.

10.3. No conforme con observaciones.

Código: CAU01

Requisito no cumplido con observación: Conjunto de políticas para la seguridad de la información (A.5.1.1).

Descripción: La empresa tiene definidas políticas de seguridad de la información sin embargo se necesita tener una actualización de las políticas e implementar políticas que a lo largo del tiempo son necesarias para poder mejorar la seguridad de la información.

Evidencia: Revisar **Anexo B.**

Impacto: El no tener unas políticas de seguridad actualizadas puede generar un riesgo al momento manipular la información de la empresa ya que puede existir robos o perdida de activos importantes.

Código: CAU08

Requisito no cumplido con observación: Directrices de clasificación (A.8.2.1).

Descripción: En la empresa solo se cuenta con un documento donde se detallan los activos de información que existen, sin embargo, a este documento le falta una clasificación más detallada para así poder mejorar la seguridad de los activos.

Existe una política de clasificación de la información sin embargo no está implementada dentro de la empresa por lo cual queda invalidada la política.

Evidencia: Revisar **Anexo A** y **Anexo B.**

Impacto: El no tener una clasificación de los activos de información en la empresa hace que documentos confidenciales o de acceso restringido están a la mano de cualquier empleado y por lo tanto se puede perder o hacer mal uso de este activo.

Código: CAU12

Requisito no cumplido con observación: Control de acceso a las redes y servicios asociados (A.9.1.2).

Descripción: En la empresa existe una política de seguridad de red donde se detalla lo siguiente:

- Configuración de los equipos informáticos que tengan acceso a la red
- Actualizaciones de los equipos.
- Contraseñas de los equipos.
- Acceso al área de redes y recursos.
- Restricción de carpetas compartidas.

Sin embargo, estas políticas no son suficientes para garantizas el control de acceso a la red, además de no existir pruebas de penetración constantes no se puede saber en qué estado se encuentra el acceso a la red de la empresa.

Evidencia: Revisar **Anexo B.**

Impacto: El no tener un control del personal que accede a la red, ni hacer constantemente penetraciones para verificar el control de acceso puede generar varias brechas de seguridad donde cualquier persona externa con conocimiento en redes puede manipular y llegar a provocar un caos dentro de la empresa.

Código: CAU27

Requisito no cumplido con observación: Responsabilidades y procedimientos (A.16.1.1).

Descripción: No se encontraron procedimiento que sustenten los incidentes de la seguridad de la información en la empresa.

Sin embargo, se encontró información dentro del análisis de riesgos y un plan de contingencia a cada uno de los riesgos establecidos.

Evidencia: Revisar **Anexo G** y **Anexo H.**

Impacto: El no tener procedimiento sobre incidentes que pueden ocurrir dentro de la empresa, puede generar respuesta ineficientes y aumento de riesgo de daños sobre los activos de información de la empresa.

Código: CAU29

Requisito no cumplido con observación: Protección de datos y privacidad de la información personal (A.18.1.4).

Descripción: En la empresa existe ciertas políticas de seguridad de la información que ayudan a cumplir con algunos requerimientos de la ley de protección de datos dentro del Ecuador como:

- Políticas de seguridad para los proveedores.
- Reglas para mejorar la seguridad de los datos como contraseñas seguras y control de acceso a la información.
- Buen manejo de los datos personales por parte de los empleados

Sin embargo, la empresa no cuenta con la capacitación suficiente para mejorar e implementar todas las reglas que se necesitan para cumplir la ley de protección de datos.

Evidencia: Revisar **Anexo B.**

Impacto: La empresa puede sufrir una sanción por parte de la ley de Ecuador en caso de tener un robo de información y que la misma sea utilizada con fines lucrativos.

10.4. No conforme

Código: CAU02

Requisito no cumplido: Revisión de las políticas para la seguridad de la información (A.5.1.2).

Descripción: En la empresa no existe un documento de seguimiento y análisis a las políticas de seguridad, por lo cual se estima que desde que se creó las políticas no se han actualizado ni se han analizado nuevas políticas que pudiesen faltar.

Evidencia: No existe documento que sustente el seguimiento de las políticas de seguridad establecidas en la empresa.

Impacto: El no tener un documento de seguimiento a las políticas de seguridad genera una inestabilidad en el cumplimiento de estas, además del riesgo a tener posibles robos de información por no tener bien establecidas y actualizadas las políticas.

Código: CAU03

Requisito no cumplido: Asignación de responsabilidades para la seguridad de la información (A.6.1.1).

Descripción: La empresa no tiene una persona que se encargue de la seguridad de la información como podemos observar en las políticas de seguridad el encargado es toda el área de TI, además no existe un documento donde el área de TI asigne responsabilidades a cada uno de los miembros.

Evidencia: Revisar **Anexo B.**

Impacto: El tener un responsable en la seguridad de la información es fundamental en la toma de decisiones al momento de tener un problema con los activos de información, además la ausencia de un responsable genera falta de coordinación en la implementación y seguimiento de medidas de seguridad de la información.

Código: CAU04

Requisito no cumplido: Segregación de tareas (A.6.1.2).

Descripción: La empresa al no tener un documento de roles designados referente a la seguridad de la información tampoco tiene un documento que sustente las responsabilidades que debería tener la persona asignada.

Evidencia: No tiene un documento de asignación de actividades para el responsable de la seguridad de la información.

Impacto: El no dar responsabilidades a una persona sobre la seguridad de la información genera una falta de coordinación en el área de TI al momento de existir un problema.

Código: CAU05

Requisito no cumplido: Seguridad de la información en la gestión de proyectos (A.6.1.5).

Descripción: La empresa no tiene políticas ni procedimientos para validar la seguridad de la información en nuevos proyectos dentro de la misma.

Evidencia: No existe documento de seguridad de la información para nuevos proyectos.

Impacto: El no tener políticas y procedimientos para asegurar la información dentro de nuevos proyectos, genera que no se considere riesgos y eso a su vez puede generar pérdida o robo de información.

Código: CAU10

Requisito no cumplido: Gestión de soportes extraíbles (A.8.3.1).

Descripción: La empresa no tiene políticas de seguridad para el uso adecuado de dispositivos de almacenamiento externo.

Evidencia: No existe documentación.

Impacto: Puede existir una fuga de datos, debido a que los empleados podrían ingresar un dispositivo de almacenamiento y llevar la información valiosa de la empresa, además el no tener un control de estos dispositivos puede generar amenazas de malware y virus dentro de los computadores de la empresa.

Código: CAU16

Requisito no cumplido: Documentación de procedimientos de operación (A.12.1.1).

Descripción: En la empresa no existen un documento de procedimientos por lo cual no existen ningún tipo de instrucciones para los procesos que se ejecutan ni para las políticas establecidas.

Evidencia: No existe documentos.

Impacto: Sin documentación de procedimientos la empresa puede tener fallos debido a la falta de orientación sobre las diferentes tareas que se realizan, además sin este documento existe puede existir un retraso en la toma de decisiones en caso de algún fallo.

Código: CAU17

Requisito no cumplido: Controles contra el código malicioso (A.12.2.1).

Descripción: En la empresa no existen controles ni políticas contra el código malicioso, por lo cual, al momento de desarrollar algún sistema no se aplica ninguna regla que ayude a controlar o mitigar las brechas de seguridad y así evitar el robo de información.

Evidencia: Revisar el **Anexo B,** donde no existe ninguna política de código malicioso.

Impacto: Se puede tener un impacto negativo al momento de resguardar los activos de información de la empresa debido a que su código no tiene la seguridad necesaria o no cumple con una metodología de programación optima.

Código: CAU18

Requisito no cumplido: Copias de seguridad de la información (A.12.3.1).

Descripción: En la empresa existe una política de copias de seguridad, sin embargo, no se tomó en cuenta las copias de seguridad de los activos definidos en el documento de activo de la empresa (**Anexo A**).

Evidencia: Revisar **Anexo A** y **Anexo B.**

Impacto: El no tener bien definido los activos de información que se deben someter a una copia de seguridad pueden generar vulnerabilidades dentro de la empresa, como perdida y robo de información.

Código: CAU20

Requisito no cumplido: Instalación del software en sistemas en producción (A.12.5.1).

Descripción: En la empresa no existe un documento que detalle que software se puede instalar en los computadores de la empresa y quienes pueden instalarlo.

Evidencia: No existe un documento.

Impacto: El no tener un documento donde se detalle el software que debe estar instalado en los computadores de la empresa puede generar que cualquier programa pueda instalarse y este puede tener un programa maligno o virus, ya que no se puede llegar a saber la fuente de descarga. Todo esto puede generar brechas de seguridad y por ende un ataque cibernético.

Código: CAU21

Requisito no cumplido: Gestión de las vulnerabilidades técnicas (A.12.6.1).

Descripción: En la empresa existen un análisis de riesgo y un plan de contingencia estableció sin embargo en este no existe un análisis del software instalado dentro de los equipos informáticos ni su mitigación ante este suceso.

Evidencia: Revisar **Anexo G**.

Impacto: El no tener como riesgo las vulnerabilidades que existe al instalar software malicioso en los equipos informáticos de la empresa, puede generar un caos al momento de querer mitigar el error, ya que no existen directrices para arreglar el error.

Código: CAU24

Requisito no cumplido: Segregación de redes (A.13.1.3).

Descripción: La empresa no cuenta con un diagrama de red ni un documento de estructura del cableado de red.

Evidencia: No existe documento.

Impacto: El no tener un diagrama de red dificulta la comprensión de la topología de red en la empresa además de la ubicación física de los recursos informáticos. Y que no exista una estructura del cableado dificulta al momento de querer realizar cambios o mantenimientos al cableado de red.

Código: CAU25

Requisito no cumplido: Políticas y procedimientos de intercambio de información (A.13.2.1).

Descripción: En la empresa no existen políticas para el intercambio de información entre los empleados

Evidencia: Revisar **Anexo B,** donde no existe una política para el intercambio de información.

Impacto: El no tener unas políticas para regular el intercambio de información entre empleados puede generar un conflicto, ya que lo empleados tiene libre albedrio para pasar información por diferentes canales que no pueden ser seguros y así hay mayor posibilidad de un robo de información.

Código: CAU28

Requisito no cumplido: Notificación de los eventos de seguridad de la información (A.16.1.2).

Descripción: En la empresa solo existe un documento de eventos, pero no existe un documento que sustente el seguimiento de ese evento a demás al no existir procedimiento definidos esta actividad no puede darse en marcha.

Evidencia: No existe documento.

Impacto: Al no existir un documento de seguimiento de los eventos, no se puede saber cómo resolver en caso de que vuelva a suceder la mista catástrofe, además que no se puede saber cuáles son los puntos débiles en los que la empresa debe trabajar.

11. Conclusiones

11.1. Aspectos positivos

La gestión de claves seguras en la empresa está bien establecida por lo cual se puede asegurar la implementación de este control en los activos de información que se encuentran dentro de los computadores.

El seguimiento a los equipos informáticos se lleva de una forma adecuada con un documento que detalla lo más importante dentro del mantenimiento que se realiza a cada uno de los equipos, eso ayuda a mejorar la calidad de trabajo y asegurar los activos de la información de la empresa.

Tener un archivo el cual tenga seguimiento del personal que accede a la base de datos o al servidor de la empresa es importante, con este documento se mantiene un orden en caso de algo fallo, además el tener un oficio de acceso a este tipo de información general más seguridad para los activos de información de la empresa.

El tener reglas establecidas para los proveedores de la empresa es muy importante, porque todas las personas que necesiten información confidencial deben cumplir ciertos requisitos y así se evita al filtración o robo de información dentro de la empresa.

El establecer un documento donde se detallen los activos de información es muy importante para que la empresa tenga conocimiento de los documentos que pueden o no ser compartidos libremente por los empleados, sin embargo, se necesita tener un documento más descriptivo para poder clasificar estos activos de mejor manera como establece las normas ISO 27001.

Dentro de la empresa se observa un análisis de riesgo y un plan de contingencia establecido donde se observa algunos de los riesgos más comunes que pueden suceder dentro de una organización, sin embargo, se considera se podría mejorar este análisis de riesgos tomando

en cuenta un nuevo análisis de la situación de la empresa y así evitar que ocurra una catástrofe y no saber cómo mitigarla.

11.2.Aspectos negativos

No se tiene una política de seguridad bien detallada ni evidencia de capacitaciones a los empleados sobre la seguridad de la información dentro de la empresa.

No existe la suficiente señalética en los lugares de alto riesgo como área del servidor, ingreso al área de TI.

En la empresa no se cumple la política de restricciones de instalación de software debido a que no existe una persona encargada de verificar que cada uno de los empleados no tenga acceso a instalar cualquier software y tampoco existe un documento que sustente el software que se debe instalar dentro de los equipos de la organización.

Desde el día de su creación la empresa no ha realizado una actualización de sus políticas de seguridad de la información, lo cual no permite un buen funcionamiento de estas.

No existe un documento para la debida clasificación de los activos de información dentro de la empresa por lo cual no tiene validez un documento de activos sin tener una clasificación que ayude a mejorar la seguridad de estos y es un punto crítico a nivel de cumplimiento de las normas ISO 27001.

No existe un análisis de los riesgos que se pueden tener a nivel de redes, ni se tiene una partición de la red para controlar el acceso a internet dentro de la empresa, además no se encontró evidencia de un diagrama de red ni de un documento de estructura del cableado de la empresa.

No existe un documento con roles y responsabilidades dentro del área de TI, por lo cual no hay una persona designada para la seguridad de la información y no se cumple con la asignación de tareas de seguridad de la información a una persona responsable.

Dentro de las políticas de seguridad no se encontró ninguna política que ayude al manejo de los dispositivos de almacenamiento externos dentro de la empresa, por lo cual los empleados pueden hacer uso de estos en cualquier momento, esto genera una gran brecha de seguridad para los activos de información.

Las copias de seguridad que se realizan en la empresa no están sustentadas por un documento que asigne a que activos de información se debe realizar estas copias y cada que tiempo se debe hacer.

No se encontró ningún documento donde se detalle los procedimientos a seguir dentro de la empresa, este punto es uno de los más críticos porque se debe tener procedimientos para poder dar en marcha las políticas, plan de contingencia y demás acciones que se requiere para cumplir con las normas ISO 27001.

12. Recomendaciones

a. Actualizar y mejorar las políticas de seguridad de la empresa es un gran paso para mejorar la seguridad de la información, hay que tomar en cuenta los requerimientos que establece las normas ISO 27001 para establecer o actualizar las políticas entre las que se necesitan incorporar están:

- Políticas de clasificación y manejo de la información.
- Política de escritorio y pantalla limpios.
- Política de transferencia de información.
- Política de privacidad y protección de la información personal.
- Política de uso de dispositivos externos.

Como ejemplo de las políticas de seguridad antes mencionadas tenemos el siguiente formato, ver **ANEXO L.**

b. Generar un documento donde se detalle el seguimiento de las políticas de seguridad para así garantizar su correcto funcionamiento y cumplimiento, este documento debe ser parte del proceso del control y evaluación de ejecución de políticas y debe revisarse como sugerencia cada tres meses. Como ejemplo de un formato para el seguimiento de las políticas tenemos, ver **ANEXO M.**

c. Se necesita crear un documento de roles y responsabilidades dentro del área de TI de la empresa el mismo debe tener un análisis previo de las capacidades y destrezas de cada persona que se encuentra en el área. Una vez designado los roles la persona encargada del área de la seguridad de la información debe tener un documento de tareas asignadas y esto debe sustentarse con un documento de seguimiento.

Como ejemplo de asignación de responsabilidades a cada uno de los empleados del área de TI, se propone el siguiente formato, ver **ANEXO N.**

d. Se sugiere hacer un análisis para identificar riesgos, amenazas y vulnerabilidades que pueden tener lo nuevos proyectos a crearse dentro de la empresa para así asegurar que un nuevo proyecto cumpla con los requerimientos mínimos para la seguridad de la información.

e. Se recomienda analizar las políticas del buen uso de los recursos humanos y actualizar tomando en cuenta otros aspectos como:

- Definir cómo deben utilizar los recursos de la empresa como el computador, internet, mail entre otros.
- Dar capacitaciones de concientización y comportamiento ético y profesional.
- Que los empleados utilicen de forma responsable los activos de información de la empresa.

- Definir acciones que están permitidas y prohibidas con los activos de información.

f. Se sugiere llevar un documento el cual detalle la clasificación de los activos de información por:

- Su valor dentro de la empresa.
- Criticidad.
- Sensibilidad.

Como ejemplo se sugiere mantener el siguiente formato para la clasificación de activos de la información, ver **ANEXO O.**

g. Se recomienda generar una política de uso de los dispositivos de almacenamiento externos dentro de la empresa donde se defina:

- Quien tiene autorización a utilizar estos dispositivos
- Sugerir encriptación de los datos que se encuentran en estos dispositivos
- Proteger los datos de estos dispositivos con copias de seguridad
- Crear un documento de los dispositivos que existen en la empresa y su uso dentro de esta.

Como ejemplo de las políticas de seguridad para el uso de dispositivos de almacenamiento se tiene el siguiente formato, ver **ANEXO L.**

h. Se sugiere actualizar las políticas de seguridad de red para mejorar la seguridad de la información dentro de la empresa como:

- Monitoreo y registro de acceso a la red
- Pruebas de penetración para evaluar el acceso.
- Mejorar la autenticación por parte de los empleados.

i. Se propone mejorar la señalética dentro de la empresa en lugares donde no debe existir acceso libre a cualquier persona como:

- Acceso restringido al área de servidor.
- Solo personal autorizado en los departamentos donde existan activos de información confidenciales.
- Carteles de donde se especifique el buen uso de los computadores de la empresa.

j. Se sugiere analizar las políticas de seguridad de la información implementadas y realizar los procedimientos de cada una de las políticas para poder tener una idea más detallada de todo lo que se debe cumplir dentro de la empresa.

k. Se sugiere crear políticas y procedimiento que ayuden a mantener segura la información contra código malicioso para lo cual se debe tomar en cuenta que:

- Tener antivirus el cual ayude a detectar malware dentro de los computadores y servidores.
- Realizar capacitaciones para orientar al personal designado a la seguridad de la información sobre el software malicioso
- Capacitar a los empleados para que tengan conocimiento de cómo actuar en caso de recibir una alarma sobre software malicioso.
- Escanear periódicamente los computadores para detectar un programa maligno.

l. Se recomienda generar un documento de seguimiento de copias de seguridad donde debería constar los siguientes puntos:

- Activo al que se debe realizar una copia de seguridad.
- Frecuencia de la copia de seguridad del activo.
- Fecha de la copia de seguridad.
- Observaciones de la copia de seguridad.

Como ejemplo se sugiere seguir el siguiente formato para tener un documento de seguimiento de copias de seguridad, ver **ANEXO P.**

m. Se propone generar procedimientos que ayuden al seguimiento de instalación de software dentro de los dispositivos de la empresa para lo cual se debe tener en cuenta los siguientes puntos:

- Antes de instalar un programa debe pasar por pruebas las cuales deben realizarse fuera de los computadores de la empresa.
- Revisar los requerimientos del software da instalar y ver compatibilidad con los computadores de la empresa.
- Solo el personal autorizado puede instalar software dentro de los computadores de la empresa.
- Se debe tener un seguimiento del software instalado para verificar posibles errores y evitar algún problema.

n. Se recomienda actualizar el análisis de riesgo y analizar el riesgo vinculado con la instalación de software en los dispositivos informáticos de la empresa.

o. Se sugiere generar procedimientos los cuales estén vinculados a la seguridad de la información en los cuales estén de forma clara y detallada:

- Responsable de la gestión de incidentes dentro de la empresa.
- Procedimiento de detección, análisis y corrección de los incidentes en la empresa.
- Capacitación a los empleados sobre los procedimientos establecidos.

Y una vez generado los procedimientos tener documentos que respalden el seguimiento de estos, para así verificar su cumplimiento y su eficacia.

p. Se recomienda capacitar al personal encargado de la seguridad de la información sobre la ley de protección de datos y a su vez generar un documento que detalle el cumplimiento de esta ley mediante políticas y procedimientos dirigidos exclusivamente a este punto.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- El análisis de las normas ISO 27001 es fundamental para realizar una evaluación precisa y correcta del sistema de gestión de seguridad de la información y así garantizar el cumplimiento de los estándares y requisitos de esta.

- La planificación de la auditoria informática externa ayudo a establecer controles y procesos estructurados los cuales permitieron llevar un orden claro al momento de la evaluación.

- El generar una planificación dentro de la auditoria informática proyecta una imagen de confianza y compromiso por parte del auditor.

- La elaboración de una planificación detallada para realizar una auditoria informática con normas ISO 27001, demostró ser importante para tener una mejor identificación de todos los controles a evaluar y así garantizar una auditoría externa eficaz.

- La evaluación de las actividades de la auditoria permite identificar las fortalezas y debilidades que presenta la empresa dentro del margen de la seguridad de la información.

- El informe final de la auditoria permite tener una base sólida para la implementación de mejoras en los aspectos evaluados y calificados como negativos y así proyectar una mejora continua dentro de la seguridad de la información de la empresa.

4.2 Recomendaciones

- Se recomienda adoptar un enfoque dinámico el cual promueva una mejora constante dentro del SGSI así se asegura una mejor protección de los datos de la empresa y se evita posibles fallas o robos de los activos informáticos.

- Se recomienda capacitar al personal sobre la implementación y seguimiento de un SGSI y su importancia y dentro de la empresa para mejorar la seguridad de la información.

- Se recomienda basarse en el informe final de la auditoria para mejorar los aspectos negativos que tiene la empresa ya que los mismos están alineados a los estándares de la norma ISO 27001.

- Se recomienda siempre tener una planificación al momento de analizar e implantar políticas de seguridad dentro de la empresa para así poder tener un mejor resultado de estas.

REFERENCIAS BIBLIOGRÁFICAS

[1] A. Lisbeth Aguilera-Sánchez and A. Rene Leyva Tellez, "HERRAMIENTA PARA EL CONTROL Y SEGUIMIENTO DE LOS RECURSOS INFORMÁTICOS," 2013. [Online]. Available: https://www.researchgate.net/publication/279538957

[2] Astudillo Karina, *Hacking Ético 101*. 2013. [Online]. Available: http://www.SeguridadInformaticaFacil.com

[3] X. Barragán Martínez, "Posmodernidad, gestión pública y tecnologías de la información y comunicación en la Administración pública de Ecuador," *Estado & comunes, revista de políticas y problemas públicos*, vol. 1, no. 14, Jan. 2022, doi: 10.37228/estado_comunes.v1.n14.2022.244.

[4] Wendy Gabriela Zambrano Castillo, "Auditoría Informática orientada a los procesos de recaudación en el Gobierno Autónomo Descentralizado Municipal de Lago Agrio aplicando la metodología COBIT," 2019.

[5] E. N. El, D. Financiero, D. Gobierno, A. Descentralizado, M. De Ambato, and D. Señor Ruíz López, "AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5.0 AL PROCESO DE RECAUDACIÓN DEL MODULO DE TESORERIA DEL SISTEMA CABILDO," Jan. 2020.

[6] Tigse Moposita Jorge Luis, "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL," 2020.

[7] S. Burgos and G. Christian, "PLAN DE CONTINGENCIA INFORMATICO PARA EL AREA DE TI EN BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACION CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS.," 2020.

[8] J. Vinicio, B. Guerrero, I. David, and O. Guevara Aulestia, "ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA METODOLOGÍA NIST SP 800-30 Y NIST SP 800-115 PARA LA EMPRESA TEXTILES JHONATEX LÍNEA DE INVESTIGACIÓN: Normas y Estándares," Feb. 2021.

[9] ISOTools Excellence, "La NCh ISO 27001. Origen y evolución." Accessed: Jul. 09, 2023. [Online]. Available: https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

[10] Grupo ESGINNOVA, " ISO 27001: Cumplimiento de los requisitos legales en Seguridad de la Información." Accessed: Jul. 09, 2023. [Online]. Available: https://www.isotools.us/2014/12/16/iso-27001-cumplimiento-requisitos-legales-seguridad-informacion/

[11] ASAMBLEA NACIONAL, "LEY ORGÁNICA DE PROTECCIÓN DE DATOS," *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES SUPLEMENTO... - ANACSE*, May 2021.

[12] Sinergias Empresariales, "Auditoría ISO 27001 Sistemas de Seguridad Información." Accessed: Jul. 09, 2023. [Online]. Available: https://www.sinergiasempresariales.com/auditoria-iso-27001/#:~:text=Seg%C3%BAn%20define%20la%20ISO%2027000,cumplen%20los%20criterios%20de%20auditor%C3%ADa%E2%80%9D.

[13] Soluciones Q.E.S., “AUDITORÍA ISO 27001,” https://solucionesqes.com/servicios/auditoria-iso-27001/.

[14] Javier Sánchez Galán, “Auditoría informática.” Accessed: Jul. 09, 2023. [Online]. Available: https://economipedia.com/definiciones/auditoria-informatica.html

[15] UNIR, “Auditoría externa: características, beneficios y tipos.” Accessed: Dec. 04, 2023. [Online]. Available: https://www.unir.net/empresa/revista/auditoria-externa/

[16] CYNTHUS, “Auditoría externa y el rol de la tecnologìa informàtica.” Accessed: Dec. 04, 2023. [Online]. Available: https://www.cynthus.com.mx/auditoria-externa-y-la-tecnologia-informatica/

[17] Universidad Internacional de Valencia, “¿Qué es la seguridad informática y cómo puede ayudarme?” Accessed: Jul. 09, 2023. [Online]. Available: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

[18] Diana Cortés, “¿QUÉ ES LA TECNOLOGÍA DE LA INFORMACIÓN?” Accessed: Jul. 09, 2023. [Online]. Available: https://www.cesuma.mx/blog/que-es-la-tecnologia-de-la-informacion.html

[19] Team Asana, “Gestión de proyectos de TI: Guía para gerentes y equipos.” Accessed: Jul. 09, 2023. [Online]. Available: https://asana.com/es/resources/it-project-management

[20] C. Alberto Lima Ayala, D. Miguel Marcillo Parra, and T. Marisol Gualotuña Alvarez, “PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA EMPRESA POLITEX S.A.,” ESPE, Sangolqui, 2012. Accessed: Jul. 09, 2023. [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/6053

[21] Claudia Alvarado, “Sistema de gestión de seguridad de la información: qué es y sus etapas.” Accessed: Dec. 04, 2023. [Online]. Available: https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

[22] Rafael Marín, “¿Qué es un SGSI y como implantarlo en una empresa?,” https://www.inesem.es/revistadigital/informatica-y-tics/sgsi/.

[23] Hackbysegurity, “Auditoría Interna Informática,” Auditoría Interna Informática.

[24] Hackbysegurity, “Auditoría de Seguridad Externa o Perimetral.” Accessed: Dec. 04, 2023. [Online]. Available: https://www.hackbysecurity.com/servicios-empresas/auditoria-informatica/auditoria-externa-o-perimetral

[25] tcmetrologia, “Qué es el ciclo PDCA. Fases y Ejemplos.” Accessed: Dec. 04, 2023. [Online]. Available: https://www.tcmetrologia.com/blog/que-es-el-ciclo-pdca-fases-y-ejemplos/

[26] Jorge Hernán Gutiérrez Pineda, “La auditoría basada en riesgos es un proceso integral ajustable aplicado a toda la organización que permite indicar que, si el sistema de control interno que tiene la empresa en todo su andamiaje, está libre de errores materiales o eventos que puedan impactar sus objetivos básicos financieros.” Accessed: Dec. 04, 2023. [Online]. Available: https://portal.udea.edu.co/wps/portal/udea/web/inicio/unidades-academicas/ciencias-economicas/!ut/p/z1/jZDLCsIwEEW_pV-

QyatNliENJW1JE7EPs5GuSkGrC_H7FXGjYO3sBs65M1wU0YDiMt7nabzNl2U8PfdDTI8ucIOJhroodxoCo10HUlphKOpfgJCaYMWghgpzUMF4t2-0z0uC4hYffoyCbf4KENfjexQ_TwjKOASocpJKTKzLvoHGUgNBOu5pYQnL6BtY6-DfF9dz2w4w20klyQMLP6BI/?1dmy&page=udea.generales.interna&urile=wcm%3Apath%3A%2FPortalUdeA%2FasPortalUdeA%2FasHomeUdeA%2FUnidades%2BAcad%2521c3%2521a9micas%2FCiencias%2BEcon%2521c3%2521b3micas%2FasContenidos%2FasListado%2Fauditoria-basada-en-riesgos-la-organizacion-como-un-todo

[27] Juan Moreno, “La guía definitiva para la auditoría de procesos: Beneficios y mejores prácticas.” Accessed: Dec. 04, 2023. [Online]. Available: https://flokzu.com/es/bpm-es/auditoria-procesos/

ANEXOS

Anexo A. Ficha de activos de la empresa

Nota: Se muestra un formato debido a que los datos de este documento son confidenciales y de no acceso público.

ACTIVOS DE INFORMACIÓN MEGAKONS S.A. **Fecha:** **Encargado:**						
				Valor		
Nombre del activo	**Descripción**	**Propietario**	**Ubicación**	**Alto**	**Medio**	**Bajo**

Firma del encargado

Anexo B. Políticas de seguridad MEGAKONS S.A.

POLÍTICAS DE SEGURIDAD MEGAKONS S.A.	
1.	Acceso y control de Información
2.	Seguridad de Red
3.	Seguridad de los recursos humanos
4.	Gestión de Incidentes de Seguridad
5.	Clasificación y Etiquetado de Datos
6.	Gestión de instalación de software
7.	Gestión de Contraseñas
8.	Cifrado de información
9.	Respaldo y Recuperación de Datos
10.	Uso Aceptable de Recursos Informáticos
11.	Seguridad de la información para suministradores.
12.	Seguridad física de la información
13.	Eliminación Segura de Datos

Acceso y control de Información	
Alcance	Las políticas de gestión y acceso a la información de MEGAKONS S.A. están diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la información y los activos de la empresa y para minimizar los riesgos de seguridad
Definición	• El acceso a la información para empleados estará dividido según los roles que desempeñan cada uno en la empresa. • Se solicita que cada empleado tenga una clave segura y que no comparta la información con los demás empleados. • Las contraseñas deben cambiarse periódicamente. • Si una persona externa necesita acceso a información confidencial, deberá solicitar el permiso necesario a la persona encargada. • El área de servidores tiene un acceso restringido a cualquier persona que no sea parte del área de TI, • La persona/empleado que requiera acceso a los servidores necesita llenar una ficha en la cual se especifica el ingreso y motivo del acceso.
Responsables	Área de TI

Seguridad de Red	
Alcance	La política de seguridad de red de Megakons S.A. está diseñada para garantizar la integridad, disponibilidad y confidencialidad de los recursos de la red y la información crítica, y para proteger la infraestructura de la red de amenazas cibernéticas.
Definición	• Los equipos informáticos que tengan vínculo con redes deberán ser configurados con las mejores prácticas de seguridad. • Todos los equipos deben estar actualizados. • Las contraseñas deben cambiarse periódicamente. • Solo el personal de TI tiene acceso libre al área de redes y recursos • No se permite utilizar las carpetas compartidas entre empleados, al menos que sea necesario y aceptado por el área de TI
Responsables	Área de TI

Seguridad de los recursos humanos	
Alcance	La política de seguridad de los recursos humanos de MEGAKONS S.A. está diseñada para garantizar el buen uso de los recursos informáticos de la empresa y así salvaguardar la información que existen en los mismos.
Definición	• Los equipos informáticos que tengan vínculo con redes deberán ser configurados con las mejores prácticas de seguridad. • Todos los equipos deben estar actualizados. • Las contraseñas deben cambiarse periódicamente.
Responsables	Área de TI

Gestión de Incidentes de Seguridad	
Alcance	La Política de gestión de incidentes de seguridad de MEGAKONS S.A. tiene como objetivo establecer procedimientos y políticas para la detección, notificación, gestión y resolución de incidentes de seguridad de la información.
Definición	• Todo el personal de la empresa tiene la responsabilidad de reportar algún incidente de seguridad que se detecte. • Todos los incidentes de seguridad serán primera prioridad al momento de ser notificados. • Se abrirá canales de comunicación inmediatos para reportar este tipo de incidentes como llamadas directas al área de TI.
Responsables	Área de TI

Clasificación y Etiquetado de Datos	
Alcance	La Política de Clasificación y Etiquetado de Datos de MEGAKONS S.A. tiene como objetivo garantizar la protección y gestión adecuada de la información de la empresa en función de su nivel de confidencialidad.
Definición	• Existirá un etiquetado del tipo de documento que se tiene en la empresa. • Los etiquetados serán: Públicos, Internos, Confidenciales. • El área de TI se encargará de asignar que tipo de etiquetado tiene cada documento de la empresa.
Responsables	Área de TI

Gestión de instalación de software	
Alcance	La Política de gestión de instalación de software de MEGAKONS S.A. tiene como objetivo garantizar la protección de los datos al instalar software dentro de los dispositivos de la empresa.
Definición	• Se debe obtener la autorización previa de un responsable designado antes de instalar cualquier software en los sistemas de la empresa. • Se mantendrá un inventario actualizado de software autorizado • Se instalará únicamente software proveniente de fuentes confiables y legítimas. • Los usuarios tendrán permisos limitados para instalar software en sus dispositivos
Responsables	Área de TI

Gestión de Contraseñas	
Alcance	La Política de Gestión de contraseñas de MEGAKONS S.A. tiene como objetivo garantizar los recursos informáticos y evitar la filtración de información por robo.
Definición	• Utilizar contraseñas con al menos 12 caracteres. • Incluir una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales (¡como !, @, #, $, %, etc.). • Evitar el uso de información personal como nombres, fechas de nacimiento, nombres de mascotas, números de teléfono, etc. • No utilizar palabras comunes, secuencias de teclado (como "123456" o "qwerty") • Generar contraseñas aleatorias y no relacionadas entre sí para cada cuenta o sistema. • Cambiar las contraseñas periódicamente, al menos cada 90 días
Responsables	Área de TI

Cifrado de información	
Alcance	La Política de Cifrado de la información de MEGAKONS S.A. tiene como objetivo garantizar la seguridad de lainformación y evitar robos de esta.
Definición	• Toda información confidencial debe estar encriptada y se debe utilizar canales seguros para su intercambio. • Se debe identificar y clasificar la información sensible que requiere cifrado. • Los dispositivos de almacenamiento extraíbles cifrarse antes de almacenar información sensible. • Todos los datos sensibles almacenados en servidores, bases de datos y dispositivos móviles deben cifrarse
Responsables	Área de TI

Respaldo y Recuperación de Datos	
Alcance	La Política de Respaldo y Recuperación de Datos de MEGAKONS S.A. tiene como objetivo garantizar la disponibilidad, integridad y confidencialidad de la información crítica y los sistemas de la empresa.
Definición	• Toda información importante para la empresa debe ser respaldada. • Las copias de seguridad se deben hacer fueradel horario de trabajo. • Estas copias de seguridad deben ser guardadasen un lugar externo y confidencial.
Responsables	Área de TI

Uso Aceptable de Recursos Informáticos	
Alcance	La Política de Respaldo y Recuperación de Datos de MEGAKONS S.A. tiene como objetivo garantizar un uso seguro y eficiente de los recursos informáticos de la empresa, incluyendo computadoras, servidores, dispositivos móviles y acceso a Internet.
Definición	• Los empleados deben utilizar de manera responsable los recursos informáticos asignados para su trabajo. • Los empleados no pueden compartir información de acceso personal como contraseñas a otros empleados. • El uso de sitios web que no tengan vínculo con el trabajo de la empresa están prohibidos.
Responsables	Área de TI

Seguridad de la información para suministradores.	
Alcance	La Política de seguridad de la información para suministradores de MEGAKONS S.A. tiene como objetivo garantizar que los proveedores de la empresa no tengan libre acceso a la información confidencial.
Definición	• Los proveedores solo tendrán acceso a información que la empresa crea necesaria. • Los proveedores deben asegurar que se cumplan las leyes de privacidad de datos. • Los proveedores deben establecer políticas de seguridad según las normas ISO 27001. • En caso de algún siniestro se debe informar inmediatamente al encargado del área de TI de la empresa. • Los proveedores deben capacitar a su personal sobre la seguridad de la información de su empresa y de la empresa a la que otorgan sus servicios. • Estas capacitaciones deben estar documentadas y tener evidencia clara y concisa.

Seguridad física de la información.	
Alcance	La Política de Respaldo y Recuperación de Datos de MEGAKONS S.A. tiene como objetivo garantizar que la eliminación de datos, documentos impresos, dispositivos de almacenamiento y equipos obsoletos se realice de manera segura y de acuerdo con las normas de seguridad de la información.
Definición	• Se requiere el uso de tarjetas de identificación personal • La sala de servidores debe contar con acceso restringido y medidas de seguridad. • Vigilancia constante mediante sistemas de cámaras y alarmas, con registros de acceso y monitoreo continuo. • Los equipos informáticos deben estar asegurados físicamente para prevenir robos.

Eliminación Segura de Datos	
Alcance	La Política de eliminación segura de datos de MEGAKONS S.A. tiene como objetivo garantizar que la eliminación de datos, documentos impresos, dispositivos de almacenamiento y equipos obsoletos se realice de manera segura y de acuerdo con las normas de seguridad de la información.
Definición	• Todos los dispositivos de almacenamiento que tengan información confidencial de la empresa deberán ser formateados de manera segura y así asegurar que no queden ningún tipo de datos. • Los documentos impresos que contengan información importante deberán ser destruidos de forma adecuada. • Se deberá llevar un registro de todas las eliminaciones que existan tanto de dispositivos como de documentos físicos.
Responsables	Área de TI

Anexo C. Oficio de acceso a información confidencial en MEGAKONS S.A.

Ambato

MEGAKONS S.A

Luis Alberto Valencia, Ambato

Estimado/a (jefe del área de TI):

Yo, **NOMBRE COMPLETO,** con CI: CEDULA, por medio de la presente, me dirijo a usted con el propósito de solicitar acceso a cierta información confidencial de relevancia para **RAZÓN/MOTIVO**.

A continuación, se detallan los aspectos requeridos:

INFORMACIÓN CONFIDENCIAL MEGAKONS S.A.	
Cargo del solicitante	
Tipo de Información	
Uso de la información	
Fecha de acceso	
Fecha final	

Entiendo y reconozco plenamente la naturaleza confidencial de la información solicitada. Aseguro que la utilizaré únicamente para los fines mencionados y mantendré la confidencialidad de esta, siguiendo los protocolos y políticas de seguridad establecidos por la empresa.

Atentamente,

_____

Nombre

Cargo

Teléfono

Correo Electrónico

Anexo D. Control de accesos a los servidores y base de datos en MEGAKONS S.A.

CONTROL DE ACCESO A SERVIDORES Y BASE DE DATOS MEGAKONS S.A.

Fecha:
Encargado:

Numero	Usuario	Cargo	IP usuario	IP servidor	Fecha Inicio	Fecha Fin	Motivo	Firma

Anexo E. Control de mantenimiento de equipos informáticos en MEGAKONS S.A.

MANTENIMIENTO DE EQUIPOS INFORMÁTICOS MEGAKONS S.A. Fecha: Encargado:								
Fecha	Equipo	Encargado del equipo	Tipo de Mantenimiento		Descripción del Mantenimiento	Responsable	Estado	Observaciones
			Preventivo	Correctivo				

Firma del encargado

Anexo F. Seguimiento de eventos en MEGAKONS S.A.

FICHA DE GESTIÓN DE EVENTO MEGAKONS S.A.							
Fecha de Inicio: **Duración de ficha:**							
Fecha/Hora	**Incidente**	**Responsable**	**Duración**	**Consecuencia**	**Solución**	**Firma/Sello**	**Observaciones**

Firma del encargado

Anexo G. Análisis de Riesgos de MEGAKONS S.A.

RIESGOS MEGAKONS S.A.	
Numero	**Riesgo**
RIESGO 1	Robo de información
RIESGO 2	Phishing
RIESGO 3	Invalides de licencias pagadas
RIESGO 4	Fallas en unidades de almacenamiento
RIESGO 5	Incendios
RIESGO 6	Sismos
RIESGO 7	Inundaciones
RIESGO 8	Fallas en la red
RIESGO 9	Sustracción de información
RIESGO 10	Cortes de servicio eléctrico
RIESGO 11	Accesos no autorizados
RIESGO 12	Fallas de hardware

RIESGO = PROBABILIDAD X SEVERIDAD				
EVALUACION DEL RIESGO		**SEVERIDAD**		
		Baja **1**	Media **2**	Alta **3**
PROBABILIDAD	Baja **1**	R4,R5,R6,R7,	R3,R10,R12	
	Media **2**	R9,R11	R8	
	Alta **3**			R1,R2

ANÁLISIS DE RIESGO 1	
RIESGO	Robo de información
DETECCIÓN	• Amenazas por parte interna o externa de la empresa. • Falta de información que forma parte de los activos de la empresa. • Inconsistencia en los recursos informáticos o en los valores monetarios de la empresa.
PREVENCIÓN	• Monitoreo constante a los empleados que utilizan algún recurso informático. • Realizar copias de seguridad constantemente y guardarlas en algún sitio externo fuera del alcance de los empleados o agentes externos.
CORRECCIÓN	• Informar a la entidad máxima sobre el robo de información (Gerente). • Determinar como se produjo el robo de información. • Trabajar con el personal de TI de la empresa para la recuperación de la información en caso de ser posible.

ANÁLISIS DE RIESGO 2	
RIESGO	Phishing
DETECCIÓN	• Correos no deseados en los correos personales o de la empresa de los empleados. • Alerta de seguridad en el computador
PREVENCIÓN	• Capacitaciones a los empleados sobre la seguridad de la información y la no divulgación en la web. • Comprobar la fuente del correo electrónico antes de ingresar alguna información. • Acudir al área de TI en caso de recibir un correo extraño.
CORRECCIÓN	• Cambiar contraseñas que se hayan ingresado y del correo electrónico.

ANÁLISIS DE RIESGO 3	
RIESGO	Invalides de licencias pagadas
DETECCIÓN	• Mensajes de alerta por falta de clave de activación. • Pausa en el funcionamiento del programa sin licencia.
PREVENCIÓN	• Mantener un monitoreo de las licencias que se tienen en la empresa. • Realizar actualizaciones del software de paga. • Realizar un documento de todos los softwares que necesitan licencia con su fecha de inicio y caducidad.
CORRECCIÓN	• Informar al área de TI, para que ingrese la nueva licencia del software. • Tener un computador con todas las licencias al día en caso de emergencia.

ANÁLISIS DE RIESGO 4	
RIESGO	Fallas en unidades de almacenamiento
DETECCIÓN	• No se inicia el sistema operativo del computador. • No detecta el dispositivo de almacenamiento el computador. • Perdida de información sin alguna explicación.
PREVENCIÓN	• Capacitación a los empleados a tener sus documentos importantes en la nube. • Revisar el estado de los discos duros y en caso de necesitar un cambio realizarlo. • Tener dispositivos de almacenamiento de respaldo.
CORRECCIÓN	• Buscar una copia de seguridad de la información del empleado. • Cambiar el dispositivo de almacenamiento de inmediato.

ANÁLISIS DE RIESGO 5	
RIESGO	Incendios
DETECCIÓN	• Deterioro de la infraestructura de la empresa
PREVENCIÓN	• Capacitaciones a los empleados en caso de un incendio. • Tener un seguro que cubra los bienes informáticos.
CORRECCIÓN	• Determinar por prioridad los elementos afectados y sustituirlos. • Realizar una evaluación completa de todos los daños causados y emitir un informe.

ANÁLISIS DE RIESGO 6	
RIESGO	Sismos
DETECCIÓN	• Deterioro de la infraestructura de la empresa.
PREVENCIÓN	• Capacitación sobre los riesgos en caso de un sismo. • Realizar copias de seguridad constantemente y evitar guardarlas dentro de la empresa • Contratar un seguro ante catástrofes naturales.
CORRECCIÓN	• Hacer uso de los seguros contratados por la empresa • Analizar las prioridades en la restauración de los recursos informáticos

ANÁLISIS DE RIESGO 7	
RIESGO	Inundaciones
DETECCIÓN	• Deterioro en la infraestructura de la empresa.
PREVENCIÓN	• Capacitación sobre riesgos en caso de una inundación. • Realizar copias de seguridad constantemente y guardar fuera de la empresa. • Contratar un seguro que cubra inundaciones.
CORRECCIÓN	• Hacer uso del seguro contratado • Determinar cómo se produjo el siniestro. • Analizar las prioridades de restauración de equipos y sistemas informáticos.

ANÁLISIS DE RIESGO 8	
RIESGO	Fallas en la red de la empresa.
DETECCIÓN	• Inconsistencia en la navegación de la web. • Fallas en el uso del sistema de la empresa. • Falla en la comunicación entre empleados vial mail.
PREVENCIÓN	• Realizar mantenimiento del cableado de red. • Tener segmentado el uso del internet por departamentos y prioridades. • Capacitar al personal sobre el buen uso del internet
CORRECCIÓN	• Analizar el causante de la falla de red. • Determinar prioridades en conexión de internet. • Acudir al proveedor de internet en caso de ser necesario.

ANÁLISIS DE RIESGO 9	
RIESGO	Sustracción de información
DETECCIÓN	• Inconsistencia en la información de la empresa. • Falta de información de la empresa.
PREVENCIÓN	• Firma de confidencialidad de los datos con los empleados. • restricción de uso de dispositivos de almacenamiento dentro de la empresa.
CORRECCIÓN	• Buscar una copia de seguridad de los datos alterados o robados. • Determinar la persona que se esa sustrayendo o alterando la información. • Acudir al código penal para la debida sanción del personal.

ANÁLISIS DE RIESGO 10	
RIESGO	Cortes de servicio eléctrico
DETECCIÓN	• Fallo en las actividades en las que intervienen los recursos informáticos.
PREVENCIÓN	• Adquirir un generador de energía externo en caso de algún fallo eléctrico por parte del proveedor. • Tener reguladores de voltaje para evitar corrientes de energía fuertes que puedan dañar los dispositivos.
CORRECCIÓN	• Activar el generador de energía para que no se pare las actividades. • Llamar al proveedor de energía eléctrica para verificar el fallo que existe. • Dar prioridad a las actividades que más necesiten de energía eléctrica.

ANÁLISIS DE RIESGO 11	
RIESGO	Accesos no autorizados
DETECCIÓN	• Personal de la empresa con información que no le pertenece. • Amenazas externas por información personal de empleados o clientes. • Inconsistencia en los datos de la empresa.
PREVENCIÓN	• Manejar un buen uso de contraseñas. • Generar roles y usuarios para cada uno de los empleados de la empresa. • Dar charlas sobre la ética y manejo de los datos de la empresa.
CORRECCIÓN	• Informar a la entidad máxima sobre el acceso no autorizado de información (Gerente). • Determinar la persona y/o empleado que tuvo acceso. • Con la copia de seguridad verificar si los datos no han sido alterados.

ANÁLISIS DE RIESGO 12	
RIESGO	Fallas de hardware
DETECCIÓN	• Bajo rendimiento del recurso informático. • Apagones o reinicios inesperados del recurso informático.
PREVENCIÓN	• Monitoreo constante a los recursos informáticos de la empresa. • Mantenimiento preventivo cada 6 meses. • Realizar pruebas específicas de los recursos.
CORRECCIÓN	• Informar al encargado del área de TI sobre la falla que tiene el equipo informático. • Realizar un cambio inmediato del hardware para evitar los cortes de actividades.

Anexo H. Plan de contingencia de MEGAKONS S.A.

RIESGO	Robo de información (R1)
EVENTO	Perdida de información sensible de la empresa.
RESPONSABLE	Área de TI
Actividades:	
1. Informar a los empleados y gerente de la empresa sobre el robo de	
2. Verificar que el daño no se siga propagando.	
3. Trabajar con el área de TI y si es necesario personas externas	
4. En caso de no recuperar la información, recurrir a la copia de	
5. Capacitar al personal sobre la seguridad de la información.	

RIESGO	Phishing (R2)
EVENTO	Robo de información al personal de la empresa mediante correo electrónico.
RESPONSABLE	Área de TI
Actividades:	
1. Revisar los correos electrónicos de la empresa para verificar correo	
2. Bloquear el correo malicioso.	
3. Cambiar contraseñas que están comprometidas por parte del	
4. Capacitar al personal sobre los distintos ataques que se pueden	

RIESGO	Invalides de licencias pagadas (R3)
EVENTO	Aplicaciones sin correcto funcionamiento o desactualizadas.
RESPONSABLE	Área de TI
Actividades:	
1. Identificar el software que está generando el problema.	
2. Verificar si la licencia caduco o solo necesita una actualización.	
3. Ingresar nueva licencia o actualización.	
4. Monitorear frecuentemente las licencias de paga que tiene la	

RIESGO	Fallas en unidades de almacenamiento (R4)
EVENTO	No inicia el sistema operativo de los computadores.
RESPONSABLE	Área de TI
Actividades:	
1. Informar al área de TI sobre el problema.	
2. Verificar que todos los cables estén bien conectados.	
3. Verificar que el monitor tenga señal.	
4. En caso de daño en la unidad de almacenamiento, retirar y cambiar	
5. Intentar recuperar la información que se encontraba en la unidad	
6. Pasar datos de la unidad antigua a la nueva.	

RIESGO	Incendios (R5)
EVENTO	Incendio de algún recurso informático en la empresa.
RESPONSABLE	Área de TI
Actividades:	
1. Mantener la calma de todo el personal de la empresa.	
2. Verificar que el incendio no siga propagándose.	
3. Poner a salvo al personal.	
4. Evaluar los daños causados por el incendio.	
5. Administrar el regreso del personal y actividades según la prioridad.	

RIESGO	Sismos (R6)
EVENTO	Sismo por causa natural.
RESPONSABLE	Área de TI
Actividades:	
1. Mantener la calma de todo el personal de la empresa.	
2. Evacuar a todo el personal.	
3. Analizar los daños causados por el sismo.	
4. Administrar el regreso del personal y actividades según la prioridad.	

RIESGO	Inundaciones (R7)
EVENTO	Inundación por daño interno en el canal de agua potable.
RESPONSABLE	Área de TI
Actividades:	
1. Evacuar al personal de la empresa.	
2. Verificar que no exista corriente de luz que interfiera con el agua y	
3. Apagar el suministro de luz en toda la empresa.	
4. Contactar al proveedor de agua para arreglar el daño	
5. Regresar a las actividades por prioridad.	

RIESGO	Fallas en la red (R8)
EVENTO	Fallas en la conectividad de internet
RESPONSABLE	Área de TI
Actividades:	
1. Informar al área de TI sobre la falla.	
2. Verificar que los cables, routers y switch estén debidamente	
3. Cambiar dispositivo o cables que tengan alguna falla.	
4. Contactarse con el proveedor de internet para verificar el fallo.	
5. Volver a las actividades normales en la empresa.	

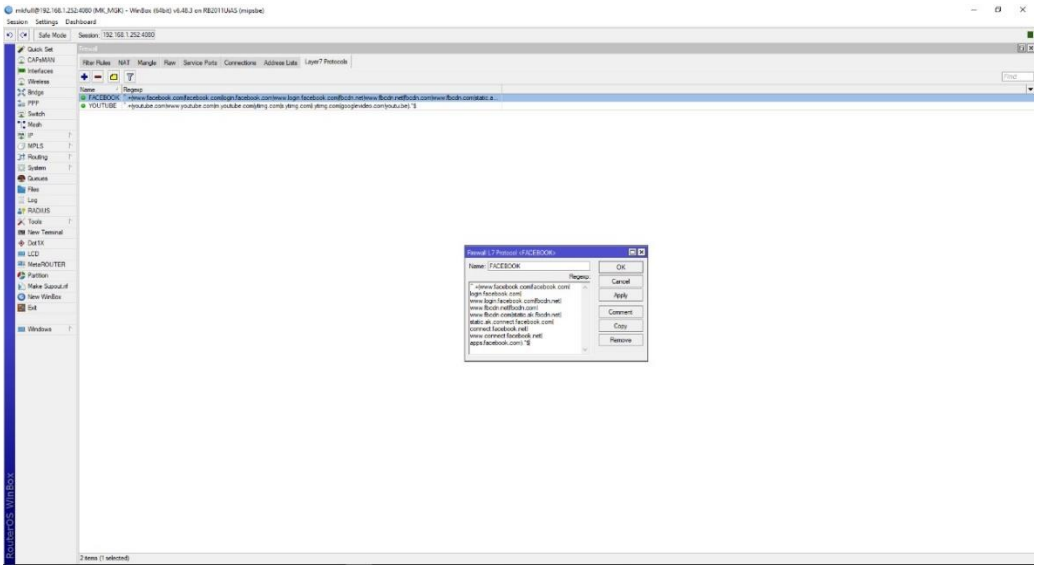
RIESGO	Sustracción de información (R9)
EVENTO	Personal que se lleva información sensible de la empresa.
RESPONSABLE	Área de TI
Actividades:	
1. Verificar la información que se está sustrayendo y el personal que	
2. Notificar a las autoridades sobre lo sucedido.	
3. En caso de ser necesario recurrir a la copia de seguridad de la	
4. Exponer el caso a las autoridades pertinentes.	
5. Capacitar al personal sobre la ética y la protección de los datos de la	

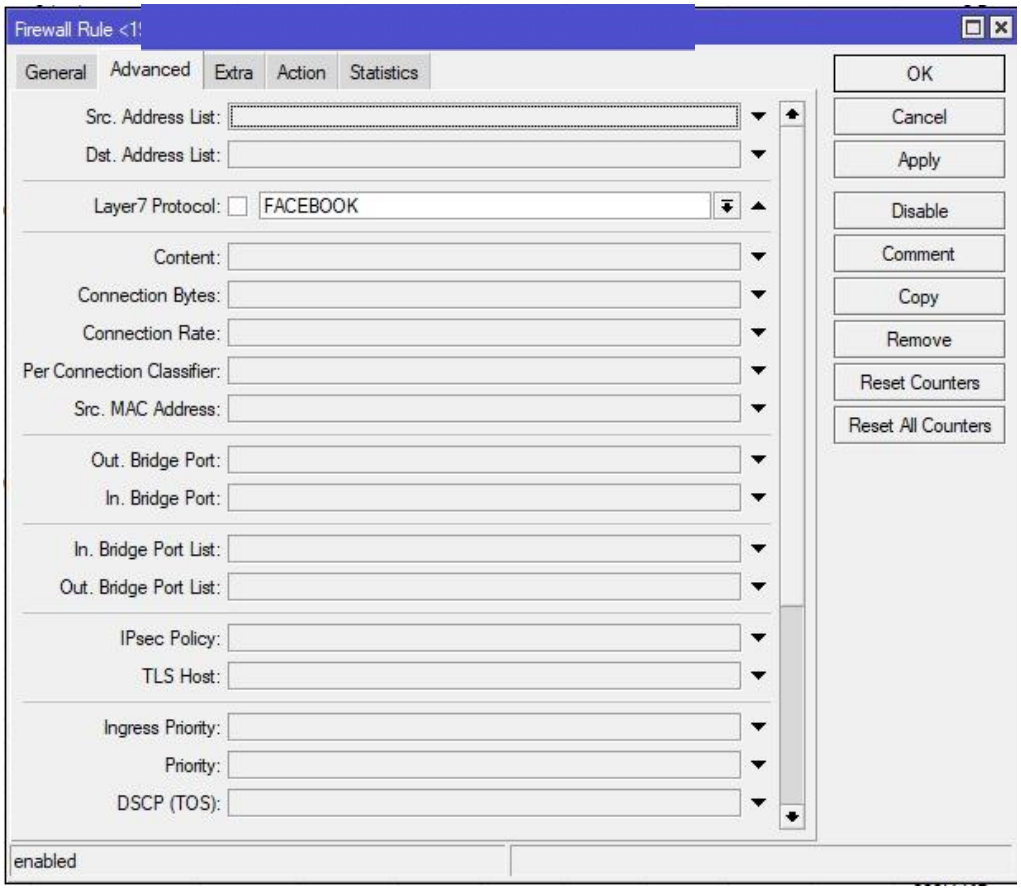
RIESGO	Cortes de servicio eléctrico (R10)
EVENTO	Corte de luz improvisto en la empresa.
RESPONSABLE	Área de TI
Actividades:	
1. Mantener la calma en toda la empresa y de ser necesario evacuar.	
2. Activar los generadores de energía externos de la empresa.	
3. Retornar a las actividades según la prioridad que exista en la	

RIESGO	Accesos no autorizados (R11)
EVENTO	Personal de la empresa ingresando a datos no autorizados o sensibles.
RESPONSABLE	Área de TI
Actividades:	
1. Informar a la gerente sobre lo sucedido.	
2. Evaluar el alcance del daño.	
3. Trabajar con el área de TI para verificar que la información este	
4. En caso de no recuperar la información, recurrir a la copia de	
5. Dar roles a los usuarios para evitar intrusos en la información	

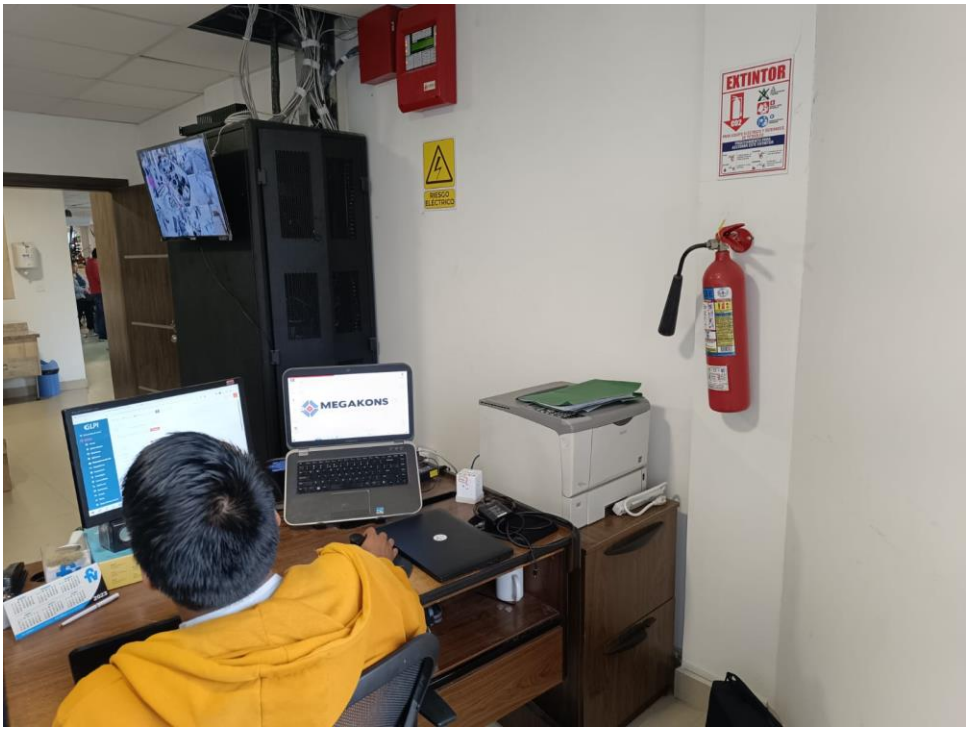
RIESGO	Fallas de hardware (R12)
EVENTO	Perdida o daños en el hardware de la empresa.
RESPONSABLE	Área de TI
Actividades:	
1. Verificar cual es el dispositivo informático que esta dañado.	
2. Analizar cuando se realizo el ultimo mantenimiento del equipo	
3. Arreglar o en caso extremo sustituir el equipo afectado.	
4. Capacitar al personal sobre el buen uso de sus recursos	

Anexo I. Configuración de restricción de redes sociales en los equipos informáticos de MEGAKONS S.A.

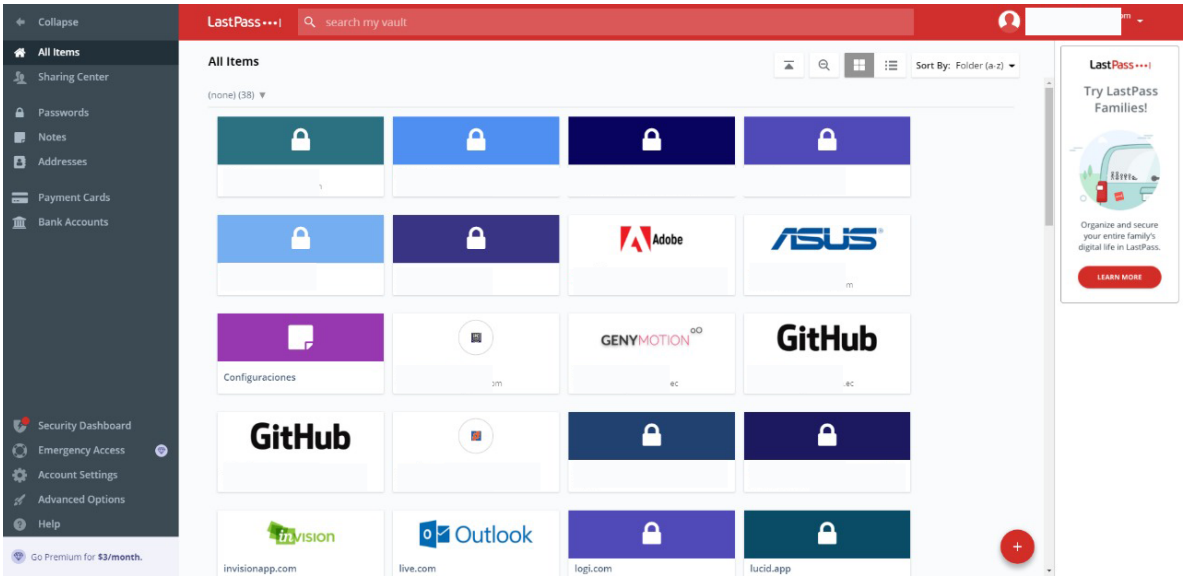




Anexo J. Señalética del área de sistemas de MEGAKONS S.A.



Anexo K. Gestor de contraseñas de MEGAKONS S.A.



.

Anexo L. Políticas de seguridad recomendadas por el investigador.

Nota: Estas políticas deben pasar por un proceso de control y evaluación.

Clasificación y manejo de la información	
Fecha de aceptación:	
Fecha de implementación:	
Objetivo	Su propósito principal es establecer directrices claras las cuales ayuden a tener una mejor clasificación y manejo de los activos de información de la empresa MEGAKONS para asegurar su confidencialidad, integridad y disponibilidad.
Definición	Los activos de información deben estar clasificados por: • Tipo de activo • Su valor en la empresa • Tu criticidad • Su sensibilidad Los activos de información de la empresa deben tener restricciones de acceso, transmisión, almacenamiento y eliminación. Se debe definir un control de acceso basado en roles y necesidades específicas. Se debe orientar y capacitar al personal sobre el buen uso de los activos de información de la empresa.
Responsable	Ing. David Parra
Cargo	Jefe de área de TI

Escritorio y pantalla limpio	
Fecha de aceptación:	
Fecha de implementación:	
Objetivo	Su propósito principal es establecer normas para mantener un entorno de trabajo más seguro y libre de documentos sensibles o información que pueda comprometer a la empresa MEGAKONS S.A.
Definición	El escritorio o puesto de trabajo del empleado debe mantenerse limpio y despejado al final de cada jornada. No dejar ningún tipo de documento sobre el escritorio cuando no se esté utilizando. Guardar documentos físicos en lugares con seguridad como cajones con llaves o candados. Evitar tener contraseñas en notas o cuadernos que tengas alcance a cualquier persona. Bloquear la pantalla del computador cuando no se esté utilizando o el personal se tenga que retirar de su área de trabajo.

	Configurar pantalla para su bloqueo automático después de un cierto tiempo de inactividad.
Responsable	Ing. David Parra
Cargo	Jefe de área de TI

Transferencia de información	
Fecha de aceptación:	
Fecha de implementación:	
Objetivo	Su propósito principal es establecer normas para asegurar la trasferencia de datos dentro y fuera de la empresa MEGAKONS S.A. y así asegurar la protección de la información.
Definición	Se debe utilizar canales seguros y aprobados por el área de TI para transferir información de la empresa como el correo electrónico asignado a cada uno de los empleados. Tener un registro de las transferencias de datos confidenciales de la empresa donde debe incluir, fechas, tipo de información y destinatarios. Encriptar la información importante antes de transferir. No utilizar dispositivos de almacenamiento externo dentro de la empresa.
Responsable	Ing. David Parra
Cargo	Jefe de área de TI

Privacidad y protección de la información personal.	
Fecha de aceptación:	
Fecha de implementación:	
Objetivo	Su propósito principal es establecer normas para asegurar la protección de datos personales dentro de la empresa MEGAKONS S.A.
Definición	• Especificar el propósito de recopilación de datos personales. • Especificar la manera de obtención para asegurar su transparencia. • Tener el consentimiento de los individuos antes de recopilar su información • Implementar medidas de seguridad adecuadas para proteger los datos personales.
Responsable	Ing. David Parra
Cargo	Jefe de área de TI

Uso de dispositivos de almacenamiento externo.	
Fecha de aceptación:	

Fecha de implementación:	
Objetivo	Su propósito principal es establecer normas para asegurar la trasferencia de datos dentro y fuera de la empresa MEGAKONS S.A. y así asegurar la protección de la información.
Definición	Para el uso de estos dispositivos se debe tener autorización previa del encargado de la seguridad de la información de la empresa. Todos los datos almacenados dentro de estos dispositivos deben ser encriptados. Se debe tener estos dispositivos con contraseñas seguras. Se debe tener copias de seguridad de los datos almacenados en los dispositivos. Se debe tener un registro de todos los dispositivos de almacenamiento externo que existen en la empresa. En caso de pérdida o robo, notificar de manera inmediata al personal encargado.
Responsable	Ing. David Parra
Cargo	Jefe de área de TI

Anexo M. Formato de documento de seguimiento para las políticas de seguridad de la información.

Documento de Seguimiento de Políticas de Seguridad de la Información de MEGAKONS S.A.

Fecha:

Fecha del seguimiento de las políticas de seguridad de la información.

Introducción:

Definir una breve descripción del propósito e importancia del documento.

Objetivos:

Definir los objetivos a cumplir con el documento.

Responsabilidades:

Describir los responsables del seguimiento de estas políticas y su asignación de tareas

Procedimientos de Seguimiento:

Describir los pasos a seguir para verificar el cumplimiento y funcionamiento de las políticas establecidas.

Acciones Correctivas y Mejoras:

Describir como se manejará las correcciones y mejoras de las políticas que lo necesiten.

Conclusiones:

Resumen de los hallazgos mas importantes dentro de lo analizado.

_____

Firma de responsable

Anexo N. Asignación de roles y responsabilidades del personal del área de TI.

Roles y responsabilidades en el Área de TI					
Rol	**Persona encargada**	**Responsabilidades**	**Nivel de responsabilidad**	**Habilidades requeridas**	**Área de enfoque**
Describir el tipo de rol que va a cumplir dentro de la empresa.	Cargo de la persona que va a cumplir el rol.	Tareas y responsabilidades para cumplir por parte de la persona asignada	Nivel de complejidad de las responsabilidades asignadas (Alto, medio, bajo)	Conjunto de habilidades que necesita la persona encargada para poder cumplir con las responsabilidades.	Descripción del área a la que se va a encargar la persona asignada.

Anexo O. Clasificación de activos de información.

Nota: Importancia de la empresa hace referencia a como el activo contribuye a los objetivos de la empresa. El nivel de criticidad hace referencia a la importancia en caso de pérdida para la continuidad de la empresa. El nivel de sensibilidad se refiere al grado de confidencialidad del activo.

		Clasificación de activos de información MEGAKONS S.A.									
Código	**Activo**	**Ubicación del activo**	**Importancia en la empresa**			**Nivel de criticidad**			**Nivel de sensibilidad**		
			Alta	**Media**	**Baja**	**Alto**	**Medio**	**Bajo**	**Alto**	**Medio**	**Bajo**
Código del activo de información	Nombre del activo de información	Ubicación física o virtual del activo.									

Anexo P. Control y seguimiento de las copias de seguridad de los activos de información de MEGAKONS S.A.

Nota: Esta sugerencia debe ser sometida a evaluaciones y aceptación por parte de gerencia

Control de copias de seguridad							
Código	**Activo**	**Frecuencia**	**Fecha de copia**	**Encargado**	**Fecha de comprobación de la copia de seguridad**	**Encargado de la copia de seguridad**	**Observaciones**
Código asignado al activo de información.	Nombre del activo a respaldar	Frecuencia de la copia de seguridad (diario, semanal, mensual, semestral)	Fecha que se realizó la copia de seguridad	Persona encargada de la copia de seguridad creada	Fecha en la que se comprobó que la copia de seguridad se haya realizado correctamente	Encargado de la creación y revisión de la copia de seguridad.	Observaciones en caso de ser necesario