UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

Proyecto de graduación

Para optar por el grado de Bachillerato en Ingeniería en Informática

PROPUESTA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD DE INFORMACIÓN, BASADA EN LA NORMATIVA ISO/IEC 27001:2022 Y COBIT 5 EN ESPAÑOL Y LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN PARA LA EMPRESA COPY PRINTER ADVANCED SRL, UBICADA EN SAN JOSÉ

SEBASTIÁN SÁNCHEZ PIÑAR

AUTOR

CARLOS AGUILAR MORA

TUTOR

DANIEL ÁLVAREZ GARRO

LECTOR

San José, Costa Rica

Marzo, 2024

DEDICATORIA

El presente proyecto de graduación lo dedico, en primer lugar, a Dios, quien me brindó salud, capacidad y sabiduría para continuar día tras días en momentos difíciles a lo largo de mi carrera universitaria.

En segunda instancia, a mi madre, quien ha sido un pilar fundamental en mi formación personal, ya que con amor, paciencia y fortaleza me ha apoyado en cada momento de mi vida.

A mi tía Aude, quien es como una segunda madre y ha velado por mí, durante este arduo camino, desde la niñez hasta este momento en el que busco convertirme en un profesional.

A mi papá, por brindarme su apoyo y ser una fuente de inspiración profesional para continuar creciendo y aprendiendo.

A mis tíos, Elberth y Susan, por brindarme apoyo en momentos importantes de formación profesional, con el fin de brindar esa guía para salir adelante; siempre estuvieron ahí apoyándome y nunca dudaron de mis capacidades.

Por último y no menos importantes, a mis hermanos, Johan, Fernando, Catalina y mi prima Michelle, todos ellos, también, forman parte integral de este gran logro.

AGRADECIMIENTOS

Al concluir esta etapa de gran importancia en mi vida, agradezco, en primer lugar, a Dios por darme la oportunidad de estar con vida y proveer los medios necesarios para el crecimiento personal y profesional; también por brindarme dirección en los momentos de dificultad y prueba.

Por otra parte, extiendo un profundo agradecimiento a mi madre, porque con su apoyo y motivación he logrado cumplir mis metas y, por supuesto, a mis hermanos y familiares más cercanos, quienes con su ejemplo y palabras de aliento me impulsan para seguir adelante y no desfallecer, por enseñarme que el esfuerzo y la dedicación en lo que haces es vital para crecer y ser mejores cada día.

Agradezco también a los docentes, quienes en cada clase impartida hicieron posible mi formación profesional, por inculcar los valores de la responsabilidad, respeto y ética, los cuales son fundamentales para ejercer mejores relaciones humanas.

Por último, agradezco a la empresa Copy Printer Advanced SRL, principalmente al gerente Elberth Méndez Jiménez, por su anuencia en cooperar para que el proyecto se desarrollara. A su vez, doy gracias a mi primer tutor Daniel Mena Bocker y Carlos Aguilar, por su tiempo invertido para concluir con éxito la investigación.

CONTENIDO

TABLAS

FIGURAS

RESUMEN EJECUTIVO

Las empresas se encuentran ante situaciones adversas de diferente índole, sin embargo, el problema de la seguridad de la información y temas estrechamente vinculados con este representan un reto para los negocios; por el cual es necesaria una debida planificación y preparación. Copy Printer Advanced no es la excepción, debido a que, actualmente, no cuenta con herramientas o sistemas aptos para proteger los activos de información y demás elementos relacionados, ante posibles amenazas cibernéticas.

Debido a lo anterior, es preciso conocer el contexto interno y externo, en el cual se desenvuelve la empresa, a través de un análisis DAFO. Por otra parte, es vital que se identifiquen los riesgos relacionados con la pérdida de la confidencialidad, integridad y disponibilidad de la información, además de crear un plan de tratamiento de riesgo, así como el diseño de políticas de seguridad de la información de acuerdo con los procesos, lineamientos y requerimientos de la empresa. El proyecto tiene como finalidad entregar una propuesta para la implementación del Sistema de Gestión de la Seguridad de la Información, utilizando como referencia la norma ISO/IEC 27001: 2022, y de forma secundaria las normas técnicas para la gestión y control de las tecnologías de información del Marco Referencial COBIT 5, con el fin de que la empresa pueda estar preparada ante amenazas y, a su vez, mitigar o disminuir las vulnerabilidades presentes en la institución. A continuación, se detalla la distribución del presente documento:

En el capítulo I, se presenta la descripción de la problemática, el planteamiento del problema, la descripción del proyecto y los objetivos. El segundo capítulo muestra el marco teórico, que es la base teórica relacionada con el Sistema de Gestión de Seguridad de la Información (SGSI). La definición de estos términos básicos respaldada con la norma ISO/IEC 27001:2022 y el Marco Referencial COBIT 5.

En el capítulo III, se especifica el método de investigación para desarrollar el trabajo investigativo, así como métodos de aplicación, tipos, fuentes y variables de investigación.

El capítulo IV es la presentación de los resultados del trabajo de investigación. Se desarrolla cada una de las actividades propuestas en el capítulo III y se discuten los resultados obtenidos.

El capítulo cinco muestra las conclusiones y recomendaciones, a partir de los resultados obtenidos de los objetivos planteados inicialmente. Por último, el capítulo VI detalla la propuesta de la investigación realizada.

CAPÍTULO I. INTRODUCCIÓN

Durante los últimos años, las empresas se han enfrentado a cambios tecnológicos, por tal motivo, han actualizado sus dispositivos e implementado nuevos sistemas informáticos, acordes a las nuevas tendencias del mercado, que han llegado para facilitar el trabajo. Sin embargo, se desconoce sobre la seguridad que se debe implementar, al adquirir y poner en funcionamiento dichos dispositivos y aplicaciones.

Aunado a lo anterior, es preciso destacar que las empresas buscan formas de almacenar datos, ya sean financieros, administrativos e incluso personales, pero son pocos los que investigan sobre cómo preparar los sistemas de información, ante las diversas amenazas que puedan afectar la continuidad de los servicios que ofrece la organización. Por su parte, ante el desconocimiento de la seguridad informática e información del aplicativo implementado, esto puede ser una puerta abierta para posibles ataques informáticos.

Si bien es cierto, existen muchas técnicas para prevenir que las organizaciones e instituciones sean vulnerables, el desconocimiento en temas de seguridad de la información se da continuamente, porque no existe personal capacitado para orientar y proponer controles de seguridad para los activos de información.

Además, toda información cuenta con datos sensibles que podrían ser debilitados ante una situación de amenaza y vulnerabilidades. Por esta razón, los expertos en seguridad de la información recomiendan aplicar normas internacionales que garanticen la seguridad y así tener confianza enfocada en la protección de la infraestructura de tecnologías de información y comunicación, que van a lo interno, desde la alta gerencia, hasta la seguridad del edificio de la empresa y externo como los proveedores y clientes, asegurando la confidencialidad, integridad y disponibilidad de la información.

Por tanto, es necesario comunicar la importancia de la seguridad de la información a los usuarios, para que se establezcan buenas prácticas y proteger todo el entorno, previniendo la posibilidad de algún daño donde se vean afectados los activos de información, ya que, en la actualidad, existen muchas personas que han sido víctimas ante eventualidades de cualquier amenaza que pone en peligro la disponibilidad, integridad y confidencialidad de esta. Por ello, la propuesta de implementación de la seguridad de información, en la empresa Copy Printer Advanced, busca mitigar riesgos asociados a los activos de la información de la compañía.

Planteamiento del problema

La empresa en la cual se lleva a cabo la investigación se denomina Copy Printer Advanced SRL., dedicada a la venta, alquiler y soporte técnico de equipos multifuncionales de sistemas de impresión, especializados en la utilización de la marca Ricoh y Laner; se encuentra ubicada en Pozos, Santa Ana, San José. Además, cuenta con 14 años de experiencia en el mercado, donde satisface las diversas necesidades en empresas de diferentes naturalezas, por ejemplo, centros educativos públicos y privados, librerías, telecomunicaciones, centros de fotocopiado y demás negocios dedicados a la comercialización de bienes y servicios.

De igual manera, la empresa cuenta con técnicos debidamente capacitados, para la oportuna solución de los problemas que presenten los clientes, con la finalidad de brindar un excelente servicio y que los inconvenientes no sean sinónimo de retraso en las operaciones de los negocios con los cuales existe una relación comercial.

A continuación, se muestran los problemas detectados en la empresa Copy Printer Advanced SRL.:

Problemas para establecer, implementar, mantener y mejorar el contexto de seguridad

No existen criterios para establecer, implementar, mantener y mejorar el contexto de seguridad, al no contar con un sistema de gestión de seguridad de la información, donde se conozcan las políticas de seguridad, ya que no existe una política seguridad general, por lo que representa un riesgo para los activos de información, por no tener implementados controles ni procedimientos adecuados según la necesidad del negocio.

Empleados molestos por la tardía respuesta en la eventualidad de un incidente

Debido a que existe ausencia de política de continuidad negocio, ante eventos como desastres naturales y ataques cibernéticos, hay empleados molestos por la tardía respuesta ante la eventualidad de un incidente, ya que no se cuenta con un equipo con roles y responsabilidades que brinde respuesta inmediata. Por lo tanto, la respuesta a eventualidades que compromete la confidencialidad, integridad y disponibilidad debe utilizarse con el fin de reducir la probabilidad o el impacto de los incidentes en el futuro, y así realizar mejoras en la capacitación, relacionadas a temas de manejos de incidentes de la seguridad de la información.

Por su parte, la problemática se da porque no existen profesionales capacitados para la mejora de conocimiento, facilitando que estas personas identifiquen la seguridad de la información, los problemas y las causas, para que se pueda brindar una respuesta de manera rápida y efectiva. Adicionalmente, no existe capacitación que cumpla con todos los requisitos de seguridad, a fin de que los empleados conozcan cómo usar la información correctamente.

Divulgación de la información por personas no autorizadas

Genera la pérdida de confidencialidad, exponiéndose a amenazas como el robo, modificación y divulgación de información sensible en muchas ocasiones. A causa de que la empresa no informa los acuerdos a los empleados que utilizan la información confidencial, además de la importancia de protegerse, usarse y cómo se debe acceder a ellos de manera responsable y autorizada, por lo que debe ser un acuerdo legal que describe información confidencial, que las partes compartirán entre sí y no divulgarán a la otra parte.

Desconocimiento de controles necesarios para proteger la información

Provoca el inadecuado conocimiento del valor de los activos ante eventos inesperados, al no existir responsables de las tareas de gestión, métodos de estimación del impacto y la probabilidad de ocurrencia de los posibles riesgos.

Dado que no existen controles y programas, para el *malware* que quiere dañar los dispositivos ante esta técnica; invertir en la seguridad es una de las soluciones para proteger los equipos y la información. La detección de *malware* por sí sola no suele ser suficiente y normalmente debe ir acompañada de procedimientos operativos para evitar su introducción.

Además, no existen fechas establecidas para la realización de los respaldos; sí se realizan, pero no existe un procedimiento formal. Por lo que, al no contar con una estrategia de copia de seguridad diaria y semanal, automatizada para bases de datos y sitios web, a fin de que, en caso de corrupción o violación de la integridad de los datos, se pueda restaurar la información.

Objetivo general

Aplicar la norma ISO/IEC 27001:2022 y COBIT 5 en la empresa Copy Printer Advanced SRL, planteando un modelo de seguridad de la información, que asegure el cumplimiento de la disponibilidad, confidencialidad e integridad de la información.

Objetivos específicos

1. Determinar el contexto de la organización, a través del análisis obtenido de una matriz DAFO, con la finalidad de que se origine un buen sistema de gestión de seguridad de la información.
2. Identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, para que se conozcan con precisión.
3. Crear un plan de tratamiento de riesgo, seleccionando, implementando y verificando controles que permitan el establecimiento de indicadores, aplicando como referencia el Marco Referencial COBIT 5 y la norma ISO 27001.
4. Diseñar políticas de seguridad de la información acordes con los procesos, lineamientos y requerimientos de la empresa, aplicando como referencia los controles de la norma internacional ISO 27001:2022 y COBIT 5.

Justificación

Las organizaciones nacen para la satisfacción de una necesidad, ya sea de una persona o un grupo de personas, por tal motivo, existen individuos que inician ideas de negocio desde una perspectiva de subsistencia, que con el pasar del tiempo evoluciona y se convierte en un negocio lucrativo; el cual puede ser pequeño, mediano o grande, dependiendo de la visión de crecimiento determinada por los encargados de direccionarlo.

Adicionalmente, la ciberseguridad es uno de los retos importantes que las empresas deben implementar, ya que, durante los últimos años y ante el crecimiento de equipos tecnológicos, se ha visto el aumento de ataques informáticos, donde las empresas se exponen a la pérdida de datos sensibles y, por ende, reputación en el mercado.

La seguridad de la información no debe estar únicamente relacionada con la protección de datos con los que se relacionan constantemente, tales como datos financieros, administrativos, médicos, educativos, de dispositivos informáticos, entre otros; que deben estar bien resguardados, porque son parte de la cotidianidad de las diferentes labores de las organizaciones. Estos datos se pueden encontrar en las redes sociales como Facebook, Instagram, Twitter, YouTube y todos aquellos en los que se comparte o publica información personal o laboral, además, existe desconocimiento sobre los sitios donde se encuentran los datos, por lo que el problema más común de las personas es desconocer a quién se le está compartiendo la información.

Las organizaciones deben establecer políticas, donde los empleados tengan el conocimiento necesario, sobre la importancia de la protección de datos, así como de los recursos humanos, técnicos y seguridad física del edificio, asegurando mitigar vulnerabilidades ante amenazas y con ello estar preparados, ante posibles ataques informáticos y desastres naturales, garantizando la disponibilidad, integridad y confidencialidad de la información.

Debido a lo anterior, se propone implementar el Sistema de Gestión de la Seguridad de la Información, tomando como principal referencia la norma ISO/IEC 27001: 2022; asimismo, de forma secundaria, las normas técnicas para la gestión y control de las tecnologías de información del Marco Referencial COBIT 5, con la finalidad de estar preparados ante posibles amenazas y mitigando vulnerabilidades en la organización. Considerando, a su vez, la legislación vigente en Costa Rica como lo son: la Ley N.º 8968 de protección de datos de la persona frente al tratamiento de sus datos personales y la Ley N.º 9048 Delitos informáticos.

Viabilidad técnica

Para el desarrollo de la propuesta, se necesita de una computadora portátil con las siguientes características de *hardware* y *software*:

Hardware:

- Procesador: Intel(R) Core (TM) i7-1065G7 CPU @ 1.30GHz 1.50 GHz.
- RAM instalada: 8,00 GB (7,77 GB usable).
- Tipo de sistema: Sistema operativo de 64 bits, procesador basado en x64.
- Lápiz y entrada táctil Compatibilidad del lápiz y la función táctil con 10 puntos táctiles.

Software:

- Windows 10 o superior.
- Paquete office 365 con respectiva licencia.
- Explorador de internet Chrome.

Viabilidad operativa

Existe compromiso de la alta Gerencia y personal operativo para cumplir con lo establecido en la propuesta. Actualmente no cuenta con auditor interno, pero el gerente general tiene experiencia y se encuentra en disposición para que se administre y se cumpla el programa propuesto, además, el personal no se ve afectado al implementar la propuesta.

Viabilidad económica

En cuanto al costo del *hardware y software,* es variable, ya que la empresa cuenta con las herramientas por utilizar; actualmente cuenta con licencia Office 365 y explorador de internet Chrome, cumpliendo así con lo requerido.

Con respecto a la propuesta y si se concreta la implementación del sistema de gestión de seguridad de la información, se debe contratar personal externo requerido, para que guíe el proceso, por lo tanto, el costo puede variar según la necesidad de la empresa.

Sin embargo, la empresa no tendrá que asumir ningún costo para desarrollo de la propuesta, esto debido a que hay un acuerdo entre esta y el estudiante, por ser un proyecto de graduación.

Viabilidad legal

Para la propuesta se toma en cuenta la Ley N.º 9048 de Delitos informáticos y Ley N.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales en Costa Rica (Asamblea Legislativa de Costa Rica, 2011; 2012). También, está basada en las regulaciones que establece la norma ISO/IEC 27001:2022, COBIT 5 y las normas para la gestión y el control de las tecnologías de la información que propone el Ministerio de Ciencia, Innovación Tecnologías y Comunicaciones. Por tanto, con respecto a la propuesta, es viable, ya que no se viola ninguna ley que establece la legislación de Costa Rica.

Alcances

El alcance de la propuesta es identificar, tratar los riesgos y diseñar políticas de seguridad de información, para mantener un nivel aceptable ante riesgos, donde se pretende minimizar eventos que afectan la pérdida de la confidencialidad, integridad y disponibilidad, prevaleciendo la seguridad de información. Se incluyen no solo controles técnicos, sino también revisiones de riesgos sobre empleados, activos, recursos, procesos, al igual que políticas y leyes de la República de Costa Rica.

La parte principal del proyecto es la creación de un sistema de gestión de seguridad de la información que incorpore planes de continuidad del negocio y gestión de riesgos, permitiendo analizar y monitorear estos planes para establecer una estrategia de seguridad de la información. Reducir el riesgo mediante controles que puedan influir en el mismo. Asimismo, asegurar la continuidad de los procesos críticos del negocio ante distintos tipos de amenazas prevaleciendo la confidencialidad, integridad y disponibilidad de la información.

Alcance funcional

El alcance funcional para realizar la propuesta se basa en la norma ISO/IEC 27001:2022 y el Marco Referencial COBIT 5 para la gestión de riesgos, con el objetivo de optimizar los riesgos tomando en cuenta el compromiso de la alta Gerencia y empleados de la empresa. Además, se busca reducir eventos indeseados y lograr la mejora continua en procesos.

Para la propuesta de la implementación del Sistema de Gestión de Seguridad de la Información, se utiliza como fuente secundaria el Marco Referencial COBIT 5 para la identificación de los riesgos en conjunto con la norma ISO 27001:2022 como fuente primaria. En este apartado, se busca establecer, implementar y mantener un sistema de gestión de seguridad de la información, estableciendo una política, procedimientos y controles que permitan cumplir con la aplicabilidad de un sistema de seguridad.

- Identificar las prioridades de la organización.
- Determinar el contexto de la organización.
- Crear una matriz de análisis FODA

Por otro lado, se busca crear un plan de continuidad de negocio, mediante un documento donde se detallen controles para minimizar riesgos en los que la empresa se pueda ver afectada ante una eventual interrupción del negocio, por tanto, dicho documento tiene como fin establecer medidas que garanticen la continuidad del negocio.

- Crear un documento con el contenido del plan de continuidad de negocio.
- Crear roles, responsabilidades y autoridades del equipo encargado de la continuidad del negocio.
- Crear una lista de contactos de las personas que participaran en el plan de continuidad del negocio. (Nombre, apellidos, rol, área y números de teléfonos).

Así mismo, se realiza un apartado para la gestión de riesgos y de acuerdo con los resultados obtenidos en la identificación de amenazas y vulnerabilidades, se propone diseñar controles de seguridad de información. Adicionalmente, la propuesta tiene la capacidad de reducir eventos indeseados y lograr la mejora continua en los procesos.

- Crear una tabla con la clasificación de los escenarios de activos que evidencie los criterios de riesgos y el impacto.
- Desarrollar un plan de tratamiento de riesgos, creando una matriz de clasificación, evaluación y respuesta a los riesgos.
- Crear una tabla del plan de tratamiento de riesgos.

Por último, se crea un apartado donde se detallan la política y controles de seguridad de la información según los problemas detectados en la empresa Copy Printer Advanced, se toma como base parte de los Objetivos de Control de los cuatro dominios que establece el Anexo A

del Estándar de la Norma ISO/IEC 27001:2022 y procesos relacionados a seguridad y ciberseguridad del Marco Referencial COBIT 5.

- Desarrollar una política de seguridad de la información. (propósito, estrategia, objetivo, lineamientos generales y reporte de incidencias).
- Desarrollar las políticas específicas de seguridad de la información, estableciendo normas técnicas para la Gestión y el Control de las Tecnologías de la Información, orientado en el modelo COBIT5. También, establecer controles organizacionales, de personas, físicos y tecnológicos, acorde a lo establecido en el anexo A de la norma 27001:2022.

Alcance metodológico

Previamente, se realizó una reunión con el gerente general de la empresa donde él mismo detalló los problemas que tiene en relación con la seguridad de información. Por lo que, ante la necesidad de un documento que establezca políticas de seguridad, se propone la implementación de un Sistema de Gestión de Seguridad de la Información donde se pueda establecer, mantener y mejorar procesos.

Para recolección de datos, se aplica una entrevista a los colaboradores de la empresa y así obtener resultados que permitan identificar debilidades, amenazas, fortalezas y oportunidades de la empresa.

Por otro lado, se hace una revisión documental de la norma ISO 27001 y COBIT 5 para guía de la identificación de riesgos, amenazas y vulnerabilidades, así mismo, para la creación de políticas de seguridad de la información.

Alcance tecnológico

Se requiere apoyo tecnológico para investigar temas relacionados con la propuesta, por lo que se utiliza Google Chrome para la búsqueda de fuentes de información relacionadas con las normas y otros documentos guías para definición de conceptos. También, se requiere de una computadora con programa Office 365 y Windows 10 o superior para la investigación y redacción del documento final.

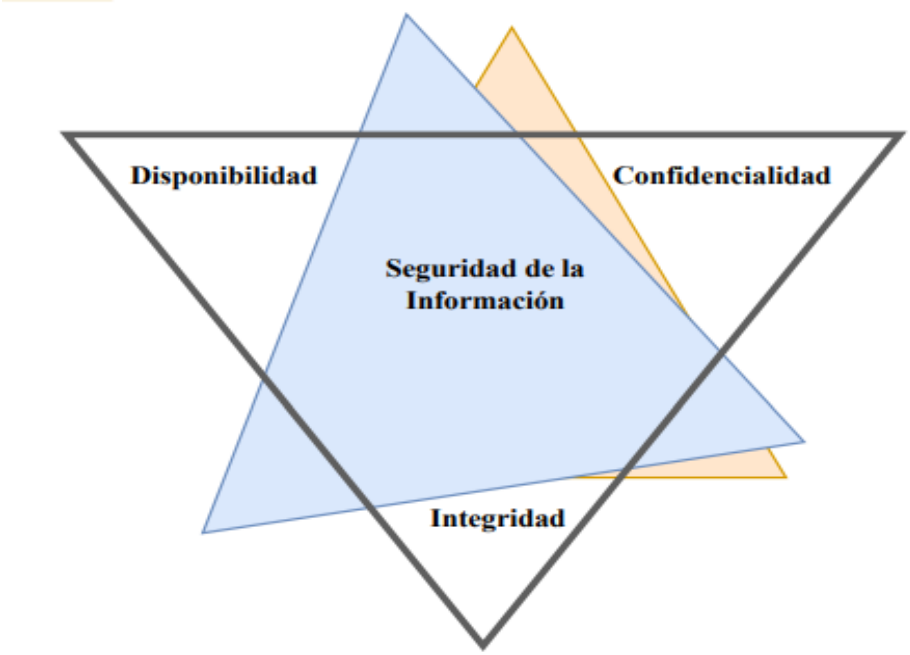
CAPÍTULO II. MARCO REFERENCIAL

En este capítulo, se muestra información sobre los principales conceptos que se estudian en esta investigación. En primera instancia, la empresa se sometió a una entrevista inicial, donde se definieron cuatro problemas de seguridad de la información, por lo que la principal referencia es implementar un Sistema de Gestión de Seguridad de la Información. Según Rojas-Pupo (2021):

> Se basa en una orientación a riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como en el análisis de los procesos claves de la organización para determinar planes y estrategias que garanticen la continuidad de la seguridad de la información. (p. 10)

Con la finalidad de lograr un mejor entendimiento de lo antes citado, se presenta la figura 1.

Figura 1. *Pilares de seguridad de la información.*



Fuente: Elaboración propia.

A los tres conceptos que anteriormente se mencionan, se les conoce en conjunto como la Triada de la seguridad de la información, y con ello se consigue que sea confidencial, es decir, que la información esté bien resguardada y con acceso restringido. También, hace referencia a

que la información debe estar completa y exacta; por último, debe ser accesible y estar a disposición cuando se requiera.

Los sistemas de información son mucho más que el "*mouse*" del ordenador y el *software*; por esta razón, es importante que las empresas cuenten con sistemas de gestión de seguridad de la información, donde se conozcan con claridad las políticas de seguridad. No obstante, y por la experiencia de robo de información a muchas organizaciones, se han implementado eventos que van más allá de la evolución de los servicios de información y comunicación, proporcionando resiliencia ante ataques informáticos, ya que en su mayoría ocasionan manipulación de datos y robo de la información, la cual es valiosa para dichas instituciones, ya que contienen datos sensibles de la población en la mayoría de los casos.

> La seguridad en la actualidad necesita ser altamente eficiente, una mayor conciencia sobre los riesgos ayuda en la toma de decisiones, los riesgos pueden ser identificados, evaluados y atenuados. El conocimiento es la clave para mantener políticas de seguridad efectivas y buenas prácticas de prevención de riesgos con enfoques de mejora continua y por ello la implementación un Sistema de Gestión de la Seguridad de la Información es imprescindible en las organizaciones. (Martín, 2021, p. 496)

Por tanto, es importante que las empresas implementen un Sistema de Seguridad de la Información, mediante normas y marcos referenciales que rigen los procesos y guías de buenas prácticas, para minimizar eventos que pueden ocasionar daños en los activos de información. Para lo cual, es necesario contar con el personal capacitado en el área de seguridad informática, pues es requerido para aplicar modelos de seguridad de la información, donde se conozca el objetivo de disponer políticas de seguridad según la necesidad del negocio.

> El avance de la tecnología y el poco conocimiento para contrarrestar las amenazas y riesgos de ataques ha provocado pérdidas cuantiosas en las compañías, por ese motivo se han explotado esas vulnerabilidades para provocar ataques informáticos que atentan con la continuidad de las actividades de las empresas debido a esto las empresas deben de contar con tecnologías que aumenten y protejan la seguridad de la información en las mismas. (Andrade y Chávez, 2018, p.16)

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) establecen la norma ISO/IEC 27000 y su familia de normas, como un

documento para la gestión de seguridad que sirve de guía de buenas prácticas en la implementación de un sistema de seguridad de la información, ya que permiten identificar oportunamente posibles riesgos a los que se podrían enfrentar las empresas. Aunque con la aplicación de un Sistema de Gestión de Seguridad de la Información basado en una norma de seguridad no se garantiza que la empresa esté 100% segura ante posibles amenazas, sí se minimizan las vulnerabilidades y permite tener el conocimiento guía para garantizar la continuidad de los servicios.

> Es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (ISO/IEC 27000, 2018). Es una norma internacional comúnmente usada debido a lo adaptable que es su aplicación en las organizaciones, ayuda a evaluar e implementar un sistema de seguridad mediante una serie de procedimientos que tienen como fin, proteger la información. (Sánchez-González, 2020 p.29)

Con respecto al documento estándar internacional ISO 27001:2022, es donde se abarcan los 4 dominios y 93 controles que establece la norma. Para mejorar la norma ISO 27001, se ha actualizado continuamente según la necesidad del entorno, prevaleciendo la confidencialidad, integridad y disponibilidad, para la seguridad de la información, que se consigue con la implementación de unos requisitos, a fin de detectar riesgos mediante un Sistema de Gestión de Seguridad de la Información.

Por su parte, en la presente investigación se ven integradas las cinco normas de la familia ISO 27000, mismas que proporcionan apoyo y guía mediante la evaluación, para mantener, establecer y mejorar un Sistema de Gestión de Seguridad de la Información. A continuación, se menciona la relación que tiene cada una de ellas, con respecto a la norma ISO 27001:

ISO 27001: la última actualización de esta norma fue en el año 2022 donde se redujo a 4 dominios, que proporcionan controles para protección de la privacidad, ciberseguridad y seguridad de la información, con el fin de establecer requisitos generales para la implementación de un Sistema de Gestión de Seguridad de la Información. Por tanto, en lo que se refiere a esta norma:

> La norma ISO/IEC 27001 es aplicable a cualquier tipo de organización, independientemente de su naturaleza, tamaño o sector de actividad. Esta norma detalla los requisitos necesarios para establecer, implementar, mantener y mejorar constantemente un Sistema de Gestión de Seguridad de la información (SGSI), considerando los objetivos y riesgos de la organización. Igualmente, ofrece flexibilidad en el cumplimiento de los requisitos, lo que facilita la utilización de diferentes metodologías. (Gómez y Fernández, 2018)

ISO 27002: guía para la implementación de controles necesarios para implementar un Sistemas de Gestión de Seguridad de la Información, descritos en el Anexo A de la norma ISO 27001. De acuerdo con Abad-Chávez y Cruz-Calderón (2022):

> El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. (p.28)

ISO 27003: esta norma es la principal guía de buenas prácticas para el diseño e implementación de un Sistemas de Gestión de Seguridad de la Información, tomando en cuenta los requisitos que establece la norma ISO 27001. Por su parte, Torres-Romero (2021) indica que la norma ISO 27003: “Es la guía de implementación de un SGSI e información acerca del uso del ciclo Deming (PDCA), el propósito es orientar hacia una buena implementación efectiva del modelo de seguridad” (p.49).

ISO 27004: proporciona métricas para la evaluación de un Sistema de Gestión de Seguridad de la Información, de acuerdo con los controles del Anexo A de la norma ISO 27001, tal como lo indica Tovar-León (2019):

> En este estándar se especifican las técnicas de medida y las métricas que son aplicables a un Sistema de Gestión de Seguridad de la Información y los controles relacionados. Las métricas se utilizan para la medición de los controles implementados de acuerdo al anexo A. (p.27)

ISO 27005: es la principal guía de gestión de riesgos para la seguridad de la información y establecer requisitos en los activos de la empresa.

> Norma de apoyo a conceptos generales que vienen especificados en la ISO 27001, diseñada para ayudar a aplicar la seguridad de la información basada en un enfoque de gestión de riesgos. Se puede aplicar a todo tipo de organizaciones e implica conocer todos los conceptos, modelos, procesos y términos descritos en la norma ISO 27001 e ISO 27002. (Tovar-León, 2019, p.28)

Por otro lado, el Marco Referencial COBIT 5 se basa en cinco principios con el fin de alcanzar los objetivos propuestos en la gobernanza. De acuerdo con León-Manzanares y Puma-Sañomamani (2022), los principios de COBIT 5 son:

- Satisfacer las necesidades de las partes interesadas: Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficio y la optimización de los riesgos y el uso de recursos, por tanto, COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI.
- Cubrir la empresa de extremo a extremo: COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, cubre todas las funciones y procesos dentro de la empresa, además, considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin.
- Aplicar un marco de referencia único integrado: Existen muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.
- Hacer posible un enfoque holístico: Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos.
- Separar el gobierno de la gestión: El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. (p. 22)

Por su parte, Albornoz-Cabrera (2022) argumenta sobre dicho modelo lo siguiente:

> COBIT 5 proporciona un marco integral que ayuda a las organizaciones a lograr sus objetivos corporativos de gestión de TI. En pocas palabras, ayuda a las empresas a crear un valor óptimo a partir de la tecnología de la información mientras equilibra la generación de ganancias, optimiza los niveles de riesgo y la utilización de recursos. COBIT 5 permite que la TI sea operada y administrada de manera integral en toda la organización, cubriendo todas las áreas funcionales de TI y de negocio de las que es responsable, teniendo en cuenta los intereses de TI de las partes interesadas, tanto internas como externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, comerciales, sin fines de lucro o del sector público. (p.42)

Aunado a lo anterior, el marco de referencia COBIT se puede definir como una guía de buenas prácticas para el control de los activos de información. Así mismo, está relacionado con la gestión de riesgos y también, con la continuidad de negocio mediante la gobernanza. Por esta razón, muchas organizaciones buscan desarrollar e implementar un modelo como este, para obtener beneficios ante posibles riegos, debido a que, con la identificación prematura, se puede minimizar el impacto negativo que afecta los activos de información de la empresa. Otro argumento por destacar es el de Perales-Barrios (2020), al mencionar lo siguiente:

> COBIT 5 proporcionará un marco integrador de gobierno y administración de tecnología de información necesarios e importantes. Ya que, un marco general único sirve como una fuente integrada y consistente de guía en un lenguaje común, no usando términos técnicos. Isaca, Asociación de Auditoría y Control de Sistemas de Información, busca en este principio facilitar al usuario de COBIT 5 con el mapeo de prácticas y actividades de referencias de terceros. (p.40)

Sin duda alguna, al aplicar el modelo COBIT se ven involucradas las partes interesadas a nivel interno, como la alta Gerencia y proveedores. Además, en el entorno externo se involucran los regulares, esto con el fin de lograr mejoras en la toma de decisiones y prácticas sanas para proveer beneficios a la empresa.

Considerando que la norma ISO/IEC 27001:2022 y el Marco Referencial COBIT 5 son normativas para asegurar la calidad de todos los servicios prestados y los productos de las empresa de acuerdo con las necesidad, utilizando las mismas metodologías de desarrollo, debidamente documentados y sujetos a los correspondientes procesos de seguimiento y

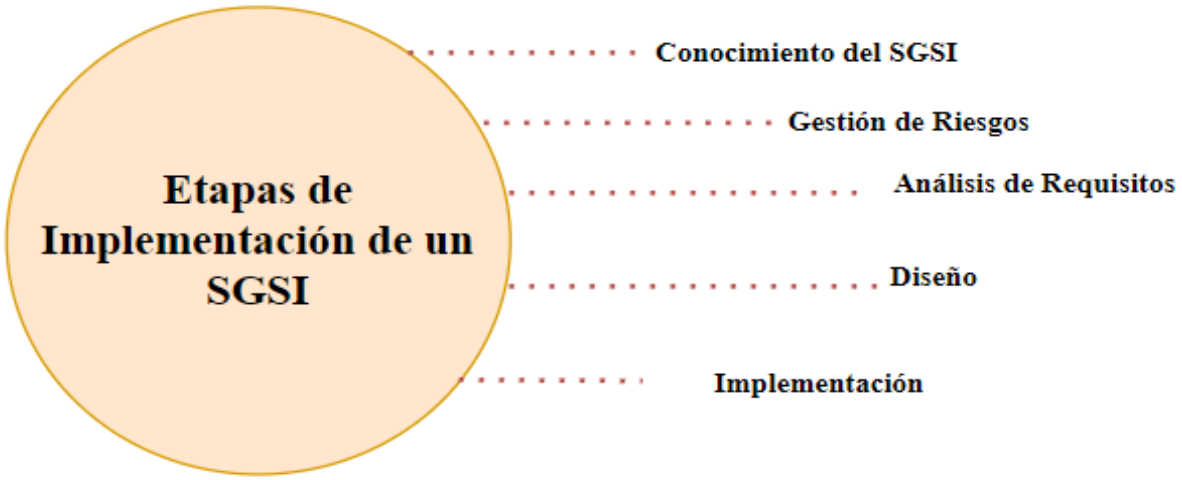
evaluación, para que los productos y servicios sean elaborados de acuerdo con los requerimientos de las expectativas, centrado en la eficiencia y la mejora continua; el Ministerio de Innovación, Tecnología, Telecomunicaciones de Costa Rica (MICITT) diseñó un marco normativo donde establecen las normas técnicas para la gestión y el control de las tecnologías de la información, con el objetivo de que las instituciones proporcionen la agilidad necesaria para detectar y responder ante las necesidades internas y de la comunidad, mediante la gobernanza de TI, gestión de riesgos entre otros, en el cual se ven involucradas las normativas COBIT 5 y ISO 27001. Por tanto, se considera dicho documento como guía para la propuesta.

Dicho lo anterior, para la implementación de un Sistema de Gestión de Seguridad de la Información, según la norma ISO 27001, se establecen cinco etapas, que son:

- Conocimiento del Sistema de Gestión de Seguridad de la Información.
- Gestión de Riesgos.
- Análisis de Requisitos.
- Diseño.
- Implementación del Sistema de Seguridad.

Sin embargo, es necesario aclarar que la investigación se basa únicamente en los primeros cuatro puntos, ya que lo que se está formulando es una propuesta.

Figura 2. *Etapas de Implementación.*



Fuente: Elaboración propia.

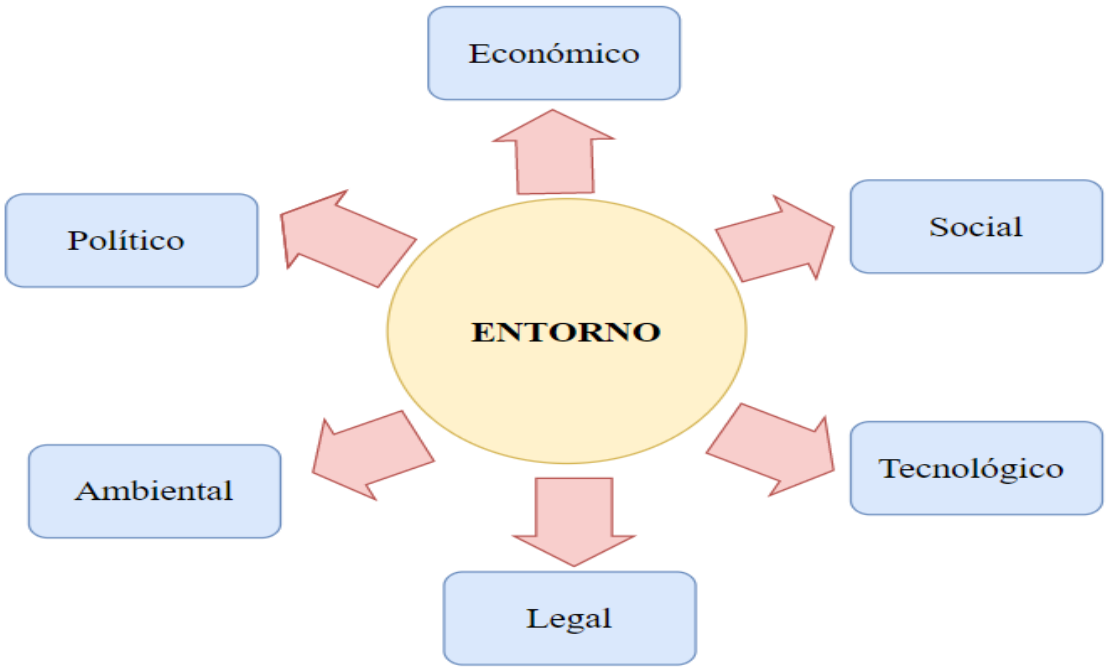
Conocimiento del Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001:2022

Determinar el contexto de la organización se basa en conocer el entorno en el que se encuentra la empresa, realizando un estudio que permita identificar las debilidades, amenazas, fortalezas y oportunidades.

> Ante estos desafíos, las organizaciones tienen la obligación de ser lo suficientemente flexibles para transformar toda la estructura de negocios, y así responder a cambios estratégicos y retos del mercado. En tal sentido, para alcanzar una posición de ventaja competitiva, se necesita examinar de manera crítica el entorno, con el objetivo de identificar oportunidades externas y crear capacidades internas; se ha pasado de ser organizaciones estáticas a insertarse en un mundo dinámico, con altas exigencias que demandan una visión sistémica e integral. (González et al., 2019, p. 243)

Adicionalmente, las organizaciones están expuestas a diferentes perspectivas que en algunas situaciones pueden afectar la capacidad para lograr resultados exitosos. Destacando que los principales problemas se pueden presentar a lo interno y externo de la organización.

Figura 3. *Tipos de entorno a los que se exponen las organizaciones.*



Fuente: Elaboración propia.

Por lo que se refiere a entornos de la organización, se destaca el valioso aporte de Nery-Kameta et al. (2019), pues consideran situaciones vinculantes con la temática antes mencionada, argumentando que:

> Las nuevas organizaciones, las nuevas personas y la progresiva globalización se encuentran asociadas con las emergentes economías, y la innovación humana y el progreso tecnológico, el cual ofrece un panorama del marco del entorno de mercado donde las organizaciones desean tener permanencia. Sin embargo, es una evolución que se ha dado por las megatendencias, que tienen como característica el comercio internacional y la expansión, por lo que es importante el papel que desempeña la organización al enfrentar estos cambios, ya que las nuevas organizaciones son el motor de la economía actual, más ahora que es evidente la importancia del intercambio de bienes y servicios entre naciones, como bien puede ser organizaciones y personas, las cuales todas estas se encuentran inmersas en la nueva era de la información y que ya no se pueden seguir las mismas prácticas organizacionales clásicas, pues nos encontramos en nuevos contextos y tendencias. (p.27)

En este sentido, el comportamiento de las empresas depende en gran medida de las condiciones de los diferentes entornos, por lo que es necesario efectuar estudios constantes sobre la afectación, ya sea positiva o negativa, que estos tengan en la operación de los negocios; misma que puede darse a nivel interno o externo, para lo que también existen diversas herramientas empresariales útiles que miden dichos efectos. Indudablemente, los entornos son cambiantes y cada día más exigentes, por lo tanto, surge la necesidad de investigarlos continuamente, con la finalidad de no perder vigencia en el mercado en el cual se está operando, lo que también supone una ardua labor para quienes administran o son propietarios de empresas.

Por tanto, se presentan, a continuación, diferentes aportes sobre el entorno económico, social, tecnológico, legal, ambiental y político, destacando sus principales características o variables que influyen en cada uno de ellos.

Entorno económico: con respecto al entorno económico de una organización, Plá-Ayora (2023) alude a que:

> El modelo de consumo mundial contemporáneo se transforma gradualmente en uno que respeta los límites naturales del planeta. El énfasis en el desarrollo

> económico se reorienta hacia la búsqueda del bienestar, lo que reduce las desigualdades sociales tanto entre los países como dentro de ellos. Hace uso de tecnologías de captura de carbono y alcanza emisiones negativas. (p. 63)

En definitiva, lo económico representa un elemento de gran valía, tanto a nivel interno como externo de las organizaciones, por lo tanto, los cambios en este se convierten en ventaja o desventaja para las empresas En este sentido, toma fuerza el poder adquisitivo de las personas y las diferentes necesidades a satisfacer, de acuerdo con la dinámica cotidiana de los hogares, puesto que el recurso monetario es el que dinamiza la economía. Asimismo, ocurren eventos en determinadas regiones, que afectan de forma directa e indirecta las operaciones de los negocios, lo que trae consigo alza en los precios de la materia prima, más impuestos o aranceles, escasez de productos y servicios, restricciones al comercio, baja rentabilidad de los negocios, cambios en las políticas monetarias y cambiarias, entre otros elementos.

Entorno social: el siguiente punto trata sobre el entorno social, para lo cual Vecdis Tecnogestion (2021) argumenta que:

> Los factores sociales o socioculturales son aquellos que tienen que ver con la realidad social del lugar dónde se ubica la empresa. En este caso, los estudios serán sociólogos. Ejemplo de ello son la movilidad social, estilo de vida, nivel educativo, religión, distribución de la renta, hábitos de consumo, entre otros. (p.4)

Aunado a lo anterior, es preciso mencionar que las empresas, al intentar establecerse en un determinado lugar, es necesario que efectúen estudios sobre la población que allí habita, así como de sus alrededores, debido a que muchas de ellas traen consigo ideas de negocio, que pueden ser o no aceptadas por las personas, debido a su sistema de creencias, valores e ideologías, o bien aspectos culturales que les impiden determinadas situaciones o comportamientos; esto en referencia a lo externo. Sin embargo, al interior de las organizaciones, se deben propiciar ambientes laborales acogedores para los trabajadores, condiciones dignas para ejercer sus funciones, oportunidades de aprendizaje y crecimiento a través de diferentes herramientas, así como incentivos que generen la motivación de las personas.

Entorno tecnológico: otro de los entornos que se encuentra en auge es el tecnológico, el cual hace que las empresas sean cada vez más competitivas en el mercado; por ello, Arrieta et al. (2021) resaltaN que:

> La tecnología es cambiante y cada vez más innovadora, la cual se ha convertido en un elemento fundamental en el ámbito empresarial, por tal razón las organizaciones deben aprender a acomodar sus estrategias basadas en niveles tecnológicos que faciliten el buen uso de estas y les permita a las empresas romper barreras, resolver problemas, facilitando el crecimiento de las organizaciones y su nivel de competitividad. (p.249)

Sin lugar a duda, la tecnología se ha convertido en una de las herramientas más importantes y destacadas en los diferentes ámbitos de la vida tanto personal, laboral como empresarial, por ello surge la necesidad de estar en sintonía con los diferentes cambios y avances que presenta, con la finalidad de ofrecer a los clientes mejores productos, servicios, experiencias, entre otras cuestiones de interés. Dichos cambios han provocado transformaciones drásticas en el comportamiento de las personas físicas y jurídicas.

No obstante, a pesar de que el ámbito tecnológico genera grandes posibilidades de crecimiento e innovación, trae consigo una serie de problemas, en los cuales se ven amenazados los datos e información de los individuos; prueba de ello son los diversos ataques cibernéticos ocurridos a instituciones gubernamentales del país, lo que también provoca que las entidades preparen planes ante este y otros riesgos, así como preparar los sistemas informáticos y al personal para disminuir las afectaciones negativas.

Entorno legal: en relación con el entorno legal, Flores y Núñez (2023) mencionan que:

> Cualquier proyecto de pre-factibilidad requiere la realización de un estudio legal el cual consta de una serie de reglas y códigos en materia legal, civil y penal. Este estudio legal es fundamental para el proceso de constitución y operación de la empresa, este estudio permite conocer ampliamente la legislación que compete al proyecto en cada una de sus etapas. (p.37)

Es así como las organizaciones deben conocer a profundidad la legislación aplicable en Costa Rica, de acuerdo con la naturaleza de sus negocios, con la finalidad de acatarlas y no incurrir en problemas legales por incumplimiento a la normativa vigente. A pesar de que algunas leyes generan desventajas en determinadas empresas e incluso provocan la quiebra, sirven para

regular el mercado de bienes y servicios, asegurando a la población la producción y comercialización de productos de alta calidad y bajo estándares permitidos. De igual forma, desde el ámbito empresarial, se requiere de la aplicación de leyes que norman el actuar de los patronos y colaboradores ante las diversas situaciones que se presenten, por lo tanto, allí toman fuerza los derechos y obligaciones de ambas partes.

Entorno político: en lo que respecta al entorno político, Torres (2019) afirma que en este:

> Se analizan los factores asociados a la clase política que influyen en la actividad futura de la empresa, y pueden ser: las subvenciones públicas dependientes de los gobiernos, la política fiscal de los diferentes países, las modificaciones en los tratados comerciales y posibles cambios de partidos políticos en los gobiernos, y sus ideas sobre la sociedad y la empresa. (p.6)

El aspecto político siempre ha sido un tema de debate para diversos sectores de la sociedad, pues claramente muchos aspectos en los que interfiere dicha temática repercuten en el quehacer de las empresas, mismas que sostienen la economía del país y el mundo. Por lo tanto, es preciso conocer el plan de trabajo de quienes gobiernan la nación, y con ello analizar las posibles afectaciones en los negocios, y de ser necesario, acudir a las entidades correspondientes con el propósito de exponer asuntos determinantes y generar un consenso entre ambas partes.

Entorno ambiental: por otra parte, se describe el entorno ambiental de una organización, en el cual Amador (2022) asegura que:

> Los aspectos ecológicos tienen que ver con todos los factores relacionados directa o indirectamente con el medioambiente. Cualquier cambio en la regulación gubernamental o tendencias sociales para la protección del medioambiente afectan a la empresa. Así mismo, se pueden mencionar leyes sobre el uso de la energía, la conservación del ambiente, la gestión de residuos y la emisión de gases, entre otras. (p.2)

Tal como lo menciona Amador (2022), existen determinadas regulaciones o bien legislación que se vinculan con el medioambiente, el cual es un tema de gran interés a nivel global, por lo tanto, las empresas deben efectuar sus operaciones, considerando generar el menor impacto posible en el ambiente, pues de este obtiene los recursos para su actividad productiva y comercial. Por otro lado, es necesario indicar que, a lo largo de los años, suceden fenómenos

naturales que afectan los negocios, por lo que se debe prever planes ante tales eventualidades, llámese inundaciones, deslizamientos, huracanes, ondas tropicales, incendios forestales, entre otros.

Definitivamente, las empresas deben gestionar acciones o estrategias en pro del medioambiente donde desarrolla la actividad económica, con el propósito de contribuir con la preservación de este, para que las futuras generaciones puedan gozar de los diferentes recursos y vivir en un entorno que pueda catalogarse como deseable, limpio u óptimo, para llevar a cabo las actividades cotidianas.

Gestión de riesgos basada en la Norma ISO 27001:2022 y el Marco Referencial COBIT 5

En relación con la gestión de riesgos, existen acciones para tratarlos, permitiendo identificar y formular un plan de tratamiento de riesgos, a fin de evitar que se materialicen en los Sistemas de la Información.

> La tecnología de la información ha venido tomando interés en los últimos años por su función de brindar soporte, sostenibilidad y crecimiento empresarial, evaluando riesgos y generando valor, de esta manera COBIT es un Marco de trabajo de Gobierno y Gestión que ha evolucionado con los años y en esta última versión ha permitido que otros estándares del mercado entren a mejorarlo; optimizando y fortaleciendo el Gobierno y la Gestión generando más valor a los interesados. (Carrascal, 2023, p.17)

Asociado a lo anterior, el Marco Referencial COBIT permite minimizar que el riesgo relacionado con el uso de tecnologías de información en una organización sea identificado y que se realice la gestión correcta, para asegurar la continuidad del negocio. El riesgo es una incertidumbre, no obstante, Ávila y Caloggero (2022) indican:

> Los riesgos tecnológicos se encuentran subestimados en los procesos de negocio, estos normalmente son apartados a especialistas técnicos y se debe tener en cuenta que juegan un papel sumamente crítico en la protección de información por lo cual la dirección requiere mantener reglas y políticas las que aseguren los objetivos del negocio y que prevengan posibles eventos no deseados, se detecten con tiempo y se corrijan. Asimismo, esto conlleva a implementar un plan de riesgos para las tecnologías de información. (p.2)

Adicionalmente, es importante mencionar que el marco referencial COBIT 5 establece un modelo de evaluación de 37 procesos y 5 dominios, tales como procesos de evaluar, dirigir y monitorear (EDM); así mismo, procesos de alinear, planificar y organizar (APO), procesos de construir, adquirir e implementar (BAI), procesos de entregar, servicio y soporte (DSS) y procesos de supervisar, evaluar y valorar (MEA).

En contraste con lo anterior, para el desarrollo de la propuesta, se utilizan procesos de entregar, servicio y soporte (DSS) y también, procesos de alinear, planificar y organizar (APO). En síntesis, los dominios DSS05, DDS06 y APO13 son los que se aplican en este documento, ya que son procesos que garantizan la seguridad y ciberseguridad del negocio.

El Marco Referencial COBIT 5 y la Norma ISO 27005 que especifica a la norma ISO 27001 la implementación de un Sistema de en Información en cuanto a gestión de riesgos establecen criterios cualitativos y cuantitativos visuales para evaluar el nivel riesgo en los activos de información, por esta razón, Peñaloza (2019) indica que:

> El estudio ayudará a identificar el valor de incidencia que tiene cada una de las variables analizadas sobre la operatividad de la empresa, representando un riesgo inherente a su giro de negocio, riesgo sobre el cual se planteará la propuesta metodológica del ciclo para la gestión operativa en las diferentes empresas objeto de estudio, permitiendo que se optimicen los recursos que intervienen en los procesos empresariales y cumplir con sus objetivos de manera eficaz, eficiente, oportuna. (p.4)

Definitivamente, es importarte la buena práctica de la valoración y tratamiento de riesgos, ya que permite identificar la magnitud del impacto y la probabilidad de ocurrencia ante una situación prevista. Por consiguiente, COBIT 5 establece criterios cualitativos y cuantitativos visuales, para el cálculo de la evaluación de riesgos a través de una tabla.

Tabla 1. *Criterios probabilidad de ocurrencia*

Probabilidad de Ocurrencia			
Criterio Cualitativo	**Descripción**	**Criterio Cuantitativo Visual**	**Valor Porcentual**
Poco probable	Podría ocurrir algunas veces (Pocas veces)	1	**33%**
Probable	Puede ocurrir en algún momento	2	**66%**
Muy Probable	La expectativa de ocurrencia se de en la mayoría de las circunstancias	3	**100%**

Fuente: Elaboración propia.

Tabla 2*. Criterios magnitud del impacto*

Magnitud del Impacto			
Criterio Cualitativo	**Descripción**	**Criterio Cuantitativo Visual**	**Valor Porcentual**
Bajo	Hay una indisponibilidad entre 15 y 30 minutos	1	**33%**
Considerable	Hay una indisponibilidad entre 30 y 60 minutos	2	**66%**
Alto	Hay una indisponibilidad por mayor a 60 minutos. Es necesario un establecer un mecanismo de procesamiento alterno	3	**100%**

Fuente: Elaboración propia.

A su vez, el nivel de riesgo es la combinación del resultado de probabilidad e impacto, ante esto, según el resultado del riesgo, se puede dar la pérdida de confidencialidad, integridad y disponibilidad de la información. Según León-Acurio et al. (2018) en relación con el marco referencial COBIT 5:

> COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho

> de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. (p.21)

Por otra parte, la gestión de riesgo permite medir, edificar y clasificar, para establecer políticas de seguridad de información y procedimientos, donde el riesgo se mide en términos de impacto y probabilidad. Por ende, el primer punto para calcular el riesgo es realizar un inventario de activos y clasificarlos.

Figura 4. *Fórmula para calcular el nivel de riesgo.*

Fuente: Elaboración propia.

Para llegar a la conclusión del nivel de riesgo, se deben estudiar una serie de procesos, los cuales se enlistan de la siguiente forma:

- Identificar los activos de información.
- Propietarios de activos de información.
- Identificar amenazas de los activos de la información.
- Identificar vulnerabilidades de los activos de la información.
- Y controles existentes.

Los activos en la seguridad información se refieren a todo lo que tiene valor en la empresa, tales como activos físicos, tecnológicos, de personas y de información, que están expuestos a amenazas. Seguidamente, se mencionan algunos ejemplos:

- *Hardware.*
- *Software*.
- Redes.
- Organización.
- Información física.
- Información digital.

- Información trasmitida digitalmente.
- Instalaciones.

Las amenazas son causa de un incidente que compromete los activos y la seguridad de información, mediante las premisas de confidencialidad, integridad y seguridad de información. Estas están presentes en el entorno, gracias al crecimiento de las tecnologías de información y datos que hoy se conocen como *big data.* Al respecto, Balseca et al. (2021) resaltan que:

> La tecnología continuará evolucionando, las organizaciones seguirán siendo cada vez más dependientes de las TIC, por consecuencia las amenazas relacionadas a dichos avances se mantendrán e inclusive podrán aumentar debido a configuraciones técnicas deficientes, la inadecuada gestión o la falta de capacidades y competencias técnicas de los proveedores de las tecnologías. El análisis de grandes cantidades de datos en el área de la seguridad de la información es considerado como un área de trabajo reciente, y requiere de una amplia investigación, así como establecer una arquitectura tecnológica que ofrezca una alta capacidad de almacenamiento, flexibilidad técnica y con una inversión de capital menos costosa, para hacer frente a las amenazas informáticas, con el apoyo del análisis de datos con herramientas de Big Data. (p.166)

Adicionalmente, las amenazas se presentan por varios factores, las cuales en muchas ocasiones no se pueden controlar, pero sí reducir el riesgo al que se exponen. Por tal motivo, el identificar las amenazas permite identificar vulnerabilidades en los activos; algunos ejemplos son:

- Desastres naturales.
- Fallas en los sistemas de información.
- Ataques cibernéticos.
- Ilegalidad de software.
- Fraude.
- Accesos no permitidos.

Las vulnerabilidades son debilidades de los activos, que están expuestos a una amenaza y causan un mayor impacto, en muchas ocasiones se da la pérdida de datos, pérdidas materiales,

entre otros, así como la reputación de la empresa. En lo que respecta a vulnerabilidad, Guevara et al. (2023) argumentan que:

> La identificación de las vulnerabilidades es sumamente importante debido a que nos muestra los posibles caminos que un atacante podría explotar y aquellos activos que la empresa y/o persona ofrece. El desconocimiento sobre la seguridad de información puede resultar muy perjudicial sobre todo para una empresa debido a la información que manejan y las consecuencias que pueden surgir económicamente y en su reputación en caso sufran de un ciberataque, aspectos como la falta de control de accesos o la demora en las actualizaciones de sus aplicativos contribuyen a aumentar la posibilidad de sufrir una amenaza. (p.12)

Por tanto, las amenazas están ligadas a las vulnerabilidades, mismas que pueden manifestarse a lo interno y externo de la organización, para ello, a continuación, se muestran ejemplos:

- Ausencia de políticas de seguridad de la información.
- Ignorancia de un plan de continuidad de negocio.
- Desconocimiento de la importancia de la seguridad.
- Defectos en controles de acceso.
- No existen respaldos de la información.
- Ausencia de medidas frente ataque informáticos.
- Falta de medidas ante desastres naturales.
- No existe segregación de funciones.
- Desconocimiento de la prevención de fuga de datos.

Tabla 3. *Riesgos de los activos de información*

Activo de Información	Amenaza	Vulnerabilidad
Edificio.	Terremotos.	Construcción insegura del edificio.
Datos Financieros.	Divulgación de información.	Ausencia de políticas de seguridad de la información.
Equipos de comunicación.	Error de uso.	Falta de capacitación a usuarios.
Empleados.	Fraudes.	Defectos en controles de acceso.

Fuente: Elaboración propia.

Análisis de requisitos para la implementación de un Sistema de Gestión de Seguridad de la información

Con respecto al análisis de requisitos, es importante que la organización cuente con recursos, competencia, concienciación, comunicación e información documentada, con el fin de una buena gestión de un Sistema de Gestión de Seguridad la Información, bajo la norma ISO 27001 y el Marco de Referencia COBIT 5. A continuación, se detallan los requisitos mencionados anteriormente:

- Recursos: la organización debe contar con los recursos necesarios para mantener y dar seguimiento al Sistema de Gestión de Seguridad de Información.
- Competencia: la organización debe contar con el personal capacitado, para dar seguimiento al plan del Sistema de Gestión de Seguridad de Información competente, basándose en la formación, educación y experiencia. También, es de suma importancia que cuente con recurso humano idóneo, para realizar auditorías y que sea capaz de evaluar y conservar los objetivos propuestos.
- Concienciación: primeramente, debe existir compromiso de la alta Gerencia, para llevar a cabo lo establecido en el Sistema de Gestión de Seguridad de la Información, por lo tanto, todo el personal de la organización tiene que estar informado de las políticas de seguridad de la información y conocer de las implicaciones de cumplir los requisitos del sistema.
- Comunicación: La organización debe comunicar a las partes internas y externas, para cumplir con los objetivos del Sistema de Gestión de Seguridad de la Información, donde se incluyan procesos del contenido de la comunicación, cuándo y a quién comunicar.
- Información: la organización debe asegurar cuando se genera y actualiza la información documentada. Por lo que la información documentada debe contar con el formato requerido, la revisión y aprobación de las partes interesadas. Además, se debe asegurar que la documentación esté disponible cuando se necesite y mantenerla protegida, es decir, que cumpla con los criterios de seguridad de información.

Diseño de políticas de seguridad de información

Una vez analizadas las necesidades de la empresa y contemplando el contexto al que la empresa se enfrenta, se debe considerar diseñar políticas de seguridad de información que permitan establecer procedimientos, controles y buenas prácticas adecuadas para el manejo de esta. Al respecto, Toro-Castillo (2023) indica que, para garantizar la seguridad:

> Es donde las entidades deben diagnosticarse para conocer su esto de madurez, conocer si tienen políticas de seguridad aplicadas e incluso debe diseñar su propia política de seguridad, definiendo responsabilidades y tareas por cada grupo, teniendo en cuenta lo propuesto por gobierno en línea dentro de su metodología, sobre todo en sus procesos misionales; las entidades deben tener un plan de contingencia en cuanto a seguridad de datos y una debida manipulación de ellos; es decir la única forma de poder brindar confianza a los ciudadanos y garantizar el buen uso de su información, es aplicado todo un modelo de seguridad ya sea el MSPI Modelo de Seguridad y Privacidad de la información definido por MINTIC, o la certificación de la norma ISO 27001, en todas sus fases desde el diagnostico hasta los procesos de evaluación y mejora continua de cada uno de los riesgos, todo esto acompañado de herramientas de TI que acompañen estos procesos, es decir una buena parte de ejecución de los presupuestos de TI ahora van dirigidos a asegurar y salvaguardar la información. (p.14)

Es importante que Copy Printer Advanced pueda mitigar los riesgos de información técnica y comercial al implementar políticas de seguridad de la información para la empresa, considerando todos los aspectos de amenazas, riesgos y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. En lo que respecta a políticas de seguridad de la información:

> COBIT es un marco de referencia para el gobierno y la gestión de la información y la tecnología, dirigido a toda la empresa, define los componentes para crear y sostener un sistema de gobierno: procesos, estructuras organizativas, políticas y procedimientos, flujos de información, habilidades e infraestructura; con COBIT al definir un diseño de gobierno permitiría a la empresa u organización observar y definir los aspectos importantes dentro de la institución para crear un sistema de

> gobierno adecuado. (ISACA, 2019b, citado por Alvarado-Sarango y Andrade-López, 2021, p. 273)

Por lo tanto, la política es una medida que se debe cumplir, para que la organización alcance sus objetivos propuestos, donde se ven involucradas las partes internas de la compañía. En conclusión, para la propuesta se crean políticas, tomando como referencia los controles del Anexo A Normativo ISO 27001:2022 y el Marco Referencial COBIT 5 de los controles APO13, DSS05 y DSS06 que garantice la seguridad de la información, minimizando el riesgo. A continuación, se describen dichos controles:

Controles organizacionales: en materia de controles organizacionales, se busca proponer lineamientos para la gestión de la seguridad de la información orientados a orientar y apoyar la gestión de la seguridad de la información según los requerimientos de las empresas.

Controles de personas: se busca recomendar controles para la capacitación permanente del personal y responsabilidades, un ejemplo, son los acuerdos de trabajo que deben definir las responsabilidades del personal y de la organización en materia de seguridad de la información.

Controles físicos: se propone establecer controles físicos diseñados para implantar procedimientos que busquen proteger el lugar de trabajo, tales como seguridad física de oficinas e instalaciones, protección contra amenazas físicas y ambientales, entradas físicas, perímetros de seguridad, entre otros.

Controles tecnológicos: se propone recomendar medidas idóneas para proteger los datos que se generan en la organización y así asegurar los recursos de información de ataques informáticos y otros riesgos asociados que comprometan a los activos de información. Además, proteger los sistemas y aplicaciones de información.

Controles de seguridad y ciberseguridad:

- ***APO13: Gestionar la seguridad.*** En lo que respecta a la gestión de la seguridad en una organización, permite reducir el riesgo al que se enfrentan continuamente en torno a lo interno y externo de la organización, como lo indica Beleño-García (2023), el proceso de control APO13: Gestionar la seguridad:

  > Busca mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de tolerancia de riesgo de la empresa, estableciendo y manteniendo un SGSI, definiendo y administrando un plan de

tratamiento de riesgos de la seguridad de la Información, y monitoreando y revisando el SGSI. (p.35)

- ***DSS05: Gestionar los servicios de seguridad.*** En relación con la gestión de los servicios, son la base para que el negocio pueda ofrecer los servicios sin interrupciones, por tanto, la gestión de los servicios de seguridad busca proteger a la organización de robo y pérdida de la información. Según Sianipar et al. (2018), DSS05 indica: "Este proceso protege la información de la empresa, manteniendo un nivel aceptable de riesgo de seguridad de la información en la empresa de acuerdo con las políticas de seguridad" (p.193).
- ***DSS06: Gestionar los controles de procesos de negocio.*** En cuanto a las organizaciones, deben incluir el análisis y seguimiento de procesos para identificar fallas y oportunidades de mejora y rendimiento en los servicios que ofrecen. Considerando a Jarsa y Christianto (2018), mencionan que el proceso DSS06: "determina controles de procesos de negocio apropiados para asegurar que la información relacionada sea procesada en relación con el negocio de la empresa" (p.283).

CAPÍTULO III. MARCO METODOLÓGICO

Enfoques de la investigación

El enfoque determina el camino que va a llevar la investigación, es el punto de vista desde el cual se observa el tema para obtener un resultado. Adicionalmente, brinda apoyo para realizar el análisis y alcanzar resultados que ayudarán en el diseño y estructura de un tema determinado. A continuación, se describen los tres tipos de enfoques más utilizados para el desarrollo de una investigación.

Enfoque cuantitativo

La metodología de investigación cuantitativa utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente. En lo que respecta a los enfoques, Maldonado (2018) enfatiza sobre el de tipo cuantitativo lo siguiente:

> Este enfoque está fundamentado en la medición numérica, el conteo de los datos y la utilización de la estadística para establecer con exactitud los factores de comportamientos en una población o muestra. Utiliza las variables para la recolección de los datos. Es deductivo, objetivo, medible y comprobable. (p.35)

Por lo tanto, la principal característica de este enfoque es medir variables con contenido numérico, a través de la selección de una población y, por consiguiente, la determinación de la muestra, a la cual se le aplican instrumentos de recolección de datos, para fundamentar las variables seleccionadas en forma precisa y objetiva.

Enfoque cualitativo

El enfoque de investigación cualitativo busca establecer las preguntas durante la investigación o generar nuevas interrogantes. Según Hernández et al. (2022), el enfoque cualitativo puede entenderse de la siguiente manera:

> Un primer aspecto que debemos explicar con claridad en el diseño metodológico son las razones por las que el enfoque cualitativo nos permitirá abordar el problema y cumplir con los objetivos propuestos. Nos puede guiar la pregunta ¿por qué he optado por un enfoque cualitativo? Es importante que reflexionemos sobre sus ventajas para entender el problema de investigación. Al elaborar nuestra argumentación, podemos considerar también las investigaciones revisadas para

> evidenciar cómo el enfoque cualitativo ha contribuido a obtener los resultados. No obstante, puede ser que encontremos también investigaciones con un enfoque cuantitativo; ante ello, podemos explicar las ventajas de una investigación más bien descriptiva con una aproximación cualitativa a la realidad, las experiencias de otras y otros investigadores, y sus resultados. De lo anterior, se deduce que la característica particular de tal enfoque es la descripción de determinados fenómenos, mediante la utilización de diferentes métodos o instrumentos, según sea la necesidad del investigador y el alcance de la investigación. (p.32)

Enfoque mixto

Por otro lado, en el enfoque de la investigación mixto, Padilla y Marroquín (2021) aluden a que:

> En el Enfoque Mixto, dada la naturaleza del problema, se podría concebir un estudio de carácter híbrido. El investigador se podría aproximar al problema, por medio de ambas rutas. Por una parte, el enfoque cuantitativo permite asignar valores numéricos para analizar datos a través de la estadística, verificación de hipótesis y poder incluso generalizar resultados (si la muestra es representativa). Sin embargo, en muchos casos se requiere profundizar e interpretar el fenómeno, y es allí cuando se complementa con la ruta Cualitativa. (p.339)

Básicamente, este enfoque es el complemento perfecto para aquellas investigaciones con variables cualitativas y cuantitativas, destacando lo relevante de cada una, a fin de obtener un resultado idóneo para quienes fungen como beneficiarios de proyectos investigativos.

Enfoque seleccionado

Para el desarrollo de la investigación, se utiliza el enfoque mixto, con el fin de fundamentar de manera cualitativa y cuantitativa el análisis, descripción y abordaje del proyecto, permitiendo obtener resultados más acertados para la toma de decisiones de la empresa.

Tipos de investigación

Según el tipo de investigación, permitirá conocer de forma general los elementos, procesos, aspectos o bien variables, para efectuar con mayor rigor estudios posteriores contemplados de acuerdo con los objetivos de la investigación. Adicionalmente, dependiendo de

la investigación, busca aclarar en forma ordenada y precisa, aquellos aspectos que no son fácilmente interpretados por el lector.

Investigación descriptiva

En cuanto al tipo de investigación denominado descriptivo, Guevara et al. (2020) mencionan que este tipo de investigación: "tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utiliza criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes" (p.166). Por tanto, la descripción es fundamental, ya que, en las investigaciones, existen variables que deben ser caracterizadas y también definidas para lograr un mayor entendimiento por parte del lector y, a su vez, obtener un trabajo con información valiosa a nivel descriptivo.

Tipo de investigación seleccionada

Una vez definidos los tipos de investigación, se determina que la descriptiva es la que se utiliza para el desarrollo del proyecto investigativo, debido a que el trabajo por realizar en cada uno de los objetivos presenta la particularidad de que deben describirse, tomando en cuenta la información, pautas o procesos a seguir, de acuerdo con la Norma ISO/IEC 27001:2022 y Objetivos de Control para Tecnologías de la Información y Relacionadas (COBIT 5) en español; es decir, al presentar información descrita y definida correctamente, se logra un mejor abordaje de la temática seleccionada.

Fuentes de información

En este sentido, las fuentes facilitan la investigación, redacción y desarrollo de los apartados en forma consciente y con datos e información fehaciente, para el cumplimiento de los objetivos planteados en el proyecto. Peña-Vera (2022) menciona que las fuentes de información de una investigación son importantes:

> Cuando se emprenden procesos de investigación científica es preciso dedicar un segmento importante de tiempo para indagar sobre los elementos teóricos, que sustentan el tema sobre el que se esté indagando. En este punto se consultan fuentes de información variadas para tomar los aportes que otros autores hayan hecho al respecto. La amplitud de esta búsqueda va a depender de distintos

> factores, tales como el volumen de fuentes que existan en torno al tema, el tipo de investigación que se esté desplegando, la profundidad y exhaustividad planteada en los objetivos de investigación, entre otros. (p.6)

Fuentes primarias

Como lo plantean Molina y Méndez (2019): "Las fuentes de información primarias son aquellas que contienen información original, la cual es publicada por primera vez y que es el resultado de un trabajo intelectual" (p.10). Por lo tanto, dichas fuentes serán, en primera instancia, el gerente general de Copy Printer Advanced SRL, puesto que dicha persona tiene el conocimiento sobre la operación del negocio en la actualidad, por ello es necesario conocer su opinión y criterios para desarrollar los objetivos planteados en la investigación. De igual forma, los empleados son necesarios para solicitarles información mediante un instrumento, sobre determinados aspectos de la temática investigativa. Asimismo, el documento oficial de la NORMA ISO/IEC 27001:2022 y el de Objetivos de Control para Tecnologías de la Información y Relacionadas (COBIT 5) en español son de gran relevancia, ya que serán la principal guía para el tema en estudio. Además, se establece como fuente de información primaria, los empleados de la empresa en estudio.

Fuentes secundarias

Alvarado-Bustamante (2019) expresa que, en las fuentes secundarias, se: "Interpreta y analizan fuentes primarias. Las fuentes secundarias son textos basados en fuentes primarias e implican generalización, análisis, síntesis, interpretación o evaluación" (p.15). En consecuencia, la documentación que se pretende emplear como apoyo para la realización del proyecto son: libros electrónicos, PDF (formato de documentos portátiles), trabajos finales de graduación de proyectos similares, revistas y sitios web confiables.

Fuentes terciarias

Busca identificar y hallar fuentes primarias y secundarias que permiten guiar las definiciones de los conceptos claves de la investigación. En lo que respecta a fuentes terciarias, Molina y Méndez (2019) manifiestan que: "una fuente de información terciaria es aquella que contiene información recopilada de una fuente secundaria, contiene, por ende, y a la vez, información primaria" (p.10). Se infiere que, ofrece síntesis de dichas fuentes, ya que permite

identificar lo relacionado con fuentes primarias y secundarias como lo son diccionarios y enciclopedias.

Descripción de variables

Se basa en medir el cumplimiento de lo propuesto, Freire (2019) menciona que: “Las variables intervienen como causa o como efecto en el proceso investigativo. Las variables que se van a investigar quedan identificadas desde el momento en que se define el problema” (p.172). Por lo que, sin variables, la investigación no tendría un sentido lógico y aceptable para dar respuesta a los objetivos formulados.

Definición conceptual

Es la variable donde se amplía la definición de conceptos, según Freire (2019), la:

> Definición conceptual de la variable: Básicamente, constituye una abstracción articulada en palabras conceptualmente, para facilitar su comprensión y su adecuación a los requerimientos prácticos de la investigación. Es definirla. Representa la expresión del significado que el investigador le atribuye, y con ese sentido se debe entender durante toda la investigación. También es conocida como la función nominal de la variable a medir (nombre que la identifica). (p.172)

Es decir, es una descripción o bien el significado de lo escrito como variable.

Definición operacional

Este tipo de variable está relacionada con un adecuado estudio de la literatura, Espinoza (2019) indica que la variable operacional es el: “proceso en la cual se transforma la Variable, de conceptos abstractos a términos concretos, observables y medibles” (p.173). En este sentido, en tal definición se debe especificar el método de medición de las variables.

Definición instrumental

Es el instrumento por el cual recolecta la información, dependiendo de los sujetos, pueden ser uno o varios. Para Moreno (2018), la definición instrumental: “es aquello en la que se aclara como se estudiará la variable que se acaba de definir, los medios o instrumentos para

recoger la información” (párr.1). Es preciso definir con claridad los instrumentos de recolección de datos según la variable seleccionada de cada objetivo específico.

Cuadro de variables

La tabla 4 muestra información detallada sobre las variables por utilizar en cada objetivo específico de la investigación.

Tabla 4*. Cuadro de variables*

Objetivo específico	Variables	Variable conceptual	Variable operacional	Variable instrumental
Determinar el contexto de la organización, a través del análisis obtenido de una matriz DAFO, con la finalidad de que se origine un buen Sistema de Gestión de Seguridad de la Información.	Contexto de la organización.	Para Valbuena (2018), el contexto de la organización es "el entorno empresarial", "la combinación de factores y condiciones internas y externas que pueden tener un efecto en el enfoque de una organización hacia sus productos, servicios e inversiones y las partes interesadas" (párr.3).	Entrevista semiestructurada.	Guía de entrevista.

Objetivo específico	Variables	Variable conceptual	Variable operacional	Variable instrumental
Identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, para que se conozcan con precisión.	Riesgo.	De acuerdo con Fernández-Orozco, G. (2021), el riesgo: "es la posibilidad de que se ejecute un impacto determinado en un activo o en toda la organización" p.24).	Revisión documental.	Guía de temas por investigar.

Objetivo específico	Variables	Variable conceptual	Variable operacional	Variable instrumental
Crear un plan de tratamiento de riesgo, seleccionando, implementando y verificando controles que permitan el establecimiento de indicadores, aplicando como referencia el Marco Referencial COBIT 5 y la norma ISO 27001.	Plan de tratamiento de riesgo.	La Alcaldía de Medellín (2023) argumenta que un plan de tratamiento de riesgo es: Acciones que se definen para reducir los riesgos de Seguridad Digital que superan el nivel de riesgo aceptable de la organización, y que su resultado corresponde al producto de la probabilidad de ocurrencia por el impacto que ocasionaron o podrían ocasionar las amenazas por el aprovechamiento de las vulnerabilidades de los activos de seguridad digital de la organización. (párr.1)	Matriz de valoración del riesgo.	Cuadro donde se describe el riesgo, magnitud del impacto, probabilidad de ocurrencia y nivel del riesgo.

Objetivo específico	Variables	Variable conceptual	Variable operacional	Variable instrumental
Diseñar políticas de seguridad de la información acordes con los procesos, lineamientos y requerimientos de la empresa, aplicando como referencia los cuatro dominios del anexo A y 93 controles de la norma internacional ISO 27001:2022.	Políticas de seguridad de la información.	Según la Escuela Europea de Excelencia (2020) las políticas de seguridad de la información son un "conjunto de directrices estratégicas promul gadas por una organización para garantizar que todos los empleados, usuarios o interesados las adopten y diseñen procesos y procedimientos que sigan estos principios de modo alineado" (párr.4).	Cuestionario y Entrevista	Formulario con preguntas.

Fuente: Elaboración propia.

Población y muestra

La población que forma parte de la investigación y a la cual se le aplica el cuestionario, son nueve empleados de la empresa Copy Printer Advanced SRL, por ende, se considera como un tipo de muestreo no probabilístico, en el que, de acuerdo con Hernández y Carpio (2019): "se seleccionan cuidadosamente a los sujetos de la población utilizando criterios específicos, buscando hasta donde sea posible representatividad" (p.76). Por lo tanto, la clasificación de este tipo de muestreo que se considera utilizar es por conveniencia y, según Hernández-Ávila y Escobar (2019):

> Este método se caracteriza por buscar con mucha dedicación el conseguir muestras representativas cualitativamente, mediante la inclusión de grupos aparentemente típicos. Es decir, cumplen con características de interés del

> investigador, además de seleccionar intencionalmente a los individuos de la población a los que generalmente se tiene fácil acceso o a través de convocatorias abiertas, en el que las personas acuden voluntariamente para participar en el estudio, hasta alcanzar el número necesario para la muestra. (p.79)

En síntesis, se utiliza la clasificación antes mencionada por el total de la población sujeto de estudio y la cercanía. Por lo tanto, gracias a lo antes mencionado, existe la posibilidad de que la totalidad de empleados den respuesta al instrumento por utilizar.

Instrumentos para la recolección de datos

Para el desarrollo de la investigación, se utilizan tres instrumentos de recolección de datos, los cuales son: entrevista semiestructurada, revisión documental y cuestionario, por ende, seguidamente se presenta la definición de cada uno con su respectiva descripción del motivo de su empleo.

Entrevista semiestructurada

Primeramente, Sánchez et al. (2018) indican que las entrevistas semiestructuradas son una: "técnica en la que el entrevistador efectúa la entrevista tomando como base un guion general, aunque las preguntas son abiertas y no están estandarizadas" (p.60). Para este caso, se pretende implementar este tipo de técnica, debido a que sirve como guía al momento de su aplicación, por lo tanto, es fundamental tener presentes las variables por estudiar en lo que respecta al contexto de la organización y con ello cumplir con la información requerida para el proyecto. Para ello, se emplea un instrumento llamado guía de la entrevista, además, el medio por el cual se lleva a cabo dicha técnica es personal o bien virtual, de acuerdo con la disposición del sujeto de investigación.

Revisión documental

De igual forma, se recurre a la revisión documental que, desde la posición de Useche et al. (2019), consideran que:

> Es la exploración exhaustiva de textos y documentos sobre un tema en particular. Se usa esta técnica para seleccionar y extraer información sobre la variable, desde diferentes ópticas abordadas, permitiendo profundizar sus conocimientos sobre el tema y la variable en términos de integración, corroboración y crítica. (p.48)

En este sentido, es relevante acudir a una revisión detallada y exhaustiva mediante documentos que proporcionen un apoyo al desarrollo del proyecto, puesto que es necesario conocer sobre la temática de los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, que han sido investigados por otros autores, permitiendo ser una guía para el constructo teórico-práctico. Por lo tanto, se considera la utilización o lectura de documentos como trabajos finales de graduación de proyectos similares, formato de documentos portátiles (PDF), revistas, libros, entre otros, por ende, el instrumento de implementación es una guía de temas por investigar, utilizando como medio computadora con acceso a internet.

Cuestionario

Por otro lado, Ander-Egg (2003, citado en Useche et al. 2019) argumentan que el cuestionario:

> Consiste en un conjunto más o menos amplio de preguntas formuladas con el propósito de conseguir respuestas, a fin de obtener datos e información sobre un tema o problema específico. Se trata de un instrumento rigurosamente estandarizado que traduce y operacionaliza determinados problemas que son objeto de investigación. (p.32)

De modo que el cuestionario se utiliza como técnica para recopilar información sobre los controles de COBIT 5 y del Anexo A de la Norma ISO 27001, empleando para tal efecto, el instrumento denominado formulario con preguntas aplicado a los empleados de la empresa Copy Printer Advanced SRL, bajo el tipo de muestreo no probabilístico por conveniencia.

Proceso para la recolección y análisis de datos.

Para este apartado, es necesario efectuar primeramente una debida preparación de cada uno de los instrumentos seleccionados con una revisión previa, para continuar con la etapa de aplicación de estos, utilizando la población o muestra definida, con la finalidad de recolectar la información deseada. Por lo tanto, es preciso señalar que, en dicha etapa, se deben efectuar grabaciones o anotaciones, que son un respaldo utilizado para acceder posteriormente y realizar los análisis pertinentes, que deben ser presentados mediante tablas, gráficos o en prosa, dependiendo del instrumento aplicado y el objetivo con el que se implementa. Por ende, se toma en cuenta el uso de los formularios de Google Forms para la aplicación del cuestionario y, a su

vez, utilizar los resultados que se registran a través de las gráficas generadas por la herramienta. Por otro lado, se considera aplicar la entrevista de forma personal al gerente general, asistente contable y, también, al ingeniero de sistemas de la empresa, con el fin de generar una mejor comprensión del documento por aplicar.

Por otra parte, para el empleo de la entrevista semiestructurada, se debe realizar, en primer lugar, la guía de entrevista, que incluye temas relacionados con el contexto de la organización a nivel interno y externo. Además, las respuestas se registran de forma escrita y mediante una grabación de voz, para generar un buen análisis de la información brindada. De igual forma, es preciso destacar que, una vez efectuada la entrevista, se procede a efectuar el análisis externo e interno, seguido de la elaboración de la matriz DAFO, en la cual se determinan todas las estrategias necesarias para su implementación.

En cuanto a la revisión documental, se necesita para conocer con mayor detalle y explicación lo relacionado con los riesgos y consecuentemente se va redactando el apartado correspondiente. No obstante, dentro de los instrumentos aplicados, se contempla una matriz de valoración del riesgo basada en COBIT 5 y la norma ISO 27001, que se realiza a través de un cuadro, para el que, en primera instancia, se requiere precisar de los riesgos de la empresa y, posteriormente, hacer las valoraciones para asignar un valor numérico que al final dan como resultado el nivel de riesgo.

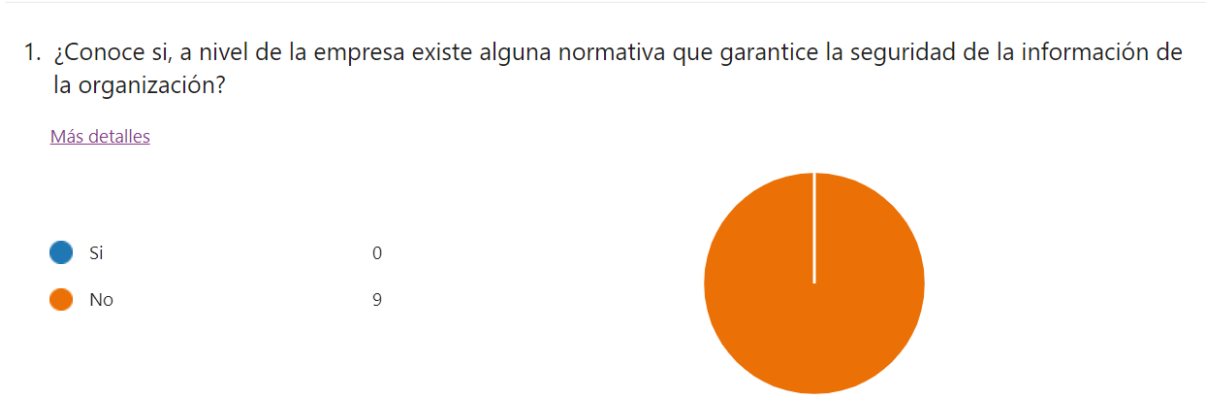
Otro aspecto relevante de mencionar es que, una vez que la información se encuentre recolectada, es importante que el análisis e interpretación sean coherentes con el objetivo para el cual se formularon los instrumentos; por ende, es imprescindible que, al momento de documentar las respuestas, no existan alteraciones intencionales, que generen ambigüedad y distorsión en la investigación.

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

Encuesta

La encuesta fue aplicada a nueve empleados de la empresa con el objetivo de recolectar información para el desarrollo de la propuesta del proyecto final de graduación.

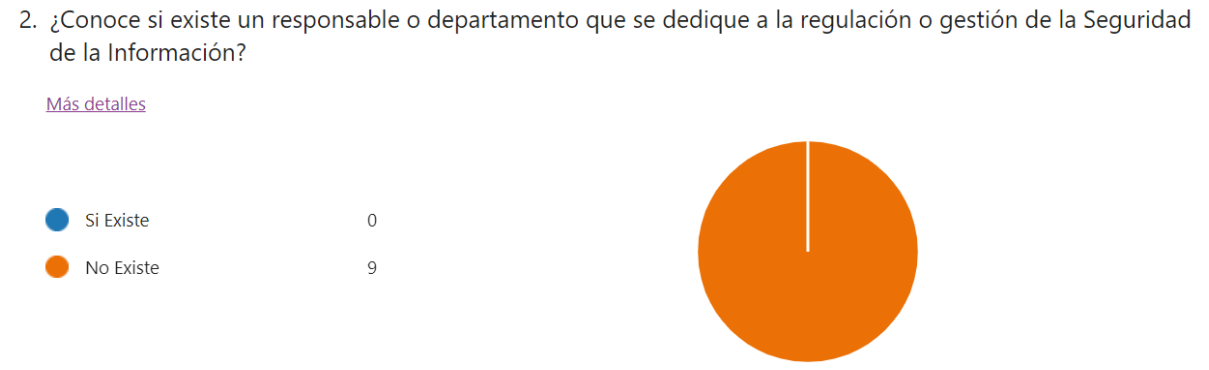
Figura 5. *Política de seguridad de la información*



Fuente: Elaboración propia.

En respuesta a la primera pregunta planteada en el cuestionario, los resultados indicaron que el 100% de los encuestados indicaron no conocer si existe alguna normativa que garantice la seguridad de la información de la organización.

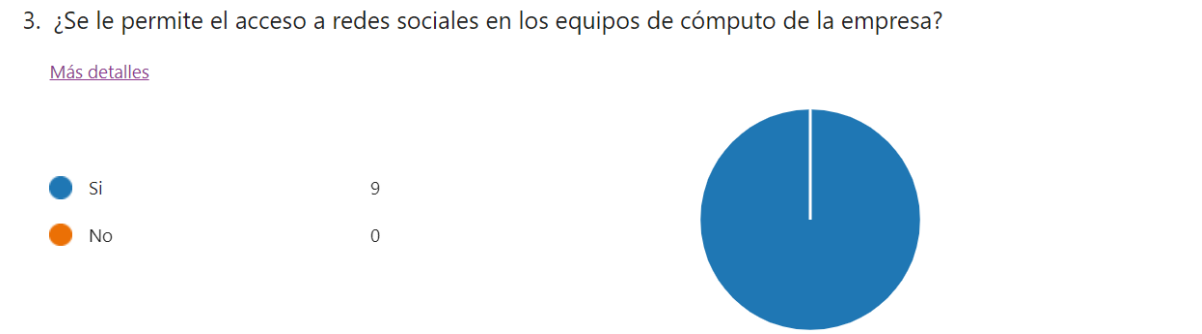
Figura 6. *Encargado de seguridad de la información*



Fuente: Elaboración propia.

El 100% de los empleados afirman que no existe un responsable o departamento que se dedique a la regulación o gestión de la seguridad de la información.

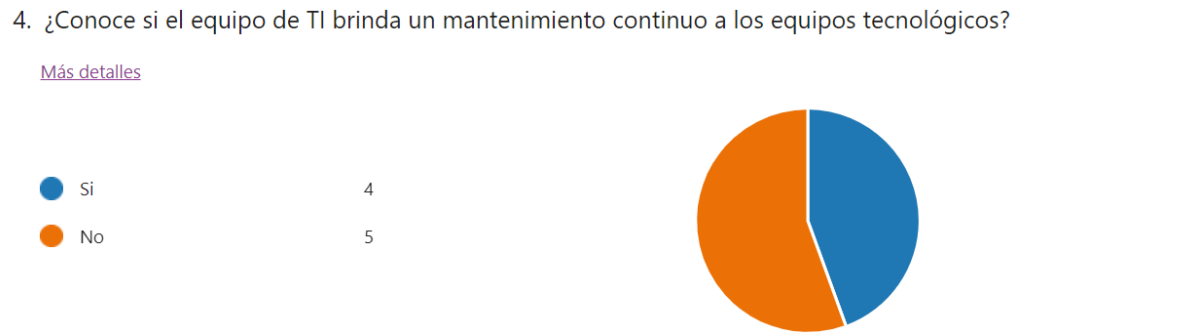
Figura 7. *Seguridad en los servicios de red*



Fuente: Elaboración propia.

Tal como se observa en la figura 7, el 100% de los encuestados señala que se les permite el acceso a redes sociales en los equipos de cómputo de la empresa.

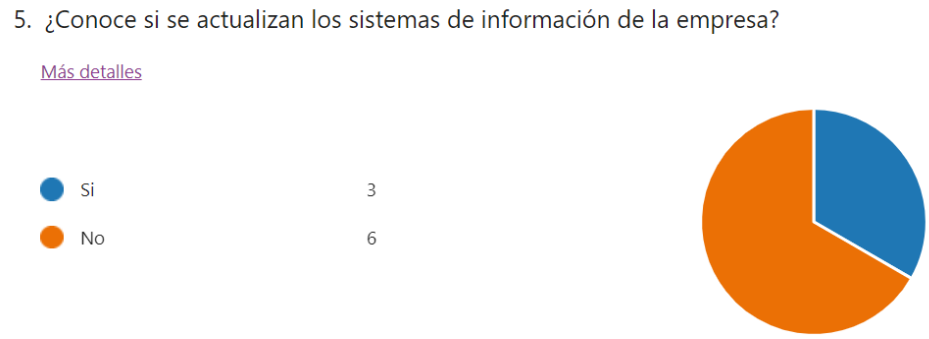
Figura 8. *Mantenimiento en equipamiento tecnológico*



Fuente: Elaboración propia.

Se puede observar que, en la pregunta anterior, el 44% de los encuestados afirma que sí conocen que el equipo de TI brinda un mantenimiento continuo a los equipos tecnológicos, mientras que el 56% manifiesta lo contrario.

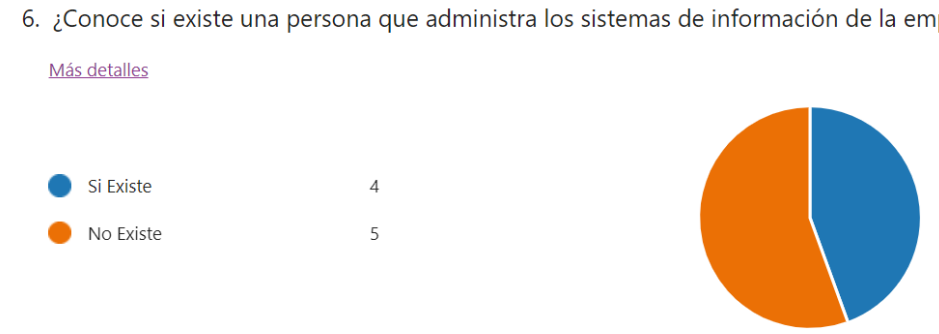
Figura 9. *Protección de los sistemas de información*



Fuente: Elaboración propia.

Con base en la pregunta anterior, el 67% de los encuestados aseguran que no conocen si se actualizan los sistemas de información de la empresa; mientras que el 33% indican que no conocen del proceso.

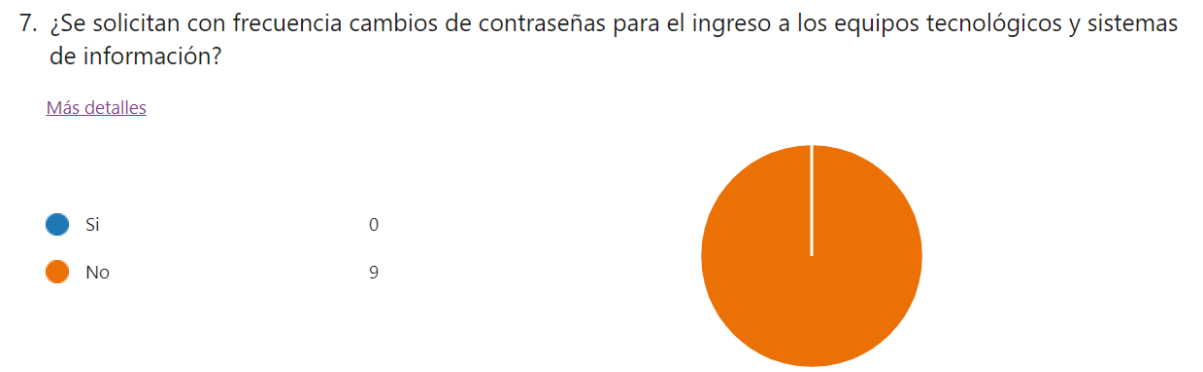
Figura 10. *Responsabilidades*



Fuente: Elaboración propia.

Del total de encuestados, 5 empleados indicaron que no existe una persona que administra los sistemas de información, mientras que 4 colaboradores afirman que existe del detalle de la pregunta planteada.

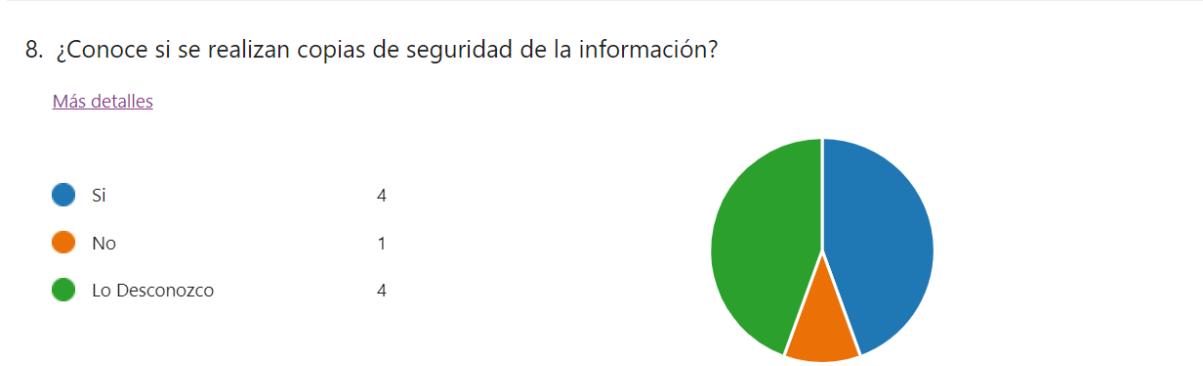
Figura 11. *Autenticación segura*



Fuente: Elaboración propia.

De acuerdo con la figura 11, el 100% de los empleados afirma que no se solicitan con frecuencia cambios de las contraseñas para el ingreso a los equipos tecnológicos y sistemas de información.

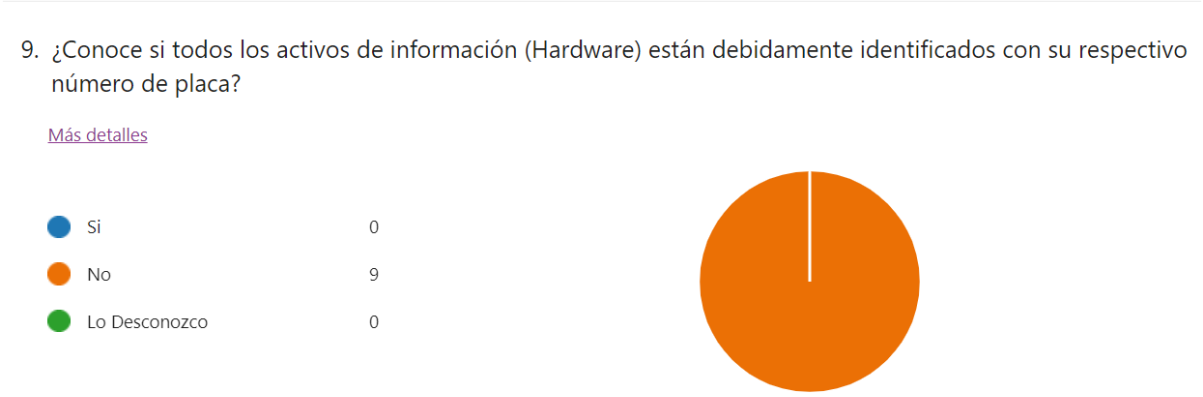
Figura 12. *Respaldo de información*



Fuente: Elaboración propia.

Se puede observar en la pregunta anterior, que el 44% de los empleados afirman que desconocen si se realizan copias de seguridad de la información, mientras que el otro 44% indica que sí se realizan. Por otra parte, solo un colaborador indica que no se realizan.

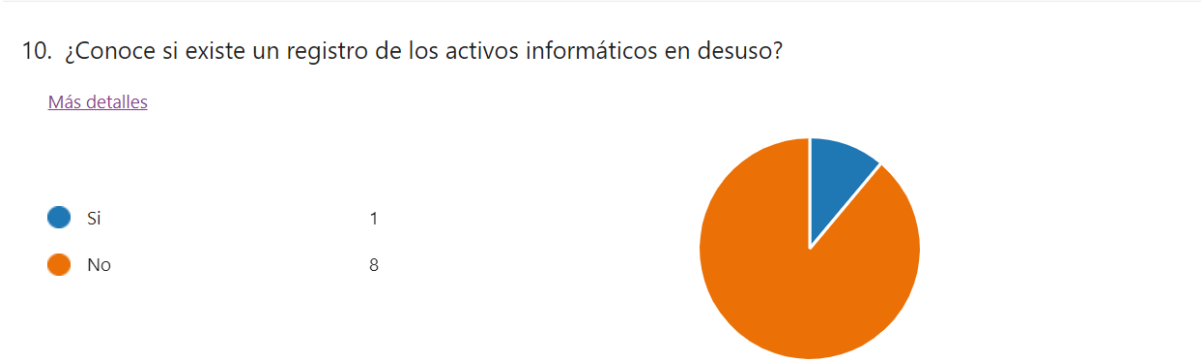
Figura 13. *Etiquetado de información*



Fuente: Elaboración propia.

Como se observa en la pregunta anterior, el 100% de los empleados no conocen de dicho procedimiento.

Figura 14. *Eliminación segura o reutilización de equipo*



Fuente: Elaboración propia.

En la figura 14, se observa que ocho empleados no conocen que existe un registro de los activos informáticos en desuso, pero un funcionario afirma que sí lo hay.

Figura 15. *Seguridad del cableado*

Fuente: Elaboración propia.

En respuesta a la última pregunta planteada en el cuestionario, el 88% de los encuestados afirma que el tendido de cables de red sí está debidamente protegido por canaletas; mientras que el 11% de los empleados de la organización indicó que no a la pregunta planteada

Entrevista

La entrevista fue aplicada al gerente y jefe de soporte técnico de la empresa con el objetivo de recolectar información para el desarrollo de la propuesta de implementación del Sistema de Gestión de Seguridad de la información, por lo que las respuestas son de carácter confidencial para fines académicos.

Se logra detectar que no existe un encargado para garantizar la seguridad de la información, ya que los entrevistados indican que no se ha visto necesario. No obstante, es preciso un encargado de la seguridad para prevenir y reducir al mínimo los efectos que puedan ocasionar los riesgos asociados a seguridad de información. En cuanto al manejo y control del inventario de los activos de información, ante la respuesta por parte de los entrevistados, se puede evidenciar que no hay un adecuado control del inventario, ya que el gerente financiero dice que ningún activo está registrado. Por lo anterior, es importante mantener una adecuada gestión de inventario para el buen funcionamiento de la información en la empresa.

Con base en la información sensible que maneja la empresa, se logra denotar que no hay proceso para el tratamiento de esta información, además, existe desconocimiento sobre cuáles son los activos críticos que están expuestos ante amenazas. Debido a ello, es importante implementar controles para evitar la pérdida de información sensible que puede ocurrir de manera accidental o mal intencionada y por esto puede causar daños financieros y de reputación.

Cabe mencionar que el gerente de la empresa indicó que delegan a un tercero la información que consideran sensible como los datos contables. De ahí que la empresa debe aplicar medidas de seguridad adecuadas para la protección de datos sensibles, como establecer derechos de acceso a la información y cifrado de datos.

Por otro lado, se deduce que existe riesgo de pérdida de la información porque el acceso a los equipos y sistemas de información no es restringido, por lo que todo el personal puede ingresar a datos que maneja la empresa. Por tanto, es importante establecer controles para el acceso seguro a la información y a los sistemas mediante la identificación y autenticación de usuario**.** En cuanto a los datos incluidos en los sistemas, no se encuentran encriptados, por lo cual, es evidente que los empleados de Copy Printer Advanced no tienen conocimiento de los riesgos a los que están expuestos ante amenazas.

Con respecto a las herramientas o soluciones que protejan los equipos donde se almacena información sensible, así como los sistemas informáticos de la empresa, se evidencia que la única herramienta para la protección de los equipos y sistemas de información es un antivirus McAfee. Por tal motivo, es necesario que se respalde la información continua e implemente nuevas técnicas para el almacenamiento de los datos.

Con base en lo anterior, es posible determinar que la empresa sí cuenta con medios de almacenamiento de datos, tales como base de datos del sistema y un disco duro externo, pero es importante fortalecer e implementar otros dispositivos para el resguardo de datos. Sin embargo, la disponibilidad de datos es vulnerable y puede afectar los servicios que ofrece la empresa ante una posible pérdida de la información. Por esto, es necesario implementar procedimientos y políticas para conservar la seguridad de la información ante cualquier eventualidad como desastres naturales y ataques cibernéticos. Tampoco existen pruebas que se realicen para determinar que los datos de la información se mantengan íntegros, por tal motivo, la información que maneja la empresa puede tener variaciones entre los datos originales y los almacenados en el sistema.

Según protocolos de seguridad para la preparación e instalación de los equipos de impresión a terceros, se puede deducir que actualmente no existe un protocolo formal para la preparación e instalación de los equipos de impresión a terceros, por tanto, establecer un protocolo de seguridad para la manipulación de los equipos puede garantizar el funcionamiento de estos ante robos, desastres naturales y cualquier otra amenaza.

Por último, la empresa no cuenta con un plan de respuesta de incidentes informáticos y otras amenazas para mitigar y resolver incidencias con el apoyo estratégico y organizado. También, se determina que no existe un proceso para identificar los activos de información según su clasificación; por lo anterior, es importante identificar y asegurar la información mediante la clasificación y, de esta manera, conservar su valor.

Análisis DAFO

Los resultados del análisis DAFO se obtuvieron por medio de la entrevista semiestructurada, en la cual se identifican debilidades, amenazas, fortalezas y oportunidades; asimismo, se determinan estrategias necesarias para el fortalecimiento de la empresa a futuro. En la tabla 5, se describen las amenazas. debilidades, amenazas, fortalezas y oportunidades; también, se realiza un análisis estratégico. A continuación, se describen.

- **FO (MAXI-MAXI) Estrategia para maximizar fortalezas y oportunidades:** en este caso, la empresa puede aprovechar sus fortalezas y las oportunidades que brinda el mercado para promocionar sus productos o servicios.
- **DO(MINI-MAXI) Estrategia para minimizar las debilidades y maximizar las oportunidades:** esta estrategia es el resultado de un análisis de varias debilidades y oportunidades, para minimizar las debilidades y maximizar las oportunidades.
- **FA(MAXI-MINI) Estrategia para maximizar fortalezas y minimizar amenazas:** se basa en una evaluación de las fortalezas de la organización y las amenazas existentes en su entorno. Por lo tanto, busca tomar medidas para maximizar las ventajas y minimizar las amenazas.
- **DA (MINI-MINI) Estrategia para minimizar las debilidades y amenazas:** se busca sacar conclusiones de la evaluación y hacer una revisión en profundidad de las acciones necesarias para reducirlas.

Tabla 5. *Matriz DAFO*

MATRIZ DAFO	**Fortalezas**	**Debilidades**
	F1. Personal comprometido con la empresa.	**D1.** Falta de capacitaciones y entrenamiento en seguridad informática.
	F2. Manejo de datos en sistema de información y aplicaciones.	**D2.** No aplica copia de seguridad de los registros de los clientes.
	F3. Equipos tecnológicos de última generación.	**D3.** Conexiones a redes públicas desprotegidas.
	F4. Servicio de internet de fibra óptica en de alta velocidad.	**D4.** Infraestructura tecnológica vieja.
	F5. Utilización de canaletas para la distribución de cables de red.	**D5.** Cableado de redes mezclados con cables eléctricos.
	F6. Disco duro externo para el almacenamiento de la información.	**D6.** No existe un plan de emergencia ante desastres naturales.
	F8. Antivirus McAfee	**D7.** No existe cronograma para realizar copias de seguridad.
Oportunidades	**Estrategia FO *maxi-maxi***	**Estrategia DO *mini-maxi***
O1. Concientizar y capacitar frecuentemente a todos los empleados en buenas prácticas del uso de la información.	**F1-O1:** Fomentar el uso adecuado de la información crítica de la empresa mediante la implementación de una política que establezca información de buenas prácticas de seguridad de información.	**D1-D6-O1:** Inscribir a funcionarios en cursos de ciberseguridad que se imparte gratuitamente por parte de la empresa Microsoft.
O2. Crear una política de contraseñas seguras, del manejo adecuado de los equipos y de la información.	**F3-O2:** Implementar un sistema para acceso a la información mediante la autentificación de dos pasos.	**D3-O2:** Capacitar al personal para el uso correcto del antivirus McAfee.
O3. Crear un plan de actualización de los sistemas y aplicaciones.	**F2-F6-O3:** Implementar una aplicación de parches automatizada y programada para lograr el cumplimiento de parches.	**D2-D7-O3:** Establecer fechas de actualizaciones de equipos y copias de datos para garantizar disponibilidad e integridad de datos.

O4. Crear política de acceso remoto.	**F3-O4:** Determinar las acciones por realizar para aprovechar al máximo las funciones de cada equipo y sus sistemas y aplicaciones.	**D3-O4:** Cotizar una VPN para el acceso remoto.
O5. Mejorar la gestión de infraestructura tecnológica.	**F4-F3-F05-O5:** Implementar un sistema para recopilar datos en tiempo real para la toma rápida de decisiones.	**D4-O5:** Implementar una infraestructura de TI de computación en la nube.
Amenazas	**Estrategia FA *maxi-mini***	**Estrategia DA *mini-mini***
A1. Desastres naturales.	**F1-A1:** Implementar un plan de evacuación ante la presencia de desastres naturales.	**D6-A1:** Conformar una brigada de evacuación para liderar el proceso, capacitación y aplicación del plan.
A2. Divulgación no intencional.	**F1-A2:** Capacitar a los empleados para que sean menos propensos a plantear amenazas no intencionadas y sean más conscientes del comportamiento sospechoso en los demás.	**D1-A3:** Implementar un *software* de monitoreo de datos y otras actividades.
A3. Ataques cibernéticos.	**F4-F8-A3**: Contratar un profesional con la suficiente formación para prevenir y hacer frente a cualquier ataque informático.	**D3-A3:** Implementar herramientas como proxy de red, cortafuegos o VPN para establecer canales de comunicación seguros y barreras de seguridad contra amenazas externas.
A4. Fallas de red.	**F3-A4:** Desarrollar un plan de acción eficaz para minimizar el impacto provocado por posibles fallas de red.	**D5-A4:** Aplicar estándares vigentes que cumplan con los requisitos y procedimientos de la instalación de cableado estructurado de red.
A5. Pérdida de copias de seguridad	**F5-A5:** Instalar y configurar de manera secundaria una herramienta que permita automatizar tareas de copias de seguridad de manera personalizada.	**D7-A5:** Desarrollar un plan de protección de la información.

Fuente: Elaboración propia.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El desarrollo de esta propuesta se determina a partir de los objetivos planteados inicialmente. Complementando el marco metodológico del trabajo, se puede concluir respecto a los objetivos que:

Con base en el análisis DAFO, se determina que la empresa se encuentra en una constante exposición a variantes internas y externas, ya que existe falta de capacitaciones y entrenamiento en seguridad informática, además de conexiones a redes públicas desprotegidas y ausencia de controles para el resguardo de la información; por lo que se exponen a ataques informáticos, fallas de red, pérdida de información confidencial y otra amenaza asociada a la seguridad de la información. Es posible concluir que, mediante el análisis DAFO, se extrajeron resultados satisfactorios.

Aunado al análisis de la entrevista a los empleados de la organización, se identifica que existen riesgos que no están siendo detectados, puesto que no está presente un adecuado control de la información crítica que maneja la empresa; se carece de un registro de inventario; no hay conocimiento del valor de los activos de la información y existe desconocimiento de seguridad de la información. De este modo, se logra satisfactoriamente la identificación de riesgos relevantes.

Luego del análisis de resultados, se detecta que no existe control de seguimiento a riesgos, ya que no se tienen identificados y tampoco se conoce del valor de cada activo de información, por tanto, la necesidad de tratar los riesgos es fundamental para identificar y proporcionar su continuo seguimiento, por lo que el análisis de resultados valió un papel satisfactorio en la gestión de riesgos.

Como resultado de la entrevista y encuesta aplicada a funcionarios de la organización, se determina que la empresa Copy Printer Advanced carece de controles y procedimientos para garantizar la seguridad de la información; por lo cual, no cuenta con un documentado oficial que referencia acciones que permitan garantizar la continuidad de servicios, ya que, al existir conocimiento insuficiente sobre el adecuado control e importancia que tienen los activos de la información y también la ausencia de políticas de seguridad que guíen a las buenas prácticas, por tanto, se crean controles y procedimientos de manera satisfactoria.

En conclusión, de acuerdo con la necesidad de la empresa, la propuesta proporciona una metodología para la implementación de un Sistema de Gestión de la Información, permitiendo alcanzar en la medida posible los objetivos de la empresa. Por cuanto, al contar con un documento donde se establezcan controles y procedimientos para garantizar la seguridad, esta acción permite identificar riegos y minimizar eventos que comprometan la seguridad de la información.

Recomendaciones

Como resultado de la realización de la propuesta del proyecto de graduación, a continuación, se brindan recomendaciones a la empresa Copy Printer Advanced SRL., para su adecuado abordaje en el tiempo.

Se recomienda, a la gerencia, la implementación del Sistema de Gestión de Seguridad de la Información, bajo la norma ISO/IEC 27001 y el Marco Referencial COBIT 5, pues los mismos establecen mejores prácticas para gestionar la seguridad, ciberseguridad y protección de la privacidad; todo lo anterior en un tiempo no mayor a tres meses, es decir, a partir del 1 de julio de 2024, ya que pueden darse cambios de procedimientos que actualmente se realizan en la empresa.

A la gerencia y al encargado de la seguridad de la información, se les recomienda tener en cuenta los cambios y actualizaciones de la norma internacional y el marco de referencia utilizado en la propuesta, por lo que se considera necesario realizar una revisión el 1 de agosto de 2026. Lo anterior para verificar que el marco de referencia COBIT 5 y normas de estandarización internacional ISO27001 siguen siendo los más adecuados para la organización. Es importante mencionar que los métodos presentados en este proyecto seguirán siendo efectivos en términos de las mejores prácticas utilizadas.

Otro punto que se recomienda, a la gerencia y encargado de la seguridad de la información, es brindar a todos los empleados una formación, concienciación y educación sobre la seguridad de la información, informando las políticas de seguridad, normas, controles y procedimientos establecidos, así como actualizaciones de todo lo anterior, con el fin de garantizar el éxito del Sistema de Gestión de Seguridad de la Información, esto a partir de entregada la propuesta, es decir, el 30 de junio de 2024.

Por último, para el futuro se recomienda a la gerencia y si se llega actualizar el Sistema de Gestión de Seguridad de la Información bajo otras normativas, preferir siempre los marcos de referencia y mejores prácticas reconocidos en la industria y que son desarrollados a partir del conocimiento, la experiencia y las recomendaciones de una gran cantidad de profesionales.

CAPÍTULO VI. PROPUESTA

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

Proyecto de graduación

Para optar por el grado de Bachillerato en Ingeniería en Informática

PROPUESTA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD DE INFORMACIÓN, BASADA EN LA NORMATIVA ISO/IEC 27001:2022 Y COBIT 5 EN ESPAÑOL Y LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN PARA LA EMPRESA COPY PRINTER ADVANCED SRL, UBICADA EN SAN JOSÉ

SEBASTIÁN SÁNCHEZ PIÑAR

AUTOR

San José, Costa Rica

Marzo, 2024

CONTENIDO

INTRODUCCIÓN

Durante los últimos años, las empresas se han enfrentado a cambios tecnológicos, por tal motivo, han actualizado sus dispositivos e implementado nuevos sistemas informáticos, acordes a las nuevas tendencias del mercado, que han llegado para facilitar el trabajo. Sin embargo, se desconoce sobre la seguridad que se debe implementar, al adquirir y poner en funcionamiento dichos dispositivos y aplicaciones.

Aunado a lo anterior, es preciso destacar que las empresas buscan formas de almacenar datos, ya sean financieros, administrativos e incluso personales, pero son pocos los que investigan sobre cómo preparar los sistemas de información, ante las diversas amenazas que puedan afectar la continuidad de los servicios que ofrece la organización. Por su parte, ante el desconocimiento de la seguridad informática e información del aplicativo implementado, esto puede ser una puerta abierta para posibles ataques informáticos.

Si bien es cierto, existen muchas técnicas para prevenir que las organizaciones e instituciones sean vulnerables, el desconocimiento en temas de seguridad de la información se da continuamente, porque no existe personal capacitado para orientar y proponer controles de seguridad para los activos de información.

Además, toda información cuenta con datos sensibles que podrían ser debilitados ante una situación de amenaza y vulnerabilidades. Por esta razón, los expertos en seguridad de la información recomiendan aplicar normas internacionales que garanticen la seguridad y así tener confianza enfocada en la protección de la infraestructura de tecnologías de información y comunicación, que van a lo interno, desde la alta gerencia, hasta la seguridad del edificio de la empresa y externo como los proveedores y clientes, asegurando la confidencialidad, integridad y disponibilidad de la información.

Por tanto, es necesario comunicar la importancia de la seguridad de la información a los usuarios, para que se establezcan buenas prácticas y proteger todo el entorno, previniendo la posibilidad de algún daño donde se vean afectados los activos de información, ya que, en la actualidad, existen muchas personas que han sido víctimas ante eventualidades de cualquier amenaza que pone en peligro la disponibilidad, integridad y confidencialidad de esta. Por ello, la propuesta de implementación de la seguridad de información, en la empresa Copy Printer Advanced, busca mitigar riesgos asociados a los activos de la información de la compañía.

Objetivo general

Aplicar la norma ISO/IEC 27001:2022 y COBIT 5 en la empresa Copy Printer Advanced SRL, planteando un modelo de seguridad de la información, que asegure el cumplimiento de la disponibilidad, confidencialidad e integridad de la información.

Objetivos específicos

1. Determinar el contexto de la organización, a través del análisis obtenido de una matriz DAFO, con la finalidad de que se origine un buen sistema de gestión de seguridad de la información.
2. Identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, para que se conozcan con precisión.
3. Crear un plan de tratamiento de riesgo, seleccionando, implementando y verificando controles que permitan el establecimiento de indicadores, aplicando como referencia el Marco Referencial COBIT 5 y la norma ISO 27001.
4. Diseñar políticas de seguridad de la información acordes con los procesos, lineamientos y requerimientos de la empresa, aplicando como referencia los controles de la norma internacional ISO 27001:2022 y COBIT 5.

Registro de activos de información

Se identificaron los activos de información de la empresa, ya que es un recurso para el desarrollo del Sistema de Gestión de Seguridad de la Información. A continuación, se mencionan de manera general los activos de información:

Línea base de software autorizado: son todas aquellas aplicaciones que se utilizan para la gestión del proceso del negocio.

Tabla 6. *Línea base de software autorizado*

Software	Software de aplicación (Chrome, Office 365, One Drive, McAfee)
	Sistema de Información
	Sistema operativo (Windows 11)
	Paperless

Fuente: Elaboración propia.

Datos: son todos los datos recopilados, gestionados, transmitidos y destruidos.

Tabla 7. *Datos*

Datos	Copias de Seguridad
	Base de datos

Fuente: Elaboración propia.

Hardware: el equipo físico necesario para gestionar las personas y las operaciones de la empresa.

Tabla 8. *Hardware*

Hardware	Computadora portátil
	Computadora de escritorio tipo mini torre
	Impresora multifuncional
	Fotocopiadora
	Unidad de potencia (UPS)
	Teclado
	Mouse
	Disco duro Externo
	Proyector
	Tablet
	Switches
	Modem
	Teléfono IP
	Cables de Red
	Patch panel
	Adaptadores
	Gabinete

Fuente: Elaboración propia.

Personas: en esta categoría se encuentra tanto la planilla general de la empresa como todos aquellos que tengan acceso a información de esta.

Tabla 9. *Personas*

Personas	Empleados
	Proveedores
	Clientes

Fuente: Elaboración propia.

Información digital: son documentos que están en formato de digital

Tabla 10. *Información digital*

Información Digital	Contratos Clientes
	Contratos Empleados
	Lista de Clientes
	Números de cuentas clientes
	Correspondencia
	Depósitos bancarios
	Documentos de garantías
	Colillas de pago empleados
	Información Financiera
	Pagos de clientes
	Pagos a proveedores
	Registros Contables
	Actas de recepción
	Planes de mantenimiento
	Actas de entrega
	Registros de incidentes
	Control de facturas
	Registros de atención de clientes
	Registros de consumo de suministros
	Catálogo general de suministros
	Manuales

Fuente: Elaboración propia.

Información física: *S*on documentos que están en formato de papel.

Tabla 11. *Información física*

Información Física	Contratos Clientes
	Contratos Empleados
	Lista de Clientes
	Números de cuentas clientes
	Correspondencia
	Depósitos Bancarios
	Documentos de garantía
	Colillas de pago empleados
	Información financiera
	Pagos de clientes
	Pagos a proveedores
	Registros contables
	Actas de recepción
	Planes de mantenimientos
	Actas de entrega
	Registros de incidentes
	Control de facturas
	Expedientes de empleados

Fuente: Elaboración propia.

Instalaciones: lugares físicos en los que se alojan los activos de información.

Tabla 12*. Instalaciones*

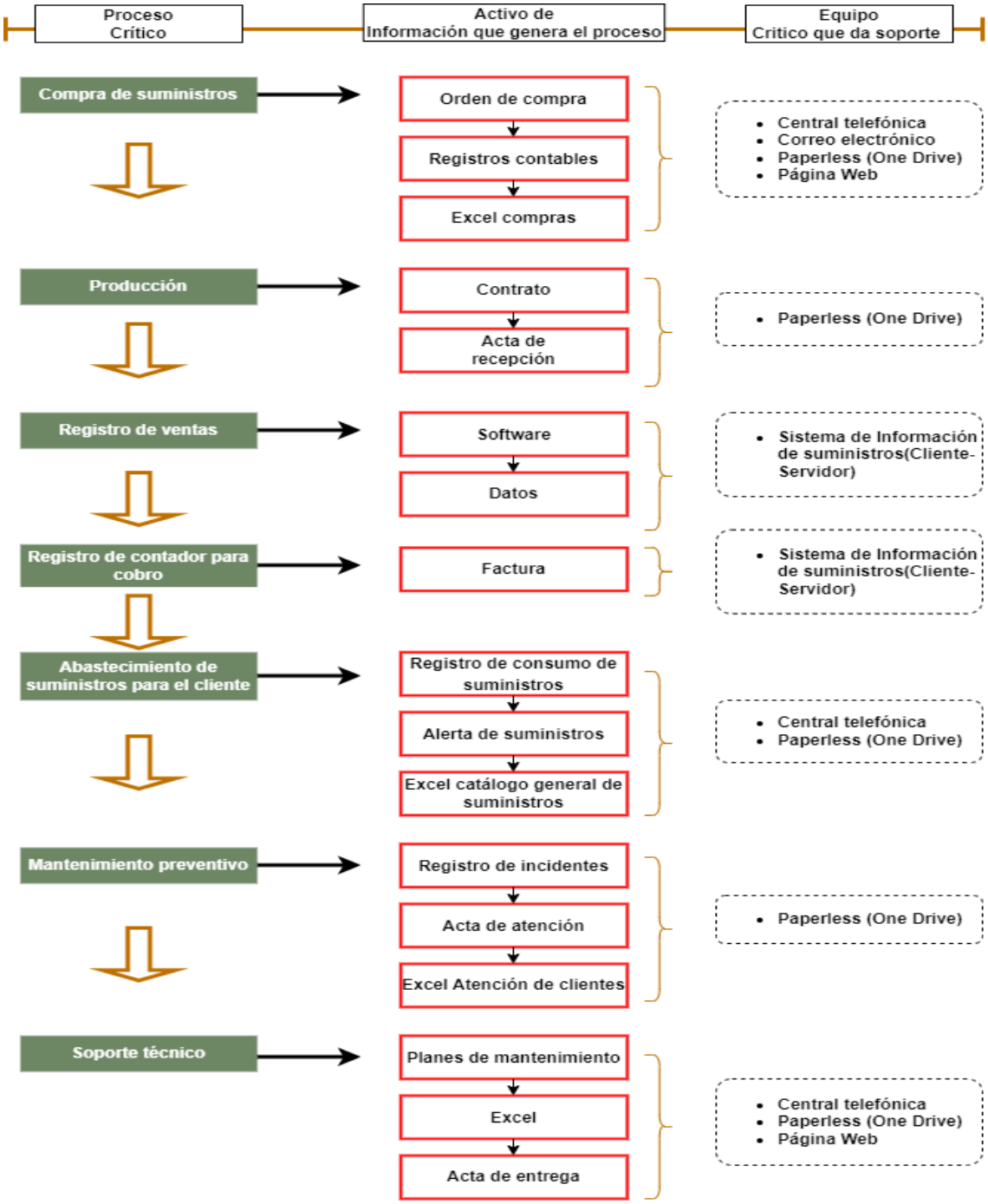
Instalaciones	Edificio
	Oficina
	Bodega
	Archiveros
	Escritorios
	Sillas
	Aire acondicionado
	Dispensador de agua

Fuente: Elaboración propia.

Procesos críticos de la empresa

A continuación, se especifican los procesos críticos de la empresa, donde se menciona el activo de información que da soporte al proceso y el equipo crítico que brinda soporte.

Figura 16. *Procesos críticos*



Fuente: Elaboración propia.

Gestión de riesgos

Para la gestión de riesgos, se utiliza como referencia la norma ISO 27005 apoyando los conceptos generales de la norma ISO 27001 y asociado al marco referencial COBIT 5. El riesgo es todo aquello que puede ser utilizado con fines malintencionados para causar perjuicios a los usuarios en la empresa u organización. Además, puede ser tomado como la posibilidad de que se produzca un impacto determinado, ya sea en un activo de la información o en toda la organización.

Amenazas y vulnerabilidades en los activos de información

La tabla 13 detalla las vulnerabilidades presentes en cada activo y las amenazas que pueden explotarlas. La amenaza se basa en aprovechar la afectación que ocasiona la vulnerabilidad en activo de la información. Por su parte, la vulnerabilidad es el efecto que ocasiona o puede provocar la amenaza.

Tabla 13. *Amenazas y vulnerabilidades*

ACTIVOS	AMENAZA	VULNERABILIDAD
Hardware	Fuego	Afectación de la integridad por destrucción de los datos.
	Daños por agua	Afectación en la continuidad de servicios que ofrece la empresa, ya que podrían presentarse daños en la infraestructura tecnológica por la exposición al agua, por lo que causaría pérdidas económicas.
	Desastres naturales	Afectación en ingresos y ventas por interrupción de servicios, ya que podría haber fallas en infraestructuras de telecomunicaciones.
	Corte de suministro eléctrico	Personal se ve afectado en sus labores por pérdida de continuidad de servicios al no contar con UPS confiables.
	Robo	Pérdida de datos e información al no contar con un respaldo apropiado.
	Degradación del *hardware*	Los empleados presentan baja productividad por el rendimiento de equipo.

ACTIVOS	AMENAZA	VULNERABILIDAD
Software	Errores de configuración de software	Afectación en funcionamiento del sistema, ya que puede bloquear datos y afecte la disponibilidad de la información.
	Pérdida de servicio de software	Afectación al acceso de los datos.
	Alteración no autorizada al software	Pérdida de la integridad, ya que un usuario podría manipular exactitud de la información.
	Virus de computación	Un usuario podría acceder a sitios maliciosos o abrir correos con contenido malicioso y generar una infección de código malicioso a los equipos de la red por falta de capacitación a los empleados.
	Errores de uso por parte de los usuarios	Afectación en exactitud de los datos.
	Escape de la información	Pérdida de confianza de los clientes al verse afectada la confidencialidad de la información.
	Análisis de trafico de red	Un usuario ingrese a sitios de internet no confiable y ocasione el ingreso de un código malicioso a causa de no contar con una conexión segura a internet (VPN).
Datos	Abusos de derecho	Un empleado puede ingresar a información confidencialidad y publicarla a terceros al no contar con un sistema de identificación y autenticación de usuarios.
	Manipulación con el software	Un usuario puede ingresar al sistema y modificar datos contables y con ello afectar la integridad de los datos.
	Análisis de trafico de red	Un usuario ingrese a sitios de internet no confiable y ocasione el ingreso de un código malicioso a causa de no contar con una conexión segura a internet (VPN).
	Falta de capacidad de restauración	Pérdida de datos contables y clientes puede provocar inexactitud en ventas y cobros, ya que no existe una política de seguridad de información para establecer fechas y procedimientos para la realización de copias de seguridad continuas.

ACTIVOS	AMENAZA	VULNERABILIDAD
Personas	Errores de empleados	Un empleado ingresa datos contables erróneos al sistema, lo que provoca inexactitud en ingresos.
	Divulgación de información	El encargado de recursos humanos puede divulgar información personal de un empleado y el afectado pueda demandar a la empresa por el no cumplimiento de la Ley 8968, ya que no existe una política de seguridad de la información que contenga acuerdos y restricciones de los empleados.
Información física	Fuego	Afectación de la integridad por destrucción de los datos.
	Daños por agua	Afectación en el estado documentos físicos por contacto con el agua.
	Desastres naturales	Afectación en ingresos y ventas por interrupción de servicios.
	Pérdida de información	Pérdida de la disponibilidad a la información no resguardada adecuadamente.
	Escape de la información	Pérdida de confidencialidad a lo no existir acuerdos con empleados.
Información digital	Espionaje remoto	Pérdida de la confidencialidad de la información, ya que no existe una conexión segura a internet que garantice la confidencialidad de la información.
	Robo	Afectación en disponibilidad de datos e información.
	Virus de computación	Alteración de la información al contar con sistemas y aplicaciones desactualizadas.
	Pérdida de información	Pérdida de confidencialidad, integridad y disponibilidad de la información, al no resguardar copia de la información en un sitio diferente a las instalaciones.

ACTIVOS	AMENAZA	VULNERABILIDAD
Instalaciones	Fuego	Afectación de la integridad por destrucción de los datos.
	Daños por agua	Afectación en la continuidad de servicios que ofrece la empresa, ya que podría presentarse daños en la infraestructura tecnológica e información física por la exposición al agua, lo que causaría pérdidas económicas.
	Desastres naturales	Interrupción de servicios al no existir un plan de recuperación de desastres naturales.

Fuente: Elaboración propia.

Valoración de los activos de la información

El objetivo de la valoración de los activos de información es determinar el impacto que puede sufrir la empresa por pérdida de confidencialidad, integridad y disponibilidad. En la tabla 14, se muestra el criterio cuantitativo y cualitativo para identificar la valoración de los activos de la información, basado en la norma ISO 27001 y el marco referencial COBIT 5:

Tabla 14. *Criterios para la valoración de activos de la información*

Nivel de Valor	Valor	Criterio
5	Crítico	Daño extremadamente grave
4	Muy alto	Daño muy grave
3	Alto	Daño grave
2	Bajo	Daño importante
1	Muy bajo	Daño menor
0	Insignificante	Irrelevante

Fuente: Elaboración propia, con base en la información recolectada del marco referencial COBIT 5.

Para obtener esta evaluación, se sostuvo conversaciones con los responsables de los procesos de la empresa, quienes entienden la importancia de cada activo dentro de esta para

determinar el nivel de confidencialidad, integridad y disponibilidad que requiere cada proceso a fin de cumplir con las operaciones del negocio.

La tabla 5 especifica el valor cuantitativo presente en cada activo de información y menciona la razón para asignar valor a cada activo de información.

Tabla 15. *Valoración de activos de información por tipo de activo*

Hardware		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	3	La información almacenada debe ser vista únicamente por personal autorizado.
Integridad	3	Es necesaria la integridad en los activos de *hardware*, ya que se almacenan datos de clientes y contables.
Disponibilidad	2	Se puede trabajar, aunque los equipos tecnológicos no estén disponibles, ya que se puede recurrir a información física u otros aparatos de almacenamientos.
Datos		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	4	La información que se almacena en los sistemas de información debe ser confidencial, ya que se almacenan datos de usuarios, clientes, proveedores y datos contables.
Integridad	3	La información debe mantenerse integra, es decir, sin alteraciones con el fin de garantizar exactitud y fiabilidad de la información.
Disponibilidad	2	Es importante tener siempre disponible la información de los usuarios, pero si no estuviera disponible en este momento y se la obtuviera después, no afecta críticamente las operaciones de la empresa.
Software		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	1	Este es un *software* estándar, el cual no es confidencial para todos los empleados.

Integridad	2	Es necesario asegurar que la información de los servidores no sea alterada ni modificada sin autorización, para que no se perjudique el negocio.
Disponibilidad	2	El *software* debe estar disponible durante horas de trabajo, pero si hay un problema con una computadora, en otra computadora puede ser usado.
Información Digital		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	3	Debido a que la información que se maneja es de clientes, proveedores y empleados, es necesario que pueda ser vista por personal autorizado para que no sea modificada.
Integridad	3	Es necesario que la documentación no sea alterada, ni se produzca pérdidas de esta, debido a que son el único respaldo físico de contratos, procedimientos, etc.
Disponibilidad	2	Se debe acceder a la información en cualquier momento que sea requerido.
Información Física		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	3	Debido a que la información que se maneja es de clientes, proveedores y empleados, es necesario que pueda ser vista por personal autorizado para que no sea modificada.
Integridad	3	Es necesario que la documentación no sea alterada, ni se produzca pérdidas de esta, debido a que son el único respaldo físico de contratos, procedimientos, etc.
Disponibilidad	2	Se debe acceder a la información en cualquier momento que sea requerido.
Personas		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	2	Cierta información debe ser manejada al interior de la empresa, por lo cual no debe ser divulgada.
Integridad	0	No hay aspectos de integridad relacionados con los empleados, clientes y proveedores.
Disponibilidad	2	Los empleados deben estar disponibles para resolver posibles problemas que se presenten.

Instalaciones		
Pilar fundamental de la seguridad de la información	**Valor**	**Motivo**
Confidencial	1	El edificio no tiene por qué ser confidencial.
Integridad	3	Se debe proteger la integridad física del edificio, ya que ahí es donde encuentran los equipos que almacenan la información crítica de la empresa.
Disponibilidad	3	Siempre debe estar disponible, ya que probablemente cause la interrupción de actividades propias de la empresa.

Fuente: Elaboración propia, con base en la información del marco referencial COBIT 5.

Seguridad y plan de tratamiento de los riesgos

El plan de tratamiento de riesgo es el proceso de modificar el riesgo mediante la implementación de controles. Para lograr la seguridad de la información exitosa durante el proceso de gestión de riesgos, se requiere del análisis de vulnerabilidades y amenazas ya identificadas en la empresa y, de esta manera, cuantificar el daño potencial que puede existir ante dichas amenazas, así como desarrollar pasos y procedimientos de mitigación para lograr un nivel de riesgo aceptable o tolerado sostenible. En la tabla 16 se muestran los niveles de tolerancia con los que se identifica.

Tabla 16. *Nivel de tolerancia del riesgo*

NIVEL DEL RIESGOS	CALOR
Riesgo Aceptable	Si el evento llegara a presentarse, no representa un impacto importante para la Empresa.
Riesgo Tolerante	Si el evento llegara a presentarse, tendría un bajo impacto o efecto sobre algunas actividades de la Empresa.
Riesgo Alto	Si el evento llegara a presentarse, tendría un alto impacto, comprometiendo los objetivos de la Empresa o la continuidad de las operaciones por paralización de los procesos principales.
Riesgo Extremo	Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo los objetivos de la empresa o la continuidad de la empresa.

Fuente: Elaboración propia, basado en la normativa ISO 27001

En la tabla 17, se observa un mapa de calor donde se representa la probabilidad e impacto que se puede obtener al ser explotada una amenaza. Se diseñó de cinco por cinco y 25 cuadrantes, divididos en cuatro niveles de tolerancia de los riegos.

Tabla 17. *Mapa de calor*

Matriz de Riesgos		**Impacto**				
		Muy Bajo	**Bajo**	**Considerable**	**Alto**	**Muy Alto**
Probabilidad		**1**	**2**	**4**	**8**	**16**
Muy Alta	**5**	5	10	20	40	80
Alta	**4**	4	8	16	32	64
Media	**3**	3	6	12	24	48
Baja	**2**	2	4	8	16	32
Muy Baja	**1**	1	2	4	8	16

Fuente: Elaboración propia, basado en la normativa ISO 27001.

En la tabla 18, se muestra una matriz de seguridad de riesgos que compone el análisis, la evaluación del riesgo inherente y el riesgo residual una vez implementado el plan complementario.

Tabla 18. *Seguridad de riesgos (Nivel de riesgo inherente)*

IDENTIFICACIÓN DEL RIESGO				EVALUACIÓN DEL RIESGO		
Identificador de riesgo	**Detalle**	**Escenario**	**Categoría**	**Probabilidad**	**Impacto**	**Nivel Riesgo Inherente**
R1	**Falta de capacitación hacia el personal, en temas de Seguridad de la Información**	Un usuario podría acceder a sitios maliciosos o abrir correos con contenido malicioso y generar una infección de código malicioso a los equipos de la red.	Afectación tecnológica	Muy Alta (5)	Considerable (4)	Riesgo Alto (20)
R2	**Falta de sistemas de protección contra incendios**	Sobrecarga eléctrica que provoque un cortocircuito y haya un incendio y haya afectación de la integridad por destrucción de los datos.	Afectación en la Información física e infraestructura tecnológica	Muy Alta (5)	Alto (8)	Riesgo Extremo (40)
R3	**Falta de mantenimiento del cableado estructurado de redes**	Fallas en infraestructuras de telecomunicaciones que afecte ingresos y ventas por interrupción de servicios.	Afectación tecnológica y económica	Alta (4)	Alto (8)	Riesgo Extremo (32)
R4	**UPS no confiables por falta de mantenimientos**	Corte de suministro eléctrico afectado la continuidad de servicios.	Afectación económica	Baja (2)	Considerable (4)	Riesgo Tolerante (8)
R5	**Falta de un sistema o dispositivo de sincronización de *backup***	Se presenta un fallo en una computadora y se ocupa restaurar, el encargado de respaldos de información no realiza respaldos continuamente, por lo que, genera pérdida de datos e información.	Afectación tecnológica	Media (3)	Alto (8)	Riesgo Alto (24)
R6	**Pruebas de rendimiento de equipos tecnológicos deficientes**	Los empleados presentan baja productividad por el rendimiento de equipo.	Afectación económica	Media (3)	Considerable (4)	Riesgo Tolerante (12)
R7	**Seguridad de acceso lógico ineficiente**	Un usuario olvida su contraseña para el acceso de datos y bloquee el acceso a los demás usuarios.	Afectación tecnológica	Muy Alta (5)	Alto (8)	Riesgo Extremo (40)
R8	**No existe revisiones de *backup* para garantizar la integridad de datos**	Un usuario identifica inexactitud de los datos contables de varios clientes	Afectación económica	Alta (4)	Alto (8)	Riesgo Extremo (32)
R9	**Falta de acuerdos con los empleados**	Un empleado divulga información crítica de un cliente, lo que causa pérdida de confianza de los clientes al verse afectada la confidencialidad de la información.	Afectación social y económica	Media (3)	Alto (8)	Riesgo Alto (24)
R10	**No existe una**	Un usuario ingrese a sitios de internet no confiable	Afectación	Alta	Alto	Riesgo

IDENTIFICACIÓN DEL RIESGO				EVALUACIÓN DEL RIESGO		
Identificador de riesgo	**Detalle**	**Escenario**	**Categoría**	**Probabilidad**	**Impacto**	**Nivel Riesgo Inherente**
	herramienta que garantice conexión segura a internet (VPN).	y ocasione el ingreso de un código malicioso.	tecnológica	(4)	(8)	Extremo (32)
R11	**Las contraseñas de ingreso al sistema de información no son confiables**	Un empleado puede adivinar la contraseña de otro empleado con privilegios de administrador e ingresar a información y puede manipularla.	Afectación tecnológica	Alta (4)	Alto (8)	Riesgo Extremo (32)
R12	**Falta de un sistema que eficiente de control de acceso**	Un antiguo empleado que aún tiene acceso al sistema de información puede ingresar al sistema y modificar datos contables y con ello afectar la integridad de los datos.	Afectación tecnológica	Alta (4)	Alto (8)	Riesgo Extremo (32)
R13	**Personal no capacitado en temas leyes laborales**	El encargado de recursos humanos puede divulgar información personal de un empleado y el afectado pueda demandar a la empresa por el no cumplimiento de la Ley 8968, ya que no existe una política de seguridad de la información que contenga acuerdos y restricciones de los empleados.	Afectación social y económica	Baja (2)	Alto (8)	Riesgo Alto (16)
R14	**Seguridad de acceso físico ineficiente**	Un empleado ingrese al taller de mantenimiento y robe.	Afectación económica	Alta (4)	Considerable (4)	Riesgo Alto (16)
R15	**Falta de un inventario de activos de información de hardware**	Se vende un equipo que la empresa no tiene disponible en *stock*.	Afectación tecnológica	Alta (4)	Considerable (4)	Riesgo Alto (16)
R16	**Falta de un inventario de activos de información de Software**	No se compran licencias de aplicaciones adecuadas, ya que no se conoce del total de aplicaciones instaladas en los equipos de cómputo.	Afectación tecnológica	Alta (4)	Considerable (4)	Riesgo Alto (16)
R17	**Falta de acuerdos bien definidos con proveedores**	Un proveedor incumple con las fechas de pago acordado en el contrato	Afectación económica	Media (3)	Considerable (4)	Riesgo Tolerante (12)

Fuente: Elaboración propia.

En la tabla 19, se muestra una matriz de seguridad de riesgos que compone el análisis, la evaluación del riesgo residual una vez implementado el plan compensatorio.

Tabla 19. *Seguridad de riesgos (Nivel de riesgo Residual)*

PLAN COMPENSATORIO		**EVALUACIÓN DEL RIESGO**		
Identificador de riesgo	**Medida a implementar**	**Probabilidad.**	**Impacto.**	**Nivel Riesgo Residual**
R1	Generar capacitaciones para el personal en temas de seguridad de la Información.	Media (3)	Considerable (4)	Riesgo Tolerante (12)
R2	Instalar y dar mantenimiento continuo a detectores de humo, extintores y sistema de rociadores automático.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R3	El cableado eléctrico y de telecomunicaciones que transmite datos o admite servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. Implementar lo que indica la normativa TIA/EIA-568-B que especifica los requisitos de componentes y transmisión para los sistemas de cableado de telecomunicaciones.	Muy Baja (1)	Alto (4)	Riesgo Tolerante (8)
R4	Realizar escaneos de vulnerabilidades internos y externos al menos una vez por semestre para la infraestructura tecnológica, todos los hallazgos detectados deberán corregirse de acuerdo con los procesos documentados.	Muy Baja (1)	Considerable (4)	Riesgo Aceptable (4)
R5	Establecer fechas para realizar copias de seguridad de la información, del *software* y del sistema una vez a la semana y se debe verificar su integridad periódicamente. Se debe establecer el día, hora y encargado para ejecutar el respaldo de la información.	Muy Baja (1)	Alto (4)	Riesgo Tolerante (8)
R6	Establecer y mantener un proceso seguro de la configuración (*hardening*) basado en un marco de ciberseguridad internacionalmente aceptado (por ejemplo: CIS) para la infraestructura de red. Deben establecerse mecanismos de revisión anuales de cumplimiento de esta configuración y se deberán documentar las excepciones.	Muy Baja (1)	Considerable (4)	Riesgo Aceptable (4)
R7	Establecer y mantener un inventario de todo el personal con acceso a la infraestructura tecnológica, este inventario debe incluir todas las cuentas de usuario, así como de administración y servicio. Las cuentas, los roles y sus privilegios, deben ser revisadas al menos de forma semestral y aprobadas por el superior jerárquico. Las	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)

PLAN COMPENSATORIO		EVALUACIÓN DEL RIESGO		
Identificador de riesgo	**Medida a implementar**	**Probabilidad.**	**Impacto.**	**Nivel Riesgo Residual**
	cuentas inactivas deberán ser deshabilitadas.			
R8	Asignar un equipo encargado para la gestión de incidentes que planifique y alinee la seguridad de la información según las políticas establecidas y también, brinde seguimiento a las medidas de seguridad para fomentar el cumplimiento.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R9	Elaborar un documento que sea claro y preciso que establezca el Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales Ley N.º 37554-JP de la república costarricense.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R10	Implementar *software* de protección contra código malicioso en todos los activos de la infraestructura tecnológica.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R11	Establecer requisitos para implementar contraseñas seguras.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R12	Establecer y mantener un inventario de todo el personal con acceso a la infraestructura tecnológica, este inventario debe incluir todas las cuentas de usuario, así como de administración y servicio. Las cuentas, los roles y sus privilegios, deben ser revisadas al menos de forma semestral y aprobadas por el superior jerárquico. Las cuentas inactivas deberán ser deshabilitadas.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R13	Implementar procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales con respecto al uso de material sobre el que puedan existir derechos de propiedad intelectual.	Muy Baja (1)	Alto (8)	Riesgo Tolerante (8)
R14	Instalar y monitorear contantemente cámaras y alarmas para la detección de personas no autorizadas. Además, colocar dispositivo por huella dactilar para el control de acceso.	Baja (2)	Considerable (4)	Riesgo Tolerante (8)
R15	Establecer y mantener un inventario preciso, detallado y actualizado de la infraestructura tecnológica. Asegúrese de que el inventario registre al menos: el nombre del dispositivo, la dirección de red (si es estática) y la función o servicio. Revisar y actualizar el inventario al menos una vez al año.	Baja (2)	Considerable (4)	Riesgo Tolerante (8)
R16	Elaborar y mantener un inventario detallado de todo el software instalado en la infraestructura de la infraestructura tecnológica. El inventario de *software* debe documentar el nombre, el fabricante, la versión y el propósito. Revisar y actualizar el inventario al menos una vez al año. Únicamente se deberá mantener las versiones de *software* que cuenten con el debido soporte.	Baja (2)	Considerable (4)	Riesgo Tolerante (8)

PLAN COMPENSATORIO		EVALUACIÓN DEL RIESGO		
Identificador de riesgo	**Medida a implementar**	**Probabilidad.**	**Impacto.**	**Nivel Riesgo Residual**
R17	Establecer y mantener contratos relacionados con la implementación de servicios de interacción directa con la infraestructura tecnológica. La política debe abordar como mínimo la clasificación, el inventario, la evaluación, el seguimiento, requisitos de ciberseguridad, así como la cancelación de la relación con los proveedores de servicios. Revisar y actualizar la política anualmente, o cuando ocurran cambios significativos.	Muy Baja (1)	Considerable (4)	Riesgo Aceptable (4)

Fuente: Elaboración propia.

Política de Seguridad de la Información

Propósito

Se espera que todo el personal de la compañía Copy Printer Advanced SRL. debe comprometerse a proteger los pilares fundamentales de la seguridad de la información, tales como la confidencialidad, integridad y disponibilidad de la información, así como los recursos y activos para asegurar el desempeño de las funciones y el cumplimiento de los requisitos normativos, operativos y contractuales.

Estrategia

Implementar una política utilizando como referencia marcos de trabajos para la gestión de riesgos a la información y sus activos informáticos, a través de lineamientos y controles que permitan el mantenimiento y cumplimiento de esa política de seguridad.

Objetivo

Proteger la confidencialidad, integridad y disponibilidad de la información estableciendo controles físicos y lógicos en los activos de la información, con la finalidad de prevenir los ingresos, modificaciones, robo y divulgación de la información de personas no autorizadas. Así mismo, garantizar la continuidad de prestación de servicios de la empresa en caso de incidentes mayores de seguridad y, de esta manera, incentivar al personal a ser partícipes en la seguridad de la información, con la finalidad de minimizar riesgos asociados.

Definiciones

Confidencialidad: Protege a la información de que esté disponible para usuarios, entidades o procesos no autorizados.

Integridad: Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados.

Disponibilidad: Permite que la información esté disponible solamente para los usuarios autorizados en el tiempo que lo requieran.

Activo de información: es cualquier recurso que genere valor para la empresa. Dentro de los activos informáticos, se encuentran las bases de datos, sistemas operativos, *software*, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.

Vulnerabilidad: es una falla presente en un activo y que pueda ser explotada por intrusos.

Amenaza: es la probabilidad de que ocurra un hecho indeseado y que tenga un efecto negativo sobre un activo.

Riesgo: es la probabilidad de que se materialice una amenaza y determine el nivel de impacto en una organización.

Control: son medidas que se implementan con el fin de mitigar los riesgos.

***Hardware*:** es el conjunto de componentes físicos de los que está hecho el equipo.

***Software*:** es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

Datos: son representaciones simbólicas (vale decir: numéricas, alfabéticas, algorítmicas, etc.) de un determinado atributo o variable cualitativa o cuantitativa,

Información digital: documentos almacenados digitalmente mediante aplicaciones fijas del negocio.

Información física: resguardo de documentos impresos de manera física como en archiveros.

Lineamientos generales

1. Todos los funcionarios se comprometerán a mantener la información lo más segura posible.
2. Queda prohibida la reproducción total o parcial de documentos confidenciales, así como el daño fraudulento a los equipos de cómputo, *software*, cables de datos, fuentes de alimentación o cualquier activo de información de la empresa, sin la debida autorización o consentimiento de la gerencia de la entidad.
3. Es responsabilidad de todos los colaboradores conocer y acatar las indicaciones en esta política, así como los procedimientos asociados.

Reporte de incidencias

Es responsabilidad de cualquier funcionario notificar casos de violación de los controles establecidos en este documento, en relación con la política de seguridad; debe notificarlo inmediatamente al jefe del departamento de TI, para formalizar el incidente, posibles causas o mal funcionamiento, así como recomendaciones o controles para mitigar el problema.

Procedimientos para la implementación de controles de seguridad de la información

La siguiente es una propuesta para establecer procedimientos a fin de cumplir con el manejo de los controles de seguridad de la información.

Tabla 20. *Procedimiento políticas generales*

PROCEDIMIENTO POLÍTICAS GENERALES		
No.	**Actividad**	**DESCRIPCIÓN**
1	Define y elabora las políticas de seguridad de información.	El jefe de Departamento de TI construye la propuesta de políticas de seguridad con base en los procesos de la entidad, así como en buenas prácticas en gestión y controles de seguridad de la información.
2	Evalúa y ajusta las políticas de seguridad de la información.	El jefe de Departamento de TI presenta la propuesta de políticas a las demás áreas involucradas.
3	Aprueba la política a nivel organizacional.	El jefe de Departamento de TI presenta la propuesta definitiva de la Política de Seguridad para aprobación a la Gerencia general para su respectiva revisión y aprobación.
4	Divulgación de la política de seguridad.	El jefe del Departamento de TI divulga a todos los empleados la seguridad de la información.

Fuente: Elaboración propia.

Tabla 21. *Procedimiento capacitación*

PROCEDIMIENTO CAPACITACIÓN		
No.	**ACTIVIDAD**	**DESCRIPCIÓN**
1	Define y elabora propuesta de capacitación a todo el personal de la empresa.	El jefe de Departamento de TI analiza las vulnerabilidades detectadas que puedan afectar las políticas y procedimientos de seguridad de información.
2	Define el plan de capacitación a todo el personal de la empresa.	El jefe de Departamento de TI establece el plan de capacitación para los funcionarios nuevos y antiguos a temas por tratar: 1. Objetivos propuestos. 2. Público objetivo. 3. Medios de comunicación. 4. Responsables de cada tarea. 5. Cronograma de actividades. 6. Metodología a aplicar.
3	Ejecución y evaluación del plan de capacitación a todo el personal de la empresa.	El jefe de Departamento de TI desarrolla las actividades de capacitación propuestas en el plan de capacitación y se evalúa el nivel de entendimiento del tema, mediante la aplicación de pruebas al final de estas.
4	Monitoreo de los avances del plan de capacitación.	El jefe de TI realiza un monitoreo de las métricas del proceso de capacitación a todo el personal de la empresa y con base en los resultados, gestiona las mejoras al esquema de sensibilización.

Fuente: Elaboración propia

Tabla 22. *Procedimiento identificación de vulnerabilidades*

PROCEDIMIENTO IDENTIFICACIÓN DE VULNERABILIDADES		
No.	**ACTIVIDAD**	**DESCRIPCIÓN**
1	Realiza pruebas de detección de vulnerabilidades	• Inicia la ejecución de pruebas de penetración e inspección de código en los recursos informáticos seleccionados. • Extrae el informe del resultado de las pruebas, generado como salida del procedimiento de la actividad anterior.
2	Identificación y validación de las vulnerabilidades.	El jefe de Departamento de TI identifica las posibles vulnerabilidades que podrían ser aprovechadas para el rompimiento de los controles de seguridad de información, considerando: a) Resultados generados por la herramienta de monitoreo. b) Vulnerabilidades anteriores. c) Incumplimiento al estándar de Seguridad. d) Incumplimiento a las políticas de Seguridad. • Recopila la información adicional disponible, para la confirmación o aclaración de la vulnerabilidad mediante: a) Realización de entrevistas al personal. b) Observación visual del entorno asociado con la vulnerabilidad. c) Verificación de documentos de aceptación de la vulnerabilidad.
3	Clasificación de la vulnerabilidad	El jefe de Departamento de TI clasifica las vulnerabilidades en categorías para su análisis teniendo en cuenta: a) Resultados generados. b) Informes anteriores. c) Huecos de seguridad. d) Reportes de incidentes.
4	Definición del plan de acción	El jefe de Departamento de TI decide, con base en los resultados del análisis anterior u otros aspectos relevantes, si el riesgo es aceptado o si se aprueba un plan la iniciación.
5	Definición del plan de acción	Si el riesgo es aceptado por el jefe de Departamento de TI: a) Documenta la aceptación del riesgo mediante un acta, estableciendo la justificación de la aceptación y el período de esta.
6	Implementación los cambios	El jefe de Departamento de TI ejecuta el plan de acción establecido y certifica los cambios. En el evento en que no sea posible llevar a cabo algún correctivo en el corto plazo, documenta e informa a la gerencia general señalando las razones.
7	Seguimiento plan de acción	Realiza seguimiento al desarrollo del plan propuesto sobre las acciones definidas y el tratamiento de la vulnerabilidad.

Fuente: Elaboración propia.

Tabla 23. *Procedimiento gestión de incidentes*

PROCEDIMIENTO GESTIÓN DE INCIDENTES		
No.	**ACTIVIDAD**	**Descripción**
1	Detecta y reporta el incidente de seguridad	Cualquier funcionario que detecte una anomalía o mal funcionamiento de un equipo o sistema deberá reportarlo al jefe del Departamento de TI, así mismo, si detecta alguna evasión de los controles de seguridad, deberá informar al jefe del Depto. de TI. El jefe del Departamento de TI deberá generar la documentación respectiva detallando, al menos: - Número de registro del incidente - Posibles causas o detalle del mal funcionamiento - Conclusiones - Recomendaciones -Controles para mitigar o evitar el problema en futuras situaciones.
2	Categoriza el incidente de seguridad	Si se confirma que el reporte se trata de un incidente válido: clasifica el incidente en la categoría correspondiente, estableciendo el tipo más adecuado entre los siguientes: a) Ataques por virus b) Incidentes de acceso físico c) Incidentes de red d) Incidentes de comunicaciones e) Incidentes de base de datos f) Incidentes de aplicativo g) Ataques a la red de datos y recursos tecnológicos h) Incidentes humanos
3	Documentación del incidente	• Si el reporte no corresponde a un incidente de seguridad, el jefe de Departamento de Seguridad: a) Documenta en el formato las razones por las cuales no se considera un incidente de seguridad. • Documenta en la Bitácora de Incidentes de Seguridad de la Información, archiva el formato correspondiente y cierra el incidente.
4	Análisis y definición de las acciones de protección de seguridad de información	El jefe de Departamento de Seguridad de la Información determina si el incidente afecta a la empresa y su impacto.
5	Ejecución de plan de acción de seguridad de información	El jefe de Departamento de Seguridad de Información debe: • Notificar a los implicados las acciones a tomar. • Proceder con las acciones documentadas según el tipo de incidente identificado y el impacto definido. • Determinar el grado de daño causado a los recursos informáticos o información de la empresa, mediante la revisión detallada de los sistemas afectados y lo identificado en la documentando los hallazgos, así como los daños detectados durante su revisión. • Definir el plan de trabajo la implantación de las acciones correctivas requeridas, de acuerdo con los daños evidenciados. • Definir y documentar el esquema requerido para el monitoreo en producción de la correcta realización y efectividad de las acciones ejecutadas sobre los recursos informáticos, asignando los responsables correspondientes para su ejecución.

Fuente: Elaboración propia.

Relación entre los controles ISO 27001 y dominios de seguridad y ciberseguridad del marco referencial COBIT 5

Tabla 24. *Relación de controles y objetivos de la norma ISO 27001 y COBIT 5*

Relación de controles y objetivos de la norma ISO 27001 y COBIT 5 proceso relacionado a seguridad y ciberseguridad			
ISO 27001:2022	**COBIT 5**		
Control	**Dominio**	**Objetivo**	**Práctica**
Todo el Anexo de la Norma -Organizacionales -Personas -Físicos -Tecnológicos	APO13	Gestionar la seguridad	01-Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).
			02-Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.
			03-Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).
	DSS05	Gestionar los servicios de seguridad	01- Proteger contra software malicioso.
			02-Gestionar la seguridad de la conectividad y de la red.
			03-Gestionar la seguridad de *end point*.
			04-Gestionar la identidad del usuario y el acceso lógico.
			05-Gestionar el acceso físico a los activos de I&T.
			06-Gestionar documentos sensibles y dispositivos de salida.
			07-Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.
	DSS06	Gestionar los controles de procesos de negocio	01-Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.
			02-Controlar el procesamiento de información.
			03-Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.
			04-Gestionar errores y excepciones.
			05-Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.
			06-Asegurar los activos de información.

Fuente: Elaboración propia, basado en la norma ISO 27001 y el marco de referencia COBIT 5.

Controles de seguridad de la información

Los siguientes controles están basados en los controles del anexo A de la norma ISO 27001:2022 y las buenas prácticas del proceso relacionado a seguridad y ciberseguridad del marco de referencia COBIT 5. A continuación, se indican los controles de implementación:

1.1. Inventario y control de los activos de hardware.

1.1.1 Establecer y mantener un inventario de la infraestructura

1.1.2 Establecer y mantener un diagrama de red detallado

1.1.3 Establecer y mantener una eliminación segura

1.2 Inventario y control de los activos de software.

1.2.1 Establecer y mantener un inventario de aplicaciones

1.2.2 Establecer una lista de software autorizado

1.3 Gestión de proveedores de servicios.

1.3.1 Establecer y mantener una política de gestión de proveedores de servicios

1.3.2 Establecer y mantener una política de gestión de la prohibición de servicios del proveedor

1.3.3 Establecer y mantener una política de seguridad de relaciones con proveedores

1.4 Configuración segura.

1.4.1 Establecer y mantener un proceso de configuración seguro

1.5 Administración de cuentas y control de accesos.

1.5.1 Establecer y mantener un inventario de cuentas

1.5.2 Establecer una política de contraseñas

1.6 Gestión de vulnerabilidades.

1.6.1 Establecer y mantener un proceso de gestión de vulnerabilidades

1.6.2 Realizar análisis de vulnerabilidades internos y externos

1.6.3 Realizar una gestión de parches y actualizaciones

1.7 Defensa contra código malicioso.

1.7.1 Implementar y mantener software contra código malicioso

1.7.2 Actualizar de forma automática las firmas contra código malicioso

1.7.3 Utilizar herramientas de protección basadas en comportamiento

1.8 Gestión de Copias de seguridad.

1.8.1 Establecer fechas para realizar copias de seguridad de la información

1.9 Gestión de incidentes de seguridad de la información.

1.9.1 Constituir Responsabilidades y Procedimientos

1.9.2 Establecer una política para la respuesta a incidentes de seguridad de la información

1.10 Gestión de cumplimiento de la privacidad y protección de la información personal.

1.10.1 Establecer e implementar derechos de propiedad intelectual

1.10.2 Establecer y mantener una política para la protección y privacidad de la información de carácter personal.

1.11 Seguridad de las instalaciones.

1.11.1 Establecer una política para seguridad del cableado

1.11.2 Instalar dispositivos de detección de incéndienos en las instalaciones

1.11.3 Instalar dispositivos de monitoreo y acceso a las instalaciones

Seguidamente, se detallan los controles de implementación:

1.1. Inventario y control de los activos de hardware

Objetivo: Conocer la totalidad de los activos que necesitan ser monitoreados y protegidos, así como apoyar en la identificación de activos no autorizados y no administrados.

1.1.1 *Establecer y mantener un inventario de la infraestructura*
Establecer y mantener un inventario preciso, detallado y actualizado de la infraestructura tecnológica. Asegúrese de que el inventario registre al menos: el nombre del dispositivo, la dirección de red (si es estática) y la función o servicio. Revisar y actualizar el inventario al menos una vez al año.
1.1.2 *Establecer y mantener un diagrama de red detallado*
Establecer y mantener un diagrama de red preciso, detallado y actualizado de la infraestructura tecnológica. El diagrama deberá incluir información detallada de la red, así como información de los protocolos y puertos utilizados. Revisar y actualizar el diagrama de red al menos una vez al año o cuando se den cambios significativos en la infraestructura.
1.1.3 *Establecer y mantener una eliminación segura*
Los equipos físicamente (*hardware),* principalmente los discos duros de las computadoras y externos, se deben destruir por completo. Revisar la información almacenada claramente en cada activo antes de su eliminación.

1.2. Inventario y control de los activos de software

Objetivo: La gestión activa del *software* es fundamental para prevenir ataques. Múltiples vulnerabilidades explotadas provienen de versiones vulnerables de *software.* El objetivo de este apartado es mantener un adecuado control de los activos de *software* para prevenir este tipo de situaciones.

1.2.1 *Establecer y mantener un inventario de aplicaciones*
Elaborar y mantener un inventario detallado de todo el *software* instalado en la infraestructura tecnológica. El inventario de *software* debe documentar el nombre, el fabricante, la versión y el propósito. Además, revisar y actualizar el inventario al menos una vez al año. Únicamente se deberá mantener las versiones de *software* que cuenten con el debido soporte.
1.2.2 *Establecer una lista de software autorizado*
Mantener una lista actualizada del *software* autorizado, actualizar al menos cada 6 meses la lista de *software* autorizado y documentar las excepciones con el debido plan de remediación.

1.3. Gestión de proveedores de servicios

Objetivo: Existen numerosos ejemplos donde un incidente proviene de un tercero con quien la empresa mantiene alguna relación comercial. El objetivo de este apartado es establecer mecanismos que permitan asegurar de forma básica las relaciones con terceros, así como definir las responsabilidades en cuanto a la protección de la información y los activos.

1.3.1 *Establecer y mantener una política de gestión de proveedores de servicios*
Establecer y mantener una política de gestión de proveedores de servicios, para aquellos contratos relacionados con la implementación de servicios de interacción directa con la infraestructura tecnológica. La política debe abordar como mínimo la clasificación, el inventario, la evaluación, el seguimiento, requisitos de ciberseguridad, así como la cancelación de la relación con los proveedores de servicios. Revisar y actualizar la política anualmente o cuando ocurran cambios significativos.
1.3.2 *Establecer y mantener una política de gestión de la prohibición de servicios del proveedor*
Establecer y mantener una política de gestión de la prohibición de servicios del proveedor, para conservar los niveles acordados de seguridad y prestación de servicios conforme con los acuerdos con los proveedores. Asegurarse de revisar los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos.
1.3.3 *Establecer y mantener una política de seguridad de relaciones con proveedores*
Establecer y mantener una política de seguridad de relaciones con proveedores para garantizar la protección de los activos de la organización accesibles a los proveedores. Se debe incluir los requisitos para abordar los riesgos de seguridad de la información relacionados con la tecnología de la información y las comunicaciones y las cadenas de suministro de productos.

1.4. Configuración segura

Objetivo: Establecer la línea base de configuración requerida para mantener la seguridad de la infraestructura.

1.4.1 *Establecer y mantener un proceso de configuración seguro*
Establecer y mantener un proceso seguro de la configuración (*hardening*) basado en un marco de ciberseguridad internacionalmente aceptado (por ejemplo: CIS) para la infraestructura de red. Deben establecerse mecanismos de revisión anuales de cumplimiento de esta configuración y se deberán documentar las excepciones.

1.5. Administración de cuentas y control de accesos

Objetivo: Establecer los mecanismos mínimos necesarios para prevenir accesos no autorizados a los activos.

1.5.1 *Establecer y mantener un inventario de cuentas*
Establecer y mantener un inventario de todo el personal con acceso a la infraestructura tecnológica, este inventario debe incluir todas las cuentas de usuario, así como de administración y servicio. Las cuentas, los roles y sus privilegios deben ser revisadas al menos de forma semestral y aprobadas por el superior jerárquico. Las cuentas inactivas deberán ser deshabilitadas. El inventario, como mínimo, debe contener: • El nombre de la persona responsable de la cuenta. • El detalle de la cuenta de usuario (FQDN). • El tipo de cuenta (usuario, administración) • El departamento.
1.5.2 *Establecer una política de contraseñas*
Implementar una política de contraseñas en las cuentas que se identificaron en el inventario del punto 1.4.1 Establecer y mantener un inventario de cuentas, donde cada usuario tenga una contraseña única con al menos las siguientes características: • Contraseñas de al menos 8 caracteres. • Que contengan mayúsculas, minúsculas, números y al menos un carácter especial. • Que implementen mecanismos para forzar su complejidad. Las contraseñas deberán cambiarse al menos cada 90 días cuando no se utilice Autenticación Multifactor (MFA).

1.6. Gestión de vulnerabilidades

Objetivo: Establecer un proceso adecuado para gestionar las vulnerabilidades de la infraestructura, con la finalidad de minimizar el riesgo de sufrir un incidente de ciberseguridad asociado a la explotación exitosa de la debilidad de un activo.

1.6.1 *Establecer y mantener un proceso de gestión de vulnerabilidades*
Establecer y mantener un proceso de gestión de vulnerabilidades documentado que incluya al menos cobertura de análisis y remediación. Revisar y actualizar la documentación anualmente, o cuando ocurran cambios significativos que puedan afectar este control.
1.6.2 *Realizar análisis de vulnerabilidades internos y externos*
Realizar escaneos de vulnerabilidades internos y externos al menos una vez por semestre para la infraestructura tecnológica, todos los hallazgos detectados deberán corregirse de acuerdo con los procesos documentados.
1.6.3 *Realizar una gestión de parches y actualizaciones*
Implementar y ejecutar un proceso de parchado o aplicación de actualizaciones al menos de forma semestral.

1.7. Defensa contra código malicioso

Objetivo: Implementar controles para la protección contra código malicioso en la infraestructura de la organización, como una medida para prevenir infecciones que pudieran generar fugas de información, denegación de servicios o daños a los activos.

***1.7.1** Implementar y mantener software contra código malicioso*
Implementar *software* de protección contra código malicioso en todos los activos de la infraestructura tecnológica
***1.7.2** Actualizar de forma automática las firmas contra código malicioso*
Configurar las actualizaciones automáticas de las herramientas contra código malicioso.
***1.7.3** Utilizar herramientas de protección basadas en comportamiento*
Usar *software* contra código malicioso basado en el comportamiento.

1.8. Gestión de copias de seguridad

Objetivo: Evitar la pérdida de datos mediante copias de seguridad con frecuencia y regularmente.

1.8.1 *Establecer fechas para realizar copias de seguridad de la información*
Establecer fechas para realizar copias de seguridad de la información, del *software* y del sistema una vez a la semana y se debe verificar su integridad periódicamente. Se debe establecer el día, hora y encargado para ejecutar el respaldo de la información.

1.9. Gestión de incidentes de seguridad de la información

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de vulnerabilidades e incidentes de seguridad.

***1.9.1** Constituir responsabilidades y procedimientos*
Asignar un equipo encargado para la gestión de incidentes que planifique y alinee la seguridad de la información según las políticas establecidas y también brinde seguimiento a las medidas de seguridad para fomentar el cumplimiento.
***1.9.2** Establecer una política para la respuesta a incidentes de seguridad de la información*
Establecer los procedimientos de comunicación necesarios entre los usuarios y el equipo de gestión de incidentes o cualquiera que deba ser informado de las acciones y el estado del proceso de resolución de incidentes. Mantener un registro de las incidencias.

1.10. Gestión de cumplimiento de la privacidad y protección de la información personal

Objetivo: Establecer lineamentos para garantizar la protección y la privacidad de los datos de forma responsable y cumpliendo con lo establecido en la legislación de Costa Rica.

***1.10.1** Establecer e implementar derechos de propiedad intelectual*
Implementar procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales con respecto al uso de material sobre el que puedan existir derechos de propiedad intelectual.
***1.10.2** Establecer y mantener una política para la protección y privacidad de la información de carácter personal.*
Elaborar un documento que sea claro y preciso que establezca el Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales ley N° 37554-JP de la República costarricense.

1.11. Seguridad de las instalaciones

Objetivo: Mantener procedimientos para evitar daño y pérdida de los activos de información

***1.11.1** Establecer una política para seguridad del cableado*
El cableado eléctrico y de telecomunicaciones que transmite datos o admite servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. Implementar lo que indica la normativa TIA/EIA-568-B que especifica los requisitos de componentes y transmisión para los sistemas de cableado de telecomunicaciones.
***1.11.2** Instalar dispositivos de detección de incendios en las instalaciones*
Instalar y dar mantenimiento continuo a detectores de humo, extintores y sistema de rociadores automático.
***1.11.3** Instalar dispositivos de monitoreo y acceso a las instalaciones*
Instalar y monitorear contantemente cámaras y alarmas para la detección de personas no autorizadas. Además, colocar dispositivo por huella dactilar para el control de acceso.

CONCLUSIONES

El desarrollo de esta propuesta se determina a partir de los objetivos planteados inicialmente. Complementando el marco metodológico del trabajo, se puede concluir respecto a los objetivos que:

En conclusión, de acuerdo con la necesidad de la empresa, la propuesta proporciona una metodología para la implementación de un Sistema de Gestión de la Información, permitiendo alcanzar en la medida posible los objetivos de la empresa. Por cuanto, al contar con un documento donde se establezcan controles y procedimientos para garantizar la seguridad, esta acción permite identificar riegos y minimizar eventos que comprometan la seguridad de la información.

Con base en el análisis DAFO, se determina que la empresa se encuentra en una constante exposición a variantes internas y externas, ya que existe falta de capacitaciones y entrenamiento en seguridad informática, además de conexiones a redes públicas desprotegidas y ausencia de controles para el resguardo de la información; por lo que se exponen a ataques informáticos, fallas de red, pérdida de información confidencial y otra amenaza asociada a la seguridad de la información. Es posible concluir que, mediante el análisis DAFO, se extrajeron resultados satisfactorios.

Aunado al análisis de la entrevista a los empleados de la organización, se identifica que existen riesgos que no están siendo detectados, puesto que no está presente un adecuado control de la información crítica que maneja la empresa; se carece de un registro de inventario; no hay conocimiento del valor de los activos de la información y existe desconocimiento de seguridad de la información. De este modo, se logra satisfactoriamente la identificación de riesgos relevantes.

Luego del análisis de resultados, se detecta que no existe control de seguimiento a riesgos, ya que no se tienen identificados y tampoco se conoce del valor de cada activo de información, por tanto, la necesidad de tratar los riesgos es fundamental para identificar y proporcionar su continuo seguimiento, por lo que el análisis de resultados valió un papel satisfactorio en la gestión de riesgos.

Como resultado de la entrevista y encuesta aplicada a funcionarios de la organización, se determina que la empresa Copy Printer Advanced carece de controles y procedimientos para garantizar la seguridad de la información; por lo cual, no cuenta con un documentado oficial que

referencia acciones que permitan garantizar la continuidad de servicios, ya que, al existir conocimiento insuficiente sobre el adecuado control e importancia que tienen los activos de la información y también la ausencia de políticas de seguridad que guíen a las buenas prácticas, por tanto, se crean controles y procedimientos de manera satisfactoria.

REFERENCIAS

Abad-Chávez, M. y Cruz Calderón, F. (2022). *Aplicación de la Norma internacional ISO/IEC 27002: 2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022* [Tesis de grado, Universidad César Vallejo]. Repositorio institucional. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/107284/Abad_CM-Cruz_CF-SD.pdf?sequence=1&isAllowed=y

Alvarado-Sarango, D. J. y Andrade-López, M. A. (2021). Gestión de Gobierno de TI basado en COBIT 2019, para el Colegio de Bachillerato" Sara Serrano de Maridueña". *Polo del Conocimiento: Revista científico-profesional*, *6*(11), 270-306. https://dialnet.unirioja.es/descarga/articulo/8219399.pdf

Albornoz-Cabrera, N. D. (2022). *Mejora de proceso de gestión de proyectos de TI bajo el enfoque de COBIT 5 y PMBOK 6 para la empresa Eterniasoft* [Universidad Peruana Unión, Tesis de grado]. Repositorio institucional. https://repositorio.upeu.edu.pe/handle/20.500.12840/5541

Alcaldía de Medellín. (25 de enero de 2023). *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.* GOV. https://www.medellin.gov.co/es/centro-documental/plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-de-la-informacion/

Alvarado-Bustamante, J. S. (2019). *Estudio ergonómico en el área de bodega patio de la Empresa Naportec SA* [Tesis Doctoral, Universidad de Guayaquil]. Repositorio institucional. http://repositorio.ug.edu.ec/bitstream/redug/46222/1/ALVARADO%20BUSTAMANTE%20JOS%c3%89%20STALIN.pdf

Amador-Mercado, C. Y. (2022). El análisis PESTEL. *UNO Sapiens Boletín Científico de la Escuela Preparatoria*, 4(8), 1-2. https://repository.uaeh.edu.mx/revistas/index.php/prepa1/article/view/8263/8494

Andrade-Chila, J. C. y Chávez-Loor, C. E. (2018). *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía internacional GYM ECUAINTERGYM S.A. de la ciudad de Guayaquil* [Tesis de grado, Universidad de

Guayaquil]. Repositorio Universidad de Guayaquil. http://repositorio.ug.edu.ec/handle/redug/32606

Arrieta-Jiménez, V., Cervantes-Borrero, Y. E., De La Cruz-Lara, L. M. y López-Cadena, D. M. (2021). La importancia del diagnóstico estratégico en las organizaciones. *Revista Económicas CUC*, 42(2), 243-254. https://dialnet.unirioja.es/servlet/articulo?codigo=8439250

Asamblea Legislativa de Costa Rica. (2011). *Ley 8968: Ley de Protección de la Persona frente al tratamiento de sus datos personales.* Sistema Costarricense de Información Jurídica. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

Asamblea Legislativa de Costa Rica. (2012). *Ley 9048: Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.* Sistema Costarricense de Información Jurídica. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

Avila-Irigoin, J. P. W. y Caloggero-Sangama, C. T. (2022). *Sistema de gestión de riesgos de TI usando las ISO 27001 y 31000 en la empresa LABE CORPORATION SAC* [Tesis de grado, Universidad César Vallejo]. Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/93690

Balseca-Chávez, F., Colina-Vargas, A. M. y Espinoza-Mina, M. A. (2021). Identificación de amenazas informáticas aplicando arquitecturas de Big Data. *INNOVA Research Journal*, *6*(3.2), 141-167. http://201.159.222.115/index.php/innova/article/view/1860/1953

Beleño-García, B. A. (2023). *Propuesta de un Modelo de Gestión de Seguridad y Privacidad de la Información para la Gobernación del Huila* [Tesis de Maestría, EAN Universidad]. Repositorio institucional. https://repository.universidadean.edu.co/bitstream/handle/10882/12410/BelenoBrayan2022.pdf?sequence=1&isAllowed=y

Carrascal, A. (2023). *Marco de trabajo para la gestión de servicios de TI bajo un enfoque ágil, para la consecución de la Política de Gobierno Digital en sus dominios de Sistemas de Información y Servicios Tecnológicos, en entidades públicas territoriales.* Fundación Universidad del Norte.

http://manglar.uninorte.edu.co/bitstream/handle/10584/11344/91044491.pdf?sequence=1&isAllowed=y

Escuela Europea de Excelencia. (24 de diciembre de 2020). *Política de seguridad de la información: qué debería contener de acuerdo con ISO 27001*. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2020/12/politica-de-seguridad-de-la-informacion-que-deberia-contener-de-acuerdo-con-iso-27001/

Espinoza-Freire, E. E. (2019). Las variables y su operacionalización en la investigación educativa. Segunda parte. *Revista Conrado*, 15(69), 171-180. http://scielo.sld.cu/pdf/rc/v15n69/1990-8644-rc-15-69-171.pdf

Fernández-Orozco, G. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí* [Trabajo de Maestría, Universidad de las Fuerzas Armadas]. Repositorio institucional. http://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Flores, D. J. S. y Núñez, J. A. C. (2023). *Estudio de factibilidad de creación de una agencia de publicidad que brinde servicios para las empresas del sector MIPYME* [Trabajo de Maestría, Unitec]. Repositorio institucional. https://repositorio.unitec.edu/xmlui/bitstream/handle/123456789/8963/11313129-11043033-julio2015-m01-t.pdf?sequence=1&isAllowed=y

Freire, E. E. E. (2019). Las variables y su operacionalización en la investigación educativa. Segunda parte. *Revista Conrado*, *15*(69), 171-180. https://conrado.ucf.edu.cu/index.php/conrado/article/view/1052/1068

Gómez, L. y Fernández, P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR Internacional. https://tienda.aenor.com/libro-como-implantar-un-sgsi-segun-une-en-iso-iec-27001-y-su-aplicacion-en-el-esquema-nacional-de-seguridad-edicion-2018-12450

González, J., Salazar, F., Ortiz, R. y Verdugo, D. (2019). Gerencia estratégica: herramienta para la toma de decisiones en las organizaciones. *Telos: Revista de Estudios Interdisciplinarios en Ciencias Sociales*, *21*(1), 242-267. http://ojs.urbe.edu/index.php/telos/article/view/3002/3869

Guevara-Alban, G., Verdesoto-Arguello, A. E. y Castro-Molina, N. E. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Revista Científica Mundo de la Investigación y el Conocimeinto*, *4*(3), 163-173 https://www.recimundo.com/index.php/es/article/view/860/1363

Guevara-Vega, E. M. D., Delgado-Deza, J. R. y Mendoza de los Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información: una revisión sistemática. *Revista Científica de Sistemas e Informática*, *3*(1), e461-e461. https://revistas.unsm.edu.pe/index.php/rcsi/article/view/461/836

Hernández, C. E. y Carpio, N. (2019). Introducción a los tipos de muestreo. *Revista Alerta*, 2(1), 76-79. file:///C:/Users/User/Downloads/7746%20(1).pdf

Hernández-Ávila, C. E., y Escobar, N. A. C. (2019). Introducción a los tipos de muestreo. *Alerta, Revista científica del Instituto Nacional de Salud*, *2*(1(enero-junio)), 75-79. https://camjol.info/index.php/alerta/article/download/7535/7746

Jarsa, V. y Christianto, K. (2018). IT Governance Audit with COBIT 5 Framework on DSS Domain. *KINETIK: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *3*(4), 279–286. https://doi.org/10.22219/kinetik.v3i4.665

León-Manzanares, N., y Puma-Sañomamani, C. (2022). *Propuesta de mejora del proceso de Gestión de Incidentes y Peticiones de Servicio bajo el enfoque de las buenas prácticas de COBIT 5 e ITIL v3 en la Universidad Peruana Unión* [Tesis de Licenciatura, Universidad Peruana Unión]. Repositorio institucional. https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/5544/Noemi_Tesis_Licenciatura_2022.pdf?sequence=4&isAllowed=y

León-Acurio, J.V., Mora-Aristega, J.E., Huilcapi-Masacon, M.R, Tamayo-Herrera, A. y Armijos-Maya, C. (2018). COBIT como modelo para auditorías y control de los sistemas de información. *Polo del conocimiento*, *3*(4), 17-36. https://polodelconocimiento.com/ojs/index.php/es/article/view/439/pdf

López-López, A. M. y Arguello de Castro, F. (2022). *Análisis de la tendencia de camiones de comida como modelo de negocio gastronómico, desde la perspectiva del empresario y del cliente, en los parques de Calle Vieja Food Truck Park y ntre Calles en 2020 y 2021*. [Tesis de pregrado, Universidad Técnica Nacional]. Repositorio institucional.

https://repositorio.utn.ac.cr/bitstream/handle/20.500.13077/714/ANALISIS%20DE%20LA%20TENDENCIA%20DE%20CAMIONES.pdf?sequence=1&isAllowed=y

Maldonado-Pinto, J. E. (2018). *Metodología de la investigación social: Paradigmas: cuantitativo, sociocrítico, cualitativo, complementario*. Ediciones de la U.

Martín, T. D. L. R. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495-506. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

Molina, D. V. y Méndez, H. S. (2019). Fuentes de información y recursos electrónicos en los laboratorios de Farmacotécnia. *Revista Ciencia y Salud Integrando Conocimientos*, *3*(1), ág-10. https://revistacienciaysalud.ac.cr/ojs/index.php/cienciaysalud/article/view/19/12

Moreno-Galindo, E. (09 de marzo de 2018). *Definición instrumental de las variables.* Tesis investigación científica. Recuperado el 4 de marzo de 2024 de https://tesis-investigacion-cientifica.blogspot.com/2018/03/definicion-instrumental-de-las-variables.html#:~:text=La%20definici%C3%B3n%20instrumental%20de%20las,que%20se%20recolectar%C3%A1%20la%20informaci%C3%B3n.

Nery-Kameta, S. A., Celaya-Figueroa, R., y Prado-Gamboa, C. A. (2019). Análisis de teorías y la nueva era de las organizaciones: adaptándose al nuevo ser humano. *Revista Universidad y Empresa*, *21*(37), 9-30. http://www.scielo.org.co/pdf/unem/v21n37/2145-4558-unem-21-37-9.pdf

Ortega, A. O. (2018). *Enfoques de Investigación*. https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf

Padilla-Avalos, C. A., y Marroquín-Soto, C. (2021). Enfoques de Investigación en Odontología: Cuantitativa, Cualitativa y Mixta. *Revista estomatológica herediana*, *31*(4), 338-340. http://www.scielo.org.pe/pdf/reh/v31n4/1019-4355-reh-31-04-338.pdf

Peña-Vera, T. (2022). Etapas del análisis de la información documental. *Revista Interamericana de Bibliotecología*, *45*(3). http://www.scielo.org.co/pdf/rib/v45n3/2538-9866-rib-45-03-e4.pdf

Peñaloza-Titosunta, P. J. (2019). *Propuesta metodológica del ciclo para la gestión operativa en empresas comerciales en función del Cobit 5* [Tesis de Maestría, Universidad del Azuay]. Repositorio institucional. https://dspace.uazuay.edu.ec/bitstream/datos/9010/1/14655.pdf

Perales-Barrios, Y. V. (2020). *Desarrollar e interpretar un sistema de gestión para el registro de un software en INDECOPI y la auditoría basándose en los principios de la metodología de COBIT 5 en una Universidad Privada* [Trabajo de grado, Universidad Católica de Santa María]. Repositorio institucional. https://repositorio.ucsm.edu.pe/handle/20.500.12920/10195

Plá-Ayora, D. (2023). *Fracaso en la gestión de la crisis climática mundial. Análisis crítico de la actual legislación* [Tesis Doctoral, Universitat Politècnica de València]. Repositorio institucional. https://riunet.upv.es/bitstream/handle/10251/191189/Pla%20-%20Fracaso%20en%20la%20gestion%20de%20la%20crisis%20climatica%20mundial%20Analisis%20critico%20de%20la%20actual%20legislac....pdf?sequence=1&isAllowed=y

Rojas-Pirca, J. S. y Quispe-Mallqui, C. (2022). *Propuesta de un modelo de gobierno de tecnologías de información basado en COBIT 5 para la mejora de la gestión de incidentes en una Fintech* [Trabajo de grado, Universidad Tecnológica del Perú]. Repositorio institucional. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5735/J.Rojas_C.Quispe_Tesis_Titulo_Profesional_2022.pdf?sequence=1&isAllowed=y

Rojas-Pupo, Y. (2021). *Metodología para la gestión de la seguridad de la información como contribución a la continuidad del negocio* [Tesis de Maestría, Universidad de Holguín]. Repositorio institucional. https://repositorio.uho.edu.cu/handle/uho/8471

Sánchez-Carless, H. H., Reyes-Romero, C. y Mejía-Sáenz, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística.* Universidad Ricardo Palma. https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Sánchez-González, W. G. (2020). *Modelo de Gestión de Seguridad de la Información para Proyectos de TI Basado en ISO 27000 Y Scrum para Entidades de Registro Civil en el Ecuador* [Tesis Doctoral, Universidad Tecnológica Empresarial de Guayaquil]. Repositorio institucional. http://biblioteca.uteg.edu.ec:8080/handle/123456789/1175

Sianipar, Y. T., Widiyanti, N. W., y Agustini, A. T. (2018). Evaluasi Sistem Informasi Pengupahan PT. Tempu Rejo Menggunakan COBIT 5 Domain DSS. *AKTSAR: Jurnal Akuntansi Syariah, 1*(2), 187. https://doi.org/10.21043/aktsar.v1i2.5096

Teodoro, E. N. (2018). *Tipos de Investigación.* Universidad Santo Domingo de Guzmán. http://repositorio.usdg.edu.pe/bitstream/USDG/34/1/Tipos-de-Investigacion.pdf

Toro-Castillo, J. A. (2023). *La transformación digital y su impacto dentro de la seguridad de la información en Colombia*. Los Libertadores Fundación Universitaria. https://repository.libertadores.edu.co/bitstream/handle/11371/5684/TORO_JONIER_2023.pdf?sequence=1&isAllowed=y

Torres-Arriaga, M. G. (2019). *Análisis PESTEL*. UDG Virtual.http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/2973/1/An%C3%A1lisis%20PESTEL.PDF

Torres-Romero, M. D. C. (2021). *Análisis en seguridad informática basado en la norma internacional ISO/IEC 27001, para el diseño de un modelo que permita la verificación de integridad de documentos informáticos* [Trabajo de grado, Escuela Superior Politécnica de Chimborazo]. Repositorio institucional. http://dspace.espoch.edu.ec/bitstream/123456789/14948/1/20T01477.pdf

Tovar-León, A. E. (2019). *Implementación de un modelo de seguridad y privacidad de la información basada en la norma internacional ISO/IEC 27001 de 2013 en la Corporación Nasa Kiwe* [Tesis Doctoral, Uniautónoma del Cauca). Repositorio institucional. https://repositorio.uniautonoma.edu.co/bitstream/handle/123456789/116/T%20S-P%20047%202019.pdf?sequence=1&isAllowed=y

Useche, M. C., Artigas, W., Queipo, B. y Perozo, É. (2019). *Técnicas e instrumentos de recolección.* Gente Nueva.

Valbuena, C. (30 de noviembre de 2018). *¿Cómo analizar el contexto de la organización?* Kawak. Recuperado el 4 de marzo de 2024 de https://blog.kawak.net/mejorando_sistemas_de_gestion_iso/como-analizar-el-contexto-de-la-organizacion

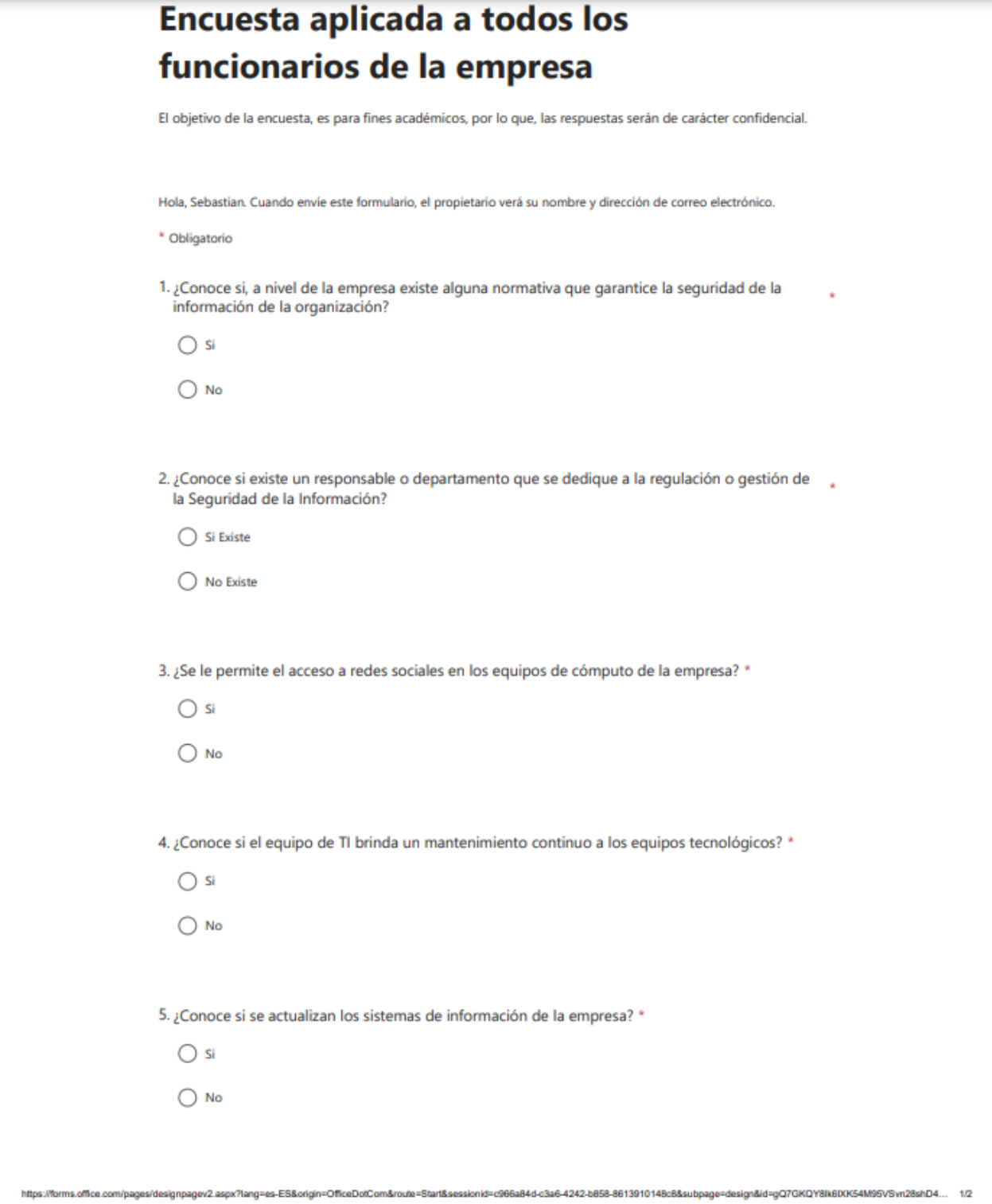
Valle, A., Manrique, L. y Revilla, D. (2022). *La investigación descriptiva con enfoque cualitativo en educación.* Pontificia Universidad Católica del Perú.

https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/184559/GU%c3%8dA%20INVESTIGACI%c3%93N%20DESCRIPTIVA%202022.pdf?sequence=1&isAllowed=y

Vecdis Tecnogestion. (2021). *Análisis PESTEL*. https://vecdis.es/wp-content/uploads/2021/05/PESTEL-ANA%CC%81LISIS-1.pdf

APÉNDICES

Apéndice 1. Encuesta aplicada a todos los empleados de la empresa



Encuesta aplicada a todos los funcionarios de la empresa

El objetivo de la encuesta, es para fines académicos, por lo que, las respuestas serán de carácter confidencial.

Hola, Sebastian. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico.

* Obligatorio

1. ¿Conoce si, a nivel de la empresa existe alguna normativa que garantice la seguridad de la información de la organización? *

- ◯ Si
- ◯ No

2. ¿Conoce si existe un responsable o departamento que se dedique a la regulación o gestión de la Seguridad de la Información? *

- ◯ Si Existe
- ◯ No Existe

3. ¿Se le permite el acceso a redes sociales en los equipos de cómputo de la empresa? *

- ◯ Si
- ◯ No

4. ¿Conoce si el equipo de TI brinda un mantenimiento continuo a los equipos tecnológicos? *

- ◯ Si
- ◯ No

5. ¿Conoce si se actualizan los sistemas de información de la empresa? *

- ◯ Si
- ◯ No

6. ¿Conoce si existe una persona que administra los sistemas de información de la empresa? *

- ◯ Si Existe
- ◯ No Existe

7. ¿Se solicitan con frecuencia cambios de contraseñas para el ingreso a los equipos tecnológicos y sistemas de información? *

- ◯ Si
- ◯ No

8. ¿Conoce si se realizan copias de seguridad de la información? *

- ◯ Si
- ◯ No
- ◯ Lo Desconozco

9. ¿Conoce si todos los activos de información (Hardware) están debidamente identificados con su respectivo número de placa? *

- ◯ Si
- ◯ No
- ◯ Lo Desconozco

10. ¿Conoce si existe un registro de los activos informáticos en desuso? *

- ◯ Si
- ◯ No

11. ¿El tendido de cables de Red está debidamente protegidos por canaletas? *

- ◯ Si
- ◯ No

Apéndice 2. Entrevista aplicada al gerente administrativo de la empresa

ENTREVISTA GERENTE ADMINISTRATIVO FINANCIERO

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.
Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Nombre del entrevistado	
Puesto que ocupa	

PREGUNTA		**RESPUESTA**
Pregunta 1	¿Se ha nombrado un responsable de Seguridad de Información en la empresa? ¿Por qué motivo?	
Pregunta 2	¿Todos los activos de información se encuentran registrados en un inventario y cuál es el proceso de gestión de este inventario?	
Pregunta 3	Partiendo del concepto, sensible: es todo lo que puede causar perjuicio hacia la empresa. (Daño de imagen, daño monetario). ¿Conoce usted algún proceso en el cual se comparta información crítica, sensible o delicada de la organización con algún tercero? ¿Cuál o cuáles?	
Pregunta 4	¿Cómo es el control que se maneja en la empresa para el tratamiento de información sensible?	
Pregunta 5	¿Cuál es el proceso para controlar el acceso a la información y a los sistemas?	
Pregunta 6	¿Están los datos encriptados en sus sistemas (archivos digitales, medios de almacenamiento, terminales, servidores)?	

Pregunta 7	¿Conoce si existen herramientas o soluciones que protejan los equipos donde se almacena información sensible, así como los sistemas informáticos de la empresa? ¿Cuál o cuáles?	
Pregunta 8	¿Cuál o cuáles dispositivos utilizan para el almacenamiento de los datos?	
Pregunta 9	¿Cada cuánto se realizan copias de seguridad para garantizar la disponibilidad de los datos?	
Pregunta 10	¿Cada cuánto se realizan pruebas de las copias de seguridad para garantizar la integridad de los datos?	
Pregunta 11	¿Conoce cuáles controles de monitoreo y acceso cuentan los cuartos de telecomunicaciones? ¿Cuales?	
Pregunta 12	¿La organización cuenta con un protocolo de seguridad para la preparación e instalación de los equipos de impresión a terceros? ¿Cual?	
Pregunta 13	¿Conoce si ha ocurrido algún tipo de incidente informático que comprometa la seguridad de la información? ¿Cuáles medidas se tomaron para solventar el incidente?	
Pregunta 14	¿Existe clasificación general (público, uso interno o confidencial) de cada activo de información? ¿Cuál es el proceso para identificarlo?	

Apéndice 3. Entrevista realizada al jefe de soporte técnico.

ENTREVISTA JEFE DE SOPORTE TÉCNICO

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.
Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Nombre del entrevistado	
Puesto que ocupa	

PREGUNTA		**RESPUESTA**
Pregunta 1	¿Se ha nombrado un responsable de Seguridad de Información en la empresa? ¿Por qué motivo?	
Pregunta 2	¿Todos los activos de información se encuentran registrados en un inventario y cuál es el proceso de gestión de este inventario?	
Pregunta 3	Partiendo del concepto, sensible: es todo lo que puede causar perjuicio hacia la empresa. (Daño de imagen, daño monetario). ¿Conoce usted algún proceso en el cual, se comparta información crítica, sensible o delicada de la organización con algún tercero? ¿Cuál o cuáles?	
Pregunta 4	¿Cómo es el control que se maneja en la empresa para el tratamiento de información sensible?	
Pregunta 5	¿Cuál es el proceso para controlar el acceso a la información y a los sistemas?	

Pregunta 6	¿Están los datos encriptados en sus sistemas (archivos digitales, medios de almacenamiento, terminales, servidores)?	
Pregunta 7	¿Conoce si existen herramientas o soluciones que protejan los equipos donde se almacena información sensible, así como los sistemas informáticos de la empresa? ¿Cuál o cuáles?	
Pregunta 8	¿Cuál o cuáles dispositivos utilizan para el almacenamiento de los datos?	
Pregunta 9	¿Cada cuánto se realizan copias de seguridad para garantizar la disponibilidad de los datos?	
Pregunta 10	¿Cada cuánto se realizan pruebas de las copias de seguridad para garantizar la integridad de los datos?	
Pregunta 11	¿Conoce cuáles controles de monitoreo y acceso cuentan los cuartos de telecomunicaciones? ¿Cuales?	
Pregunta 12	¿La organización cuenta con un protocolo de seguridad para la preparación e instalación de los equipos de impresión a terceros? ¿Cual?	
Pregunta 13	¿Conoce si ha ocurrido algún tipo de incidente informático que comprometa la seguridad de la información? ¿Cuáles medidas se tomaron para solventar el incidente?	
Pregunta 14	¿Existe clasificación general (público, uso interno o confidencial) de cada activo de información? ¿Cuál es proceso para identificarlo?	

Apéndice 4. Bitácora inventario de hardware

El propósito de la tabla es almacenar el inventario de activos de información a nivel *hardware.*

Inventario de hardware							
Identificador del equipo	**Descripción**	**Marca**	**Modelo**	**Identificador del proveedor**	**Fecha de adquisición**	**Contrato que da soporte**	**Garantía**
						Fecha de vencimiento	**Fecha de vencimiento**

Fuente: Elaboración propia.

Apéndice 5. Bitácora eliminación de activos de información

El propósito de esta tabla es almacenar los activos de información que se diseñen por daño o deterioro.

Eliminación de activos de información						
Detalle del equipo	**Marca**	**Modelo**	**Serie**	**Identificador del activo**	**Acción Borrado de información**	**Fecha de eliminación**

Fuente: Elaboración propia.

Apéndice 6. Bitácora inventario de software.

El propósito de esta tabla es almacenar el inventario de activos de información a nivel *software.*

Inventario de Software								
Identificador de la aplicación	**Aplicación**			**Fecha implantación**	**Base de datos utilizada**		**Identificador del proveedor**	**Propósito**
	Nombre	**Descripción**	**Versión**		**Nombre**	**Versión**		

Fuente: Elaboración propia.

Apéndice 7. Bitácora registro de proveedores

El propósito de esta tabla es describir el catálogo de proveedores de TI contratados por la entidad.

Registro de Proveedores					
Identificador del proveedor	**Nombre**	**País**	**Nombre del contacto**	**Teléfono del contacto y ext.**	**E-mail del contacto**

Fuente: Elaboración propia.

Apéndice 8. Bitácora registro de cuentas de usuario

El propósito de esta tabla es describir el catálogo de los empleados con acceso al sistema informático de la empresa.

Registro de cuentas de Usuario								
Usuario	**N.º de cedula**	**Nombre**	**Estado**		**Perfiles Asociados**		**Fecha de caducidad del usuario**	**Fecha de vencimiento de la clave**
			Activo		**Administrador**			
			Desactivado		**Digitador**			
			Inhabilitado		**Consultor**			
			Activo		**Administrador**			
			Desactivado		**Digitador**			
			Inhabilitado		**Consultor**			
			Activo		**Administrador**			
			Desactivado		**Digitador**			
			Inhabilitado		**Consultor**			
			Activo		**Administrador**			
			Desactivado		**Digitador**			
			Inhabilitado		**Consultor**			
			Activo		**Administrador**			
			Desactivado		**Digitador**			
			Inhabilitado		**Consultor**			

Fuente: Elaboración propia.

Apéndice 9. Bitácora registro del comité encargado de la seguridad de la información

El propósito de esta tabla es conocer la composición del Comité encargado de la seguridad de la información

Composición del Comité de Seguridad de la Información					
Nombre	**Puesto que desempeña en empresa**	**Cargo que desempeña en la seguridad de la Información**	**Ubicación**	**N.º de teléfono**	**Correo electrónico**

Fuente: Elaboración propia.