UNIVERSIDAD CATÓLICA DE CUENCA

Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001.

Caso de Estudio: "Diario El Mercurio Cia. Ltda."

Autor: Esteban Fernando Castillo Durán.

Asesores: Ing. Fernando Illescas Peña. Mg

Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2023.

Certificación de Asesores

Se certifica que:

El informe de investigación “Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Caso de Estudio: Diario El Mercurio”, de autoría del señor Ingeniero de Sistemas Esteban Fernando Castillo Durán, CC: 010417436-2, ecuatoriano, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Julio, 2023.

_____	_____
Ing. Fernando Illescas Peña. Mg	Ing. Juan Carlos Ortega Castro. Mg
Asesor Científico	Asesor Metodológico

Certificación de Autoría

Certifico que:

"Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Caso de Estudio: Diario El Mercurio", es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Julio, 2023.

_____

Ing. Esteban Castillo Durán.

CC: 010417436-2

Agradecimiento.

Un agradecimiento especial a mi familia, pilar fundamental con su constante apoyo en todos mis proyectos y objetivos, a mi tutor el Ingeniero Fernando Illescas, así como al director del programa el Ingeniero Juan Carlos Ortega quienes, con su conocimiento y constante ayuda, han sido una guía muy importante para poder cumplir con este objetivo.

Dedicatoria.

Este trabajo está dedicado a mis padres, a mi hermano, a todos mis familiares quienes me han motivado a seguir adelante a pesar de las adversidades, a mi persona, por tratar de superarme constantemente y continuar cumpliendo mis metas.

Resumen.

El presente documento comprende el estudio realizado en la empresa “Diario El Mercurio Cia. Ltda.” El cual abarca la fase inicial de planificación para la implementación de un sistema de gestión de seguridad de la información comúnmente conocido o abreviado como SGSI, el mismo que posteriormente a la entrega de esta documentación, queda a criterio de la directiva de la empresa los procedimientos a seguir para realizar dicha implementación, contando con una base sólida que incluye las pautas necesarias de tal manera que se permita realizar el proceso de una manera satisfactoria.

Este proceso se ha realizado bajo el estricto cumplimiento de las actividades comprendidas dentro de la norma ISO27001 y sus familias derivadas, con lo cual se abarcan varias aristas comprendidas en la seguridad de la información.

Palabras clave: Sistema de gestión de seguridad de la información, etapas implementación S.G.S.I., ISO 27001, modelo de madurez, inventario de activos de información, análisis de riesgos sobre activos de información.

Abstract.

This document includes the study carried out in the company "Diario El Mercurio Cia. Ltda." Which covers the initial planning phase for the implementation of an information security management system commonly known or abbreviated as ISMS, the same that after the delivery of this documentation, the procedures are at the discretion of the company's directive to follow to carry out said implementation, having a solid base that includes the necessary guidelines in such a way that the process can be carried out satisfactorily.

This process has been carried out under strict compliance with the activities included in the ISO27001 standard and its derived families, which covers several edges included in information security.

Keywords: Information security management system, S.G.S.I implementation stages, ISO 27001, maturity model, inventory of information assets, risk analysis on information assets.

Índice.

Contenido

Índice de figuras.

Índice de tablas.

Capítulo I. Introducción.

1.1 Situación problemática.

La realidad latinoamericana en temas de ciberseguridad refleja un déficit muy alto en comparación con otras regiones a nivel global, y esta problemática se acentúa principalmente en países en vías de desarrollo; concretamente en el caso del Ecuador, el tema de los ciberataques es constante, tal como se detalla en investigaciones previamente realizadas Agencia AFP (2019); Diario El COMERCIO (2021), de este particular nace la necesidad a nivel de las empresas de protegerse contra este tipo de amenazas, las cuales siempre están presentes y que suponen un riesgo muy elevado para las mismas.

1.2 Problema científico.

¿Cuál es el grado de madurez de la empresa en temas de seguridad de la información?

1.3 Objeto de estudio.

El objeto de estudio es la empresa en la cual se pretende realizar dichoproceso es DIARIO EL MERCURIO CIA. LTDA., la cual mantiene a su planta matriz en laciudad de Cuenca ubicada en la Avenida de las Américas y Francisco Ascázubi (diagonal a Coralcentro), cuenta con 3 agencias en la ciudad, así como también agencias en las ciudadesde Quito y Guayaquil respectivamente.

El delimitar el trabajo sobre el objeto de estudio, permitirá a lo largo de todo el proceso definirlas métricas a utilizarse para poder cubrir con los distintos procesos que este estudio requiere realizar.

1.4 Campo de acción.

El campo de acción comprende la fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I) basado en la normativa ISO 27001, dicho proceso abarca varios ejes temáticos entre los cuales podemos indicar:

- Justificación del proyecto a la directiva.
- Ejecución de un análisis GAP para determinar la situación actual en la cual se encuentra la empresa y el mismo que servirá como punto de partida durante todo el proceso.

- Elaborar un inventario de activos de información con el cual se pueda identificar los activos críticos a proteger.
- Realizar un estudio de riesgos y vulnerabilidades aplicados a los activos críticos de la empresa, así como también, un análisis de las vulnerabilidades encontradas tanto en los activos como en la infraestructura de la organización.
- Redactar un informe técnico con los resultados obtenidos el finalizar el proceso y que contenga las recomendaciones y sugerencias finales para la toma de decisiones.

1.5 Objetivos.

General.

Completar la fase inicial (análisis) del ciclo de vida de un Sistema de Gestión de Seguridad de la Información (S.G.S.I), proceso estrictamente basado en la norma ISO 27001, que permita evaluar la situación de la empresa en materia de seguridad de la información, y a través de un informe técnico final, brindar las pautas adecuadas para la toma de decisiones acertadas por parte de los directivos.

Específicos:

- Solicitar autorización y documentación a la directiva, que sirva de fundamentación para iniciar con el proceso.
- Realizar un análisis de madurez, para conocer el estado de la empresa.
- Entregar un informe técnico, con los resultados y las recomendaciones a sugerirse, para la implementación y mitigación de los riesgos detectados.

1.6 Justificación.

Los ataques y vulneraciones a los sistemas informáticos son un problema frecuente día a día alrededor de todo el mundo, y es de conocimiento general tal como lo menciona Aguilar (2021), que la realidad de Latinoamérica en temas de ciberseguridad tiene todavía muchísimo trabajo pendiente por realizarse, ya que los gobiernos en los países de la región apenas empiezan a tomar conciencia de la importancia que tiene esta rama de las ciencias informáticas y también de la parte legal competente a este contexto.

Recientemente se ha conocido por ejemplo que, en Europa se ha aprobado el primer borrador de la **Ley de Servicios Digitales (DSA),** la cual ya está en vigor, pero empezará a

aplicarse a partir del próximo año a nivel continental según la publicación consultada Pastor (2022) lo que representa un avance significativo en temas de derechos desde el punto de vista del usuario y al mismo tiempo exige un mayor nivel de responsabilidad por parte de las empresas y plataformas que proveen servicios o información.

De igual manera en nuestra región se han empezado a implementar propuestas de leyes entre los países, algunos ya se encuentran en plena ejecución, otros como el caso del Ecuador empezarán a aplicar la Ley de Orgánica de Protección de Datos Personales, lo cual está previsto para el próximo año, de tal manera que permitan encaminar a los estados a un rumbo en conjunto con un fin común, el cual garantice los derechos de instituciones, empresas y personas a proteger su información.

De esta problemática podemos concluir que el estar preparados para contrarrestar ataques y vulneraciones de la seguridad de la información es indispensable tanto a nivel personal como institucional, lo cual requiere conocimiento y compromiso por parte nuestra y de la sociedad en general, pero de aquí surge otro problema y es el desconocimiento en muchos casos de cómo ocurren los ataques y también de cómo prevenirlos.

Según manifiesta en su estudio Moran Maldonando (2021), la situación actual de las empresas en el sector público en nuestro país refleja el alarmante dato y es que casi en su totalidad se encuentran expuestas a ataques de diferente índole lo cual a nivel país se convierte en un problema extremadamente preocupante ya que la información que manejan las diferentes entidades gubernamentales si bien son de carácter público, no toda la información debería encontrarse disponible dependiendo el grado de sensibilidad de la misma para que cualquier persona tenga libre acceso a la misma.

Es ahí en donde dichas instituciones deberían poner énfasis en protegerlas, recordemos el caso del ataque informático sufrido por la empresa pública CNT, el cual según investigación realizada por el portal de noticias Suarez (2023), reveló que aproximadamente en el país se reportan un promedio de 10.000 denuncias de delitos informáticos anualmente Salcedo (2021).

No obstante, el problema no se limita netamente al ámbito del sector público, también se registran estos eventos en el sector privado, así como en el ámbito particular o personal, tal y como ocurrió a finales del año 2021 con el Banco del Pichincha según indica Díaz (2021), evento en el cual la infraestructura tecnológica de la institución se vio afectada, por lo cual los clientes prefirieron optar por cambiarse hacia otras entidades financieras por temor a que este

tipo de situaciones pueda comprometer sus cuentas, este tipo de eventos desencadenan en la pérdida de credibilidad e imagen empresarial.

El sector empresarial en la ciudad de Cuenca, no es la excepción y como en el resto del territorio nacional como ya hemos expuesto y contrastado con las fuentes de información, los ataques son frecuentes, es difícil poder estimar la cantidad de ataques diarios a las empresas ya que esto depende primero del ámbito en el cual operan, del tamaño de la misma, de su infraestructura entre otros parámetros que definen el riesgo potencial al cual se encuentran expuestas.

El caso de "Diario El Mercurio", al ser un medio de comunicación de ámbito local, no se encuentra exento de amenazas y es por ello que, al no contar con un plan de gestión de riesgos de la información, el nivel de exposición a las amenazas es bastante alto, de aquí nace la oportunidad de realizar este proyecto el cual vienen a complementar los esfuerzos por parte de la directiva en proteger sus activos de información y de esta manera mitigar dichos riesgos en la medida de lo posible ya que los riesgos no se pueden eliminar en su totalidad en ningún caso.

Según el artículo de Arévalo et al. (2017), existen varias metodologías que nos permiten realizar el análisis de riesgos, las cuales pueden ser aplicables o no, dependiendo de las características que posee cada empresa, y a partir de esta poder realizar todo el proceso del análisis, la evaluación y posteriormente poder ofrecer los resultados deseados como producto final del ámbito que comprende este proyecto.

El siguiente paso es la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en base a los resultados de este proyecto, dicha implementación según menciona Novoa & Barrera (2019) también debe cumplir con una metodología determinada por los resultados obtenidos previamente para de esta manera poder realizar un seguimiento mediante auditorías periódicas, que permitan plasmar un proceso de mejora continua dentro de la empresa.

Hay que indicar que, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) posee su propio cronograma de actividades y requiere también definir un presupuesto basado en el cálculo de costos de los elementos necesarios (hardware, software, capacitación, etc) el mismo que forma parte de otro informe técnico, pero cabe mencionar que la **implementación de dicho sistema no forma parte de este proyecto**, ya que la decisión de

realizarlo o no dependerá exclusivamente de las decisiones que tomen los directivos a futuro, por tanto la limitación de este proyecto culmina con la entrega del informe técnico.

La finalidad de este proyecto se justifica económicamente y también a nivel de reputación, ya que la importancia que mantienen los activos de información dentro de una empresa es trascendental cuando se trata de activos críticos dentro de la misma, es por ello que se debe prestar especial énfasis en la protección de los mismos, dado que de materializarse una potencial amenaza total o parcialmente en los mismos pueden representar pérdidas graves para la compañía, no solamente en temas financieros, sino que también en términos de prestigio y reputación.

Casos como los ocurridos en entidades financieras en el país Díaz (2021), han hecho que muchos de sus clientes pierdan la confianza en dichas instituciones y con ello, la migración de dichos clientes hacia otras instituciones, es por ello que con la ejecución de este proyecto se pretende evitar que casos como el mencionado puedan repetirse dentro de la empresa, lo cual se vería reflejado en pérdida de suscriptores tanto en el medio impreso, como en las plataformas digitales de la empresa lo cual para un medio de comunicación representa una situación catastrófica en términos económicos y de credibilidad.

1.7 Fundamentación Teórica.

Seguridad de la Información.

La teoría nos dice que el concepto como tal, comprende los procedimientos, prácticas y metodologías que tienen como finalidad la protección de la información como tal, así como de los sistemas y recursos de información ya que, en el mundo moderno la dependencia de la tecnología es casi que absoluta, el acceso a la información representa un riesgo potencial si las intenciones no son las adecuadas.

Por otro lado, en un sentido general, la seguridad tiene como objetivo el proteger nuestros activos de múltiples factores de riesgo como son: atacantes, desastres naturales, condiciones ambientales adversas, cortes en el suministro de energía, delincuencia o vandalismo entre otros. Al analizar lo que pretendemos asegurar, se presenta una amplia gama de activos potenciales.

Entre ellos pueden encontrarse elementos físicos que quisiéramos proteger, otros de valor inherente, o aquellos que tienen valor para una entidad. Se pueden considerar también activos

intangibles como software, código fuente o datos; de aquí comprendemos que, los activos intangibles son tan valiosos, o más, que los físicos. Se debe considerar también proteger al personal de la organización o empresa, ya que son probablemente el activo más valioso. Vega Briceño (2021).

Objetivos de la seguridad de la información.

Se sabe que, la seguridad de la información puede adaptarse en función de las características de cada organización y del sector al que dedique su actividad económica, sin embargo, existe una serie de objetivos comunes que comparten todas las organizaciones.

Estos objetivos de la seguridad de la información están agrupados dentro de la norma ISO 27001, la cual establece un modelo para la implementación de sistemas de gestión de seguridad de la información (S.G.S.I.). El objetivo principal de la ISO 27001 es la protección de los activos de información.

Debe tomar en cuenta los tres aspectos fundamentales que son los pilares de la ciberseguridad y se lo conoce como tríada CID compuesta por:

- Integridad
- Confidencialidad
- Disponibilidad

Estos conceptos se encuentran descritos a profundidad en el texto de Toro (2021), y sirven como fundamentación teórica para comprender mejor el área de conocimiento involucrada.

Ciberseguridad.

Comprende la defensa de los activos de información de ataques maliciosos, conocida también como seguridad de tecnología de la información o seguridad de la información electrónica. Es un término ampliamente difundido en varios ámbitos, desde los negocios hasta la informática móvil, y entre sus categorías podemos mencionar.

- **Seguridad de red:** se encarga de proteger una red contra intrusos, ya sean atacantes dirigidos o malware.
- **Seguridad de las aplicaciones**: enfocada en mantener el software y los dispositivos libres de amenazas. Las aplicaciones afectadas permitirían acceso a la información que debería proteger, de ahí que es importante poner énfasis en la etapa de diseño de mismo.
- **Seguridad de la información**: encargada de proteger tanto la integridad y como la privacidad de datos, en etapas de almacenamiento y tránsito.

- **Seguridad operativa:** comprende procesos y decisiones para manejar y proteger los recursos informáticos, permisos de usuarios y accesos a recursos, procedimientos que identifican cómo y dónde pueden almacenarse o compartirse los datos.
- **Recuperación ante desastres y la continuidad del negocio**: hace referencia a la forma en que una organización puede responder ante incidentes o eventos que produzcan parones operativos o pérdida de información, comprende las políticas de recuperación que permiten volver a la capacidad operativa que antes del evento.
- **Capacitación del usuario final:** trata sobre el factor más importante: las personas. Por desconocimiento o de manera intencional, una persona puede introducir accidentalmente un virus o realizar acciones que comprometan a toda una infraestructura; es por ello que capacitar al personal sobre buenas prácticas de seguridad informática es muy importante para cualquier institución.

Toda esta información a detalle se encuentra disponible en el artículo Kaspersky Labs (2023).

Pilares de la Ciberseguridad.

Según el artículo de Toro (2021) hay conceptos necesarios de tomar en cuenta.

Integridad.

Hace referencia a que la información se muestre tal y como fue concebida, sin alteraciones o manipulaciones que no hayan sido autorizadas de forma expresa, esto permite garantizar la transmisión de los datos confiables, por medio del uso de protocolos seguros.

Confidencialidad.

Indica que, solamente personas o entidades autorizadas tengan acceso a la información y que éstos no se compartan sin el permiso correspondiente de tal manera que, no se vea comprometida en ningún momento.

Disponibilidad.

Comprende que, la información esté disponible todo el tiempo para las personas o entidades autorizadas para su manejo y conocimiento, para cumplir con este parámetro, es necesario contar con medios de soporte a los cuales se puedan acceder en caso de fallos o interrupciones en servicios.

Cibedelincuentes.

Son individuos expertos en vulnerar sistemas y recursos informáticos, motivados por diferentes finalidades, como económicas, políticas, sociales, etc, que causan daños a dichos

sistemas, atentando contra los activos de información de instituciones públicas o privadas, y la información que estos manejan. Kaspersky Labs (2023).

Ciberamenazas.

Hacen referencia a los posibles riesgos presentes en el mundo digital tanto para las personas, como para instituciones e incluso a nivel gubernamental, se encuentran aumentando a un ritmo cada vez mayor, lo cual representa una cantidad cada vez mayor de filtraciones de datos que crece cada año. “Dentro de uno de los informes realizados por RiskBased Security, se reveló que 7900 millones de registros han sido expuestos por filtraciones durante el año 2019. Cifra que representa más del doble (112 %) de la cantidad de filtraciones ocurridas en el 2018.”

“Se comenta también que gobiernos alrededor del mundo en respuesta al cada vez mayor número de ciberamenazas intentan generalizar acciones que permitan ayudar a sus organizaciones a realizar y aplicar prácticas eficaces en este tema.” Kaspersky Labs (2023).

Tipos de ciberamenazas.

Las amenazas se clasifican en tres tipos:

1. **Delito cibernético** compuesto por agentes individuales o grupos que atacan sistemas con el fin de obtener beneficios económicos o producir interrupciones.
2. **Ciberataques** por lo general se basan en la recopilación de información con fines políticos.
3. **Ciberterrorismo** intenta debilitar los sistemas para causar pánico o temor.

Los métodos más utilizados por las amenazas son:

Malware.

Son programas que traen en su código instrucciones ocultas que tienen por objetivo causar daño a los equipos informáticos o apoderarse de la información contenida en ellos, generalmente es propagado a través de archivos adjuntos de correo electrónico no solicitado o de una descarga de apariencia legítima, la finalidad del atacante es obtener dinero o con fines políticos; entre los tipos que podemos indicar están:

- **Virus:** software que reproduce y extiende en un sistema informático e infecta a los archivos con código malicioso.
- **Troyanos:** pretende ser un programa distinto, pero internamente esconde código malicioso.

- **Spyware:** software que guarde un registro en secreto de toda la actividad de un usuario.
- **Ransomware:** software que cifra el contenido de archivos y datos de un usuario con la intención de pedir un rescate por la misma.
- **Adware:** programa que inyecta publicidad en determinado lugar.
- **Botnets:** equipo o equipos que contienen malware y es utilizado para realizar tareas en línea sin permiso del usuario.

Inyección de código SQL.

Viene de las siglas en inglés "Structured Query Language" y tiene por objetivo apoderarse de la información almacenada en una base de datos.

Phishing.

Son ataques generalmente utilizados mediante correos electrónicos los cuales pretenden usurpar la identidad de una persona o empresa para intentar obtener información confidencial.

Ataque "Man-in-the-middle".

Hace referencia a que un ciberdelincuente logra interceptar la comunicación entre dos individuos para robar datos.

Ataque de denegación de servicio.

Tiene por objetivo el impedir que un sistema informático de respuesta a las solicitudes que recibe, sobrecargando la infraestructura con tráfico que tiene por objetivo volver a un sistema inutilizable, comprometiendo a una organización.

Detalle completo de estos conceptos está disponible en el artículo Kaspersky Labs (2023).

Ataques y tipos de ataques.

Según la publicación de Vega Briceño (2021) los ataques pueden generarse desde múltiples enfoques y ángulos, por ello, podemos relacionar el tipo de ataque con el riesgo que representa y los controles que podríamos usar para mitigarlo. Se pueden englobar dentro de cuatro categorías: intercepción, interrupción, modificación y fabricación.

Amenazas.

Son factores que tienen el potencial de causar daño a nuestros activos.

Vulnerabilidades.

Vienen a ser las debilidades que pueden usarse para dañarnos y, que pueden aprovecharse por amenazas para afectar a un objetivo específico.

Riesgos.

Es la probabilidad de que algo malo suceda, para ello debe existir una amenaza específica pueda explotar las diversas debilidades.

Sistema de gestión de la seguridad de la información.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) definido en la ISO/IEC 27000 como componente de un sistema de gestión general, que comprende un enfoque al riesgo empresarial, con la finalidad de establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.; contiene la estructura de la organización, políticas, planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. Calder (2017)

Activos de información.

Es todo tipo de recurso que represente cierto valor para una entidad. Se encuentran sujetos a múltiples amenazas, tanto externas como internas. Calder (2017)

¿Qué es un Análisis GAP?

Comprende un proceso en el que se compara la situación actual con la situación futura deseada en temas de seguridad de la información, lo cual permite elaborar múltiples acciones que ayuden a cubrir las brechas (GAP) identificadas, es de gran utilidad para el análisis interno de una organización.

Las ventajas de este procedimiento, es que permite comparar la situación actual de la compañía, con la situación deseada para el futuro, para poder definir un plan de acción que permita alcanzar ese objetivo, y a su vez sirve de base en los procesos de mejora continua de la compañía.

Información completa disponible en el artículo de Wright (2021).

ISO – IEC 27001.

Es el estándar más difundido para los de sistemas gestión de seguridad de la información, forma parte de la familia de la ISO 27000 que a su vez comprende la protección de datos. Calder (2017).

Análisis BIA.

Es un procedimiento que forma parte del análisis de riesgos, y permite identificar las áreas críticas y los procesos medulares dentro de una institución o empresa, y nos permite identificar el impacto que estos tienen en la gestión de la misma, para poder resguardarlos prioritariamente y poder garantizar la continuidad del negocio en caso de incidentes de seguridad. Entrega como resultado varios indicadores que representan alertas para la directiva sobre las cuales debe

tomar decisiones que permitan garantizar el aseguramiento de dichas áreas y procesos. Ministerio de Tecnologías de la Información y las Comunicaciones Colombia et al. (2023).

MITRE ATT&CK®

Es una base de conocimiento desarrollada bajo marco de trabajo por MITRE Corporation, que permite a las empresas comprender sus vulnerabilidades y en base a comportamientos en tiempo real de las mismas en otros entornos, proponer soluciones para su mitigación, comúnmente utilizadas por los "equipos rojos" para descubrir y explotar vulnerabilidades, documentando todos los procesos para ayudar a conocer mejor la situación y el nivel de seguridad de una empresa, está formada por cuatro matrices: "Preparación", "Para Empresas", "Para Móviles", "Para Sistemas de Control Industrial".

La ventaja principal radica en que su utilización permite a las compañías entender la manera en que operan los ciberatacantes, para anticiparse a sus acciones y tomar los debidos correctivos. Qué es MITRE ATT CK – Definition | VMware Glossary (2022).

Metodología MAGERIT.

Es una metodología para el análisis de riesgos pertinentes al área de las tecnologías de la información, elaborada por la que actualmente es la Secretaría General de Administración Digital, del gobierno de España, actualmente se encuentra en la versión 3 y en esencia, permite realizar la implementación de la gestión de riesgos, está estructurada en tres secciones: "El método", un "catálogo de componentes o elementos" y la "guía de técnicas".

El uso de esta metodología tiene por objetivos: concientizar, analizar los riesgos de manera óptima, elaborar un plan para su tratamiento, y también preparar a las organizaciones para procesos de certificación.

En este caso de estudio se tomó como base la implementación del estándar ISO 27001, sin embargo, es importante mencionar que la norma como tal, indica qué es lo que se debe realizar, mas no indica el cómo realizarse, es por ello que aplicar una metodología es una parte fundamental, para conseguir los objetivos detallados en la norma. Secretaría General de Administración Digital et al. (2012)

Capítulo II. Diagnóstico situacional.

2.1 Metodología.

El proceso desarrollado abarca una serie de pasos, los cuales se detallaron en el cronograma de actividades realizado, con el fin de dar cumplimiento a todas las actividades que se planificaron durante la ejecución del mismo.

- **Primer paso.**

  El objetivo inicial fue recopilar la documentación necesaria (los permisos requeridos por parte de la directiva de la compañía para la ejecución del proyecto), y una vez cumplido con este requerimiento, se procede a revisar y seleccionar el material bibliográfico necesario para ser utilizado a lo largo de todo el proceso, para esto se realizó una evaluación de las fuentes digitales confiables y verificadas, tanto en inglés como en español, que sirvieron como material de sustento referencial en todos los puntos que abarca este proyecto.

- **Segundo paso.**

  Una vez seleccionado el material bibliográfico idóneo, se procedió con la ejecución de un análisis GAP mediante el cual se definió el punto de partida del proyecto, el mismo que pudo constatar la situación actual de la empresa en materia de seguridad de la información (S.I.).

- **Tercer paso.**

  A continuación, se recopiló información sobre el nivel conocimiento que tiene el personal de diferentes áreas de la empresa acerca de temas de S.I., para lo cual se la elaboró un programa de encuestas con preguntas específicas sobre el tema en cuestión.

- **Cuarto paso.**

  El siguiente paso realizado fue el levantamiento de activos de información, el cual tuvo por finalidad identificar de entre todos los activos con los que cuenta la empresa, cuáles de ellos son críticos, a fin de definir un orden jerárquico según su importancia en función de su impacto en las actividades de la empresa.

- **Quinto paso.**

  Una vez definida la lista de activos críticos, se realizó la evaluación de los riesgos, que es uno de los procesos medulares de este proyecto, ya que este proceso permite

identificar las amenazas y los riesgos a los cuales están expuestos los activos de información y el impacto dentro de la estructura de la empresa, para ello fue necesario elaborar un mapa de calor que explique claramente la relación entre la probabilidad y el impacto en función de los riesgos y amenazas que se identifiquen previamente.

- **Sexto paso.**

  Una vez se tienen claros los riesgos, se procedió a analizar las vulnerabilidades con la finalidad de identificar posibles puntos de ataque, para esto se definió una matriz que clasifica los resultados en función de su criticidad, con la finalidad de darles prioridad a los más importantes.

- **Séptimo paso.**

  Luego de concluir las pruebas, fue necesario analizar los resultados proporcionados por los procesos realizados, con lo cual se obtuvo una idea clara de las posibles soluciones a implementarse, las cuales se encuentran presentes en el informe final.

- **Octavo paso.**

  Posteriormente a la revisión de estos resultados, se procedió a elaborar un plan de mitigación de riesgos, aplicando los controles indicados en la norma ISO 27001 sobre aquellos dominios que presentaron valores nulos durante la ejecución del análisis GAP.

- **Noveno y último paso.**

  Una vez se consiguieron los resultados de todo el proceso, la etapa final consistió en la elaboración del documento final entregable para la directiva, este documento consta de dos reportes: el primero es el informe ejecutivo, el cual contiene los resultados del estudio explicados de una manera fácil de entender para los directivos, detallando las conclusiones y recomendaciones a implementarse, en función de los intereses de la empresa, el segundo documento es el informe técnico el cual contiene detalladamente un registro de todas las actividades desarrolladas, así como los resultados obtenidos de cada una de las mismas.

2.2 Análisis situacional.

Diario El Mercurio Cía. Ltda. es en la actualidad el medio de comunicación más importante en la región y se ha consolidado por 97 años como el medio de mayor relevancia en la zona del austro del Ecuador, Redacción El Mercurio (2022); razón por la cual es necesario realizar

una evaluación de la situación de la empresa en esta temática, con la finalidad de poder entregar un informe técnico con los resultados de esta investigación a la alta dirección de la compañía puesto que, la empresa actualmente no cuenta con un plan de gestión de riesgos de seguridad de la información.

2.3. Análisis comparativo.

En este apartado es necesario indicar, a manera de justificativo las razones por las cuales se optó por utilizar el estándar ISO 27001 para el desarrollo de este proyecto, y fue escogido principalmente porque es el estándar más conocido, popularizado y utilizado en América Latina, además que han sido elaborado en conjunto por la Organización Internacional de Normalización y también por la Comisión Internacional Electrotécnica, por lo cual se ha considerado que la familia de normas ISO/IEC 27000 es la adecuada para ser utilizada en este proyecto. Tecnologías de la información – Técnicas de Seguridad - Guía para la aplicación integrada de la norma INTE/ISO/IEC 27001 e INTEISO/IEC 20000-1, s. f. (2017).

Si bien existen otras normativas que permiten realizar la implementación de un S.G.S.I. en una organización, existe la guía desarrollada por el Instituto Nacional de Normas y Tecnología de EE.UU. denominada la **NIST 800-53**, que contiene las normas exigidas por el Gobierno Federal para controles específicos de privacidad y seguridad informática. Cumplimiento de NIST 800-53 | Google Cloud (2023).

Existe también la lista **CIS Controls**, desarrollado por el Center for Internet Security, la cual es una organización sin fines de lucro, que pretende ayudar tanto a gobiernos como a empresas para protegerse debidamente contra las ciberamenazas, para esto propone un conjunto de buenas prácticas basándose en información sobre ataques reales y las técnicas efectivas empleadas para su mitigación. CIS® - Center for Internet Security (2021).

2.4. Herramientas utilizadas.

Para el desarrollo de este proyecto, se han inventariado el uso de las siguientes herramientas:

- Hardware: PC dedicada a la documentación y desarrollo de los informes, hojas de cálculo, presentaciones de diapositivas, imágenes, etc.
- Software: Suite de Office, Photoshop, software gestor de citas bibliográficas Mendeley, Navegadores de internet.

- Utilitarios de oficina: hojas A4, bolígrafos, para la elaboración de las encuestas, para la impresión de los documentos entregables.

Capítulo III. Propuesta.

3.1 Alcance del S.G.S.I.

3.1.1 Reseña Histórica de la empresa.

Este medio de comunicación fue fundado en la ciudad de Cuenca el 22 de octubre de 1924, su primer director fue el doctor Carlos Aguilar Vásquez, seguido por el doctor Manuel Moreno Mora, el tercer director fue José Sarmiento Abad, todos ellos en la primera década de vida del diario.

Posteriormente sería el doctor Nicanor Merchán Bermeo, quien asumió la dirección de la empresa hasta el año 1956, fue quien impulsó el proceso de modernización y rediseño del diario; tras su muerte, le sucedió en la dirección de la empresa el ingeniero Miguel Merchán Ochoa quien asumió el cargo de director hasta la fecha de su fallecimiento suscitado en 1974, año en el cual asumió la dirección del diario el doctor Nicanor Merchán Luco conjuntamente con la licenciada Marina Merchán Luco como gerente general, quienes hasta la fecha desempeñan sus respectivas funciones dentro de la empresa. Zamora Merchán (2005).

El medio ha sufrido múltiples transformaciones tecnológicas desde sus inicios, entre las cuales se puede mencionar el cambio del tipo de impresión inicial conocido como “impresión en caliente”, que consistía en fundir plomo para obtener los lingotes que posteriormente ensamblaban las matrices que eran colocadas en la rotativa, para de esta manera iniciar el proceso de impresión, que inicialmente fue monocromático, proceso empleado hasta el año 1984 en el cual inició la impresión a color.

Entre las décadas de los ochenta y noventa, la empresa hizo frente a varios procesos de mejoras en cuanto a su infraestructura, ya que el avance en los campos informáticos permitió agilizar y reducir considerablemente los tiempos de ejecución en los procesos de producción de la empresa adquiriendo el sistema OFFSET conocido como “impresión en frío”, el cual basa su funcionamiento en la utilización de químicos y películas que dan como resultado las planchas de aluminio procesadas para su posterior uso en la rotativa, desde el año 2015 este proceso fue optimizado mediante la adquisición de equipos procesadores de planchas automatizados los cuales son utilizados hasta la actualidad. Norden (2018).

El formato impreso en la actualidad cuenta con dos secciones y dos suplementos que circulan los fines de semana junto con la edición. DIARIO EL MERCURIO CIA. LTDA., tiene a

su planta matriz en la ciudad de Cuenca ubicada en la Avenida de las Américas y Francisco Ascázubi, cuenta con 3 agencias en la ciudad, así como también agencias en las ciudades de Quito y Guayaquil; y en la empresa actualmente laboran 59 empleados en sus distintos departamentos y agencias.

3.1.2 Convergencia hacia la era digital.

En junio de 1995 se da el salto digital de la empresa, e inician una nueva etapa con "Cuenca On Line", primera plataforma de noticias en internet de la ciudad de Cuenca y su entorno. Zamora Merchán (2005).

A partir de ese momento y hasta la actualidad la empresa ha ido modificando sus herramientas informáticas para ir a la vanguardia de las nuevas tecnologías que han aparecido a lo largo de las décadas, hasta llegar a la actualidad en la cual la empresa ha evolucionado para convertirse en un medio de comunicación multiplataforma, la cual cuenta con su sitio web, así como en las múltiples redes sociales que maneja.

3.1.3 Estructura de la empresa.

Visión.

Mantenerse posicionado como el medio de comunicación más importante de la región, adaptándose al constante cambio en un mundo que evoluciona digitalmente, para continuar sirviendo a la sociedad con un trabajo íntegro, ético y de calidad.

Misión.

Brindar información y opinión consistente con los principios deontológicos basada en los principios que rigen el periodismo profesional, la misma que debe ser clara, precisa, confiable, verificable y trascendente a la comunidad, fundamentado en el derecho universal que tiene el ser humano a estar informado, lo cual aporta a construir una sociedad plurinacional y multiétnica con ciudadanos críticos y responsables en los procesos sociales.

Valores.

Los valores que rigen a Diario El Mercurio son:

- Ética.
- Honestidad.
- Profesionalismo.
- Respeto a la dignidad humana.

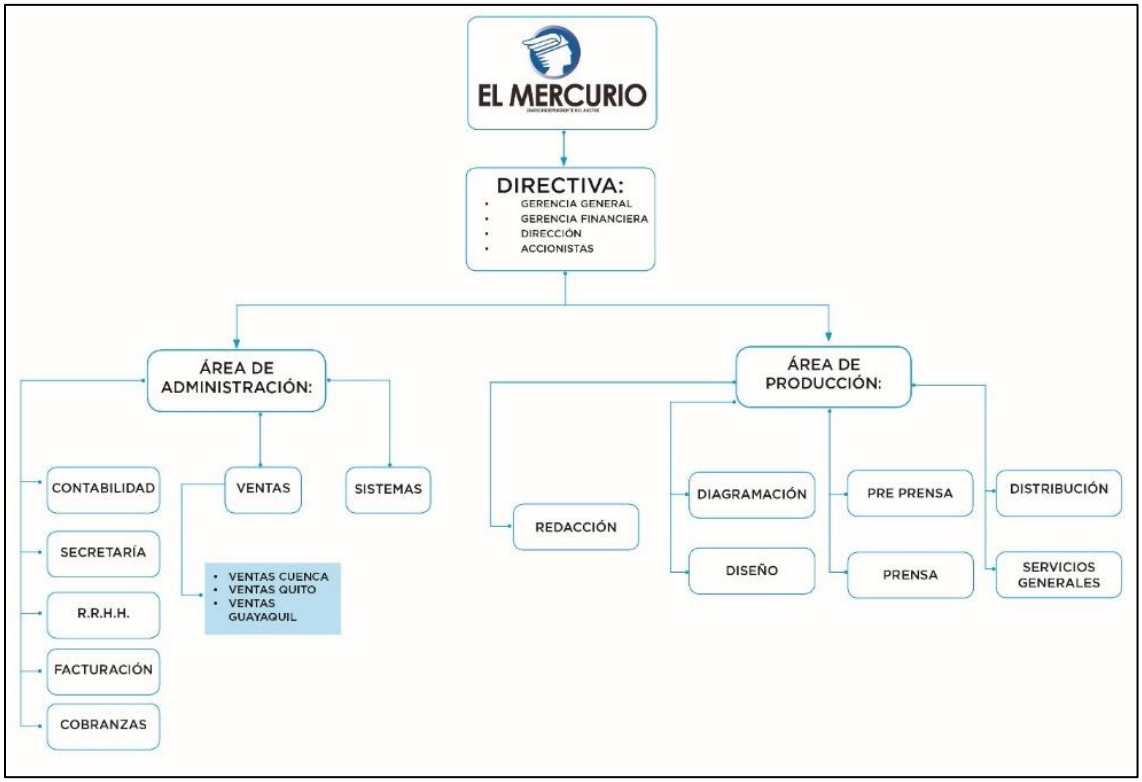
- Respeto a libertad de expresión y pensamiento.
- Responsabilidad para con la sociedad.

3.1.4 Organigrama.

La empresa está estructurada por la directiva y las dos ramificaciones que segmentan al diario en la sección administrativa y la de producción con sus respectivas dependencias departamentales, las mismas que se pueden apreciar en la ilustración que se presenta a continuación.

Ilustración 1.

Organigrama de Diario El Mercurio.



Nota. Elaborado por el autor del documento.

3.1.5 Matriz FODA.

La siguiente tabla muestra el contenido del análisis de fortalezas, debilidades, oportunidades y amenazas, aplicado a la empresa.

Tabla 1.

Análisis FODA de la empresa "Diario El Mercurio Cia. Ltda.".

F.O.D.A.		
	INTERNO	**EXTERNO**
NEGATIVOS	**DEBILIDADES** • Infraestructura desactualizada en área de producción. • Falta de comunicación de políticas internas. • Poca capacitación al personal.	**AMENAZAS** • Aparición de nuevos medios digitales. • Cambios en los hábitos de consumir información por parte de la comunidad. • Cambios en la legislación vigente que pueden afectar al sector de manera negativa.
POSITIVOS	**FORTALEZAS** • Medio de comunicación con mayor trayectoria regional. • Equipo profesional con amplia experiencia periodística. • Amplia acogida por parte de los lectores y seguidores del medio.	**OPORTUNIDADES** • Nuevas tendencias tecnológicas que puede representar nuevos nichos de mercado. • La aparición de nuevas audiencias que requieran enfoques actualizados en la manera de hacer periodismo. • Nuevas estrategias de marketing que permitan atraer a nuevos consumidores de los productos que ofrece la empresa.

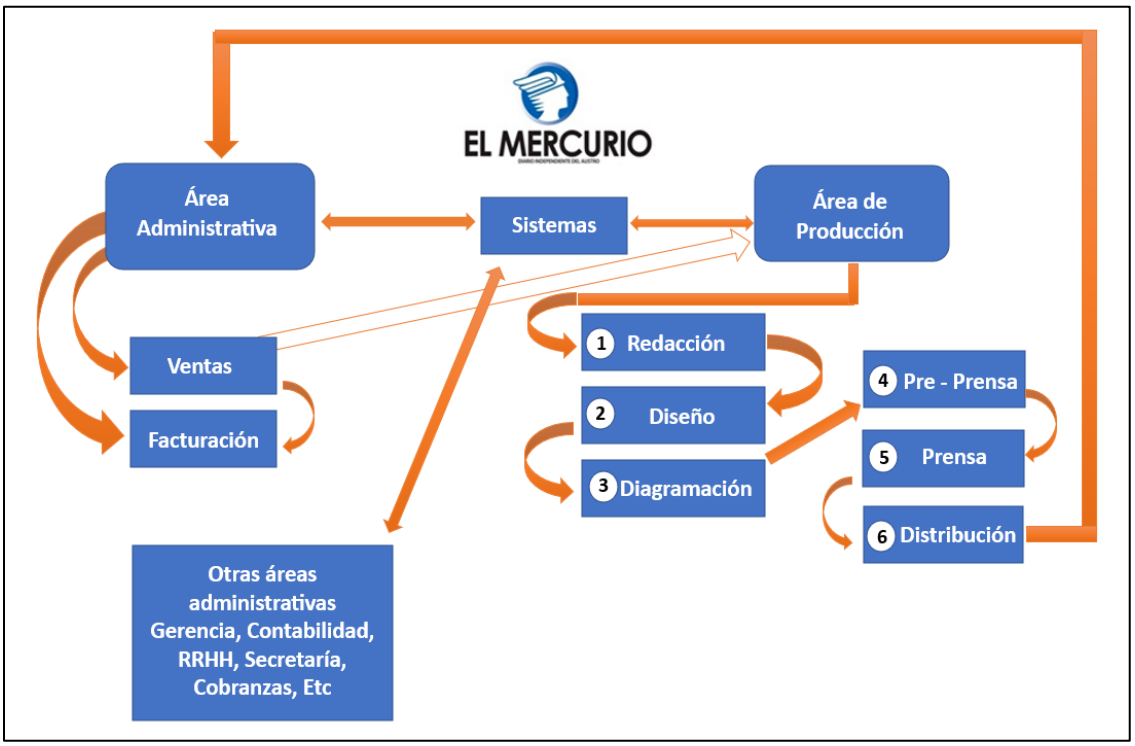
Nota. Elaborado por el autor del documento, conjuntamente con el departamento de talento humano de la compañía.

3.1.6 Mapa de Procesos.

La empresa al estar dividida en áreas administrativa y producción, es necesario definir un mapa de procesos, que conceptualice el esquema de trabajo diario de la compañía para entender de mejor manera su estructura, la siguiente ilustración representa el mapa de procesos internos de la empresa.

Ilustración 2.

Mapa de procesos de la empresa.



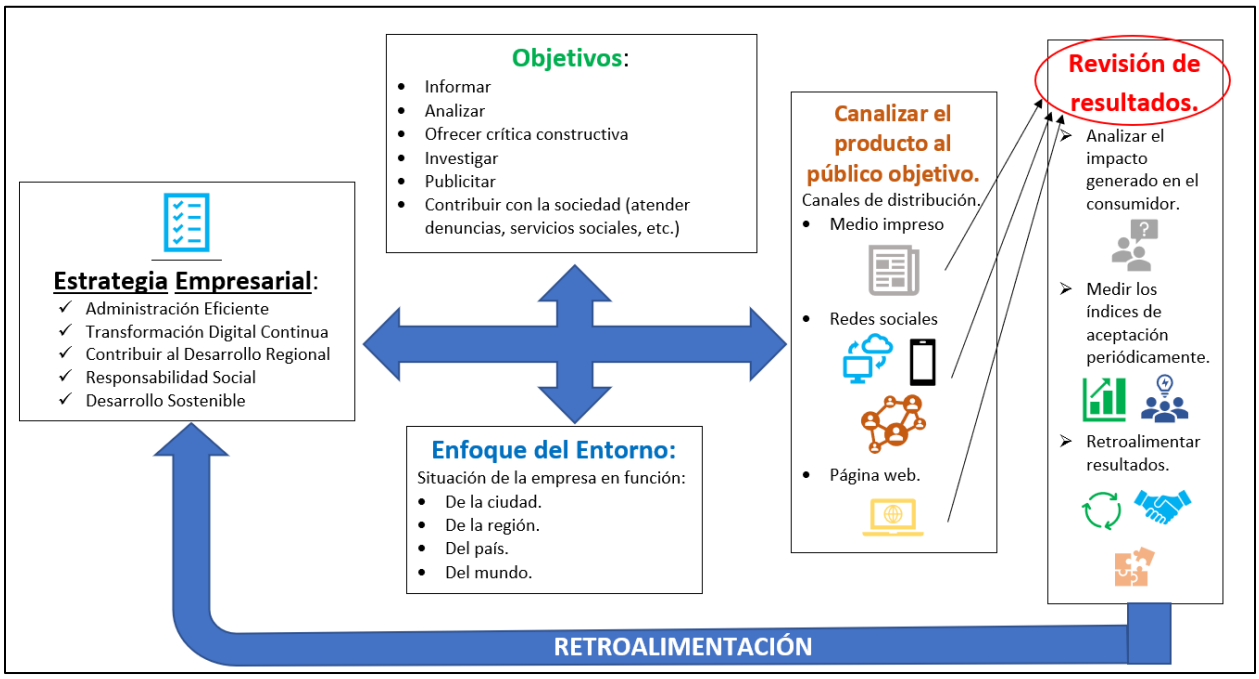
Nota. Elaboración del mapa de procesos conjuntamente entre el autor del documento, la gerencia de operaciones y el departamento de talento humano.

3.1.7 Plan estratégico.

Se encuentra distribuido en función de las características de la empresa y se puede observar en la siguiente ilustración.

Ilustración 3.

Plan estratégico de "Diario El Mercurio Cia. Ltda.".



Nota. Gráfico explicativo del plan estratégico de la compañía, elaborado en conjunto con el autor del documento, la directiva, y los directores de cada departamento.

3.2 Presentación de la propuesta del proyecto ante la directiva.

Luego de una reunión entre la directiva, el departamento de sistemas y recursos humanos, se expuso el planteamiento de la ejecución de este proyecto, justificando en primera instancia la falta de políticas internas de la empresa en seguridad de la información, ante lo cual la directiva aprobó la ejecución del proyecto y el cronograma de actividades propuesto para la realización del mismo.

3.2.1 Solicitud a la directiva.

Dando cumplimiento a los requerimientos de este tipo de proyectos, el primer paso es realizar una solicitud formal a la directiva de la empresa, en la cual se expone el tema a tratar, así como la justificación y la petición de autorización para acceder a la información necesaria y a los recursos correspondientes para la ejecución del proyecto. Esta solicitud fue realizada con fecha 18 de enero del 2023, y se recibió la respuesta de la directiva el día 19 de enero del 2023, en la cual se concede la autorización necesaria para la ejecución del proyecto de acuerdo a las condiciones

establecidas. El detalle de este proceso, que es esencial para el inicio de las actividades, se encuentra detallado con las evidencias en el **ANEXO 1**, el cual comprende ambos documentos.

3.2.2 Realidad interna de la empresa sobre seguridad de la información.

En primera instancia se debe indicar que la empresa no cuenta actualmente con políticas internas ni tampoco con un plan estratégico para la gestión de incidentes de seguridad de la información, de lo cual nace la oportunidad de poder realizar este proyecto de investigación, a fin de solventar esta necesidad y contribuir con un aporte de valor para la misma.

Además, hay que tomar en cuenta los cambios que se implementaron en el país a partir del mes de mayo, que fue cuando entró en vigencia las sanciones de la **Ley de Protección de Datos Personales,** (razón por lo cual un estudio de este tipo se convierte en mandatorio como punto de partida para una futura certificación en la familia de las normas **ISO 27000,** que representaría una de las metas a cumplir para la empresa).

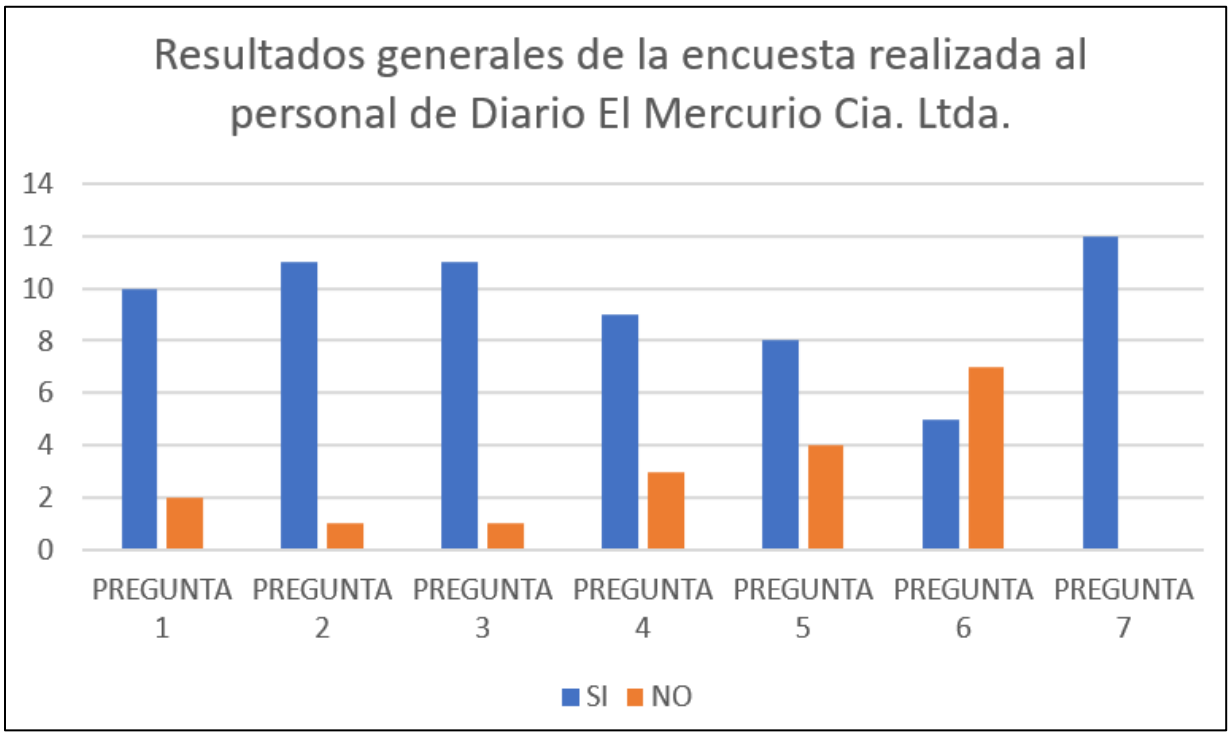
Como parte del plan de trabajo se determinó realizar una valoración general de conocimientos al personal de las distintas áreas de la empresa, la cual se ejecutó durante la primera semana de febrero de 2023, mediante una encuesta previamente elaborada de acuerdo a los conceptos básicos de seguridad de información.

Los resultados de este proceso revelaron que la realidad interna de la empresa, demanda acciones concretas principalmente en capacitación, ya que los resultados reflejaron que en su mayoría el personal es consciente de la importancia que tiene mantener la seguridad de la información que manejan y procesan diariamente en sus actividades, pero no tienen muy claro los conceptos sobre las amenazas y los riesgos a los cuales están expuestos, tomando en cuenta que, el eslabón más débil en la cadena de una institución es el factor humano Lavandeira Lema (2022), es fundamental que el personal tenga conocimiento de estos temas, a fin de evitar que represente una amenaza interna a la institución.

Los resultados de este análisis, a modo general se pueden apreciar en la siguiente ilustración, la cual resume el estado actual de conocimiento que tiene el personal en este tema.

Ilustración 4.

Resultados de la encuesta realizada al personal de distintas áreas de la empresa.



Nota. La ejecución y tabulación de los resultados, así como el formato de la encuesta fueron aprobados por la directiva en reunión previa al proceso y realizadas por el autor del documento.

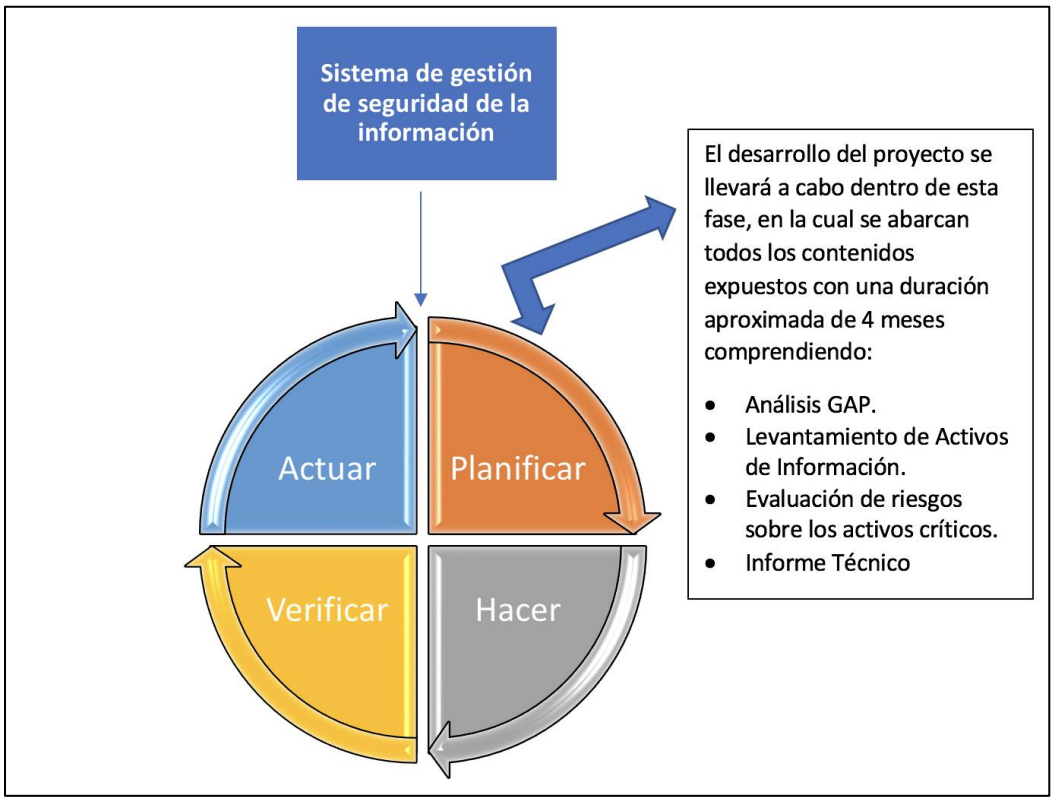
En el documento **ANEXO 2**, se encuentra detallado todo el proceso, las preguntas, los resultados y las conclusiones obtenidas mediante este procedimiento, así como también las evidencias del trabajo realizado.

3.2.3 Esquema de actividades y delimitación del proyecto.

La siguiente ilustración, indica la etapa dentro del ciclo de vida del SGSI, sobre la cual se va a desarrollar todo el proyecto, que es la fase de planificación, dentro de la cual se encuentra la etapa de análisis.

Ilustración 5.

Delimitación del proyecto.



Nota. Los pasos posteriores a la planificación, descritos en el ciclo de vida del S.G.S.I no serán objeto de este caso de estudio.

3.3 Desarrollo de actividades.

3.3.1 Resumen Ejecutivo

El presente proyecto tiene por objetivo el desarrollar un plan de gestión de riesgos, que permita mitigar las amenazas a las cuales se encuentran expuestos los activos de información de la empresa "Diario El Mercurio Cia. Ltda.", que es el caso de este estudio; para ello la metodología a emplearse está definida mediante la elaboración de un cronograma de actividades, que detalla los pasos a realizarse durante el tiempo de ejecución de este proyecto, los cuales están fundamentados en la norma ISO 27001.

Además de incluir procesos comprendidos en la evaluación de riesgos en seguridad de la información, de tal manera que sirvan como base para poder elaborar un informe técnico, que debe ser entregado a la directiva de la compañía como el producto final de este proyecto, el mismo que debe contener a detalle los resultados de los procesos realizados, las conclusiones de los mismos

y las recomendaciones a tomar en cuenta para la implementación de las respectivas correcciones a realizarse.

3.3.2 Modelo de madurez inicial.

Se ha planteado realizar un análisis de brechas (Análisis GAP) preliminar que sirva como punto de partida para todo el proyecto y posteriormente de acuerdo al cronograma de actividades definido previamente, ejecutar las tareas correspondientes a los siguientes pasos que comprende la fase de planificación de acuerdo a los parámetros establecidos en la norma ISO 27001.

Metodología empleada.

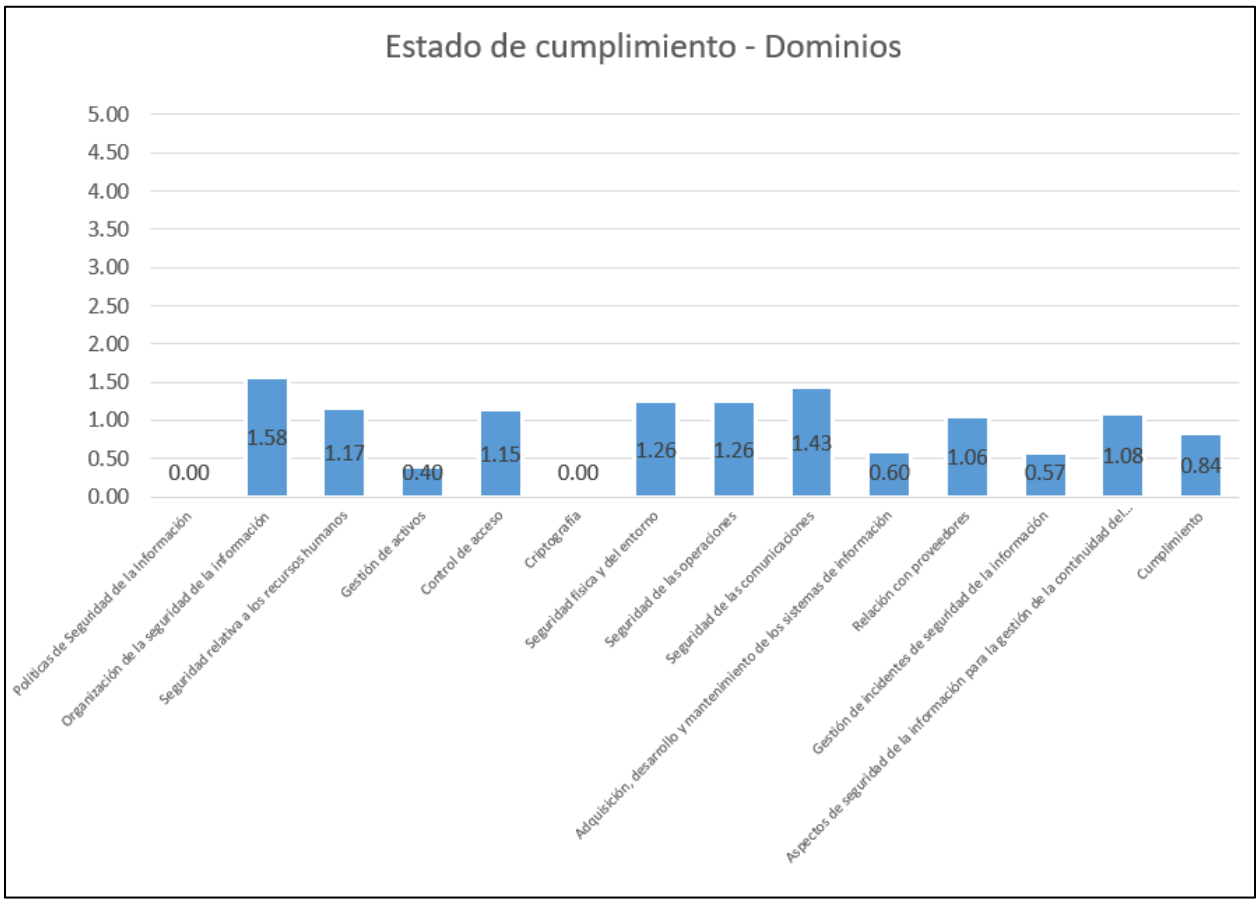
Para desarrollar la actividad, se optó por el uso de la matriz de contenidos planteada en la ISO 27002 conocida también como Anexo A de la ISO 27001, la cual se basa en completar un formulario de preguntas que comprenden los puntos desde el A5 hasta el A18 y sus respectivos subdominios la actividad comprende: el análisis diferencial, el cuestionario GAP, los controles, la matriz de responsabilidades.

Resultado inicial (Estado Actual).

Los resultados obtenidos de la matriz reflejan un valor muy bajo, lo cual era predecible ya que, al no existir un estudio previo de estas características, no hay ni políticas, ni controles establecidos en la mayoría de los dominios analizados, la ilustración siguiente refleja gráficamente los resultados obtenidos en función de los dominios.

Ilustración 6.

Estado actual de los dominios analizados.

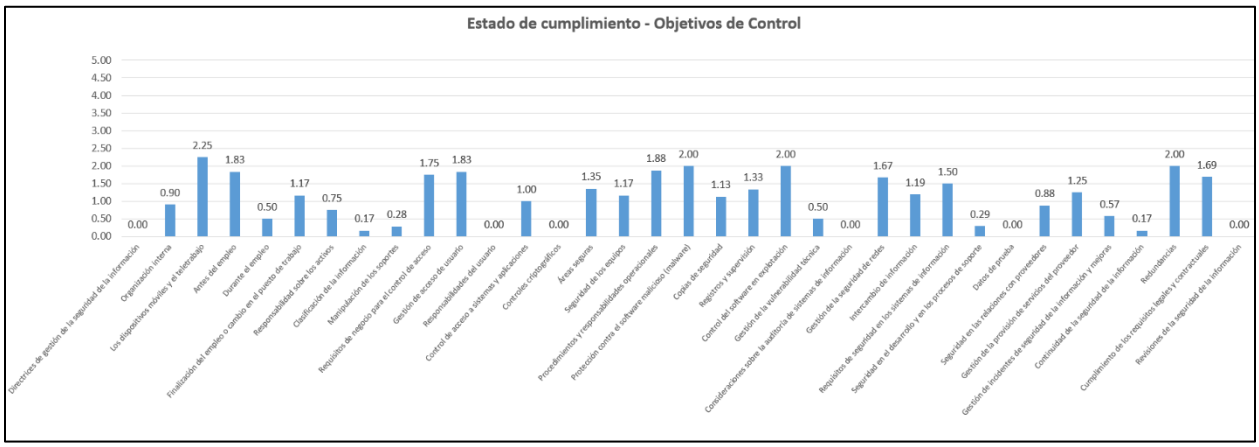


Nota. La ilustración muestra los niveles de cumplimiento iniciales de la empresa en los dominios estudiados por la norma ISO 27001.

De igual manera, la siguiente ilustración nos presenta un desglose de la situación actual en función de los objetivos de control analizados, los cuales también presentan valores bajos.

Ilustración 7.

Estado actual de objetivos de control.



Nota. Elaborado por el autor del documento, en colaboración con el jefe del departamento de sistemas y talento humano.

Una vez que se han obtenido estos resultados, el siguiente paso es realizar una comparación en función del Modelo de Madurez de la Capacidad de Ciberseguridad (CMM), el cual según se indica en la revista "seguridad360", define las 5 etapas de madurez basándose en una escala de valores de 1 al 5 detallada de la siguiente forma:

1. **Inicial**. En la cual no existen ni controles, ni políticas.
2. **Formativa**. Los controles o políticas son muy básicos o no se encuentran claramente detallados.
3. **Consolidada**. Los controles y las políticas se encuentran definidos e implementados.
4. **Estratégica**. Refleja la toma de decisiones de los indicadores considerados clave para la empresa y su evolución.
5. **Dinámica**. Existen políticas y procedimientos para alterar las estrategias a seguir dependiendo de las capacidades y los intereses de la empresa, la toma de decisiones y asignación de recursos son clave en esta etapa.

Toda esta información se encuentra detallada a profundidad en la publicación de Revista Seguridad360 (2022).

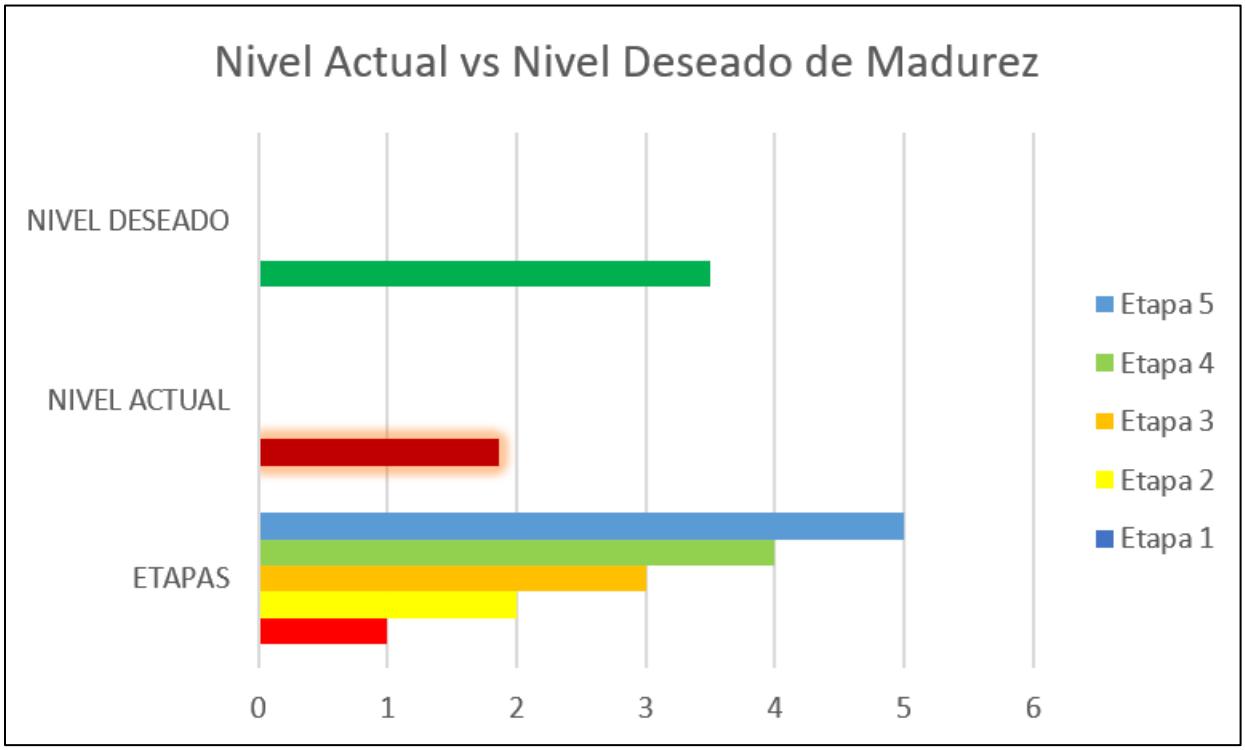
3.3.3 Escenario actual versus escenario deseado.

De acuerdo a esta escala de valores, podemos determinar que la empresa se encuentra en algún punto entre la etapa 1 y la etapa 2, ya que, en algunos aspectos no posee madurez de manera generalizada, existen otros en los cuales hay controles y procesos con un nivel de cumplimiento.

Así que, en la siguiente ilustración podemos determinar el nivel actual y compararlo en función del nivel ideal, recomendable y deseado.

Ilustración 8.

Comparativa entre el nivel actual y deseado de madurez.



Nota. Esta ilustración representa el nivel en el cual se encuentra la empresa, y también muestra el nivel deseado, que es el objetivo a alcanzar.

3.3.4 Inventario de activos de información.

Una vez determinado el estado actual de la empresa, el siguiente paso a realizar es el inventario de los activos de información de la empresa. Es importante tener claro el concepto de activo de información ya que es el objeto de estudio en esta fase del proyecto.

Se conoce como "Activo de información." A todo tipo de recurso (físico, software, personal, tangible, intangible, etc), que sea capaz de generar directa o indirectamente, información de valor para una empresa Techlib (2022).

La metodología empleada para la clasificación de los activos fue MAGERIT v3, ya que con ella se puede clasificar de una manera clara y simplificada los diferentes tipos de activos de tal manera que la información pueda tabularse ordenadamente dentro de una matriz.

Esta matriz debe contener toda la información necesaria sobre cada activo, y está estructurada de la siguiente manera:

Etiquetado A.I.: es un código que permite identificar cada activo de manera única, este código está compuesto por las letras "EM" al inicio, que indican la empresa a la cual pertenece dicho activo, en este caso la empresa es Diario El Mercurio Cia. Ltda. De lo cual se desprende (EM) para indicar la pertenencia a la misma.

A continuación, las siguientes dos letras "AI" hacen referencia a las siglas de "Activo de información (A.I.)", la tercera parte de la etiqueta para codificar, hace referencia al tipo de activo de información, como ya se indicó anteriormente la metodología MAGERIT V3, clasifica a los activos en diferentes tipos, siendo estos: Instalaciones (I), Equipos informáticos (E.I.). Redes de Comunicación (R.C.), Aplicaciones de Software (A.S.), Personal (P) y Servicios (S), para finalizar se le ha colocado un número secuencial para evitar duplicaciones en las etiquetas.

Es importante indicar que este procedimiento se lo realizó luego de ingresar toda la información en la tabla.

- **Nombre A.I**.: en esta columna se le coloca un nombre al activo que de igual manera debe ser único para evitar posibles redundancias en cada uno de los activos ingresados, dicho nombre debe identificar claramente al activo que hace referencia.
- **Descripción**: aquí se detalla información relevante que permita indicar de una manera más específica a qué hace referencia la columna "Nombre A.I.", no muy extenso, pero sí conciso.
- **Custodio**: hace referencia a la persona o área de la empresa que estarán a cargo de proteger dicho activo.
- **Propietario**: en esta sección se detalla quien es la persona o departamento en la empresa que posee o es dueño del activo en cuestión.
- **Responsable**: se detalla en esta columna la persona o departamento que administra y gestiona el A.I.
- **Tipo A.I.:** se indica en esta columna el tipo de activo al cual pertenece cada uno de los mismos, según la clasificación implementada en la metodología MAGERIT v3, la cual ya fue mencionada anteriormente.

- **Grado dependencia**: esta columna indica si dicho activo requiere de alguna manera de los otros activos que se encuentran enlistados, así por ejemplo se detallan valores porcentuales de 0% a 50%, los cuales indican que los activos requieren de otros para su funcionamiento pero de una manera parcial o leve, por otra parte los valores superiores al 50% nos indican que dichos activos requieren en gran medida de otros para poder cumplir con su función y tienen relación directa y frecuente entre los mismos.
- **Observaciones**: Aquí se detalla información técnica recopilada el momento en que se elaboró el proceso de inspección de cada uno de los activos y que de esta manera permita identificar de mejor manera a cada uno de los mismos, tales como condiciones de infraestructuras, versiones de sistemas operativos, de software, correos de contactos, etc.
- **Usuarios que tienen acceso al A.I.:** aquí se detallan los usuarios o roles que tienen acceso a cada uno de los activos, cabe mencionar que en algunos casos los usuarios pueden ser los mismos para diferentes activos
- **Permisos sobre el A.I.:** esta columna contiene la información sobre los permisos que tienen tanto roles como usuarios sobre cada uno de los activos analizados, las abreviaturas "LEC" para Lectura", "ES" para Escritura, "MOD" para Modificación y "EL" para Eliminación, se utilizaron como nomenclatura para indicar cada uno de los permisos.
- **Confidencialidad, Integridad, Disponibilidad**: para estos tres factores clave, que son considerados como los pilares de la ciberseguridad, se dispuso la clasificación mediante una tabla de valores de cada uno en una escala del 1 al 3, en la que, 1 representa el valor más bajo, es decir que las consecuencias que tienen dichas características sobre el activo analizado, es mínimo para el factor evaluado, el valor de 2 tiene consecuencias moderadas para el activo, y el valor de 3 es considerado el más alto, lo cual nos indica que las consecuencias son graves para el activo analizado en el escenario en el cual tanto la confidencialidad, la integridad y la disponibilidad se vean comprometidas para ese activo.
- **Total Valoración A.I**.: esta columna contiene el promedio de los valores asignados a los tres factores anteriores (confidencialidad, integridad y disponibilidad), este valor nos va a permitir posteriormente definir la importancia de cada uno de los mismos.
- **Clasificación A.I**.: según el tipo de información que maneja cada uno de los activos, se catalogaron como "confidencial", a aquellos activos que procesan o entregan información

de carácter reservado dentro de la empresa, a la cual tienen accesos solamente directivos y/o personal autorizado, otra categoría también es “uso interno” en la cual entran los activos que comparten información dentro de la empresa con otros activos y con diferentes departamentos de la misma.

- **Importancia A.I.:** la información de esta columna es la más importante dentro de la matriz, ya que gracias a ella podemos saber cuáles son los activos críticos de la empresa, es decir cuáles de entre todos los activos son vitales para mantener la continuidad del negocio, en otras palabras, nos permite catalogar a los activos que son imprescindibles dentro de la organización. Para poder realizar esta categorización se optó por analizar el valor promedio que obtuvimos en la columna “Total Valoración A.I.”, y se catalogó a los valores comprendidos entre 0 y 1 como “BAJO”, a los valores comprendidos entre 2 y 2,4 como “MEDIO”, y a los valores entre 2,5 y 3 se los consideró como “ALTO” en términos de importancia para la empresa. Esta información es medular para el siguiente paso en este estudio, ya que nos permite determinar la matriz de activos críticos y poder trabajar sobre ella para realizar el análisis de riesgos.

De esta manera, se procedió a llenar la matriz en Excel y se obtuvieron los siguientes resultados:

Tabla 2.

Total de activos de información analizados y que pertenecen a la empresa

TOTAL ACTIVOS:	**32**
TOTAL ACTIVOS (ALTO):	**13**
TOTAL ACTIVOS (MEDIO):	**10**
TOTAL ACTIVOS (BAJO):	**9**

Nota. Información recopilada y procesada por el autor del documento.

Todo el detalle de la información ingresada en la matriz durante esta fase del proceso fue realizado durante 4 semanas, iniciando el 20 de febrero de 2023, y se encuentra descrito en el **ANEXO 4** de este documento.

3.3.5 Selección de los activos críticos.

Luego de obtener la matriz de los activos, procedemos a determinar de entre todos ellos cuales son considerados activos críticos, este proceso es fundamental ya que únicamente aquellos considerados como tal, serán los que avancen hacia la siguiente etapa del proyecto, para esto se

toma como referencia el valor obtenido en la columna denominada "**Total Valoración A.I.**", dicha columna contiene el promedio de los valores obtenidos en las columnas "**Confidencialidad**", "**Integridad**" y "**Disponibilidad**" los cuales reflejan el comportamiento del activo en función de la tríada de la seguridad de la información, conceptos ampliamente tratados en la publicación de Luis Mendiola (2021).

El valor del promedio se clasificó utilizando la metodología MAGERIT de la siguiente manera: valores de 0 a 1.9 son considerados como importancia "**BAJO**", valores de 2 a 2.5 su importancia se etiquetó como "**MEDIO**", y valores de 2.6 a 3 son considerados como "**ALTO**", estos valores se encuentran en la columna denominada "**Importancia A.I**.".

Tomando como base que los activos críticos son todos aquellos considerados como importancia "**ALTO**", se obtuvo una tabla con 13 activos que cumplieron con las condiciones previamente establecidas y como podemos ver en la siguiente tabla, son de diferentes tipos.

Tabla 3.

Matriz de activos críticos.

ACTIVO	TIPO
Centro de Datos	Instalaciones
Servidor de aplicaciones	Equipos Informáticos
Servidor Web	Equipos Informáticos
Servidor de correo Institucional	Equipos Informáticos
Base de Datos Aplicaciones	Datos o Información
Base de Datos Suscriptores	Datos o Información
Firewall	Redes de Comunicación
Servidor para Pre Prensa	Equipos Informáticos
Equipo CTP (Copiado Directo a Plancha)	Equipos Informáticos
Sistema de gestión empresarial El Mercurio	Aplicaciones de Software
Agencia Centro	Instalaciones
Agencia El Vergel	Instalaciones
Agencia El Arenal	Instalaciones
Total Activos Críticos:	**13**
Activos tipo Instalaciones:	**4**
Activos tipo Equipos Informáticos:	**5**

Activos tipo Datos o Información:	**2**
Activos tipo Redes de Comunicación:	**1**
Activos tipo Aplicaciones de Software:	**1**

Nota. Elaboración por parte del autor del documento.

Una vez obtenida esta tabla, la siguiente etapa del proceso se centra sobre estos activos, al analizar los riesgos a los cuales se encuentran expuestos.

3.3.6 Evaluación de riesgos de los activos de información críticos.

Ya determinados los activos críticos, éstos van a ser evaluados en función de las amenazas y vulnerabilidades a las cuales están expuestos los activos analizados, con la finalidad de poder determinar la matriz de riesgo e impacto, en esta etapa vamos a emplear la metodología MAGERIT.

3.3.7 Activos considerados no críticos.

Del total de 32 activos levantados inicialmente, existe un total de 19 activos que no se encuentran dentro del rango necesario para considerarlos como críticos, la razón para ello radica en que son componentes de los cuales, si se presentaran fallas o desperfectos en los mismos son fácilmente sustituibles o reemplazables y por tanto no representa un problema para la continuidad en las operaciones de la empresa, de la misma manera, su detalle se encuentra incluido en el **ANEXO 4.**

3.3.8 Riesgos y Amenazas.

Partiendo del hecho que un riesgo es la exposición a una circunstancia adversa que debemos afrontar, en este caso enfocado a los activos de información de la empresa; es necesario para este caso de estudio, determinar el grado de exposición al cual están expuestos los activos analizados de tal manera que posteriormente se pueda elaborar un plan para su mitigación y de esta manera protegerlos de una manera más adecuada.

Los riesgos encontrados varían en función de las características de cada uno de los activos y a continuación se procede a enumerar los que han sido detectados:

Tabla 4.

Matriz de identificación de riesgos.

Causa	Riesgo o Amenaza
Desastres naturales y/o provocados	Terremotos, inundaciones, guerras, manifestaciones, pandemias,
Eventos externos a la empresa	Falla de proveedores de servicios (energía eléctrica, ISP, servicios básicos), falla de proveedores de suministros (materia prima, bobinas, tinta, planchas, etc.) ataques externos.
Eventos internos	Problemas técnicos en la infraestructura de la empresa, fallas en el proceso de producción, ataques internos, fallas de seguridad.
Acciones fortuitas y/o deliberadas	Errores humanos, fallos de hardware, fallos de software, fallos en los equipos de oficina, incendios,
Acciones humanas	Personal con problemas laborales pueden ocasionar accesos no autorizados, robo de información, fuga de datos.

Nota. Elaborado por el autor en reunión con la directiva, a fin de identificar los riesgos y amenazas de manera conjunta.

3.3.9 Matriz de probabilidad.

Según la metodología propuesta por MAGERIT, a continuación, se debe realizar la matriz que permita identificar la probabilidad que los riesgos puedan ocurrir, para ello se han detallado 5 niveles que son:

- **Improbable**: indica una probabilidad casi nula que un riesgo pueda ocurrir.
- **Posible**: indica que es muy poco probable que un determinado riesgo pueda ocurrir.
- **Ocasional**: indica que el riesgo puede materializarse en cualquier momento.
- **Probable**: un riesgo tiene una probabilidad alta que pueda ocurrir.
- **Frecuente**: el riesgo se presenta con una frecuencia muy alta.

3.3.10 Matriz de impacto.

De la misma manera que la anterior, esta matriz se encuentra elaborada en base a la misma metodología MAGERIT, y a diferencia de la anterior, ésta indica el impacto que representa para

la empresa si un riesgo llegara a materializarse, afectando directamente a la continuidad del negocio, y los niveles especificados son los siguientes:

- **Insignificante**: El impacto de la materialización de un riesgo no representa problema para la empresa.
- **Menor**: La ocurrencia de un riesgo representa un impacto mínimo para la empresa.
- **Moderado**: Un riesgo materializado representa un impacto momentáneo pero considerable para la empresa.
- **Mayor**: La materialización de un riesgo representa un impacto alto tanto en la cadena de producción de la empresa, lo cual se deriva en pérdidas económicas importantes.
- **Catastrófico**: Un riesgo identificado en este nivel, representa un impacto del nivel más alto en términos de continuidad del negocio, y la cadena de producción del mismo, dejándolo parcial o completamente paralizado, y de la misma manera produciendo la mayor pérdida posible para la empresa.

3.3.11 Riesgo inherente.

Este concepto hace referencia a todo riesgo que se encuentra intrínsecamente en los procesos y tareas, se encuentra presente cuando no se han tomado las medidas necesarias que permitan minimizar tanto la probabilidad como el impacto de los riesgos identificados, por tanto no puede ser eliminado, razón por la cual debe ser identificado correctamente por la empresa ya que puede provenir de factores externos (normativas o regulaciones a nivel gubernamental) como internos (políticas, estrategias corporativas, temas económicos, entre otros.).

La manera de identificarlos, consiste en reunir información actualizada tanto de la empresa, como de los controles internos, de tal manera que permita sistematizar y clasificar los riesgos para poder clasificarlos en función a las áreas, procesos y actividades sobre las cuales tienen influencia.

Es necesario darle un valor numérico para poder tabular los resultados para el conjunto de valores definidos tanto para la probabilidad como para el impacto, así pues, para la probabilidad tenemos la siguiente distribución:

Tabla 5.

Matriz de valores de probabilidad.

PROBABILIDAD	VALOR NUMÉRICO ASIGNADO
IMPROBABLE	1

POSIBLE	2
OCASIONAL	3
PROBABLE	4
FRECUENTE	5

Nota. La identificación de estos valores fue realizada por el autor, conjuntamente con la directiva para determinar el valor que se asignan a cada uno.

De la misma manera, procedemos a identificar los valores para el impacto, los cuales van a permitir posteriormente calcular el valor del riesgo inherente.

Tabla 6.

Matriz de valores de impacto.

IMPACTO	VALOR NUMÉRICO ASIGNADO
INSIGNIFICANTE	1
MENOR	2
MODERADO	3
MAYOR	4
CATASTRÓFICO	5

Nota. De igual manera se procedió a explicar a la directiva lo que representan cada uno de los valores, a fin de que sean conscientes de la asignación de los mismos.

La matriz para este caso de estudio es la siguiente y la información fue determinada en función a los parámetros considerados previamente y sus respectivos valores fueron proporcionados por la directiva, la cual determinó dichos valores en función de su criterio de acuerdo a la realidad de la empresa:

Tabla 7.

Matriz de riesgo inherente obtenida en función al riesgo y la probabilidad.

MATRIZ DE RIESGO INHERENTE		
RIESGO	**PROBABILIDAD**	**IMPACTO**
1. Desastres Naturales y/o provocados.	POSIBLE	CATASTRÓFICO
2. Eventos externos.	OCASIONAL	MAYOR
3. Eventos internos.	POSIBLE	MAYOR
4. Acciones fortuitas	OCASIONAL	MODERADO

5. Acciones humanas	POSIBLE	MAYOR

Nota. Los valores de esta tabla fueron proporcionados por la directiva en función a los que ellos consideran adecuados de las tablas presentadas anteriormente.

Es importante indicar que, los valores del riesgo inherente son el resultado de la multiplicación del valor de la probabilidad por el impacto, y quedan definidos de la siguiente manera:

Tabla 8.

Cálculo del riesgo inherente.

RIESGO INHERENTE	
Riesgo 1	2x5=10
Riesgo 2	3x4=12
Riesgo 3	2x4=8
Riesgo 4	3x3=9
Riesgo 5	2x4=8

Nota. Cálculos realizados por el autor del documento.

A partir de estos datos, se deriva la matriz comparativa que representa la relación entre probabilidad e impacto, quedando distribuida de la siguiente manera.

Tabla 9.

Relación "Probabilidad e Impacto".

		IMPACTO				
		INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**
PROBABILIDAD	**FRECUENTE**					
	PROBABLE					
	OCASIONAL			**9**	**12**	
	POSIBLE				**8 - 8**	**10**
	IMPROBABLE					

Nota. Elaborado por el autor del documento.

3.3.12 Mapa de calor.

Derivado de los riesgos inherentes se presenta a continuación la matriz de calor sobre la cual se analizan los riesgos y su ubicación dentro de la misma, a fin de comprender mejor cuáles son aquellos sobre los cuales se debe tomar mayor atención.

Tabla 10.

Mapa de calor derivado.

		IMPACTO				
		INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**
FRECUENCIA	**FRECUENTE**					
	PROBABLE					
	OCASIONAL			**Riesgo 4.**	**Riesgo 2.**	
	POSIBLE				**Riesgos 3. – 5.**	**Riesgo 1.**
	IMPROBABLE					

Nota. La tabla anterior permite revisar de manera visual por los tonos, la ubicación de los riesgos en función de su impacto y frecuencia, la elaboración del autor fue aprobada por la directiva.

3.3.13 Análisis de impacto al negocio. (B.I.A.)

A través de este proceso que es parte del análisis de riesgos, se identificó los procesos críticos del negocio y de esta manera poder determinar también los componentes físicos y tecnológicos que están involucrados dentro de esta fase de estudio, para así estimar los tiempos de recuperación y así garantizar un correcto desenvolvimiento del plan de continuidad del negocio.

La métrica empleada para la determinación de los valores de impacto para la empresa, está dada en función del tiempo, concretamente en el "tiempo de para en el proceso de producción" *(entiéndase como "tiempo de para" al período en el cual el departamento de producción se encuentra inactivo en horarios en los cuales esto no debería ocurrir*), ya que según ha mencionado la directiva, al ser un medio de comunicación, el producto que se ofrece a los suscriptores y al público en general, tiene que ser entregado oportunamente, lo cual implica que el proceso de producción no puede permitirse interrupciones prolongadas.

Es así que, en la siguiente tabla se detalla el impacto que tiene en el proceso de producción, cuando se presentan problemas sobre los activos que intervienen directamente en este ciclo y producen un estancamiento en las actividades comprendidas en dicho proceso.

Tabla 11.

Métricas de impacto por interrupción de procesos.

	Estimación del impacto en función del tiempo de para en el proceso de producción
Muy Alto:	Más de 180 minutos (Más de 3 horas)
Alto:	120 a 180 minutos (2 – 3 horas)
Medio:	60 a 120 minutos (1 – 2 horas)
Bajo:	0 a 30 minutos

Nota. Estos valores fueron proporcionados por la directiva.

3.3.14 Impacto económico.

Una vez definidos los rangos de tolerancia para los márgenes del proceso productivo, se procede a analizar los costos económicos que estos parones en la producción pueden representar a la empresa en términos monetarios, es necesario entonces conocer el costo de producción, para que, de esta manera podamos proyectar los costos en los diferentes rangos comprendidos en este estudio.

Se ha realizado un análisis previo a fin de obtener un promedio en el volumen de producción, tomando como muestra el volumen de los ejemplares producidos diariamente durante el mes de marzo del presente año, obteniendo los siguientes resultados.

Tabla 12.

Muestra de volumen de producción mensual.

DÍA	VOLUMEN DE PRODUCCIÓN (ejemplares)
LUNES	8.299
MARTES	7.991
MIÉRCOLES	8.010
JUEVES	7.987
VIERNES	7.959
SÁBADO	8.075
DOMINGO	8.007
TOTAL PRODUCCIÓN MARZO 2023	**56.328**

Nota. Esta información fue procesada y analizada por el autor conjuntamente con el jefe del área producción.

Acotación: el volumen diario de producción es un valor promediado de los días de cada mes, es decir se realizó la sumatoria de los valores producidos los 4 días lunes del mes, los 4 días martes y así sucesivamente, esto debido a que el volumen diario de producción no es un valor fijo, varía en base a factores como por ejemplo el número de suscriptores, y principalmente la cantidad de unidades solicitada por los distribuidores de periódicos, comúnmente conocidos en nuestro medio como canillitas, que son quienes deciden qué cantidad de productos solicitar a la empresa diariamente dependiendo de sus intereses.

Una vez obtenida esta información, se puede proseguir a identificar los costos de producción. Según conversación mantenida con los directivos del área correspondiente, supieron manifestar que, para efectos de este estudio es el costo de producción por unidad es de $0.557 ctvs, con lo cual podemos proyectar los valores económicos de potenciales pérdidas en función del tiempo de para de producción.

Si se realiza un análisis enfocado en el costo total en función a las unidades producidas mensualmente, tomando como referencia la información obtenida del proceso de producción para el mes de marzo, así pues, los costos son los siguientes;

- Número de unidades producidas (marzo 2023) = 56.328
- Costo unitario de producción = 0.557 USD

- Costo total de producción (marzo 2023) = 31.374,69 USD

Ahora, si a esta cifra se saca un promedio diario, (dividirlo para 30 días), nos representa un valor de $ 1.045,82 USD, este valor es importante ya que nos va a permitir averiguar el dato trascendental en este estudio, el cual es el valor por hora, con el cual podemos relacionar el rango de tolerancia definido anteriormente con un valor económico.

Entonces deducimos que, para una jornada de 8 horas diarias, el valor por hora equivalente es de $ 130.72 USD, una vez que obtenida esta información, el siguiente paso es trasladarlo a la tabla que contiene el rango de tolerancia y la cual nos refleja los siguientes valores económicos.

En reunión con la directiva se parametrizaron los rangos de acuerdo a sus indicaciones y se establecieron valores catalogados como: Muy Alto, Alto, Medio y Bajo, a los cuales se les asociaron valores económicos derivados del valor por hora, dato obtenido previamente, y la tabla resultante es presentada a continuación.

Tabla 13.

Impacto económico producido por interrupciones.

Estimación del impacto económico en función del tiempo de para en el proceso de producción	
Tiempo de paralización	**Valor económico**
Muy Alto (180 minutos o más):	$522,88 - +
Alto (120 a 180 minutos):	$ 261,44 - $392,16
Medio (60 a 120 minutos):	$130,72 - $ 261,44
Bajo (0 a 30 minutos):	$ 65,36

Nota. Estos valores fueron estimados conjuntamente con la gerencia financiera.

Se deduce entonces que, el margen de tolerancia mínimo para la empresa es de 0 a 30 minutos, en el cual le representa el valor más bajo de pérdida y por otro lado el valor más alto lo vemos a partir de las 4 horas de paralización, con una pérdida representativa muy alta, que en caso de escalar a la jornada completa, llegaría a cubrir el costo diario de producción en pérdidas, algo catastrófico para la empresa tanto en valor económico, como en imagen y reputación institucional, ya que representaría incumplimiento de contratos y obligaciones, lo cual puede acarrear pérdidas adicionales.

Los parámetros que se desprenden de esta etapa de análisis son sumamente importantes para el plan de continuidad del negocio, ya que nos brindan la información necesaria para actuar eficientemente en respuesta a incidentes. Estos parámetros son los siguientes:

Tiempo máximo de tolerancia en inactividad, es aquel valor que representa el período de tiempo máximo que puede estar inactivo un proceso en la empresa, antes de generar pérdidas, el valor es representado por la abreviatura **MTD**, y para este estudio el valor es un rango entre **0 a 30** minutos.

Tiempo objetivo de recuperación, hace referencia al período de tiempo transcurrido entre la interrupción de un proceso y su restablecimiento, su abreviatura es **RTO**, y el valor tolerable está en el rango de **30 a 60** minutos.

Punto objetivo de recuperación, comprende el tiempo que la empresa puede tolerar de pérdida de información, y en Diario El Mercurio, este rango está relacionado directamente con los procesos previos a la etapa de pre-prensa, es decir, comprende los procesos de redacción, diseño y diagramación, está definido por la abreviatura **RPO** y su valor está en el rango entre **0 – 120** minutos debido al desfase que existe entre la cadena de procesos enlazados.

Tiempo de recuperación de trabajo, comprende el período de tiempo que toma recuperar la información perdida e integrarla nuevamente en la cadena, su nomenclatura es **WRT** y el valor definido para la empresa es de **0 a 30** minutos ya que, si supera ese tiempo, es mejor repetir el proceso para generar otra vez la información.

3.3.15 Vulnerabilidades.

Para el análisis realizado en este punto, se tomó como base los datos obtenidos de la encuesta realizada al personal de T.I. dentro de la empresa, perteneciente al departamento de Sistemas, mediante la cual permitió conocer entre otros datos la manera en que está implementada la red, las versiones de software instaladas en los activos, tales como servidores, equipos de los diferentes departamentos, etc. con la finalidad de determinar las vulnerabilidades a las cuales se encuentran expuestos.

La persona en cargada del departamento es el Ing. Ricardo Maldonado, quien se encuentra a cargo del departamento desde el año 2022, la información fue entregada el día miércoles 22 de marzo de 2023, y en la tabla a continuación se muestran los resultados:

Tabla 14.

Encuesta a jefe de sistemas.

¿EXISTE UN MANUAL DE PROCESOS INTERNO EN EL DEPARTAMENTO?	**SI**	**NO**
¿EXISTE DISTRIBUCIÓN DE FUNCIONES EN EL DEPARTAMENTO?	**SI**	**NO**
¿SE ENTREGAN REPORTES DE ACTIVIDADES A LA DIRECTIVA?	**SI**	**NO**
¿EXISTE DOCUMENTACIÓN SOBRE LOS REQUERIMIENTOS REALIZADOS POR LOS OTROS DEPARTAMENTOS?	**SI**	**NO**
¿EXISTE UN INVENTARIO DE ACTIVOS DE INFORMACIÓN?	**SI**	**NO**
¿ESTÁ ACTUALIZADO? (SI EXISTE)	**SI**	**NO**
¿EXISTEN PROCESOS DE CONTROL DE ACCESO DE LOS USUARIOS?	**SI**	**NO**
¿ESTÁ DOCUMENTADO? (SI EXISTE)	**SI**	**NO**
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA DE RED?	**SI**	**NO**
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LOS EQUIPOS INFORMÁTICOS?	**SI**	**NO**
¿EXISTEN REVISIONES PERIÓDICAS SOBRE LAS VERSIONES DE LOS SISTEMAS IMPLEMENTADOS EN LOS DISTINTOS DEPARTAMENTOS DE LA EMPRESA?	**SI**	**NO**
¿SE REALIZAN COPIAS DE SEGURIDAD PERIÓDICAMENTE DE LA INFORMACIÓN CRÍTICA DEL NEGOCIO?	**SI**	**NO**
¿EXISTEN POLÍTICAS QUE DETALLEN LOS PROCESOS DE DESARROLLO DE APLICACIONES?	**SI**	**NO**
EL ACCESO EXTERNO (TERCEROS) TANTO A LA RED, COMO A LOS SISTEMAS DE LA EMPRESA, ¿ES MONITOREADO?	**SI**	**NO**
¿CONSIDERA QUE LA INFRAESTRUCTURA DE LA EMPRESA ESTÁ PREPARADA EN CASO DE QUE UN INCIDENTE DE CIBERSEGURIDAD OCURRA?	**SI**	**NO**
¿EXISTE ALGÚN PLAN DE CONTINGENCIA EN CASO DE QUE UN ATAQUE INFORMÁTICO LLEGUE A AFECTAR LA INFRAESTRUCTURA DE LA EMPRESA?	**SI**	**NO**
¿SE ENCUENTRAN LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA PREPARADOS PARA IMPLEMENTAR LOS REQUERIMIENTOS DETALLADOS EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES?	**SI**	**NO**

Nota. La encuesta y los resultados fueron elaborados por el autor del documento.

Del cuestionario de 17 preguntas, existe un total de 6 respuestas afirmativas y 11 negativas llegando a un total de 64%, lo cual indica que muchos controles o no existen o no están siendo útiles para la empresa, por tanto, es necesario enmendar estos parámetros.

La segunda parte de la encuesta no fue tabulada ya que estuvo basada en un cuestionario de preguntas, de las cuales el Ing. Maldonado proporcionó la siguiente información.

Número de servidores físicos (S.O. de los mismos y sus versiones.)

- "La empresa disponed de 5 servidores físicos
    - 4 Windows server2012
    - 1 Windows server2003"

Número de bases de datos (Gestores utilizados y sus versiones.)

- "Contamos con 2 Bases de datos
    - Oracle Database 12c Standard Edition Release 12.1.0.2.0 - 64bit Production"

El sistema de gestión de la empresa que se encuentra en http://192.168.200.150:7101, en qué lenguaje fue desarrollado.

- "El sistema de gestión fue desarrollado en oracle forms y oracle apex."

¿Qué empresa brinda los servicios de ISP?

- "Telefónica Movistar"

En caso de fallos por parte del proveedor ISP, ¿qué procesos se realizan para mitigar los problemas internos?

- "Se comunica a los usuarios del fallo y las afectaciones sobre los diferentes problemas,
- Sean de navegación, envíos de correo ó acceso al sistema quienes pueden o no acceder al mismo.
- Se informa sobre el tiempo estimado que indica el proveedor que estaremos sin el servicio.
- Se realiza el seguimiento correspondiente a las acciones realizadas por el proveedor para solucionar el inconveniente y estar en constante comunicación para realizar las debidas pruebas.
- Recomendación es tener un enlace de respaldo con otro proveedor, tomando en cuenta los costos que representaría para la empresa su implementación."

¿Dispone la empresa de un firewall? si la respuesta es SI, qué características tiene.

- "Si disponemos, el equipo es un **Mikrotik CCR1036-8G-2S**

- Características
    - Enrutamiento dinámico.
    - Punto de acceso.
    - Cortafuegos.
    - MPLS, VPN,
    - Calidad de servicio avanzada.
    - Balanceo de carga y enlaces.
    - Configuración y supervisión en tiempo real.
    - Administrado por RouterOS."

¿Existe documentación de los requerimientos de los usuarios?

- "Los requerimientos de los usuarios están registrados por medio de un correo electrónico de solicitud del cambio o requerimiento."

¿Hay algún control sobre los recursos que son dados de baja y la información que éstos contienen?

- "Los procesos que se realiza para dar de baja los equipos son dos el de proceso contable y el de sistemas.
- El proceso de contable se realiza durante los 5 años de amortización del equipo
- En cuanto al departamento de sistemas, se procede a realizar un respaldo de la información y su respectiva migración hacia los nuevos equipos, se le pide al usuario validar que esté completa su información, se mantiene el respaldo de esa información por un mes y se procede a borrar la información del dispositivo que se dio de baja."

Concluida la entrevista, se ha recopilado información suficiente para determinar las vulnerabilidades, las cuales siguiendo con la metodología MAGERIT, pasan a ser catalogadas en tres niveles: ALTO, MEDIO, BAJO en función de la relevancia que tiene su mitigación para que no afecte a la continuidad del negocio, la siguiente tabla muestra los valores de las vulnerabilidades detectadas.

Tabla 15.

Vulnerabilidades encontradas.

VULNERABILIDAD	CATEGORÍA
Inventario de activos de información (A.I.) desactualizado.	Medio

No existe control de acceso a usuarios.	Alto
Mantenimiento de infraestructura de red tercerizado.	Medio
No hay monitoreo de actividad de usuarios ni de terceros.	Alto
No se cuenta con plan de contingencia en caso de incidentes	Alto
Servidores con sistemas operativos desactualizados	Medio
No contar con servicio de ISP de contingencia	Alto
No existen reportes a gerencia, de incidentes o actividades	Medio
Equipos de usuarios con sistemas operativos y software antiguos	Medio
No existen políticas de responsabilidad de usuario	Alto
Posible fuga de información	Alto
No existe segmentación de red	Alto
No hay un correcto manejo de credenciales por parte del personal	Medio

Nota. Los valores asignados en la categoría, fueron analizados conjuntamente con el jefe del departamento de sistemas.

3.3.16 Plan de tratamiento de riesgos detectados.

Es necesario que el proceso se complemente con un plan adecuado que permita el correcto tratamiento de los riesgos a fin de mitigar el impacto que éstos producen, de tal manera que el riesgo residual se reduzca drásticamente.

Esta propuesta de plan, se encuentra fundamentada en los controles indicados por la ISO27001 en el Anexo A de la norma, que es sobre la cual se ha trabajado a lo largo de este proyecto, y por lo tanto el cumplimiento obligatorio de la misma va de la mano con los objetivos determinados inicialmente. Tomando las cláusulas analizadas en función a los resultados obtenidos en la matriz GAP de controles levantada previamente, definiendo claramente los responsables para garantizar el cumplimiento de los mismos, toda esta información se encuentra detallada en la tabla a continuación:

Tabla 16.

Controles a aplicarse.

CLÁUSULA	CONTROLES	RESPONSABLE
A.5.1.1	Establecer políticas para S.I. que regirán en la empresa.	Gerente General.
A.5.1.2	Revisar las políticas establecidas	Gerente General.

A.6.1.3	Establecer reglas de gestión de roles, tareas, comunicación con la directiva	Jefe Talento Humano.
A.7.2.2	Realizar programas de capacitación tanto a personal como contratistas sobre las políticas de S.I. implementadas por la empresa.	Jefe Talento Humano.
A.7.2.3	Socializar con el personal y contratistas los procesos disciplinarios establecidos por la empresa, con la finalidad que todos los conozcan perfectamente.	Gerente General.
A.8.1.1	Actualizar el inventario de A.I. periódicamente o cada vez que se realiza la adquisición de un nuevo activo.	Jefe Sistemas.
A.8.1.2	Documentar los propietarios de cada activo que conste en el inventario.	Gerente Financiero.
A.8.1.3	Establecer las reglas de uso para cada uno de los activos, de tal manera que se garantice que los usuarios no den un mal uso a los recursos disponibles en cada activo.	Gerente Financiero.
A.9.2	Definir un esquema de control de acceso a cada recurso por parte del personal, en el cual se incluya los permisos que tiene cada uno a los diferentes recursos con los cuales desarrollan sus actividades.	Jefe Sistemas.
A.9.3	Establecer una regla para la que los usuarios gestionen correctamente sus credenciales de acceso a los sistemas	Jefe Sistemas.
A.10.1	Definir un algoritmo de encriptación de datos que sea robusto, así como la custodia de las llaves públicas y privadas generadas para su uso.	Jefe Sistemas.
A.11.2.8	Establecer responsabilidades al personal, sobre la correcta protección de sus equipos al ausentarse o dejarlos desatendidos.	Jefe Talento Humano.
A.11.2.9	Adoptar políticas de escritorios y pantallas limpias y socializar su importancia con todo el personal.	Jefe Talento Humano.
A.12.4	Realizar un control y monitoreo sobre los logs de eventos generados por los sistemas de la empresa con la finalidad de establecer responsabilidades en caso de incidentes y poder entregar reportes a la directiva.	Jefe Sistemas.
A.12.6	Documentar las vulnerabilidades presentadas a partir de los incidentes suscitados, para tener una bitácora y poder a partir de estos datos, ejecutar acciones de mitigación.	Jefe Sistemas.
A.12.7	Definir un calendario para la ejecución de las auditorías, preferentemente fuera de horarios laborales a fin de evitar retrasos en la cadena de producción.	Jefe Sistemas.
A.13.1.3	Planificar y ejecutar un proceso de segregación de redes ya que es muy riesgoso que toda la infraestructura esté expuesta en una sola red global	Jefe Sistemas.

A.14.2	Definir una política que garantice el desarrollo seguro de aplicaciones ya sean elaboradas internamente o tercerizadas, acompañado de cláusulas en los contratos de adquisición que garanticen el cumplimiento de la gestión de S.I. en su desarrollo.	Jefe Sistemas.
A.16.1.1	Dentro de las políticas de S.I. definidas por la empresa, es necesario detallar el control de los incidentes, definiendo claramente, responsabilidades y acciones realizadas luego de ocurrido un incidente.	Gerente General.
A.17.1.2	Establecer los procedimientos necesarios para garantizar la continuidad de los procesos en caso de presentarse un incidente de seguridad para posteriormente poder evaluarlos mediante simulaciones y verificar su utilidad.	Jefe Sistemas.
A.18.2	Realizar una verificación del cumplimiento de las políticas de S.I. establecidas por la empresa	Gerente General.

Nota. La información contenida en la tabla anterior, fue previamente indicada a la directiva y los departamentos involucrados, así como a todos los actores involucrados.

3.3.17 Marco metodológico seleccionado para aplicar la mitigación.

Fue necesario en este punto hacer uso de un marco de trabajo en el cual se pueda fundamentar el estudio y así, completar este análisis, y se ha optado por la utilización de la plataforma **MITRE ATT&CK®** ya que, al estar ampliamente difundida, es la herramienta idónea para poder determinar las el tratamiento de las vulnerabilidades detectadas en esta fase del estudio.

Dentro de esta podemos encontrar de manera categorizada las vulnerabilidades y los controles de mitigación propuestos en la plataforma, para ser considerados como opciones al momento de elaborar el plan de tratamiento de riesgos, conjuntamente con los controles propuestos por la ISO27001 ya que la norma establece qué debe hacerse, pero deja libertad de escoger cómo realizar las tareas, razón por la cual es necesaria la elección de un marco de trabajo adecuado.

Las propuestas de mitigación para las vulnerabilidades detectadas que se encuentran categorizadas en la plataforma, son detalladas a continuación:

Control de acceso a usuarios: codificado como M1036 propone soluciones para distintos escenarios, tales como: ataques de fuerza bruta, adivinación de contraseñas, pulverización de contraseñas, rellenado de contraseñas, solicitudes de generación de doble factor de autenticación,

validación de cuentas locales y en nube, etc. La información detallada de estas soluciones se encuentra en:

Account Use Policies, Mitigation M1036 – (Enterprise | MITRE ATT&CK®, s. f.)

Fuga de datos: codificado como M1057 menciona alternativas de solución para múltiples ocurrencias entre ellas: datos de equipos, datos de dispositivos extraíbles, exfiltración a través de protocolos, exfiltración a través de medios físicos, exfiltración a través de servicios web, etc. El detalle de todas estas propuestas se encuentra publicado en:

Data Loss Prevention, Mitigation M1057 – (Enterprise | MITRE ATT&CK®, s. f.)

Segmentación de redes: catalogado con el código M1030 comprende propuestas para solucionar problemas relacionados con la estructura de redes, entre los que se menciona, manipulación de cuentas, ataques tipo MiTM, acceso a datos de configuración en repositorios, limitación de dominios, servicios remotos, configuración de puertos, apropiación de sesiones, credenciales inseguras, etc. una gran cantidad de información detallada se encuentra en:

Network Segmentation, Mitigation M1030 – (Enterprise | MITRE ATT&CK®, s. f.)

Equipos de usuarios con sistemas operativos y software desactualizado: codificado como M1051 comprende las posibles indicaciones a tomar en cuenta para evitar la explotación de equipos por software obsoleto, entre los múltiples factores como: escalamiento de privilegios, extensiones de navegador, repositorios de contraseñas, explotación de credenciales de acceso, explotación de servicios remotos, firmare corrompido, apropiación de flujos de ejecución, parches de arranque, preferencias en políticas de grupos, etc. El detalle completo de esta información se encuentra en:

Update Software, Mitigation M1051 – (Enterprise | MITRE ATT&CK®, s. f.-b)

No hay monitoreo de actividad de usuarios ni de terceros: se encuentra codificado como M1047 y menciona alternativas de soluciones a múltiples situaciones comprendidas dentro de este dominio, entre las cuales se mencionan: mecanismos de control para escalamiento de privilegios, creación o modificación de procesos de sistema, permisos sobre repositorios de datos, carpetas compartidas, monitoreo de correos, permisos de acceso a logs, modificación de proceso de autenticación, permisos sobre la infraestructura de nube, etc. para más detalles revisar la información completa en:

Audit, Mitigation M1047 – (Enterprise | MITRE ATT&CK®, s. f.)

No hay un correcto manejo de credenciales: el código correspondiente a este apartado es M1043 y detalla posibles soluciones para problemas tales como: ejecución de auto registro en el arranque de equipos, modificar la imagen del sistema, limitar puenteo de red, volcado de credenciales, etc. el detalle completo se encuentra en:

Credential Access Protection, Mitigation M1043 – (Enterprise | MITRE ATT&CK®, s. f.)

Vulnerabilidades no descritas en MITRE ATT&CK®; de la matriz de vulnerabilidades descrita anteriormente, existen algunas que no se encuentran definidas dentro del marco de trabajo que propone MITRE, es por ello que estas serán evaluadas directamente bajo los controles propuestos por la ISO27001, ya que no implican procesos técnicos para su cumplimiento.

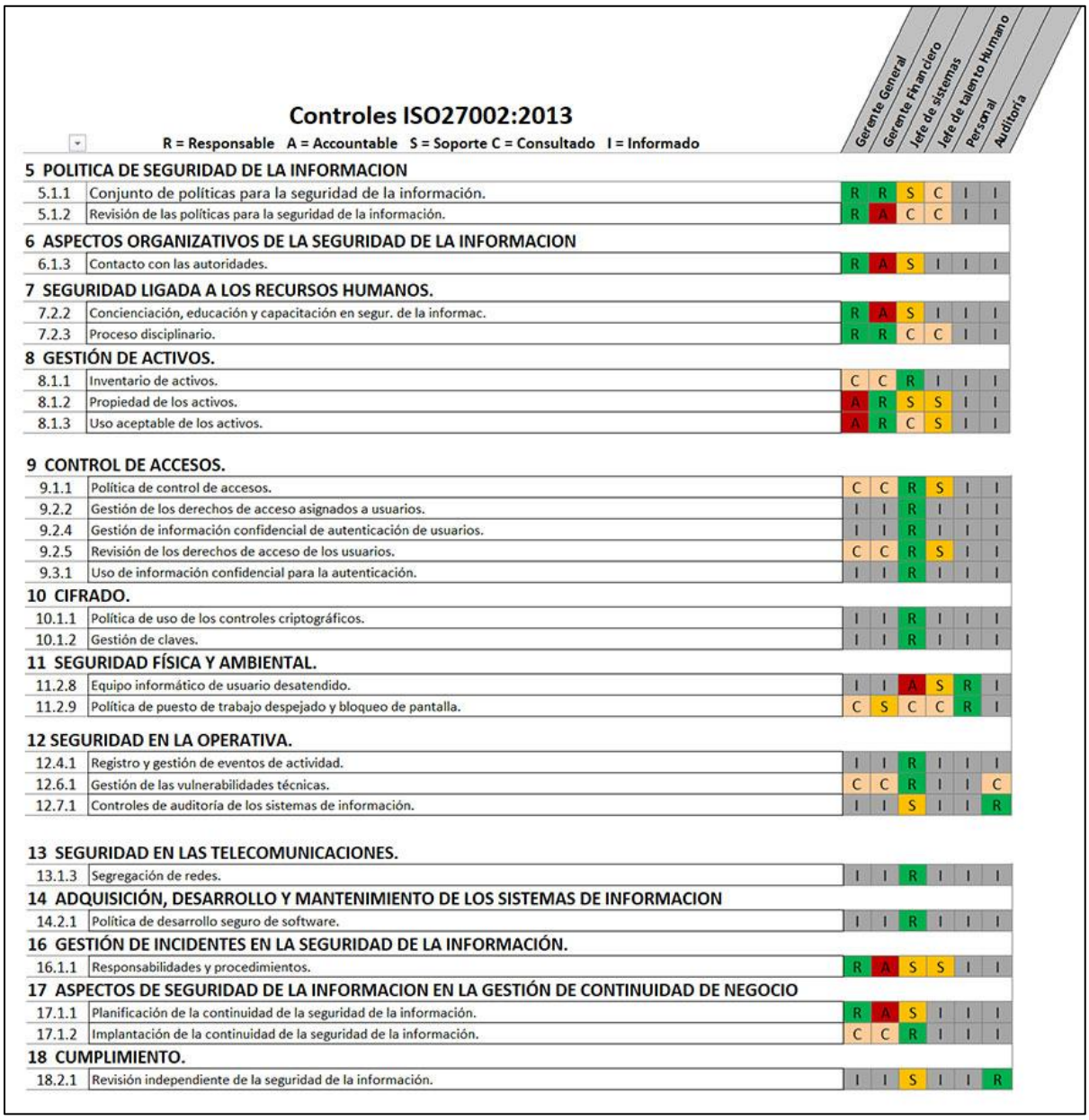
3.3.18 Matriz RASCI.

En este apartado se indica la información correspondiente a los actores comprendidos en el proceso de la gestión de los riesgos, entre ellos constan: el responsable, el aprobante, el soporte, el consultado y el informado, así también el personal involucrado en el proceso es: el gerente general, el gerente financiero, el jefe de sistemas, el jefe de talento humano, personal y auditoría, todos los valores aplicados a ellos están en función de sus roles correspondientes en los controles analizados.

La siguiente ilustración muestra la matriz en función de los controles aplicados, así como la interacción que tienen los participantes en el proceso.

Ilustración 9.

Matriz RASCI sobre los controles.



Controles ISO27002:2013

R = Responsable A = Accountable S = Soporte C = Consultado I = Informado

		Gerente General	Gerente Financiero	Jefe de sistemas	Jefe de talento Humano	Personal	Auditoría
5 POLITICA DE SEGURIDAD DE LA INFORMACION							
5.1.1	Conjunto de políticas para la seguridad de la información.	R	R	S	C	I	I
5.1.2	Revisión de las políticas para la seguridad de la información.	R	A	C	C	I	I
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION							
6.1.3	Contacto con las autoridades.	R	A	S	I	I	I
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.							
7.2.2	Concienciación, educación y capacitación en segur. de la informac.	R	A	S	I	I	I
7.2.3	Proceso disciplinario.	R	R	C	C	I	I
8 GESTIÓN DE ACTIVOS.							
8.1.1	Inventario de activos.	C	C	R	I	I	I
8.1.2	Propiedad de los activos.	A	R	S	S	I	I
8.1.3	Uso aceptable de los activos.	A	R	C	S	I	I
9 CONTROL DE ACCESOS.							
9.1.1	Política de control de accesos.	C	C	R	S	I	I
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	I	I	R	I	I	I
9.2.4	Gestión de información confidencial de autenticación de usuarios.	I	I	R	I	I	I
9.2.5	Revisión de los derechos de acceso de los usuarios.	C	C	R	S	I	I
9.3.1	Uso de información confidencial para la autenticación.	I	I	R	I	I	I
10 CIFRADO.							
10.1.1	Política de uso de los controles criptográficos.	I	I	R	I	I	I
10.1.2	Gestión de claves.	I	I	R	I	I	I
11 SEGURIDAD FÍSICA Y AMBIENTAL.							
11.2.8	Equipo informático de usuario desatendido.	I	I	A	S	R	I
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	C	S	C	C	R	I
12 SEGURIDAD EN LA OPERATIVA.							
12.4.1	Registro y gestión de eventos de actividad.	I	I	R	I	I	I
12.6.1	Gestión de las vulnerabilidades técnicas.	C	C	R	I	I	C
12.7.1	Controles de auditoría de los sistemas de información.	I	I	S	I	I	R
13 SEGURIDAD EN LAS TELECOMUNICACIONES.							
13.1.3	Segregación de redes.	I	I	R	I	I	I
14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION							
14.2.1	Política de desarrollo seguro de software.	I	I	R	I	I	I
16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.							
16.1.1	Responsabilidades y procedimientos.	R	A	S	S	I	I
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO							
17.1.1	Planificación de la continuidad de la seguridad de la información.	R	A	S	I	I	I
17.1.2	Implantación de la continuidad de la seguridad de la información.	C	C	R	I	I	I
18 CUMPLIMIENTO.							
18.2.1	Revisión independiente de la seguridad de la información.	I	I	S	I	I	R

Nota. Los actores comprendidos en la ilustración previamente mostrada, han sido informados respectivamente de sus roles y responsabilidades.

3.3.19 Tiempos estipulados.

En caso de la directiva apruebe la ejecución del plan propuesto, se debería tomar en cuenta las siguientes consideraciones:

En materia de actualización de equipos, cambio de la arquitectura de red para adoptar la segregación, el tiempo estipulado entre la solicitud, aprobación, implementación de cambios, y pruebas, no debería superar los **tres meses** en total.

En lo relacionado a la implementación de las políticas de seguridad de la información, sí es necesario que, entre la propuesta de las mismas, la aprobación por parte de la directiva, la socialización, la puesta en marcha, exista un período de al menos **seis meses**, luego de lo cual se pueda realizar una primera evaluación, de tal manera que permita contribuir al proceso de mejora continua de la empresa.

3.3.20 Riesgo residual proyectado.

Es aquel que persiste a pesar de haber elaborado un plan de mitigación de riesgos, sin lugar a dudas los valores presentes en el mismo deben reflejar una disminución muy significativa o casi total en comparación a los identificados inicialmente en la matriz de riesgos.

Cabe recalcar que, como este proyecto comprende únicamente la fase inicial del proceso para la implementación de un sistema de gestión de la seguridad en la empresa, no se tiene previsto que esta ocurra ni está contemplada dentro de este caso de estudio, al ser esa una decisión que depende completamente de la directiva de la empresa; por lo tanto los valores a continuación presentados son proyecciones o estimaciones realizadas en el supuesto caso de que los controles detallados se implementen en la organización.

Para calcular el valor del riesgo residual se procede a realizar la multiplicación de los valores de la probabilidad por el impacto, tal y como se realizó inicialmente para obtener los valores de los riesgos identificados en un principio, con la variante que el peso inherente ha sido reducido tras la aplicación de los controles propuestos en un 25% de su valor original, por tanto, la matriz a continuación presenta los valores actualizados.

Tabla 17.

Cálculo del riesgo residual proyectado.

RIESGO RESIDUAL (PROYECTADO)	
Riesgo 1	1.75x3.75=6.56
Riesgo 2	2.25x3=6.75
Riesgo 3	1.75x3=5.25
Riesgo 4	2.25x2.25=5.06

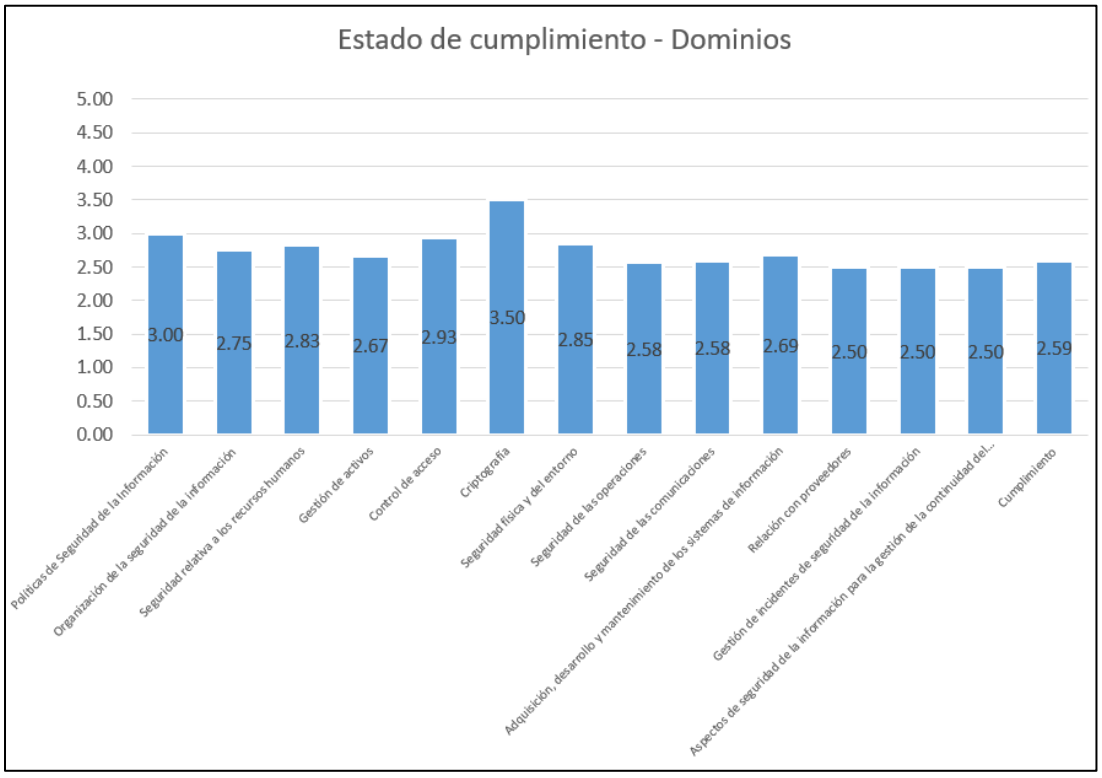
Riesgo 5	1.75x3=5.25

Nota. Las proyecciones fueron realizadas teniendo en cuenta que todas las correcciones y sugerencias han sido debidamente realizadas.

De la misma manera se puede obtener los diagramas de cumplimiento actualizados con la proyección de los nuevos valores luego de cumplir los controles propuestos en el plan de mitigación, los mismos son expuestos en las dos ilustraciones presentadas a continuación.

Ilustración 10.

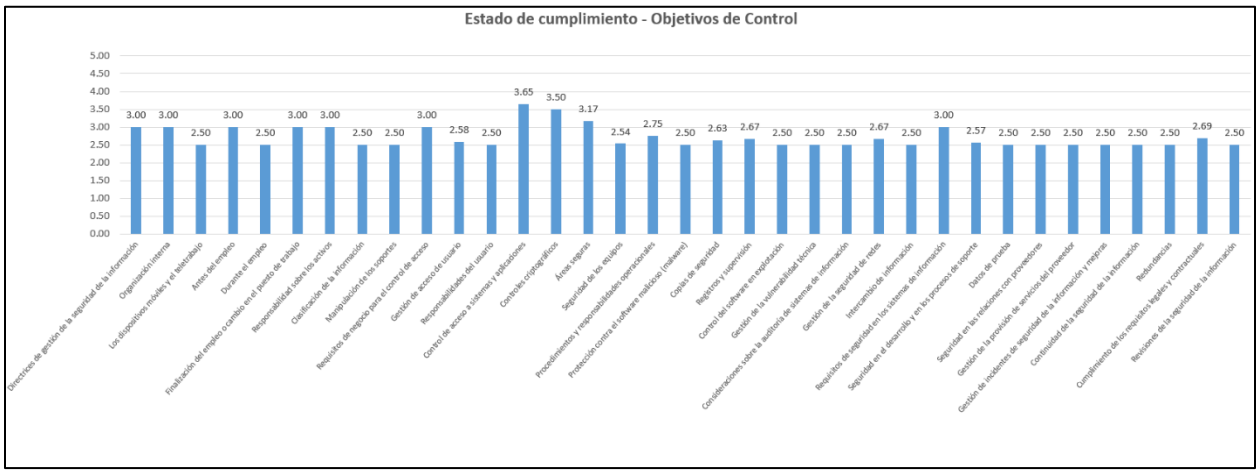
Cumplimiento de dominios luego de aplicar los controles.



Nota. Los valores de los dominios evidencian un incremento notable si las correcciones son realizadas.

Ilustración 11.

Proyección de valores actualizados de los controles.



Nota. Los controles permiten que los dominios se ajusten al nivel de madurez deseado.

Se puede identificar que los nuevos valores se acercan considerablemente al objetivo del nivel deseado de madurez, que se encuentra expuesto en la ilustración 7, el cual refleja un crecimiento a través de la implementación de los controles previstos dentro del plan de mitigación, al ser esta una proyección, los valores expuestos son estimaciones que dependen de la aprobación de la directiva de la empresa para ser ejecutados.

3.3.21 Informe Ejecutivo y Técnico.

Una vez concluido el proyecto, es imprescindible que el último paso sea la elaboración de los informes para la directiva, para ello se procedió a realizar dos documentos, el primero denominado Informe Ejecutivo, que contiene los resultados del estudio, así como los indicadores de manera resumida y de fácil comprensión, de tal manera que, conjuntamente con las conclusiones y recomendaciones, la información permita ayudar a la directiva en el proceso de la toma de decisiones que consideren prioritarias en atender.

El segundo documento, denominado Informe Técnico, está dirigido al personal del departamento de sistemas, ya que contiene información detallada sobre los procesos realizados con su respectiva explicación técnica y los resultados de todos los estudios realizados, proporcionando las métricas resultantes, de tal manera que, sean capaces de ejecutar las acciones recomendadas, de una manera completa y detallada, a fin de dar cumplimiento con las recomendaciones mencionadas.

Estos documentos se elaboraron una vez finalizado todo el proceso, se entregaron a la directiva el día 6 de julio de 2023 y se hizo constancia del debido trámite en el **ANEXO 5** adjunto en el cual se presentan las evidencias respectivas.

Conclusiones.

Luego de terminar el presente trabajo, hay varias conclusiones que se han obtenido a lo largo de todo el proceso realizado, cada etapa ha contemplado diferentes aspectos de estudio y con ellos también se han obtenido diferentes resultados que permiten evaluar todo el proyecto de investigación, se procede a enumerar las conclusiones más importantes:

- **Primera.**

  El nivel de madurez de la empresa se encuentra por debajo de lo deseado en términos de seguridad de la información, hace falta mucho trabajo para colocar a la empresa en niveles apropiados que permitan ofrecer parámetros mínimos para garantizar un adecuado manejo en temas de S.I.

- **Segunda.**

  La infraestructura de la compañía se encuentra vulnerable a ataques e incidentes ya que presenta equipos y sistemas obsoletos en gran medida, lo cual puede resultar un problema muy grande que requiere tomar en cuenta a la directiva.

- **Tercera.**

  No existen políticas de control en múltiples aspectos para los diferentes departamentos de la compañía, esto sumado al desconocimiento por gran parte del personal en temas de seguridad de la información, representan un reto muy grande para la gerencia de la empresa, ya que sin ellas no se puede llevar un orden apropiado en la administración de la misma.

- **Cuarta.**

  Es necesario realizar una inversión que permita mejorar los niveles de seguridad en la infraestructura de la empresa, aunque esto implique realizar un estudio económico preliminar para determinar un orden de prioridades con lo cual es impacto económico no sea muy significativo para la empresa.

Recomendaciones.

En base a las conclusiones obtenidas, se procede a realizar las recomendaciones pertinentes a fin de reducir el déficit encontrado tanto en temas de seguridad como de administración de la compañía, por tanto, las recomendaciones a tener en cuenta son las siguientes:

La directiva debe elaborar, aprobar y revisar a detalle un **"plan de gestión de seguridad de la información"** para Diario El Mercurio, el mismo que debe contener:

- ✓ Las políticas internas de la empresa.
- ✓ Designar un oficial de seguridad de la información.
- ✓ Establecer plan de respuesta a incidentes.
- ✓ Agendar un ciclo de simulación y pruebas de ataques en un ambiente controlado.
- ✓ Establecer un cronograma para revisión de cumplimiento, a través de auditorías.

Es recomendable para la empresa que la directiva analice la posibilidad **de implementar servicios de computación en la nube**, lo cual es una opción muy importante a tomar en cuenta ya que permite garantizar la disponibilidad de servicios en caso de incidentes y el aseguramiento de respaldos de los datos sensible.

Para disponer de estos servicios es necesario que el personal del departamento de sistemas, posea una certificación de las empresas que proveen estos servicios de tal forma que aseguren una correcta operación dentro de las plataformas, los costos varían en función de la cantidad de recursos que se desee migrar a este tipo de infraestructura, con la ventaja que sólo se paga por los recursos utilizados y su tiempo de uso, entre las plataformas más importantes que ofrecen este servicio podemos mencionar:

- ✓ Amazon Web Services (AWS).
- ✓ Oracle Cloud Computing.
- ✓ Microsoft Azure.
- ✓ IBM.
- ✓ Google, entre otros.

Se recomienda también a la directiva de la empresa, el considerar realizar una **inversión en actualización de equipos y sistemas** sobre todo en las áreas más críticas del negocio, principalmente producción, para reducir las brechas de seguridad significativamente, una inversión que comprenda, modernización de equipos, actualización de software y sus respectivas licencias,

capacitación, protección de activos, representaría un valor aproximado de $10.000 que, comparando con los costos de pérdidas potenciales resultantes de ataques informáticos, quedaría justificada por sobremanera dicha inversión.

Otra recomendación importante dirigida tanto a la directiva, como a talento humano y sistemas, es **agendar programas internos de capacitación** en los diferentes temas que abarca la de seguridad de la información, ya que en el estudio preliminar realizado para medir el nivel de conocimiento en general del personal, quedó en evidencia un déficit significativo que se tiene en esta área, es necesario tener en cuenta que, por más medidas de protección que una empresa pueda implementar y su respectiva inversión en términos económicos, siempre el factor humano debe considerarse como el eslabón más débil en una empresa.

Cabe mencionar que, todos estos puntos aquí indicados son necesarios cumplir de manera obligatoria si la empresa a futuro busca conseguir la certificación en la familia de normativas ISO 27000, por tanto, el resultado de este estudio, queda a disposición de la directiva

Bibliografía.

Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1036/

Audit, Mitigation M1047 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1047/

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198). https://doi.org/10.5354/0719-3769.2021.57067

Arévalo, F. M., Cedillo, I. P., & Moscoso, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management. Revista Killkana Técnica, 1(2), 31–42.

Calder, A. (2017). ISO27001/ISO27002: Una guía de bolsillo. En ISO27001/ISO27002: Una guía de bolsillo. IT Governance Publishing. https://search.proquest.com/docview/2133079960?accountid=34925

CIS® (Center for Internet Security). (2021). CIS Controls Spanish Translation. CIS Controls Spanish Translation V7. https://www.cisecurity.org,

Credential Access Protection, Mitigation M1043 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1043/

Data Loss Prevention, Mitigation M1057 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1057/

Díaz, V. (2021). Banco Pichincha confirma “incidente de ciberseguridad” en sus sistemas - El Comercio. https://www.elcomercio.com/actualidad/negocios/banco-pichincha-ciberseguridad-ciberataque-hackeo.html

GOOGLE. INC. (2023). Cumplimiento de NIST 800-53 | Google Cloud. Cumplimiento de NIST 800-53. https://cloud.google.com/security/compliance/nist800-53?hl=es

INTECO. (2017). Guia_apoyo_SGSI. Implantación de un SGSI en la empresa .

ISOTools Excellence. (2021). ¿Qué es la seguridad de la información y cuantos tipos hay? Blog especializado en Seguridad de la Información y Ciberseguridad. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Kaspersky Labs. (2022). ¿Qué es la ciberseguridad? Centro de Recursos - Definiciones. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lavandeira Lema, E. (2022, agosto 1). El eslabón más débil de la seguridad informática. Revista SoyCiber. https://soycyber.com/eslabon-mas-debil-seguridad-informatica/

Luis Mendiola. (2021, octubre 21). Los tres pilares de la Ciberseguridad. Instituto Artek. https://artek.edu.mx/noticia_eventos/los-tres-pilares-de-la-ciberseguridad/

Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, Dirección de Estándares y Arquitectura de Tecnologías de la Información, & Subdirección de Seguridad y Privacidad de TI. (2023). Guía para realizar el Análisis de Impacto de Negocios BIA. Guía para realizar el Análisis de Impacto de Negocios BIA.

Moran Maldonando, N. M. (2021). Estado de la ciberseguridad en las empresas del sector público del Ecuador: una revisión sistemática. Universidad Politécnica Salesiana, Guayaquil, Ecuador, 1–17. https://n9.cl/gwnhsb

Network Segmentation, Mitigation M1030 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1030/

Norden Estudio. (2018). ¿Cuáles son los principales métodos de impresión? Norden Estudio Blog. https://www.nordenestudio.es/2018/07/19/cuales-son-los-principales-metodos-de-impresion/

Novoa, H. A., & Barrera, C. R. (2019). Metodologías Para el análisis de riesgos en los sgsi Methodologies for AnAlysis of risks in the isMs.

Pastor Javier. (2022). El primer día del internet del futuro en Europa: cómo la DSA y la DMA afectarán a las Big Tech (y a nosotros). https://www.xataka.com/empresas-y-economia/primer-dia-internet-futuro-europa-como-dsa-dma-afectaran-a-big-tech-a-nosotros

Revista Seguridad360. (2022). El Modelo de Madurez de la Capacidad de Ciberseguridad. Revista Seguridad360. https://revistaseguridad360.com/noticias/capacidad-de-ciberseguridad/

Salcedo, J. S. (2021). ¿Qué revela el ataque informático a la CNT sobre la seguridad de datos en Ecuador? - Canal News Ecuador. https://canalnewsecuador.com/2021/09/21/que-revela-el-ataque-informatico-a-la-cnt-sobre-la-seguridad-de-datos-en-ecuador/

Secretaría General de Administración Digital, General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. http://administracionelectronica.gob.es/

Techlib. (2022). Activo de información - Definición y explicación. Techlib.net. https://techlib.net/techedu/activo-de-informacion/

Update Software, Mitigation M1051 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/mitigations/M1051/

Vega Briceño, E. (2021). Seguridad de la información. En Seguridad de la información. Editorial Científica 3Ciencias. https://doi.org/10.17993/tics.2021.4

VMware INC. (2023). Definición de MITRE ATT&CK. Glosario de VMware. https://www.vmware.com/es/topics/glossary/content/mitre-attack.html

Wright, T. (2021). Análisis GAP: Qué es y cómo realizarlo + plantillas gratuitas. Cascade Inc. https://www.cascade.app/es/blog/gap-analysis

Zamora Merchán, D. M. (2005). ¿Quiénes somos? Diario El Mercurio, 1–10.

Anexos.

Anexo 1.

Solicitud de autorización a gerencia y aprobación del proyecto.

Cuenca, 18 de enero de 2023

Ing. Xavier Merchán Vintimilla
GERENTE FINANCIERO DE
DIARIO EL MERCURIO CIA. LTDA.

Su despacho.-

De mis consideraciones:

Por medio de la presente, me dirijo a usted de la manera más respetuosa, con la finalidad de solicitarle su autorización para poder realizar el proyecto de graduación de la maestría que me encuentro cursando denominado: *"Fase inicial para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)",* tomando como caso de estudio a "Diario El Mercurio Cia. Ltda.", el objetivo que me motiva a realizar dicha solicitud radica en el hecho que, actualmente la empresa no cuenta con un plan de esta índole, motivo por el cual he visto la oportunidad de poder realizar un trabajo de investigación que entregue un aporte de valor para la compañía en la cual me encuentro laborando durante todos estos años, es por ello que solicito su autorización para poder desarrollar todas las actividades comprendidas en esta investigación y tener acceso tanto a la información, como a la infraestructura necesaria para completar el mismo, comprometiéndome a manejar con estricta reserva la información que sea requerida durante el desarrollo de este proceso.

Por una favorable acogida a esta solicitud, anticipo mis más sinceros agradecimientos, y deseándole éxitos en sus funciones, suscribo de usted.

Atentamente,

ESTEBAN CASTILLO

Esteban Fernando Castillo Durán.
Departamento de Computación.

EL MERCURIO
DIARIO INDEPENDIENTE DEL AUSTRO

Cuenca 19 de enero de 2023

Ingeniero
Esteban Castillo Durán
Ciudad. –

De mis consideraciones:

Con un atento saludo me dirijo a usted para informarle que ha sido aceptada su solicitud para realizar su proyecto de graduación de la maestría que se encuentra cursando denominado: "Fase inicial para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)" tomando como caso de estudio a "Diario El Mercurio Cía. Ltda."

Cabe resaltar que todas las actividades comprendidas en esta investigación tienen que ser estrictamente confidenciales ya que usted tendrá acceso a información muy delicada de la institución.

Con seguridad su aporte para la empresa con dicha investigación será muy valioso. Espero que pueda culminar sus estudios con éxito.

Atentamente,
EL MERCURIO CIA. LTDA.

Ing. Xavier Merchán Vintimilla.
GERENTE FINANCIERO

Anexo 2.

ANEXO 2.

TÍTULO:

ENCUESTAS AL PERSONAL DE DIARIO EL MERCURIO CIA. LTDA.

INVESTIGACIÓN REALIZADA POR:
ESTEBAN FERNANDO CASTILLO DURÁN.

FECHA:
6 DE FEBRERO DE 2023.

INTRODUCCIÓN.

Una parte importante para el inicio de este proyecto es determinar el estado actual de la empresa en materia de seguridad de la información ó (S.I.), y entre varios puntos a estudiar, uno de los temas fundamentales al cual debe prestarse especial atención dentro de toda empresa es el factor humano que labora en la misma, puesto que nos permite conocer el contexto interno sobre el cual se desarrollan las actividades de la empresa.

Bajo este precepto, se ha considerado de gran utilidad el tener una visión sobre los conceptos que tienen los empleados de los distintos departamentos de la empresa sobre el tema de S.I. ya que nos puede dar una idea clara de qué tan preparados están para enfrentar situaciones de potencial riesgo durante el desarrollo normal de sus actividades. Metodología aplicada.

Se ha optado por un análisis cuantitativo, el cual permite obtener los resultados y posteriormente analizarlos, todo esto a través de un formulario de tipo cuestionario, ya que nos brinda una gran facilidad al momento de tabular la información obtenida y de esta manera plasmar los resultados de una forma sencilla de comprender.

Este formulario, ha sido elaborado en función de la temática del caso de estudio, que comprende la seguridad de la información y se han desglosado las siguientes preguntas:

PREGUNTA 1:

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADESLABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?

PREGUNTA 2:

SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?

PREGUNTA 3:

¿CONSIDERA USTED IMPORTANTE CONTAR CON SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?

PREGUNTA 4:

¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?

PREGUNTA 5:

PARA USTED, ¿UN HACKER ES UN CRIMINAL?

PREGUNTA 6:

¿CONOCE USTED EL TÉRMINO PHISHING?

PREGUNTA 7:

¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?

Estructura del cuestionario.

Todo el bloque de preguntas se ha adaptado para que las respuestas sean binarias, es decir que las únicas opciones válidas sean SI o NO, se ha considerado de esta manera porque en respuestas que requieran explicación por parte de la persona que responde la encuesta, no representaría ninguna utilidad para el fin de este estudio, ya que perdería objetividad,y resultaría difícil manipular los resultados.

A más de las preguntas, el formulario especifica información básica necesaria para los procesos posteriores a la encuesta.

Fase de desarrollo.

Durante el lapso de dos días (miércoles 1 y jueves 2 de febrero de 2023), se procedió a realizar las encuestas al personal de las distintas áreas de la empresa, hay que mencionar que la empresa cuenta con un total de 59 empleados en su nómina, y de ese universo se procedió a tomar una muestra de 12 empleados, lo cual representa el 20% del total del personal, sin embargo se debe indicar que luego de la pandemia de 2020, se produjo una reducción de personal, motivo por el cual en algunos departamentos las personas responsables de las funciones pasaron a ser solamente una.

Resultados.

Una vez culminada la fase de desarrollo de las encuestas, el siguiente paso comprendió la tabulación de los resultados, de los cuales se obtuvieron los siguientes:

Primera pregunta.

"¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?"

Resultados de la primera pregunta.

Segunda pregunta.

SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA,

¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?

Resultados de la segunda pregunta.

Tercera pregunta.

¿CONSIDERA USTED IMPORTANTE CONTAR CON SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉSIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LASPERSONAS AUTORIZADAS?

Resultados de la tercera pregunta.

Cuarta pregunta.

¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?

Resultados de la cuarta pregunta.

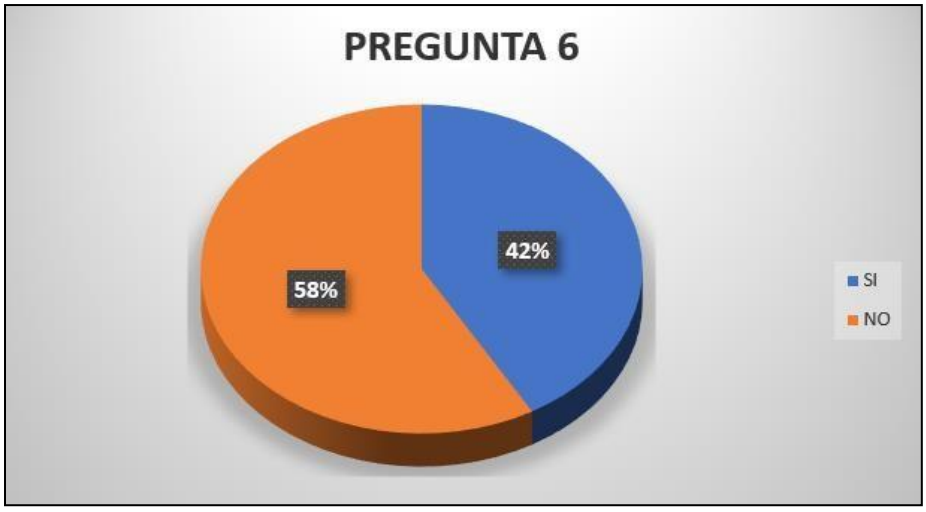
Quinta pregunta.

PARA USTED, ¿UN HACKER ES UN CRIMINAL?

Resultados de la quinta pregunta.

Sexta pregunta.

¿CONOCE USTED EL TÉRMINO PHISHING?



Resultados de la sexta pregunta.

Séptima pregunta.

¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?

Resultados de la séptima pregunta

Conclusiones.

Luego de terminado todo el proceso de tabulación de los resultados, se pudo obtener las siguientes conclusiones.

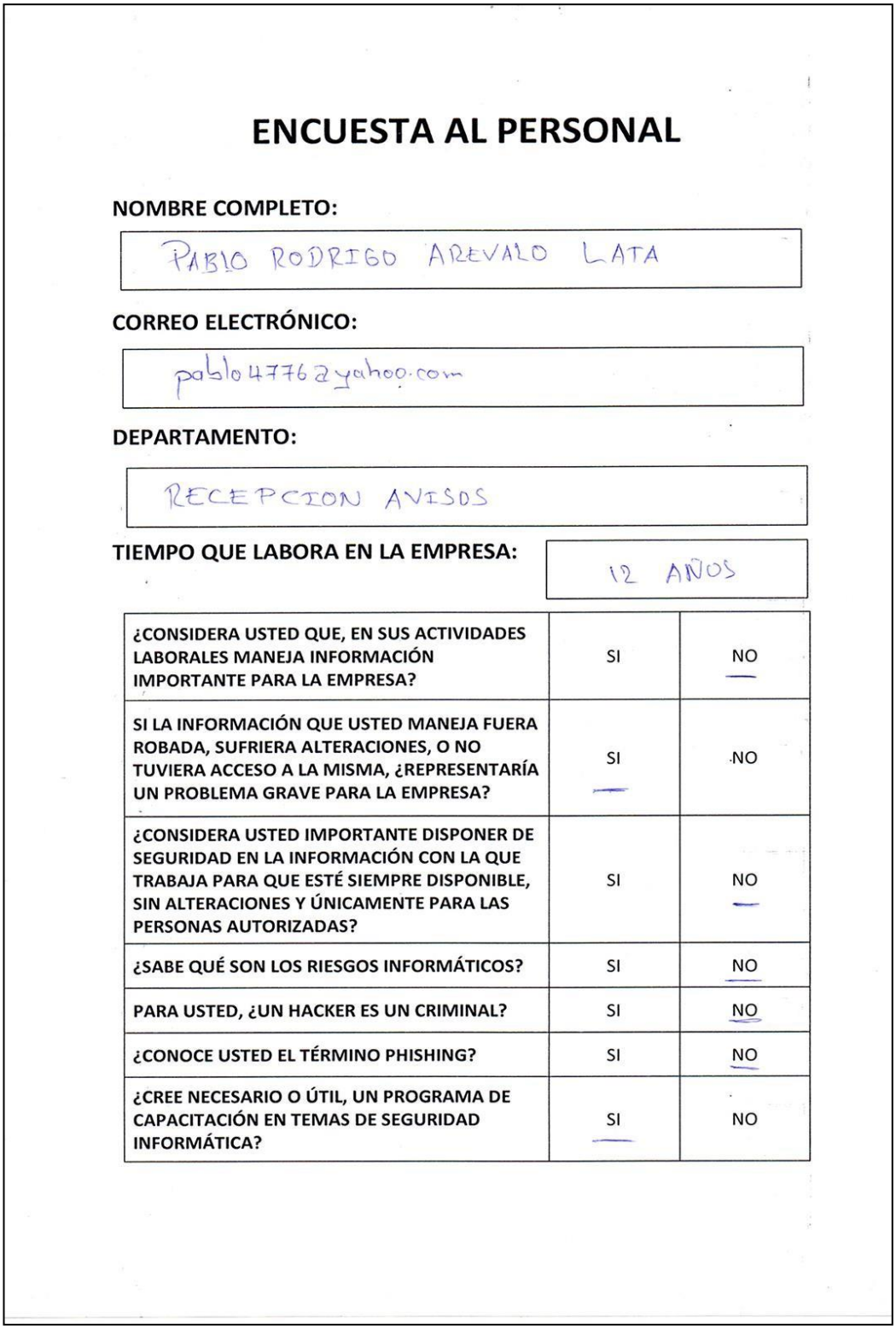
- El promedio de antigüedad de los empleados es alto, lo cual es una ventaja en términos de estabilidad y por ende de conocimiento de procesos y funciones internas.
- Casi todos los encuestados son conscientes de la importancia de la información que manejan en sus labores diarias.
- La mayor parte de los encuestados comprenden la importancia de proteger la información con la cual trabajan con el fin de evitar que las amenazas se materialicen.
- Prácticamente la totalidad de los encuestados han indicado la importancia de contar con procesos que garanticen la seguridad de la información en sus actividades.
- Al menos las tres cuartas partes de los encuestados, saben o tienen una noción sobre lo que son y lo que representan los riesgos informáticos.
- Más del 60% de los encuestados consideran que el término hacker es sinónimo de un criminal.
- Un poco más de la mitad del personal encuestado, no conoce, ni está familiarizado o ha escuchado el término phishing.
- En su totalidad los entrevistados manifestaron que consideran importante el realizar un programa de capacitación sobre S.I.

Recomendaciones.

Luego de obtener las conclusiones en base al análisis de los datos recopilados, se puede indicar que el punto fundamental es planificar y ejecutar un programa de capacitación, de tal manera que permita a todo el personal adquirir los conocimientos necesarios en materia de seguridad de la información, ya que por ejemplo, no tienen conocimiento del término phishing, a pesar de que en la actualidad es uno de los problemas más frecuentesdentro de la empresa, de igual manera la concepción errónea del término hacker es frecuente en la mayoría de los departamentos, son detalles conceptuales que vale la penaser clarificados,

esto tan solo por citar unos ejemplos, sin embargo el programa de capacitación tiene que abarcar los múltiples enfoques que comprenden la ciberseguridad, sin hacer uso de terminología técnica que pueda confundir al personal que no está muy familiarizado con estos conceptos, pero que permita aclarar todas las dudas correspondientes.

Evidencias.



ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

PABLO RODRIGO AREVALO LATA

CORREO ELECTRÓNICO:

pablo47762@yahoo.com

DEPARTAMENTO:

RECEPCION AVISOS

TIEMPO QUE LABORA EN LA EMPRESA: 12 AÑOS

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	SI	NO —
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	SI —	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	SI	NO —
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	SI	NO —
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI	NO —
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	NO —
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	SI —	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Ruth Katerine Torres Astudillo.

CORREO ELECTRÓNICO:

katerinetorresas@hotmail.com

DEPARTAMENTO:

Facturación.

TIEMPO QUE LABORA EN LA EMPRESA: 14 años.

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	SI	(NO)
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI	(NO)
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Diego Montalván

CORREO ELECTRÓNICO:

dmontalvan@elmercurio.com.ec

DEPARTAMENTO:

Redacción

TIEMPO QUE LABORA EN LA EMPRESA: 11 años

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI	(NO)
¿CONOCE USTED EL TÉRMINO PHISHING?	(SI)	NO
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

DIEGO FERNANDO ZAMORA MERCHAN

CORREO ELECTRÓNICO:

difezame@yahoo.com

DEPARTAMENTO:

PRODUCCION

TIEMPO QUE LABORA EN LA EMPRESA:

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	SI	(NO)
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	(SI)	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Miriam Patricia Calle Asmal

CORREO ELECTRÓNICO:

miriamcalle72@hotmail.com

DEPARTAMENTO:

Secretaria.

TIEMPO QUE LABORA EN LA EMPRESA: 21 años.

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI	(NO)
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

SANTIAGO BUENO

CORREO ELECTRÓNICO:

santiago.bueno@elmercurio.com.ec

DEPARTAMENTO:

COMERCIAL

TIEMPO QUE LABORA EN LA EMPRESA: 2 A 3 M

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	~~SI~~	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	~~SI~~	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	~~SI~~	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	~~SI~~	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	~~SI~~	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	~~SI~~	NO
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	~~SI~~	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Xavier Mercman Vintimilla

CORREO ELECTRÓNICO:

xavierm@elmercurio.com.ec

DEPARTAMENTO:

ADMINISTRATIVO

TIEMPO QUE LABORA EN LA EMPRESA: 19 años

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	(SI)	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Italia Elizabeth Castillo Reino.

CORREO ELECTRÓNICO:

italia_creino@hotmail.com.

DEPARTAMENTO:

Tesorería.

TIEMPO QUE LABORA EN LA EMPRESA: 5 años.

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	(SI)	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	(SI)	NO
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

María Eugenia Pachi Lojano

CORREO ELECTRÓNICO:

eugenia.1108@hotmail.com

DEPARTAMENTO:

Contabilidad

TIEMPO QUE LABORA EN LA EMPRESA: 5 años

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	(SI)	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	SI	(NO)
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	(SI)	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

HUGO PATRICIO ABAD GARANQUI

CORREO ELECTRÓNICO:

patosabad7@gmail.com.ec

DEPARTAMENTO:

PRODUCCION

TIEMPO QUE LABORA EN LA EMPRESA: 32 AÑOS

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	SI ✓	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	SI ✓	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	SI ✓	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	SI ✓	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI ✓	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI ✓	NO
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	SI ✓	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Dory Marcela Zamora Merchán

CORREO ELECTRÓNICO:

dory.zamora@hotmail.com

DEPARTAMENTO:

Redacción

TIEMPO QUE LABORA EN LA EMPRESA: 22 años

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	SI ✓	NO
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	SI ✓	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	SI ✓	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	SI ✓	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	SI ✓	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI ✓	NO
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	SI ✓	NO

ENCUESTA AL PERSONAL

NOMBRE COMPLETO:

Tatiana Paola Pinargote Asquilla.

CORREO ELECTRÓNICO:

paitopina@hotmail.com.

DEPARTAMENTO:

Recepcion

TIEMPO QUE LABORA EN LA EMPRESA: 8 años

¿CONSIDERA USTED QUE, EN SUS ACTIVIDADES LABORALES MANEJA INFORMACIÓN IMPORTANTE PARA LA EMPRESA?	SI	(NO)
SI LA INFORMACIÓN QUE USTED MANEJA FUERA ROBADA, SUFRIERA ALTERACIONES, O NO TUVIERA ACCESO A LA MISMA, ¿REPRESENTARÍA UN PROBLEMA GRAVE PARA LA EMPRESA?	(SI)	NO
¿CONSIDERA USTED IMPORTANTE DISPONER DE SEGURIDAD EN LA INFORMACIÓN CON LA QUE TRABAJA PARA QUE ESTÉ SIEMPRE DISPONIBLE, SIN ALTERACIONES Y ÚNICAMENTE PARA LAS PERSONAS AUTORIZADAS?	(SI)	NO
¿SABE QUÉ SON LOS RIESGOS INFORMÁTICOS?	(SI)	NO
PARA USTED, ¿UN HACKER ES UN CRIMINAL?	(SI)	NO
¿CONOCE USTED EL TÉRMINO PHISHING?	SI	(NO)
¿CREE NECESARIO O ÚTIL, UN PROGRAMA DE CAPACITACIÓN EN TEMAS DE SEGURIDAD INFORMÁTICA?	(SI)	NO

Anexo 3.

ENCUESTA AL PERSONAL DE T.I.

NOMBRE:

CARGO:

TIEMPO QUE LABORA EN LA EMPRESA:

¿EXISTE UN MANUAL DE PROCESOS INTERNO EN EL DEPARTAMENTO?	SI	NO
¿EXISTE DISTRIBUCIÓN DE FUNCIONES EN EL DEPARTAMENTO?	SI	NO
¿SE ENTREGAN REPORTES DE ACTIVIDADES A LA DIRECTIVA?	SI	NO
¿EXISTE DOCUMENTACIÓN SOBRE LOS REQUERIMIENTOS REALIZADOS POR LOS OTROS DEPARTAMENTOS?	SI	NO
¿EXISTE UN INVENTARIO DE ACTIVOS DE INFORMACIÓN?	SI	NO
¿ESTÁ ACTUALIZADO? (SI EXISTE)	SI	NO
¿EXISTEN PROCESOS DE CONTROL DE ACCESO DE LOS USUARIOS?	SI	NO
¿ESTÁ DOCUMENTADO? (SI EXISTE)	SI	NO
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA DE RED?	SI	NO
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LOS EQUIPOS INFORMÁTICOS?	SI	NO
¿EXISTEN REVISIONES PERIÓDICAS SOBRE LAS VERSIONES DE LOS SISTEMAS IMPLEMENTADOS EN LOS DISTINTOS DEPARTAMENTOS DE LA EMPRESA?	SI	NO
¿SE REALIZAN COPIAS DE SEGURIDAD PERIÓDICAMENTE DE LA INFORMACIÓN CRÍTICA DEL NEGOCIO?	SI	NO
¿EXISTEN POLÍTICAS QUE DETALLEN LOS PROCESOS DE DESARROLLO DE APLICACIONES?	SI	NO
EL ACCESO EXTERNO (TERCEROS) TANTO A LA RED, COMO A LOS SISTEMAS DE LA EMPRESA, ¿ES MONITOREADO?	SI	NO
¿CONSIDERA QUE LA INFRAESTRUCTURA DE LA EMPRESA ESTÁ PREPARADA EN CASO DE QUE UN INCIDENTE DE CIBERSEGURIDAD OCURRA?	SI	NO
¿EXISTE ALGÚN PLAN DE CONTINGENCIA EN CASO DE QUE UN ATAQUE INFORMÁTICO LLEGUE A AFECTAR LA INFRAESTRUCTURA DE LA EMPRESA?	SI	NO
¿SE ENCUENTRAN LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA PREPARADOS PARA IMPLEMENTAR LOS REQUERIMIENTOS DETALLADOS EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES?	SI	NO

PRIMERA PARTE

ENCUESTA AL PERSONAL DE T.I.

NOMBRE: Ricardo Maldonado

CARGO:

TIEMPO QUE LABORA EN LA EMPRESA: 6 Meses

¿EXISTE UN MANUAL DE PROCESOS INTERNO EN EL DEPARTAMENTO?	SI	NO
¿EXISTE DISTRIBUCIÓN DE FUNCIONES EN EL DEPARTAMENTO?	SI	NO
¿SE ENTREGAN REPORTES DE ACTIVIDADES A LA DIRECTIVA?	SI	NO
¿EXISTE DOCUMENTACIÓN SOBRE LOS REQUERIMIENTOS REALIZADOS POR LOS OTROS DEPARTAMENTOS?	SI	NO
¿EXISTE UN INVENTARIO DE ACTIVOS DE INFORMACIÓN?	SI	NO
¿ESTÁ ACTUALIZADO? (SI EXISTE)	SI	NO
¿EXISTEN PROCESOS DE CONTROL DE ACCESO DE LOS USUARIOS?	SI	NO
¿ESTÁ DOCUMENTADO? (SI EXISTE)	SI	NO
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA DE RED?	SI	NO
¿EXISTEN POLÍTICAS DE MANTENIMIENTO Y CONTROL DE LOS EQUIPOS INFORMÁTICOS?	SI	NO
¿EXISTEN REVISIONES PERIÓDICAS SOBRE LAS VERSIONES DE LOS SISTEMAS IMPLEMENTADOS EN LOS DISTINTOS DEPARTAMENTOS DE LA EMPRESA?	SI	NO
¿SE REALIZAN COPIAS DE SEGURIDAD PERIÓDICAMENTE DE LA INFORMACIÓN CRÍTICA DEL NEGOCIO?	SI	NO
¿EXISTEN POLÍTICAS QUE DETALLEN LOS PROCESOS DE DESARROLLO DE APLICACIONES?	SI	NO
EL ACCESO EXTERNO (TERCEROS) TANTO A LA RED, COMO A LOS SISTEMAS DE LA EMPRESA, ¿ES MONITOREADO?	SI	NO
¿CONSIDERA QUE LA INFRAESTRUCTURA DE LA EMPRESA ESTÁ PREPARADA EN CASO DE QUE UN INCIDENTE DE CIBERSEGURIDAD OCURRA?	SI	NO
¿EXISTE ALGÚN PLAN DE CONTINGENCIA EN CASO DE QUE UN ATAQUE INFORMÁTICO LLEGUE A AFECTAR LA INFRAESTRUCTURA DE LA EMPRESA?	SI	NO
¿SE ENCUENTRAN LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA PREPARADOS PARA IMPLEMENTAR LOS REQUERIMIENTOS DETALLADOS EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES?	SI	NO

Información entregada el día miércoles 22 de marzo de 2023.

SEGUNDA PARTE

ENTREVISTA AL JEFE DEL DEPARTAMENTO DE SISTEMAS.

• Número de servidores físicos (S.O. de los mismos y sus versiones.)

5 servidores físicos

- Windows server2012
- Windows server2003

• Número de bases de datos (Gestores utilizados y sus versiones.)

2 Bases

- Oracle Database 12c Standard Edition Release 12.1.0.2.0 - 64bit Production

• El sistema de gestión de la empresa que se encuentra en http://192.168.200.150:7101, en qué lenguaje fue desarrollado

El sistema de gestión fue desarrollado en oracle forms y oracle apex.

• ¿Qué empresa brinda los servicios de ISP?

Telefónica Movistar

• En caso de fallos por parte del proveedor ISP, ¿qué procesos se realizan para mitigar los problemas internos?

- Se comunica a los usuarios del fallo y las afectaciones sobre los diferentes problemas,

- -Sean de navegación.
    - Envíos de correo.
    - ó acceso al sistema quienes pueden o no acceder al mismo.
    - Se informa sobre el tiempo estimado que indica el proveedor que estaremos sin el servicio.
    - Se realiza el seguimiento correspondiente a las acciones realizadas por el proveedor para solucionar el inconveniente y estar en constante comunicación para realizar las debidas pruebas.
    - Recomendación es tener un enlace de respaldo con otro proveedor, tomando en cuenta los costos que representaría para la empresa su implementación.

• ¿Dispone la empresa de un firewall? si la respuesta es SI, qué características tiene.

- Si disponemos, el equipo es un Mikrotik CCR1036-8G-2S
- Características

- Enrutamiento dinámico,
- Punto de acceso,
- Cortafuegos,
- MPLS, VPN,
- Calidad de servicio avanzada,
- Balanceo de carga y enlaces,
- Configuración y supervisión en tiempo real
- Administrado por RouterOS

• ¿Existe documentación de los requerimientos de los usuarios?

Los requerimientos de los usuarios están registrados por medio de un correo electrónico de solicitud del cambio o requerimiento.

• ¿Hay algún control sobre los recursos que son dados de baja y la información que éstos contienen?

Los procesos que se realiza para dar de baja los equipos son dos: el de proceso contable y el de sistemas.

El proceso de contable se realiza durante los 5 años de amortización del equipo

En cuanto al departamento de sistemas, se procede a realizar un respaldo de la información y su respectiva migración hacia los nuevos equipos, se le pide al usuario validar que esté completa su información, se mantiene el respaldo de esa información por un mes y se procede a borrar la información del dispositivo que se dio de baja.

Anexo 4.

Documento de levantamiento de Activos de Información completo

Etiquetado AI	Nombre AI	Descripción	Custodio	Propietario	Responsable	Tipo AI	Grado dependencia	Observaciones	Usuarios que tienen acceso a AI	Permisos sobre el AI	Confidencialidad	Integridad	Disponibilidad	Total Valoración AI	Clasificación AI	Importancia AI
EM-AI-I-01	Centro de Datos	Ubicación física en la cual se encuentran los equipos y sistemas	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Instalaciones	20% de Activo 8%	Cuenta con un sistema de refrigeración básico	Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-02	Servidor de aplicaciones	Servidor que contiene el sistema de gestión de la empresa	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-03	Servidor Web	Servidor que contiene la página web y los recursos utilizados en línea	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% de los Activos 1 y 2; 30% del Activo 8		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-04	Servidor de Respaldos	Servidor que almacena los respaldos de las bases de datos y aplicaciones	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	2	3	1	2	Confidencial	MEDIO
EM-AI-EI-05	Servidor de correo Institucional	Servidor que gestiona el sistema de correo institucional	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% de los Activos 1 y 2; 30% del Activo 8		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	2	3	2,666666667	Confidencial	ALTO
EM-AI-DI-06	Base de Datos Aplicaciones	Base de datos que almacena información de gestión de la empresa	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Datos o información	100% del Activo 1 y 100% del Activo 2		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-DI-07	Base de Datos Suscriptores	Base de datos que almacena información sobre los suscriptores	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Datos o información	100% del Activo 1 y 100% del Activo 2		Jefe de Sistemas	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-08	Equipos de backup	Generadores, equipos UPS	Gerente de Operaciones	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	0% Dependencia		Jefe de Sistemas	N/A	1	1	3	1,666666667	Uso Interno	BAJO
EM-AI-EI-09	Terminales Administración	Equipos de cómputo utilizados por el departamento administrativo	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8	S.O. Windows 11 (12 equipos), Windows 10 (8 equipos), Ubuntu (26 equipos)	Personal del departamento de Administración	Responsable (LEC-ES-MOD-EL) - Personal (LEC-ES-MOD-E	2	2	1	1,666666667	Uso Interno	BAJO
EM-AI-EI-10	Terminales de Diseño y Diagramación	Equipos de cómputo utilizados por el departamento de diseño y diagramación	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8	Mac OS	Personal del departamento de Diseño y Diagramación	Responsable (LEC-ES-MOD-EL) - Personal (LEC-ES-MOD-E	2	2	1	1,666666667	Uso Interno	BAJO
EM-AI-EI-11	Terminales de Redacción	Equipos de cómputo utilizados por el departamento de redacción	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8	S.O. Ubuntu (14 equipos)	Personal del departamento de Redacción	Responsable (LEC-ES-MOD-EL) - Personal (LEC-ES-MOD-E	2	2	1	1,666666667	Uso Interno	BAJO
EM-AI-EI-12	Impresoras, escáneres y dispositivos de oficina	Dispositivos de uso general por los diferentes departamentos	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	100% del Activo 1 y 30% del Activo 8		Todo el personal	(LEC-ES-MOD-EL)	1	1	1	1	Uso Interno	BAJO
EM-AI-RC-13	Routers	Dispositivos para conexiones de red	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Redes de Comunicación	100% del Activo 1 y 30% del Activo 8, 90% del activo 32		Jefe de Sistemas	Responsable (LEC-ES-MOD-EL) - Personal (LEC)	3	2	1	2	Uso Interno	MEDIO
EM-AI-RC-14	Modems	Dispositivos para conexiones de red	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Redes de Comunicación	100% del Activo 1 y 30% del Activo 8, 90% del activo 32		Jefe de Sistemas	Responsable (LEC-ES-MOD-EL) - Personal (LEC)	2	3	2	2,333333333	Uso Interno	MEDIO
EM-AI-RC-15	Firewall	Dispositivos para conexiones de red	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Redes de Comunicación	100% del Activo 1 y 30% del Activo 8, 90% del activo 32		Jefe de Sistemas	Responsable (LEC-ES-MOD-EL) - Personal (LEC)	3	3	3	3	Uso Interno	ALTO
EM-AI-EI-16	Servidor para Pre Prensa	Servidor que contiene los recursos necesarios para el proceso de pre prensa	Gerente de Operaciones	El Mercurio Cía. Ltda.	Jefe de Sistemas	Equipos Informáticos	50% del Activo 1 y 30% del Activo 8	Windows Server 2016	Jefe de Sistemas, Jefe de Pre Prensa	Responsable y Personal Departamento (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-17	Equipo CTP (Copiado Directo a Plancha)	Equipo que realiza el proceso de conversión de digital a las planchas de aluminio	Gerente de Operaciones	El Mercurio Cía. Ltda.	Jefe de Pre Prensa	Equipos Informáticos	100% del Activo 16 y 30% de Activo 8		Jefe de Sistemas, Jefe de Pre Prensa	Responsable y Personal Departamento (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-EI-18	Procesadora de Placas	Equipo que realiza el proceso de conversión de digital a las planchas de aluminio	Gerente de Operaciones	El Mercurio Cía. Ltda.	Jefe de Pre Prensa	Equipos Informáticos	100% del Activo 16 y 100% del Activo 17		Jefe de Sistemas, Jefe de Pre Prensa	Responsable y Personal Departamento (LEC-ES-MOD-EL)	1	3	3	2,333333333	Uso Interno	MEDIO
EM-AI-EI-19	Reveladora de Placas	Equipo que realiza el proceso de impresión en las planchas de aluminio	Gerente de Operaciones	El Mercurio Cía. Ltda.	Jefe de Pre Prensa	Equipos Informáticos	100% del Activo 16 y 100% del Activo 17		Jefe de Sistemas, Jefe de Pre Prensa	Responsable y Personal Departamento (LEC-ES-MOD-EL)	1	3	3	2,333333333	Uso Interno	MEDIO
EM-AI-AS-20	Sistema de gestión empresarial El Mercurio	Software desarrollado para la empresa, que permite desarrollar las actividades tanto administrativas como de producción, administrando todos sus procesos	Gerente General	El Mercurio Cía. Ltda.	Jefe de Sistemas	Aplicaciones de Software	100% del Activo 1 y 100% del Activo 2, 30% del Activo 8		Jefe de Sistemas, Contabilidad	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	3	3	Confidencial	ALTO
EM-AI-AS-21	Plataformas de ofimática	Software utilizado por los diferentes departamentos de la empresa para el desarrollo de sus actividades	Gerente Financiero	Microsoft, Libre Office	Jefe de Sistemas	Aplicaciones de Software	70% del Activo 1, 30% del Activo 8, 40% del Activo 5, 100% de los Activos 9,10 y 11	Microsoft Office versión 2016, Libre Office licencia GNU	Todo el personal	(LEC-ES-MOD-EL)	2	2	1	1,666666667	Uso Interno	BAJO
EM-AI-AS-22	Plataformas de diseño gráfico	Software con licencia, utilizado por los departamentos de diseño gráfico y diagramación	Gerente Financiero	Adobe Corporation	Jefe de Sistemas	Aplicaciones de Software	80% del Activo 1, 30% del Activo 8, 40% del Activo 5, 100% del Activo 10	Adobe Creative Suite 6 Master Collection	Personal del departamento de Diseño y Diagramación	Responsable (LEC-ES-MOD-EL) - Personal (LEC-ES-MOD-E	2	2	1	1,666666667	Uso Interno	BAJO
EM-AI-AS-23	Plataforma Zoom	Software con licencia, utilizado por diferentes departamentos para realizar reuniones en línea	Gerente Financiero	Zoom Comunications	Jefe de Sistemas	Aplicaciones de Software	100% del Activo 1, 30% del Activo 8, 40% del Activo 5, 100% de los Activos 9,10,11,32	Versión 5.13	Todo el personal	Responsable (LEC-ES-MOD-EL) - Personal (LEC-ES-MOD-E	3	1	2	2	Uso Interno	MEDIO
EM-AI-P-24	Jefe de Sistemas	Encargado del departamento de Sistemas	Departamento de Sistemas	N/A	Ing. Ricardo Maldonado	Personal	N/A	N/A	N/A	N/A	3	1	1	1,666666667	Uso Interno	BAJO
EM-AI-P-25	Personal de Pre Prensa	Encargado del departamento de Pre Prensa	Departamento de Pre Prensa	N/A	Patricio Abad	Personal	N/A	N/A	N/A	N/A	3	1	1	1,666666667	Uso Interno	BAJO
EM-AI-I-26	Agencia Centro	Oficina perteneciente a la empresa, encargada del recepción de publicidad	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia Centro	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia Centro	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	2	2,666666667	Confidencial	ALTO
EM-AI-I-27	Agencia El Vergel	Oficina perteneciente a la empresa, encargada del recepción de publicidad	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia El Vergel	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia El Vergel	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	2	2,666666667	Confidencial	ALTO
EM-AI-I-28	Agencia González Suárez	Oficina perteneciente a la empresa, encargada del recepción de publicidad	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia González Suárez	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia González Suárez	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	1	2,333333333	Confidencial	MEDIO
EM-AI-I-29	Agencia El Arenal	Oficina perteneciente a la empresa, encargada del recepción de publicidad	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia El Arenal	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia El Arenal	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	2	2,666666667	Confidencial	ALTO
EM-AI-I-30	Agencia Guayaquil	Oficina perteneciente a la empresa, encargada del recepción de publicidad en la ciudad de Guayaquil	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia Guayaquil	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia Guayaquil	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	1	2,333333333	Confidencial	MEDIO
EM-AI-I-31	Agencia Quito	Oficina perteneciente a la empresa, encargada del recepción de publicidad en la ciudad de Quito	Gerente General	El Mercurio Cía. Ltda.	Jefe de Agencia Quito	Instalaciones	100% del Activo 1		Jefe de Sistemas, personal de la Agencia Quito	Custodio (LEC) - Responsable (LEC-ES-MOD-EL)	3	3	1	2,333333333	Confidencial	MEDIO
EM-AI-S-32	Servicio de Internet	Servicio contratado de Internet para la empresa y todas sus dependencias	Gerente Financiero	Telconet	Jefe de Sistemas	Servicio	0% Dependencia		Todo el personal	Responsable (LEC-ESC-MOD) - PERSONAL (LEC)	2	2	3	2,333333333	Uso Interno	MEDIO

TOTAL ACTIVOS:	32
TOTAL ACTIVOS (ALTO):	13
TOTAL ACTIVOS (MEDIO):	10
TOTAL ACTIVOS (BAJO):	9

Anexo 5.

Acta de recepción de los informes ejecutivo y técnico por parte de la directiva de la compañía

EL MERCURIO

Cuenca, 6 de julio de 2023

Ingeniero
Esteban Castillo Durán
Ciudad. –

De mis consideraciones:

Por medio de la presente, se certifica que, con fecha jueves 06 de julio del 2023, se ha hecho entrega por parte del Ing. Esteban Castillo Durán, toda la documentación resultante del proceso de estudio denominado: "Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información, (S.G.S.I) basado en ISO 27001. Caso de estudio: Diario "El Mercurio Cia. Ltda." dicha documentación consta de 2 secciones denominadas "Informe Ejecutivo" e "Informe Técnico".

Atentamente,
EL MERCURIO CIA. LTDA.

Ing. Xavier Merchán Vintimilla.
GERENTE FINANCIERO