UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE CIENCIAS E INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS:

"Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, Según la Norma ISO/IEC 27001:2013"

PARA OPTAR EL TITULO PROFESIONAL DE

Ingeniero de Sistemas e Informática

AUTORES:

BACH. Lopez Torres, Christian Bryan

BACH. Espinoza Melendez, Juan Carlos

ASESOR:

Mg. Ruben Edgar, Hermoza Ochante

ID ORCID: https://orcid.org/0000-0003-4769-0101

DNI: 42037740

LIMA- PERÚ

2022

TÍTULO

Título: P**ropuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera de Lima, 2021 según la Norma ISO/IEC 27001:2013**

Autor: Bach. López Torres, Christian Bryan
Bach. Espinoza Melendez, Juan Carlos

Asesor: Mg. RUBEN EDGAR, HERMOZA OCHANTE

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este trabajo tuvo como objetivo general presentar una propuesta de un SGSI para una empresa de consultoría financiera en Lima, basada en Norma ISO/IEC 27001:2013. La metodología básica, descriptiva, no experimental, la técnica fue la encuesta, con una muestra representada por los 18 colaboradores de la empresa. Los resultados señalaron la presencia de violaciones a la ciberseguridad, lo cual hizo necesario diagnosticar vulnerabilidades y deficiencias en gestión de la información. Asimismo, se logró determinar los mecanismos técnicos para optimizar el SGSI, el cual debe basarse en planificación, ejecución, control y acción, con un equipo de verificación y respuesta, que ayude a tener los lineamientos y directrices claras para responder de forma oportuna, eficiente y rápida a un ciberataque. De igual manera, la propuesta del SGSI regida por la Norma ISO/IEC 27001:2013, logrará proteger y resguardar los activos informáticos, certificando la disponibilidad, confidencialidad e integridad de la información, y manteniendo la permanencia de las operaciones en contingencia ante la presencia de ataques no deseados. Se concluye que un SGSI fortalecido ayudará a aminorar riesgos contra ataques cibernéticos en una empresa consultora en Lima, 2021.

Palabras claves: Sistema de Gestión de Seguridad de la Información, ISO / IEC 27001: 2013, consultora, propuesta, ciberataque.

ABSTRACT

The general objective of this work was to present a proposal for an ISMS for a financial consulting company in Lima, based on ISO/IEC 27001:2013. The basic, descriptive, non-experimental methodology, the technique was the survey, with a sample represented by the 18 employees of the company. The results indicated the presence of cybersecurity violations, which made it necessary to diagnose vulnerabilities and deficiencies in information management. Likewise, it was possible to determine the technical mechanisms to optimize the ISMS, which must be based on planning, execution, control and action, with a verification and response team, which helps to have clear guidelines and guidelines to respond in a timely, efficient manner. and quick to a cyber attack. Similarly, the ISMS proposal governed by the ISO/IEC 27001:2013 Standard will manage to protect and safeguard computer assets, certifying the availability, confidentiality and integrity of the information, and maintaining the permanence of operations in contingency in the presence of from unwanted attacks. It is concluded that a strengthened ISMS will help reduce risks against cyber attacks in a consulting company in Lima, 2021.

Keywords: Information Security Management System, ISO / IEC 27001: 2013, consultant, proposal, cyber attack..

I. INTRODUCCIÓN

1.1. Realidad problemática

A nivel mundial, las empresas e instituciones públicas, usan tecnología de la información como una herramienta fundamental para realizar sus actividades o lograr sus objetivos; mediante las diferentes cualidades que los sistemas de información (SI) ofrecen, y por otro lado, enfrentar una amplia variedad de amenazas y riesgos asociados a los contornos informáticos actuales que pueden violar la seguridad de los sistemas.

Asimismo, las vulnerabilidades y amenazas evolucionan y aumentan con las tecnologías de información, igualmente, se necesita utilizar los recursos precisos para proteger la información como los activos sensibles de la empresa, para lo cual se necesita garantizar su disposición, mantener la integridad y confidencialidad. Esto se debe a la existencia de varios contextos de amenazas, que sucederán inesperadamente, por tanto, se hace necesario que la empresa mantenga una táctica de defensa, prevención y protección, que exhiba una presencia o continuidad definida por los contextos de amenaza que ha mostrado la experiencia y que una vez superados, se permita reanudar las operaciones, transacciones y actividades efectivamente protegidas.

En Latinoamérica, Deloitte Latan (2021), expresa: la tendencia presentada en los pasados años y considerando el desarrollo de lo invertido en seguridad de información, las compañías siguen soportando rupturas de seguridad. Así, resulta peligroso que la inversión se destine no sólo a efectuar medidas de protección, también a optimizar las posibilidades de respuesta y monitoreo, tarea que aún sigue pendiente para las empresas en AL&C.

Siguiendo lo anterior, 4 empresas de cada 10 han tenido un intento de violación de su seguridad en los pasados 24 meses Así, el 70% de las organizaciones mencionan no tener certeza de lo efectivo del proceso de protección ante ataques de ciberseguridad y sólo 3% realiza prácticas para valorar su capacidad de respuestas efectivas ante un posible ataque.

En el caso Peruano, según ESET (2020), el 61% de las organizaciones peruanas consultadas afirmaron que tienen políticas de seguridad; empero, solo un 29% mencionó que poseen un plan de continuidad y respuesta de la empresa, y solo un 23%

cataloga su información. Asimismo, según la "Encuesta Global de Seguridad de la Información 2019-2020 EY (2020), el 27% de las empresas del Perú tienen ciberseguridad desde la planificación en sus iniciativas de empresa; mientras que el 51% expresa la relación entre la ciberseguridad y su línea de negocio es nula o inexistente.

En este sentido, la estrategia más adecuada para proteger la información, es establecer una adecuada gestión de seguridad de la información, con la finalidad de manejar los riesgos, para poder identificarlos y focalizar los esfuerzos de protección hacia aquellos elementos que se encuentran más expuestos a los niveles de riesgo. En este sentido la Norma ISO/TEC 27001:2013.

En este sentido tenemos que, ISO27001 se refiere a SGSI. ISO27001 se describe la confidencialidad, integridad y aseguramiento, de la data y la información, también sobre los sistemas que la manejan. La aplicación de ISO27001 trata una diferencia en referencia al resto, que mejora la imagen y la competitividad de una empresa. De igual forma. el estándar ISO27001:2013 para los SGSI permite a las empresas la valoración de riesgo y la aplicación de controles necesarios para eliminarlos (Isotools, 2021).

El problema que se plantea en la Consultoría Financiera ha sufrido ciberataques con el fin de robo y violación de información incluido: Datos corporativos y datos personales. Con la propuesta de mejoras, el problema de riesgos de seguridad de información, las amenazas continúan aumentando. Por lo cual, la propuesta de un Sistema de Gestión de seguridad de la Información para una empresa de Consultoría Financiera con funciones de SI, a fin de proteger a las empresas y la información y resistir los ciberataques a la información delicada y privada de las corporaciones.

1.2. Planteamiento del problema

Problema general

¿De qué manera la propuesta de un sistema de Gestión de Seguridad de la Información según la Norma ISO/IEC 27001:2013 beneficia a una Empresa de Consultoría Financiera de Lima, 2021?

Problemas específicos

a) ¿Cuál es el diagnosticar la situación problemática sobre deficiencias en el SGSI en una empresa de consultoría financiera en Lima, 2021?

b) ¿Cuáles son los mecanismos técnicos que permitan optimizar el SGSI en una empresa de consultoría financiera en Lima, 2021?

c) ¿Cuál es la propuesta sobre un SGSI bajo la Norma ISO / IEC 27001: 2013 para aumentar la protección de la información en una empresa de consultoría financiera en Lima, 2021.

1.3. Hipótesis de la investigación

1.3.1. Hipótesis general

Un SGSI según la Norma ISO/IEC 27001:2013 beneficiará a la empresa de consultoría financiera de Lima, 2021 protegiendo la información sensible.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Generar una propuesta de un SGSI para una empresa de consultoría financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013.

1.4.2. Objetivos específicos

a) Diagnosticar la situación problemática sobre deficiencias en el SGSI en una empresa de consultoría financiera en Lima, 2021.

b) Identificar los mecanismos técnicos que permitan optimizar el sistema de gestión de seguridad de la información en una empresa de consultoría financiera en Lima, 2021.

c) Efectuar una propuesta sobre el SGSI bajo la Norma ISO/IEC 27001:2013 para aumentar la protección de la información en una empresa de consultoría financiera en Lima, 2021.

1.5. Variables, dimensiones e indicadores

1.5.1. Variable Independiente

- ✓ **Sistema de Gestión de Seguridad de la información (SGSI)**

Según Areitio (2008), el SGSI es un sistema que busca la detección de que implementa, monitorea, y optimiza la seguridad de la información. Implementando de una estructura organizativa en las empresas, que establece procesos, políticas, procedimientos, responsabilidades y recursos.

La ISO 27001:2013 es una norma que proporciona un entorno de acción para los SGSI con el fin de proporcionar integridad, confidencialidad y disponibilidad permanente de la información, tal como el cumplir con la norma legal. La certificación ISO27001 es necesaria para proteger sus activos más sensibles e importantes, como lo es, la información de sus clientes y empleados, cuidar la imagen empresarial y cualquier información delicada. La norma ISO tiene una visión fundamentada en técnicas para efectuar, mantener y operar un SGSI (NQA, 2020).

Tabla 1
Operacionalización de las variables

Dimensiones	Dimensiones	Indicadores
Sistema de Gestión de Seguridad de la información (SGSI)	Planeación	• Análisis de la situación actual • Políticas de seguridad • Análisis de riesgo
	Ejecución (Do)	• Implementación del SGSI • Control de riesgos
	Verificación (Check)	• Verificación de implementación del SGSI • Verificación del control de riesgos
	Acción (Act)	• Acciones preventivas • Acciones correctivos

Fuente. Elaboración propia.

1.6. Justificación del estudio

1.6.1. Justificación Teórica

La presente investigación se justifica teóricamente por cuanto proveerá las condiciones de administración, viabilidad y oportunidad requerida para que la información este asegurada y apoye la consecución de los objetivos estratégicos de la empresa, mediante el aseguramiento y la protección de la información que es muy importante para garantizar la gestión administrativa, operativa y financiera, de la empresa, y con ello asegurar el cumplimiento de sus funciones.

1.6.2. Justificación Práctica

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI), significa que la empresa toma con mucha importancia la seguridad de la información, que se caracteriza a por poseer un método o modelo de seguridad que tiene una estrategia eficiente, eficaz y proactivo en la aplicación del plan que generalmente se aplica en la mitad de las organizaciones a nivel mundial que son las primeras en adoptar este tipo de modelos de seguridad.

1.6.3. Importancia del estudio

Un Sistema de Gestión de Seguridad de la Información, muestra la responsabilidad de la empresa hacia lo importante y sensible que es el tema de la Seguridad de la Información y suministra los elementos necesarios para agenciar de manera eficaz los riesgos que puedan atentar contra la seguridad de la información, esto genera confianza en sus clientes o asesorados que es básico para el desarrollo y sostenibilidad de la empresa.

El diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) desarrollado en base a un estándar de seguridad ampliamente reconocido y aceptado a nivel mundial, representado en la norma ISO 27001, permitiendo estructurar los fundamentos necesarios que permitan establecer un modelo correcto de seguridad en la consultora basado en las mejores practica para la implementación del mejor sistema de seguridad, que permitirá garantizar su mejora y desarrollo continuo debido a su permanecía y evolución en el tiempo.

1.7. Trabajos previos

1.7.1. Antecedentes internacionales

A nivel internacional Rincón (2020) en su trabajo investigativo titulado: Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la Norma Internacional ISO/IEC 27001:2013 para la empresa ESSENSALE S.A.S., expuesta ante la Universidad Nacional Abierta y a Distancia en la ciudad de Bogotá – Colombia. El objetivo principal de la investigación estuvo en el diseño de un sistema de gestión de seguridad de la información implementando la norma internacional ISO/IEC 27001:2013 para la empresa Essensale S.A.S. La metodología fue de tipo aplicada con un diseño aplicado en la investigación del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), la población y muestra estuvo compuesta por cuatro departamentos que corresponden a las áreas de Recursos Humanos, Financiero, Mercadeo y Tecnología. Como instrumento y técnica para la recolección de daros se aplicó la encuesta. Una vez finalizada la investigación y basados en los resultados obtenidos el autor concluye que quedó en evidencia que con la metodología de análisis y gestión de riesgos MAGERIT la empresa ESSENSALE S.A.S alcance un mayor y mejor control en la utilidad de sus activos en relación a los posibles riesgos que pudiera verse afectada, así como la implementación del SGSI les brindará mayor protección a los activos de la empresa, favorece a la continuidad de la operación, neutralizando todo tipo de amenaza creando confianza a clientes nuevos en el uso de los servicios y productos ofrecidos por los distintos medios tecnológicos; de igual manera se recomienda que la empresa tiene el deber de mejorar y dar a conocer los nuevos elementos presentados en el proyecto, entrenando a todo su personal de lo que se puede alcanzar con el SGSI para darle continuidad al negocio, así como a las operaciones.

En este sentido, Ordoñez y Castro (2017) en su investigación denominada: Diseño de un sistema de gestión de seguridad de la información para la compañía SISELCOM S.A.S. bajo la norma ISO 27001:2013, presentada ante la Universidad Piloto de Colombia. Bogotá – Colombia, investigación necesaria para optar a la titularidad académica de Especialista en Seguridad Informática. El principal objetivo de la investigación estuvo en el diseño de un sistema de gestión de seguridad de la información que admita la identificación de los riesgos asociados al estado actual de seguridad de los procesos y activos de información en la compañía SISELCOM S.A.S. y de igual forma establecer

los controles precisos para su protección, referenciados en la norma NTCISO-IEC 27001:2013. La metodología aplicada en la investigación fue de tipo aplicada, la población estuvo compuesta por lo empleados del área de comercial, jurídica, administrativa y de contaduría. Para la recolección de datos se aplicaron como técnicas e instrumentos la entrevista y el cuestionario, finalmente culminada la investigación el autor concluye que al efectuar el diseño del sistema de gestión de seguridad de la información bajo la norma ISO 27001:2013 para la compañía SISELCOM S.A.S, se alcanzó establecer el estado actual de desempeño frente a la norma, encontrando que la compañía está en la primera etapa de madurez de cumplimiento puesto que en la compañía nunca habían considerado la seguridad en sus procedimientos y carecían del conocimiento sobre el tema, reflejándose en las encuestas efectuadas a la gerencia y a los colaboradores donde en la mayoría de los casos se lograron respuestas negativas en relación al cumplimiento y conocimiento de los controles de la norma, de igual manera se sugiere establecer, efectuar y mantener un sistema de gestión de la calidad que este ordenado u organizado con los planes y objetivos estratégicos de negocio basados con la norma ISO 9001:2015, así como incluir el compromiso de una mejora perenne del sistema de gestión de la calidad.

Vargas et al. (2017) en su trabajo de investigación titulado: Diseño de un sistema de gestión de seguridad de la información de los registros de los usuarios de la biblioteca Chaid Neme, basado en la norma NTC-ISO-IEC 27001:2013, investigación requerida para optar a la titularidad de Especialista en Auditoría de Sistemas, presentada ante la Universidad Francisco de Paula Santander Ocaña, Colombia, donde el objetivo principal de la investigación estuvo en el diseño de un sistema de gestión de seguridad de la información, apoyado en la norma NTC-ISO-IEC 27001:2013, para la Biblioteca Chaid Neme de la Ciudad de Ocaña. La investigación aplicó un tipo de metodología descriptiva, para la recolección de datos se aplicaron como técnicas e instrumentos la observación directa, la encuesta, entrevistas no estructuradas, lista de chequeo. La población y muestra estuvo definida por los procedimientos que manipulan los usuarios de la biblioteca. Basados en los resultados que evidenciaron la carencia de conocimientos de las buenas prácticas en seguridad de la información, así como la usencia de políticas de seguridad, el autor concluye: quedó establecido que los riesgos en los que se encuentra expuesta la compañía, especialmente son por la carencia de conocimiento de buenas prácticas de seguridad de la información, por parte de los

empleados del área administrativa de la misma. Finalmente, se recomendó formalizar el sistema de seguridad a través de la documentación de los programas, políticas y procedimientos determinados para gestionar los riesgos de seguridad de información de la dependencia, así como se deberán aplicar los controles de las normas ISO 27001 que consienten la administración del funcionamiento de un sistema de localización de intrusos dentro de un Sistema de gestión de seguridad de la información.

1.7.2. Antecedentes nacionales

A nivel nacional, Benitez (2019) en su investigación titulada: "Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza" presentada ante la Universidad Tecnológica del Perú; Lima-Perú, investigación necesaria para optar a la titularidad de Ingeniero de Seguridad y Auditoría Informática. El objetivo general de la investigación estuvo en la implementación de un Sistema de Gestión de Seguridad de la información en el Departamento de Proyectos que ubicado dentro de Área de Planta en la fábrica de Radiadores Fortaleza. La metodología fue de tipo aplicada con un diseño aplicado en la investigación del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), con un nivel documental – correlacional experimental, la población y muestra estuvo compuesta por todo el personal del área de dibujo mecánico de planta, así como las jefaturas de la compañía; para la recolección de datos se aplicaron como técnicas e instrumentos la entrevista y el cuestionario. Una vez finalizada la investigación el autor concluye que para mantener los índices de Seguridad de la Información es necesario el uso controlado e inspeccionado del servicio de Internet en la compañía de Radiadores Fortaleza, así como desarrollar el Plan de Implementación de un SGSI demanda de un meticuloso trabajo, desempeño y gran esfuerzo de toda la Empresa, desde el más alto grado jerárquico de la empresa hasta los empleados de los servicios generales. El cumplimiento de las políticas, controles, metodologías y estrategias diseñadas en el desarrollo del SGSI están acompañada del compromiso de los directores de cada departamento siendo éstos los responsables de los resultados del SGSI. El resultado fue gratificante, se minimizó de manera significativa los incidentes técnicos, así como se redujo el tiempo de respuesta en el responsable de TI y en el usuario, logrando afianzar la confianza y seguridad usuario – área TI, por último, se recomendó el compromiso

general o total de los empleados de la compañía, en especial de los inversionistas ya que prestan poca atención a este tipo de herramientas.

Por su parte, Armas (2018) en su trabajo de investigación denominado: "Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016" presentado ante la Universidad Nacional Santiago Antúnez de Mayolo en Huaraz – Perú, investigación requerida para optar a la titularidad de Ingeniero de Sistemas e Informática, donde el objetivo principal del estudio estuvo en el desarrollo de un sistema de gestión de seguridad de la información, para minorar riesgos en los activos de información de la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia. La metodología aplicada en la investigación fue de tipo aplicada, descriptiva, con diseño descriptivo; para la recolección de información se aplicaron como instrumentos la entrevista, la encuesta, así como la observación. La población y muestra estuvo compuesta por diez empleados de la Sub Gerencia de Informática y Telecomunicaciones. Una vez culminada la investigación los autores concluyen que la institución carece de medidas de seguridad guiados y documentados, lo que este proyecto será de gran ayuda para el inicio en minimizar de los riesgos que existen los mismo que perjudican el futuro a la institución, la metodología MAGERIT permitió la identificación de varios puntos relevantes para la gestión y el análisis de riesgos, finalmente, recomiendan implementar el SGSI, la cual es de muy importancia para minimizar los riesgos visualizados, de igual manera se sugiere la instalación de un comité de seguridad de la información que este dirigido por el Sub Gerente de del mismo departamento, el mismo se encargara de implementar el Sistema de Gestión de Seguridad de la Información.

Yana (2018) por su parte, en su investigación denominada: Propuesta de un sistema de gestión de seguridad de la información, empleando el método MAGERIT para el Gobierno Regional Puno Caso: Proyecto especial Camélidos Sudamericanos – PECSA, 2017, expuesta ante la Universidad Privada Telesup, en la ciudad de Lima – Perú, donde el objetivo principal de la investigación estuvo en plantear un Sistema de Gestión de Seguridad de la Información, aplicando el método de MAGERIT para el Gobierno Regional Puno, Caso: Proyecto Especial Camélidos Sudamericanos – PECSA, año

2017. La investigación aplicó una metodología de tipo documental, descriptiva; con diseño no experimental, como técnicas e instrumento para la recolección de datos se aplicó la encuesta y la entrevista, La metodología aplicada para el análisis de riesgos es el MAGERIT. Al término de la investigación el autor concluye que la empresa no cuenta con un Sistema de Gestión de Seguridad de la Información, por tanto, se procedió con la realización de la metodología del método MAGERIT, por ende, se plantea: un Manual y una Política del SGSI para el Proyecto Especial Camélidos Sudamericanos – PECSA, dentro del cual se instituyen los criterios para su control, implementación, seguimiento y optimización continua del SGSI, así como se recomienda la colocación en marcha de la ejecución e implementación del Manual y Política de SGSI, para evitar la pérdida de la información el Proyecto Especial Camélidos Sudamericanos (PECSA).

1.8. Marco Teórico

1.8.1. Sistema de Gestión de Seguridad de la Información (SGSI)

a) Definición SGSI

Para esta variable, Galindo (2014) la define, como: "El conjunto de medidas reactivas y preventivas de las instituciones y de los sistemas tecnológicos y especializados que ofrecen resguardo y protección a la información manteniendo la disponibilidad, la integridad y la confidencialidad de la misma" (p. 100). Por su parte, Miranda (2013), expresa que: "es un enfoque gerencial para la seguridad. Se trata de un proceso de gestión de riesgos explicito, sistemático y amplio acerca de la seguridad. En él se contempla la determinación de objetivos, medición y planificación del desempeño" (p.25). Es importante la implementación de un SGSI, para cuidar a la empresa, evitando las inversiones mal dirigidas, que se usan para combatir riesgos sin una evaluación previa. Puede suceder también que se minimicen riesgos, permitiendo retraso en las medidas de seguridad referentes a la práctica de los cambios internos de la empresa y su entorno. Posiblemente exista, falta de transparencia en la asignación de funciones y responsabilidades en los activos de información; falta de procedimientos que cubran la respuesta necesaria y puntual ante eventos o afecte la continuidad, entre otros.

Por su parte, Cano (2011) define la Seguridad de información tal como: una actividad de análisis, de riesgos, de amenazas de escenarios, de esquemas reglamentados y buenas

prácticas, que necesitan niveles de seguridad para los procesos y para la tecnología, con la finalidad de mejorar la confianza en el almacenamiento, uso, transmisión, disposición y recuperación de la información.

Por otro lado, según la NTP-ISO/IEC 17799: Norma Técnica Peruana (2015), conceptualiza la seguridad de la información como: La información es un activo que requiere una adecuada protección. La seguridad de la información la protege de una amplia formas de amenazas a fin de asegurar el funcionamiento empresarial, disminuye los daños empresariales y optimiza las oportunidades comerciales y el retorno de la inversión y. La seguridad se logra implementando un grupo de controles, representados por: procedimientos, estructuras organizativas, , políticas, prácticas y funciones de hardware .y software tales controles se establecen, implementan, monitorean y revisan donde sea necesario, a fin de asegurar los objetivos específicos de seguridad y negocios.

b) Evaluación de riesgos

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, la evaluación de los riesgos de seguridad tiene que con "los requisitos de seguridad que se identifican a través de una evaluación sistemática de los riesgos. Estas evaluaciones de riesgos deben aplicarse repetidamente de forma periódica para poder identificar cualquier cambio que pueda incidir en los resultados de la evaluación" (p.3)

Reconocer el potencial de fallas de seguridad relacionadas con vulnerabilidades, vulnerabilidades, amenazas e impactos en los activos, el impacto de las fallas de seguridad dentro de la empresa en relación con la pérdida de integridad, confidencialidad y disponibilidad de los activos de información para investigar. Por otro lado, es importante no solo evaluar el riesgo, sino también analizar sus consecuencias globales, que pueden ir desde el simple sabotaje de la información hasta el robo o pérdida de información importante, confidencial o relacionada que haya.

c) Tratamiento del riesgo

ISO 31000 (2009) cubre: Todo lo que hace una organización conlleva un riesgo. La gestión del riesgo implica determinar, evaluar y analizar si se puede controlar tratándolo para cumplir con los estándares de seguridad. Sin embargo, establece los medios específicos a través de

los cuales una organización gestiona el riesgo y los principios que deben cumplirse para una gestión eficaz del riesgo.

Este estándar internacional recomienda la implementación, el desarrollo y la mejora continua para coordinar los procesos de gestión de riesgos en una organización. La gestión de riesgos puede incluir a toda la organización, diferentes niveles, sectores, actividades específicas, funciones y proyectos en cualquier momento. El tratamiento del riesgo incluye la selección y aplicación de medidas apropiadas para modificar los riesgos con el fin de evitar pérdidas asociadas a los factores de riesgo.

d) Prevención del riesgo

Para administrar su cobertura, debe seguir ciertos procedimientos. En este sentido, (Purdy, 2010) repite ciertos criterios de desempeño. Tener requisitos de desempeño claros y cumplirlos garantiza una gestión de riesgos eficaz y eficiente. Un principio eficaz de la gestión de riesgos en ISO 31000 es que hay que asumir el riesgo. Los principios efectivos de la gestión de riesgos en ISO 31000 es que debería:

1. Crear y proteger valor;
2. Ser parte integral de todos los procesos organizacionales;
3. Sea parte de la toma de decisiones;
4. Abordar explícitamente la incertidumbre;
5. Sea sistemático, estructurado y oportuno;
6. Estar basado en la mejor información disponible;
7. Estar hecho a la medida;
8. Tenga en cuenta los factores humanos y culturales;
9. Sea transparente e inclusivo;
10. Sea dinámico, iterativo y receptivo a cambio;
11. Facilitar la mejora continua de la organización.

e) Norma ISO/IEC 27001:2013

Para el desarrollo e implementación de sistemas de gestión de seguridad de la información se aplican estándares de seguridad que pueden ser utilizados por todo tipo

de organizaciones privadas y/o públicas. La norma ISO 27001 describe cómo debe estructurarse la seguridad de la información en cualquier tipo de empresa u organización. Definir cómo se gestiona la seguridad de la información a través de un Sistema de Gestión de Seguridad de la Información (SGSI). ISO 27001 describe los requisitos necesarios para implementar, establecer, mantener y mejorar un SGSI certificado por una organización. En la versión 2005 se aplica desde el ciclo PDCA (Plan, Do, Check, Act). Con el lanzamiento de 2013, las organizaciones son libres de elegir el modelo de mejora continua que utilizan para su SGSI.

Un SGSI: según (ISO27000, 2021) es "la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización". Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se revela ni se pone a disposición de entidades, individuos o procesos no autorizados.
- Integridad: mantenimiento de la completitud y exactitud de la información y sus métodos de proceso.

A continuación, las 4 etapas de acción para aplicar las normas ISO/IEC 27001:2013:

a) Planear. Para la implementación de un SGSI (ISO27000, 2021) según la norma se hace necesaria la Planificación que incluye actividades, utilización de recursos y objetivo a lograr en las etapas siguientes. Toda actividad asociada y los productos son producto de la calidad de las responsabilidades, que continua en la etapa de Evaluación.

Las acciones a realizar son:

- Crear la Política de Seguridad de la Información
- Nombrar al Gestor de seguridad de la información,
- Conformar el comité de Seguridad de la Información.
- Definir el plan general de seguridad de la Información
- Planificar un Programa de Trabajo Anual.

b) Hacer (Do). Para Rueda y Castillo (2017), hacer (Do): "Es la fase donde se implementa el SGSI mediante la aplicación de los controles de seguridad escogidos, asignado los responsables y la ejecución de los procedimientos" (p.2). Se debe aplicar un plan de tratamiento de riesgos, que busca lograr los objetivos de control identificados, donde se incluyen las responsabilidades, las prioridades y asignación de recursos. Se proponen controles que controlen los objetivos de control. Determinar un sistema de medidas que permita obtener los resultados comparables y reproducibles a la hora de medir la eficacia de los controles.

Indicadores:

- Plan de gestión
- Implantar SGSI
- Controles de seguridad

c) Verificar (Check). De igual forma, Rueda y Castillo (2017) expresan que la verificación: "Es la fase de monitorización del SGSI donde se verifica y audita que los controles, políticas, procedimientos de seguridad se están aplicando de la manera esperada" (p.3). En tal sentido, la empresa revisará la efectividad del SGSI según la norma ISO 27001, que cubre la política y los objetivos de seguridad del SGSI, además de corroborar los resultados de las mediciones de eficacia, de las auditorías, de los incidentes, observaciones, sugerencias realizadas por las partes interesadas.

d) Actuar (Act). La empresa, implementará en el SGSI, las actividades correctivas y preventivas, las actualizaciones identificadas, necesarias en referencia a la norma ISO27001 y aprendiendo de las experiencias de la empresa y de otras. Hay que dar a conocer las actividades de mejora, con un nivel de detalle preciso y señalar la forma de proceder Se asegurará que los upgrade implementados esten a nivel de los objetivos de la empresa (ISO27000, 2021).

Indicadores:

- Acciones Preventivas
- Acciones Correctivos

1.9 Definición de términos básicos

1.9.5Sistema de Gestión de Seguridad de la Información (SGSI)

El grupo de medidas reactivas y preventivas de las instituciones y de los sistemas tecnológicos y especializados que ofrecen resguardo y protección a la información manteniendo la disponibilidad, la integridad y la confidencialidad de la misma

1.9.2 Norma ISO 27001

La normativa ISO 27001, señala la forma de organizar la seguridad de la información en toda clase de compañías o instituciones. Está establece como manejar la seguridad de la información a través de un sistema de gestión de seguridad de la información (SGSI).

1.9.3 Ciberseguridad

En oportunidades escrita en dos palabras: (seguridad cibernética) es la dependencia de la tecnología de la información mancomunado con la seguridad, protección de datos de los sistemas informáticos y en contra de ataques maliciosos o agresiones informáticos del mundo digital.

1.9.4 Políticas de ciberseguridad

Esta, está encaminada a gestionar de manera eficaz la seguridad de la información presentada por los sistemas informáticos de la compañía, así como los activos participantes en sus procedimientos.

1.9.5. Riesgos de ciberseguridad

Estos generalmente, están relacionados a intrusiones, *phishing*, contagio de alguna clase de códigos maliciosos, entre otros. La gestión de riesgos de ciberseguridad se debe comprender como "uno de los pilares fundamentales para salvaguardar la confidencialidad, disponibilidad e integridad de los activos de información, infraestructuras críticas y datos personales en el ciberespacio".

II. MÉTODO

2.1. Tipo y diseño de la investigación

2.1.1. Tipo de investigación

Fue investigación básica, porque se buscaron generar conocimiento para su aplicación práctica encaminada a la solución de problemas que contienen objetivos previamente definidos. Para Hernandez y Mendoza (2018), estos objetivos pueden ser de mediano o corto plazo, siendo entonces una investigación dirigida a menudo a determina un uso práctico de los resultados de la investigación pura. Involucrando también el conocimiento disponible, de diferentes fuentes, con miras a una utilidad económica y social. Así que, se generó una propuesta de un SGSI, según la Norma ISO/IEC 27001:2013.

2.1.2. Diseño de la investigación

El diseño de la investigación fue no experimental. "Se denominan así los estudios en los cuales no se aplica el método experimental. Fundamentalmente es de carácter descriptivo y emplea la metodología de observación descriptiva" (Sanchez et al., 2018, p.81). Así que, en este diseño, la variable de interés para el estudio se observó tal como ocurre de forma natural.

2.1.3. Nivel de la investigación

El tipo de investigación será descriptivo. En este sentido, Hernandez y Mendoza (2018) señalan:

> Los estudios descriptivos pretenden especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Tratan de medir o recolectar datos y ofrecer información sobre los diversos conceptos, variables, dimensiones o componentes del problema a investigar. (p.108).

En este sentido, Hernandez y Mendoza (2018) mencionó que, representa un conjunto de procesos organizados de una forma consecutiva con la finalidad de comprobar ciertos supuestos. “Inicia con una idea que se delimita y genera preguntas de investigación y objetivos, se revisa la literatura y se construye un marco teórico” (p.6).

El proceso descriptivo tuvo como fin identificar, registrar y analizar las características, factores o variables que se relacionan con los procesos llevados en la empresa consultora en relación a la protección de la información. Este tipo de investigación puede entenderse como un estudio de los aspectos anteriormente mencionados, y que luego de la recolección de datos, se realizó un análisis de la variable para una posterior determinación de los efectos resultantes sobre el sistema de protección informático.

2.2. Población y muestra

2.2.1. Población

Para Arias (2017), “la población es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de investigación” (p.61).

La población estuvo representada por los procesos llevados a cabo en la consultora para el respaldo y protección de su información; así como los 18 servidores (5 ingenieros en sistemas, siendo especialistas en seguridad informática de la empresa, más 2 directivos, 2 coordinadores, 9 analistas)

2.2.2. Muestra

En este sentido, la muestra es la parte de esa población que se selecciona y sobre la cual se efectuá la medición y observación de las variables. En nuestro caso de estudio, la muestra será de tipo censal, “aquella donde todas las unidades de investigación son consideradas como muestra. De allí, que la población a estudiar se precise como censal por ser simultáneamente universo, población y muestra” (Ramírez, 2012, p.387).

La muestra estuvo representada por los procesos llevados a cabo en la consultora para el respaldo y protección de su información; así como los 18 servidores de la empresa consultora.

2.3. Técnicas para la recolección de datos

2.3.1. Técnicas

Las técnicas de recolección de datos, según Sanchez et al. (2018), "son medios que se utilizan para recoger la información en la investigación. Pueden ser directas o indirectas. Las directas son las entrevistas y las observaciones; las indirectas son los cuestionarios, las escalas, los inventarios y los tests" (p.120). En este caso se utilizó la encuesta como técnica y la observación; en la cual se aplica un instrumento de recolección de datos formado por un conjunto de preguntas cuyo objetivo es recabar información práctica. Además, la observación directa de los procesos llevados a cabo en la empresa consultora en el resguardo de su información.

2.3.2. Instrumentos

Los instrumentos son, herramienta que forma parte de una técnica de recolección de datos. Puede darse como una guía, un manual, un aparato, una prueba, un cuestionario o un test (Sanchez et al., 2018). En el caso actual, se aplicó un cuestionario, así como la observación directa relativo al estudio para la propuesta de un SGSI en la empresa consultora, considerando la evaluación, tratamiento y previsión del riesgo mediante las 4 fases del ciclo PDCA.

2.4. Validez y confiabilidad de instrumentos

2.4.1. Validez del instrumento

Para la validación de contenido de la encuesta, se utilizó el juicio de tres expertos, profesores de la universidad, así como expertos en asesoramiento de tesis.

2.4.2. Criterio de confiabilidad de instrumento

La confiabilidad de la Encuesta, será medida usando el coeficiente Alpha de Cronbach

$$\alpha = \frac{k}{(k-1)}\left(1 - \frac{\sum \sigma_i^2}{\sigma_X^2}\right)$$

Donde

k = es el número de ítems

$(\sigma_i)^2$ = varianza de cada ítem

$(\sigma_x)^2$ = varianza del cuestionario total

Según Ñaupas et al. (2018) un instrumento es confiable cuando la medición no varía de manera significativamente, ni en aplicación, ni en tiempo a diferentes sujetos. La confiabilidad genera confianza cuando, se aplica en condiciones similares, los resultados son los mismos siempre. Se recomiendad los siguientes criterios para gvalorar los coeficientes de alfa de Cronbach:

Coeficiente alfa > 0.9 es excelente
Coeficiente alfa > 0.8 es bueno
Coeficiente alfa > 0.7 es aceptable
Coeficiente alfa > 0.6 es cuestionable
Coeficiente alfa > 0.5 es pobre
Coeficiente alfa < 0.5 es inaceptable

El coeficiente del Alfa de Cronbach fue de 0.85, indicando que la fiabilidad es buena para el instrumento usado.

2.5. Procesamiento y análisis de datos

El procesamiento de datos, es una fase del proceso que incluye tareas como la organización de los datos obtenidos para codificarlos, analizarlos estadísticamente, graficarlos y contrastarlos. Por su parte, el análisis de datos, es una etapa que consiste en organizar la información obtenida para ser tratada en forma analítica, describiendo, caracterizando e interpretando la información (Sanchez et al., 2018)

Este estudio tuvo como objetivo utilizar el modelo descriptivo, la importancia de una política de seguridad de la información en la empresa consultora, donde se desarrolló una propuesta en SGSI, con el fin de mostrar la importancia de la información y cómo se debe estar debidamente protegido. Para recolectar la información se realizaron visitas in situ para observar su infraestructura y cómo se exponen los equipos, conocer mejor los procesos internos. De esta manera, se puede mencionar los siguientes pasos realizados para darle respuesta a los objetivos específicos:

- Dentro del texto descriptivo, constó de una percepción sensorial, que proporciona veracidad en la información recopilada a través de una serie de preguntas a los ingenieros de sistemas de la empresa consultora, y en conjunto con la observación directa, se hizo el levantamiento de la información para el diagnóstico de la situación actual. (Objetivo específico 1)

- Una vez analizados los inconvenientes y/o deficiencias relativo a las vulnerabilidades en la protección de la información de la consultora, se procedió a darle respuesta de cada uno de ellos mediante la identificación de mecanismos técnicos que permitan optimizar el SGSI, realizándose esto mediante el ciclo PDCA. (Objetivo específico 2)

- Para desarrollar la exploración del tema, se realizó una revisión documental en base a la Norma ISO/IEC 27001:2013 para tener una mejor comprensión del tema abordado, con esto realizar una propuesta de política de seguridad de la información. (Objetivo específico 3).

Finalmente, se analizaron estos hallazgos, comparándose con los trabajos previos, así como los aspectos teóricos, para llegar a las respectivas conclusiones y recomendaciones.

2.6. Aspectos éticos

Los aspectos éticos fundamentales en este trabajo fueron la caracterización de la no discriminación en la selección de personas sin exposición a riesgos innecesarios. En cuanto al método, se describieron las técnicas, procedimientos, equipos y materiales necesarios respetando los derechos de autor. Además, con respecto al formulario de recogida de datos utilizados, se respetaron mediante la confidencialidad del caso, lo suministrado y/o transmitido por los encuestados, en lo referente a sus percepciones y perspectivas en equipo de sus diferentes intervenciones.

Así que, se garantiza la preservación de los datos, confidencialidad y anonimato de las personas investigadas con el fin de asegurar el respeto y la prevención de daños, además de dedicar la atención necesaria a las acciones que promuevan el resguardo de los datos suministrados.

III. RESULTADOS

3.1. Diagnosticar la situación problemática sobre deficiencias en el SGSI

La investigación se desarrolló a través de la observación y el levantamiento de información mediante conversaciones e intercambio de información. Se notó desde el principio que la gran mayoría de las personas allí no tenían idea de qué es la seguridad, qué significa mantener un entorno informático seguro, ya que tenían sus contraseñas de inicio de sesión escritas en papeles adhesivos en los teclados, es decir, allí fue la falta de conocimiento de los empleados sobre lo que es mantener segura a una empresa en el campo de informática. A excepción de los ingenieros de sistemas, los demás empleados en la empresa no estaban al tanto de qué tipo de información era realmente importante, cuáles eran los posibles problemas que se tendrían en caso de falla del equipo, en un posible robo de información, a quién acudir y cuáles eran los procesos de recuperación.

Durante estas visitas, no se encontraron algún tipo de documento sobre políticas de seguridad, documentación de estructura, respaldo, plan de continuidad, contacto de los responsables de cada sistema y las respuestas generalmente no se tenían. Todo ello sin una estructura documental creada y actualizada, de forma que se pudiera agilizar cualquier contacto, soporte, recuperación en caso de incidencias. Con eso, se sugirió iniciar el proceso relevando la estructura de informática para entender qué había, saber qué proveedores de servicios de esta empresa y cómo se realizan los controles de acceso de estos y, finalmente, armar una matriz cualitativa de las deficiencias y con este documento que posibles mejoras son posibles para la implementación de una política de seguridad.

Bajo las premisas mencionadas, en este apartado se realizó el diagnóstico de la situación problemática sobre deficiencias en el sistema de gestión de seguridad de la información. Para tal fin, en primer lugar, se efectuó un inventario de los eventos de violaciones a la ciberseguridad, que se identificaron durante el año 2021 y que pueden ser catalogados como ciberataques, a partir de los datos obtenidos de la tormenta de ideas con los especialistas entrevistados y de los registros suministrados por los mismos. Es decir, los diferentes tipos de eventos ocurridos sumaron un total de 264, se incluyeron: hackeo de identidad (61 eventos), robo de información (57 eventos), infección con código malicioso (51 eventos), infección con malware (32 eventos), acceso indebido a sistemas

(25 eventos), acceso indebido a información (20 eventos), y detección de exploits (18 eventos). A continuación, el resumen de eventos (Tabla 2):

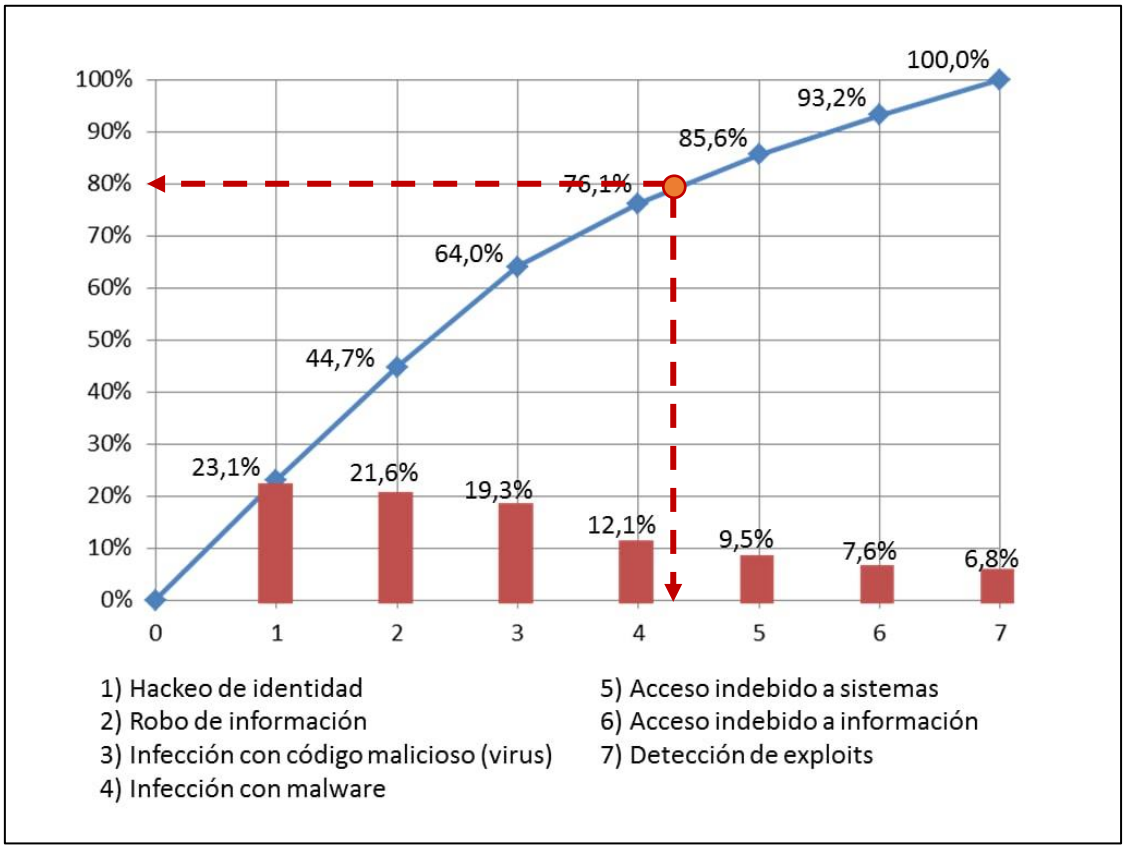
Tabla 2
Inventario de los eventos de violaciones a la ciberseguridad.

Evento de violación de la ciberseguridad	Numero de eventos	Porcentaje	Acumulado
1) Hackeo de identidad	61	23,1%	23,1%
2) Robo de información	57	21,6%	44,7%
3) Infección con código malicioso (virus)	51	19,3%	64,0%
4) Infección con malware	32	12,1%	76,1%
5) Acceso indebido a sistemas	25	9,5%	85,6%
6) Acceso indebido a información	20	7,6%	93,2%
7) Detección de exploits	18	6,8%	100,0%
Total	**264**	**100%**	

Nota. Elaboración propia en base a la información obtenida de la empresa.

Con los datos recopilados en la Tabla 2, se procedió a generar un Diagrama de Pareto, mostrado en la Figura 1, donde puede visualizarse la frecuencia en que produjo cada evento de violación a la ciberseguridad. De los resultados obtenidos, se pudo identificar que, los 4 grandes inconvenientes que ocurrieron casi representan el 80%, siendo el hackeo de identidad (23,1%) es el evento más frecuentemente observado, seguido de robo de información (21,6%), infección con código malicioso (19,3%), infección con malware (12,1%), y menor porcentaje el acceso indebido a sistemas (9,5%), acceso indebido a información (7,6%), siendo la detección de exploits (6,8%) el evento que se produjo con menos frecuencia.

Figura 1
Diagrama de Pareto.

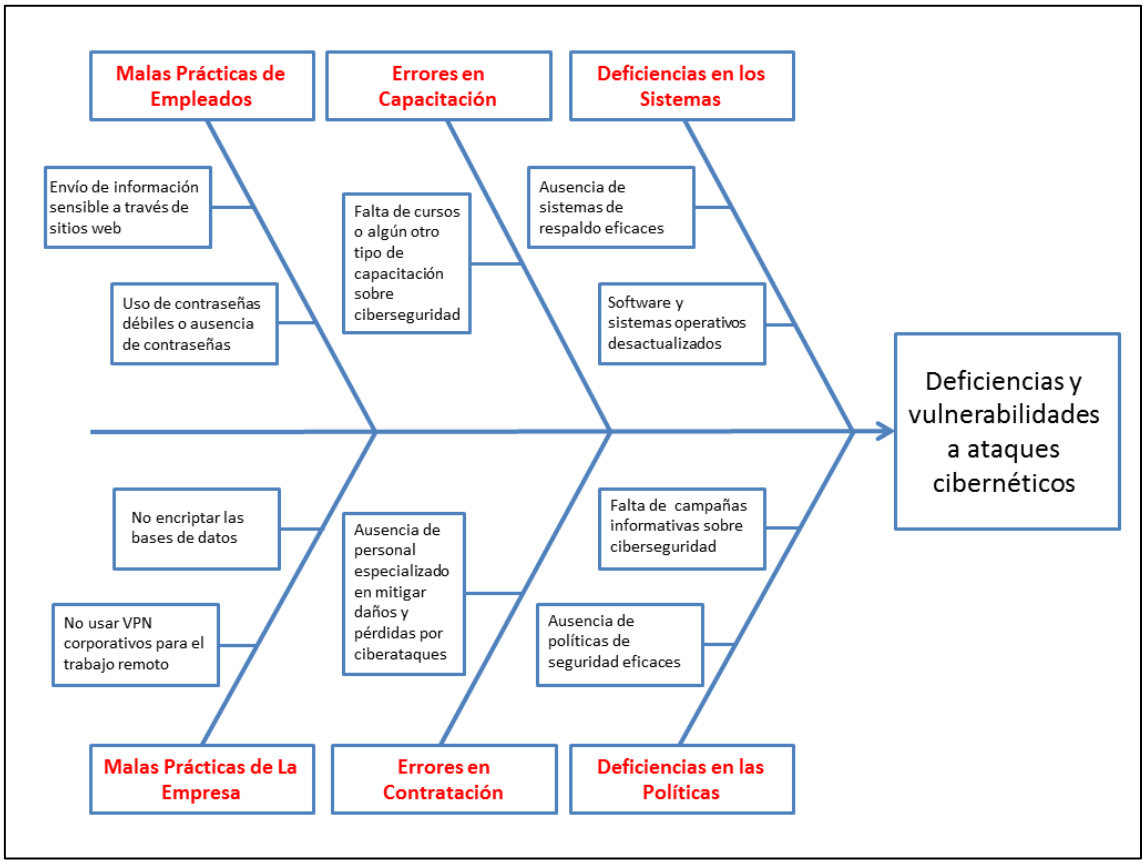


Nota. Elaboración propia.

De la misma manera, a partir de la tormenta de ideas con los especialistas entrevistados se pudo establecer un diagrama de Ishikawa, que permite identificar las causas-raíz del problema principal de la empresa que se requiere atacar: las deficiencias y vulnerabilidades ante ataques cibernéticos. Se identificaron 6 tipos de causas-raíz: malas prácticas de los empleados, malas prácticas de la empresa, errores en capacitación, errores en la contratación, deficiencias en los sistemas y deficiencias en las políticas de la empresa.

Estas causas-raíz se detallan a continuación (Figura 2):

Figura 2
Diagrama de Ishikawa.



Nota. Elaboración propia.

De la Figura 2, se destaca dentro las malas prácticas de los empleados el envío de información sensible a través de sitios web o correos electrónicos comerciales (como Gmail, Yahoo, Hotmail) y el uso de contraseñas débiles o la ausencia de contraseñas. Dentro de las malas prácticas de la empresa resaltan el no usar VPN corporativos para el trabajo remoto y el no encriptar las bases de datos.

Asimismo, resalta dentro de los errores de capacitación la falta de cursos o algún otro tipo de capacitación sobre ciberseguridad. Dentro de los errores de contratación resalta la ausencia de personal especializado en mitigar daños y pérdidas por ciberataques.

De la misma manera, se destaca dentro de las deficiencias en los sistemas la ausencia de sistemas de respaldo eficaces y la presencia de software (antivirus, antispam y firewalls) y sistemas operativos desactualizados. Por último, dentro de las deficiencias en las políticas de la empresa se tienen la ausencia de políticas de seguridad eficaces y la falta

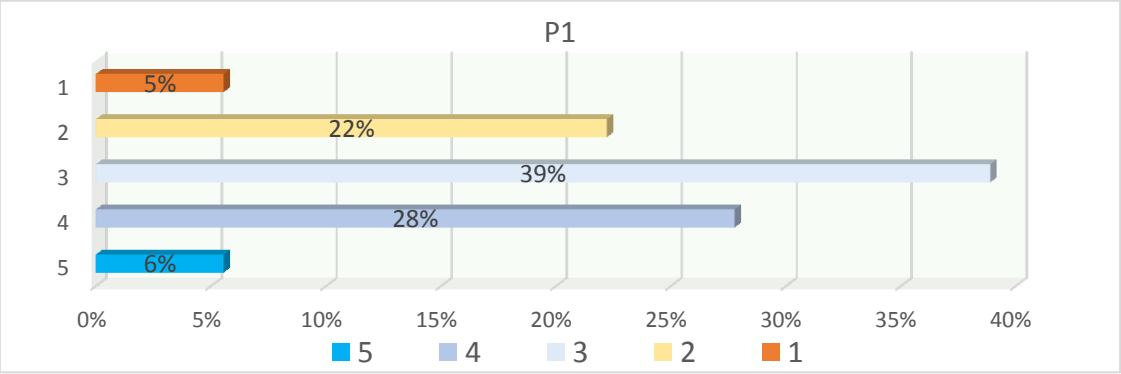
de implementación de campañas informativas sobre ciberseguridad que concienticen a los empleados.

Por otro lado, el uso de VPNs corporativas es importante, ya que su uso va más allá de la mera conexión a un data-center privado. La protección de la información en tránsito por medio de un cifrado robusto y la visibilidad de todo este tráfico, solo se podrá llevar a cabo siempre que la VPN se encuentre activa.

Las siguientes preguntas, en base a la encuesta aplicada, están relacionadas con el conocimiento sobre SGSI y la información necesaria para el análisis de la seguridad en la empresa.

Figura 3

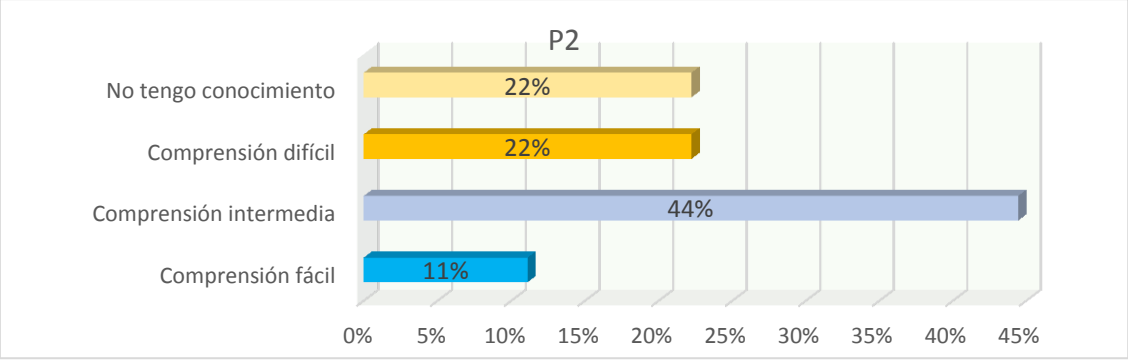
Conocimiento de las políticas de seguridad de la información que existen en la empresa



Nota. Resultados de la encuesta aplicada.

Figura 4

Calificación sobre la política de seguridad de la información de la empresa.



Nota. Resultados de la encuesta aplicada.

En relación al conocimiento sobre la política de seguridad de la información en la institución, considerando la escala de 1 (desconoce totalmente) a 5 (sabe totalmente). Así que, el 39% (grado 3) lo percibió como neutral; además, más de un tercio (34%)

consideró que lo conoce bien (grado 4 y 5); mientras que, el resto 27% manifestó lo contrario; es decir, no lo conoce bien. Asimismo, en la Figura 4, a los que tenían conocimiento sobre la política se les preguntó cómo clasificaban la comprensión, el 44% la calificó como intermedia, el 22% como difícil, y con la misma cifra (22%) no tiene conocimiento, y el 11% como fácil.

En la siguiente tabla y figura se muestran el resumen del resto de preguntas realizadas:

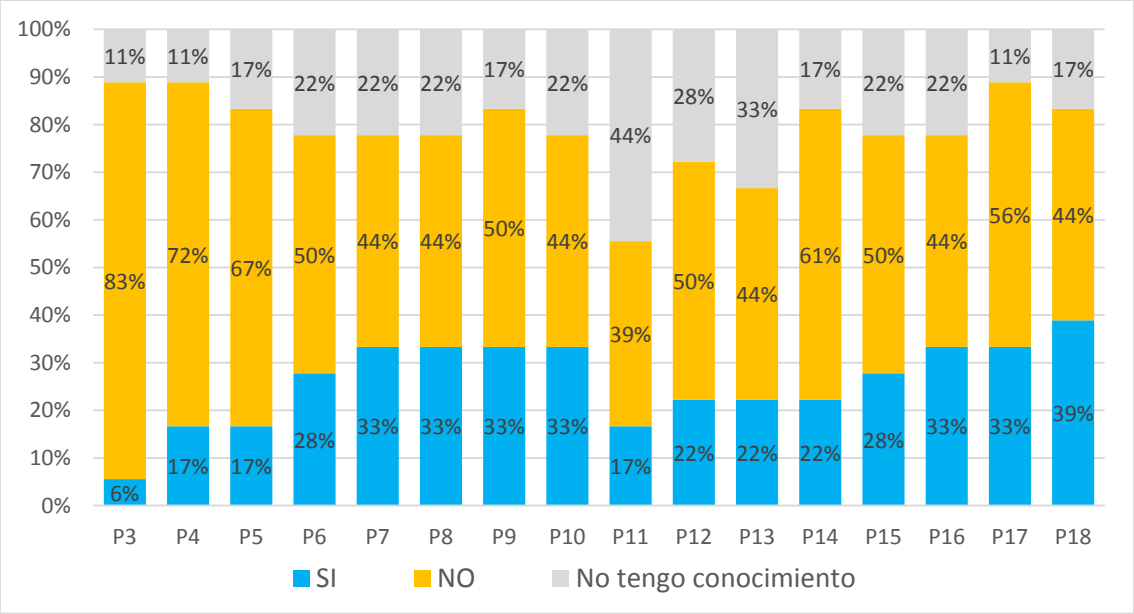
Tabla 3
Resultados del cuestionario desde pregunta 3 hasta la 18.

No.	Ítem	SI		NO		No tengo conocimiento	
		fi	%	fi	%	fi	%
P3	¿Ha recibido alguna capacitación sobre seguridad de la información?	1	6%	15	83%	2	11%
P4	Antes de iniciar sus actividades profesionales en la empresa, ¿todo usuario recibe orientación en materia de seguridad de la información y toma conocimiento de las normas existentes?	3	17%	13	72%	2	11%
P5	En su opinión, ¿los usuarios de la empresa conocen las normas de seguridad de la información existentes?	3	17%	12	67%	3	17%
P6	¿La elección de sus contraseñas siguió alguna política de seguridad de la información de la empresa?	5	28%	9	50%	4	22%
P7	¿El cambio de contraseña es periódico?	6	33%	8	44%	4	22%
P8	¿Existe un requisito por parte de los sistemas para una contraseña fuerte*?	6	33%	8	44%	4	22%
P9	¿Cuenta con respaldo de los archivos necesarios para realizar su trabajo?	6	33%	9	50%	3	17%
P10	¿Existen reglas para el uso de Internet?	6	33%	8	44%	4	22%
P11	¿El uso de Internet es monitoreado por algún organismo de TI?	3	17%	7	39%	8	44%
P12	¿Existen reglas para el uso del correo electrónico empresa?	4	22%	9	50%	5	28%
P13	¿Tu computadora tiene protección antivirus?	4	22%	8	44%	6	33%
P14	¿Ejecutas el antivirus antes de ejecutar cualquier archivo presente en cualquier medio removible (pendrives, HD, DVD, CD-ROM)?	4	22%	8	44%	6	33%
P15	¿Existe un procedimiento para reportar un incidente de seguridad de la información?	5	28%	9	50%	4	22%
P16	¿Las áreas de acceso restringido contienen una advertencia?	6	33%	8	44%	4	22%
P17	¿Las áreas de acceso restringido contienen una advertencia?	6	33%	10	56%	2	11%
P18	¿Se monitorean las acciones de los empleados y visitantes?	7	39%	8	44%	3	17%

Nota. Resultados de la encuesta aplicada.

Figura 5

Resultados del cuestionario desde pregunta 3 hasta la 18.



Nota. Resultados de la encuesta aplicada.

En la Figura 5 y Tabla 3, están los resultados para los ítems 3 al 18 del cuestionario aplicado, destacándose que la mayoría se inclinaron predominantemente por las alternativas negativas del mismo, donde percibieron que no han recibido capacitación sobre algún sistema de información, e incluso antes de iniciar sus actividades como empleados de la empresa, dificultándose conocer bien la política de protección de la información.

Consultado si recibe orientación en materia de seguridad de la información y toma conocimiento de la normativa existente, la mayoría informó que no recibió orientación y ni siquiera conocía la normativa existente. Además, en cuanto a la integridad de los datos y la copia de seguridad, se les preguntó si habían perdido datos parcial o totalmente o si algún dato se había corrompido en la computadora de su trabajo, un importante sector de los evaluados manifestó que cuando han presentado inconvenientes con su información, no tenían una copia de seguridad de los archivos necesarios para llevar a cabo la trabajo.

El resultado de las preguntas sobre las reglas de uso de internet y correo electrónico fue predominante negativo, ya que dijeron que no sabían, y en con respecto al monitoreo de internet, los servidores manifestaron que no existe monitoreo por parte de algún

organismo de TI. En cuanto a antivirus y spyware, se les preguntó si la computadora tenía protección antivirus, si su computadora de trabajo alguna vez había sido infectada con un virus y si el antivirus se ejecutaba en un medio extraíble.

Continuando con las preguntas, respecto a la existencia de un procedimiento para reportar un incidente de seguridad de la información, la mayoría que respondieron dijeron que no conocen de dicho procedimiento. Además, se realizaron consultas sobre la seguridad en el ambiente en relación a la advertencia en salas de acceso restringido, registro de entrada y salida de visitantes y seguimiento de acciones de empleados y visitantes, donde se desconocen los procedimientos para ese fin.

3.2. Identificar los mecanismos técnicos que permitan optimizar el SGSI en una empresa de consultoría financiera en Lima

En ese momento, después de identificarse que, lo que es realmente está pasando en la empresa con sus deficiencias en la protección de resguardo de su información, se definió que todo lo que se posee de información se vuelve relevante y que si bien la consecuencia de perderla o pasar información de manera indebida era insignificante y la probabilidad rara de que suceda, sería un problema grave. Al llegar en este punto, se llegó al consenso de que dentro de las políticas de seguridad se utilizaría lo que se consideraba relevante e intolerable serían las prioridades en este primer momento. Y es ahí donde se empezó el proceso de organización de la estructura, clasificándose como reglas principales, de respaldo y de restauración que no existían, indicándose también los inconvenientes podían pasar, así como la pérdida de algún dato tendría consecuencias extremas, el control de acceso a la información por sector y personas, porque una persona que no necesita acceder a esa información tiene la probabilidad de acceder posiblemente y termine usándola mal, teniendo un riesgo medio/crítico, control de acceso externo de socios y proveedores, que sin este control no se sabría lo que estaban haciendo mal, cuya consecuencia puede ser crítica y/o extrema dependiendo de la situación.

La metodología que permite optimizar el SGSI, desde un punto de vista técnico y dando solución oportuna a las vulnerabilidades encontradas, se basa en el ciclo Deming,

siendo representado a través de los módulos Planificar, Hacer, Verificar y Monitorear (PDCA) y siguiendo los lineamientos referidos en las normas ISO/IEC 27001:2013.

a) Planeación. El primer paso en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), según la norma ISO/IEC 27001, es definir el alcance y los límites del mismo, el cual debe observar las características de la empresa consultora, de su organización, ubicación, activos y tecnología, incluidos los detalles y justificaciones para cualquier exclusión del alcance.

- **Realizar un análisis de la situación actual.** En primer lugar, se debe evaluar si es factible implementar un SGSI, basado en la norma UNE-ISO/IEC 27001. Esta es una herramienta o metodología sencilla y de bajo coste que cualquier empresa puede utilizar. La norma te permite establecer políticas, procedimientos y controles con el objeto de disminuir los riesgos de tu empresa. A continuación, se presenta cada uno de los pasos que debes seguir para implementar un Sistema de Gestión de Seguridad de la Información.

  Se debe entender e identificar tu posición como empresa en materia de ciberseguridad es el primer paso para iniciar con el plan. Una muy buena práctica es realizar un análisis de riesgos, de esta manera podrás identificar que, tan vulnerable se encuentra tu empresa y cuáles son los riesgos a los que te puedes enfrentar. Algunas interrogantes que debes tener claras al momento de realizar tu análisis de riesgos son las siguientes:

  - ¿Qué procesos pueden ser más críticos y cuáles son tus activos más valiosos?
  - ¿En caso de incidente o ataque, ¿con cuántos procesos puedes contar para seguir trabajando?
  - ¿Qué datos maneja tu empresa y cuáles están en circulación?
  - ¿Cómo se transmiten tus datos de origen a fin?
  - ¿Dónde se están almacenando los datos?
  - ¿Dónde están los accesos no controlados a tu red?
  - ¿Cuál es la importancia de los datos para la empresa o para tus clientes?

- ¿Quién maneja la información más sensible de la empresa?

El análisis de riesgos consiste en identificar las principales vulnerabilidades de la empresa ante amenazas que pueden afectar al sistema informático, estas amenazas pueden ser internas o externas. El siguiente paso es definir los distintos riesgos derivados de las amenazas identificadas, así como sus posibles impactos.

- **Proponer políticas del SGSI.** Consiste crear políticas del Sistema de Gestión de Seguridad de la Información (SGSI), para reforzar los siguientes ámbitos:
  - Uso de contraseñas robustas y renovación de las mismas periódicamente.
  - Gestionar los niveles de privilegios de los usuarios.
  - Uso de dispositivos móviles (BYOD).
  - Navegación segura en la red.
  - Almacenamiento correcto de datos.
  - Control de accesos.
  - Actualizaciones de S.O. y parches de seguridad.
  - Uso del correo electrónico.
  - Pentesting.
  - Análisis de vulnerabilidades.
  - Capacitaciones en materia de ciberseguridad, etc.
- **Elegir la documentación técnica del SGSI.** Un Sistema de Gestión de Seguridad de la Información (SGSI), según la norma ISO 27001, debe incluir la siguiente documentación técnica:
  - Manual de implementación del SGSI: Este documento contiene la guía de cómo se debe implementar y seguir el Sistema de Gestión de Seguridad de la Información SGSI de la Información. Aquí se incluye toda la información como objetivos, alcance, responsables, políticas, directrices, entre otras actividades que se decidan llevar a cabo.
  - Manuales de procedimientos: Estos se relacionan con las actividades operativas, ya que estos dan los parámetros que se deben seguir para que

la gestión sea eficaz y la planificación, la operación y el control sean los adecuados en los procesos de seguridad de la información.

- Registros: Es la evidencia de la información que ha sido documentada durante toda la gestión para verificar que se estén cumpliendo con los objetivos propuestos.

- **Formular un PCI/PCA.** El Plan de Continuidad de las Tecnologías de la Información (PCI) debe ser una parte integral del Plan de Continuidad de las Actividades (PCA) en escenarios de contingencia, el cual tiene como objetivo garantizar la continuidad del negocio en caso de un fallo de las tecnologías de la información. Para establecerlo, la empresa debe realizar primero un análisis de riesgos y un análisis de impactos.

b) Ejecución (Do). Para ejecutar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), es recomendable llevar a cabo los siguientes pasos:

- **Implementar políticas del SGSI.** La implementación de políticas del Sistema de Gestión de Seguridad de la Información (SGSI), también conocidas como políticas de ciberseguridad, ayudarán a que tanto la directiva como los colaboradores tengan directrices claras y lineamientos a seguir te permitirá estar preparado y responder de manera rápida, oportuna y eficiente ante un ataque. Los elementos a considerar se pueden esquematizar de la siguiente manera:

  - **Definir el alcance del SGSI**: Se debe disponer de suficiente claridad del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), qué se logrará una vez se ponga en marcha el plan de acción, teniendo en cuenta los recursos disponibles (personal, activos, y tecnologías).

  - **Definir la política del SGSI**: Consiste en determinar los objetivos, el marco general, los requerimientos legales, los criterios con los que serán evaluados los riesgos y para esto debes establecer la metodología, que debe estar aprobada por la dirección o la junta directiva.

  - **Capacitar a los colaboradores**: Generar conciencia en los colaboradores en relación a las redes que usamos para comunicarnos, sobre todo desde

equipos empresariales, es un paso más en la disminución del riesgo. Muchas de estas redes abiertas pueden ser usadas para captar máquinas de usuarios despistados o poco protegidos, la información que pasa por ellas puede ser fácilmente robada.

- **Establecer los objetivos de control**: Consiste en definir los controles que se van a implementar, así como el cronograma recomendado para aplicar dichos controles.

- **Conformar un** equipo **de detección y respuesta.** Paralelamente a la implementación de políticas del Sistema de Gestión de Seguridad de la Información (SGSI), se debe conformar un equipo de detección y respuesta ante ciberataques, que puede estar conformado tanto por asesores externos como por personal capacitado de la empresa, lo cual es fundamental para mantener el control de los eventos y alertas de seguridad en tu empresa y la certeza de tener un equipo enfocado las 24 horas del día en este tema. Entre las actividades a desarrollar se puede incluir:
- **Identificar los riesgos:** Durante esta etapa se deben reconocer las posibles ciber-amenazas a las que puede ser vulnerable la empresa, quiénes son los responsables directos, a qué son vulnerables y cuál sería el impacto en caso de que se llegue a violar la confidencialidad, la integridad y la disponibilidad de los activos de información.
- **Analizar los riesgos:** Es necesario que se evalúe el impacto que se produciría si alguno de los riesgos evaluados se llegara a materializar, identificar cuál es la probabilidad de ocurrencia y cómo esto podría afectar a los controles que ya están implementados, de igual manera, validar si el mismo se puede asimilar o debe ser mitigado.
- **Definir los tratamientos de los riesgos:** Consiste en definir cómo se aplicarán los tratamientos de los riesgos teniendo en cuenta los controles que fueron identificados, y las responsabilidades de cada uno, implementar los controles y fomentar una cultura que permita que todos los empleados conozcan el Sistema de Gestión de Seguridad de la Información (SGSI), además, gestionar su funcionalidad y asegurar los recursos necesarios para su cumplimiento.

- **Coordinar la respuesta a incidentes de ciberseguridad:** Es de vital importancia contar con un plan de respuesta a incidentes de ciberseguridad, que proporcione una metodología clara o protocolo a ejecutarse ante un ciberataque. Estos planes deben ser socializados con toda la organización (directivos y colaboradores) y probado constantemente para evaluar su efectividad. Para ello, se puede tomar como referencia algunos estándares internacionales del mercado que son altamente reconocidos, como el Computer Security Incident Handling Guide del NIST y la ISO/IEC 27035:2013.

c) Verificación (Check). La verificación de los resultados de la implementación consiste en determinar si el mismo ha sido entendido y aplicado por todos los colaboradores o empleados, y si ha brindado resultados positivos en la protección de los activos e información de la empresa ante los ciberataques.

- **Verificar la implementación de políticas del SGSI.** Los colaboradores o empleados que realizan trabajos bajo el control de la empresa en estudio deben demostrar conocimientos sobre los siguientes elementos:
  - La política de seguridad de la información.
  - Su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información
  - Las consecuencias de que no cumplan con los requisitos del sistema de gestión de seguridad de la información.

  Los colaboradores de la empresa y el personal de otras organizaciones involucradas con la empresa (stakeholders), deben recibir una capacitación adecuada en concientización y formación en políticas y procedimientos organizacionales, relevantes para su función laboral.
- **Verificar el rendimiento del equipo de detección y respuesta.** La manera de verificar el rendimiento del personal de detección y respuesta ante los ciberataques se mide cuantitativamente en la disminución de la frecuencia de los ciberataques que han logrado ocasionar daños o pérdidas a la empresa. Por otro lado, los planes de respuesta a incidentes de

ciberseguridad deben ser probados constantemente para evaluar su efectividad. Estos planes generalmente se conciben de 4 fases: a) planificación y preparación, b) detección y análisis, c) contención, erradicación y recuperación, y d) acciones pos-incidentes.

d) **Acción (Act).** Periódicamente se debe efectuar una revisión del Sistema de Gestión de Seguridad de la Información (SGSI) para identificar si está cumpliendo con lo que señala la norma ISO 27001, con los objetivos planteados y si es efectivo, así mismo, para reportar las mejoras que deben hacer y cuáles serán las acciones a ejecutar para lograr esto. Si la evaluación de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) resulta exitosa, la empresa puede solicitar la certificación ISO 2700, lo cual contribuiría a mejorar la competitividad en el mercado, diferenciándose de las empresas que lo han conseguido, haciéndola más fiables e incrementando su prestigio.

3.3. Propuesta de mejora

Para alcanzar el resultado esperado, se evaluarán las herramientas basadas en el sistema de gestión de seguridad de la información (SGSI), cuyos criterios y métricas para evaluar estos aspectos se definirán con base en las normas para seguir un estándar de evaluación de la seguridad. En esta organización (empresa financiera), es posible que ocurra un incidente que comprometa la seguridad de un activo, independientemente de cuántas medidas se tomen para evitarlo. Considerando esto, es necesario planificar las medidas a tomar en caso de presentarse estos incidentes, de manera que facilite la solución del problema ocurrido y ayude al entorno a normalizar la ejecución de sus procesos.

1. Introducción

En este sentido, la política de fuga de información, así como la minimización de pérdidas de la misma por los ciberataques, propone una serie de medidas a tomar en caso de que se produzca un incidente de fuga de información en la empresa financiera, destacando las medidas que puede tomar cualquier miembro de en la empresa financiera

analizada, cuyas medidas a tomar. ser tomada por los miembros y equipos encargados de investigar estos incidentes.

Los requisitos que debe cumplir la empresa financiera para la implementación del SGSI según ISO 27001:2013 están separados en los siguientes apartados:

- **Contexto organizacional**. Comprender las necesidades de la organización y de las partes interesadas, además de determinar el alcance del SGSI.
- **Liderazgo**. Demostrar liderazgo, compromiso y política, además de autoridad, responsabilidad y roles organizacionales. La alta dirección debe establecer una política de seguridad de la información.
- **Planificación**. Planificación de acciones para abordar riesgos y oportunidades, objetivos de seguridad de la información.
- **Apoyo**. Proporcionar recursos, determinar la competencia, determinar la comunicación e incluir y asegurar la información documentada.
- **Operación**. Planificación y control operativo, evaluación de riesgos y tratamiento de los mismos.
- **Evaluación del desempeño**. Seguimiento, medición, análisis y evaluación de auditoría interna y revisión por la dirección.
- **Mejora**. incumplimientos y acciones correctivas.

Definida la planificación, luego establecer un plazo para la ejecución de las actividades preestablecidas.

2. Propósito, alcance y política del SGSI

La coordinación del equipo ISO/IEC 27001:2013 definirá el alcance y la política en consonancia con los órganos superiores a la misma.

a) **Propósito**. El propósito de esta política del resguardo y protección de la información es establecer un cronograma a ejecutar si ocurre un incidente en la empresa financiera que afecte su operatividad. Para ello, se espera satisfacer los siguientes puntos:
   - Especificar a qué información se refiere esta política;
   - Especificar qué tipos de incidentes y en qué clasificación cae cada uno de estos incidentes relacionados con la fuga de información, ataques cibernéticos, y resguardo de la misma;

- Especificar un plan para reportar una fuga de información, evidenciando qué acción pueden tomar los miembros de los encargados de la empresa, si se hace evidente un incidente de fuga de información;
- Especificar qué medidas se deben tomar luego de que se reporta un evento de ciberataques;
- Cumplir con las normas ISO/IEC 27001:2013.
- Evaluación y monitoreo continua en la mejora de los procesos.

b) **Alcance**. Tiene como objetivo establecer y difundir lineamientos y principios de seguridad de la información y las comunicaciones, específicos para el SGSI, para orientar sobre el uso adecuado de la información propietaria, además y en línea con lo establecido en la política de seguridad de la información existente. Esta política de seguridad de la información se aplica a:

- Los siguientes procesos realizados en la empresa financiera, tales como la gestión y acceso al código fuente de los sistemas desarrollados para tal fin.
- Gestión y acceso a bases de datos de la empresa financiera; donde todas las tecnologías utilizadas, que estén asociadas a la creación, recolección, procesamiento, almacenamiento, transmisión, análisis y disposición de información relacionada con los procesos planteados;
- Gestión y acceso a los sistemas de información, infraestructura, aplicaciones, productos, servicios, redes de telecomunicaciones y recursos relacionados con los procesos mencionados en el anteriormente;
- Gestión y acceso a todos los becarios, empleados, consultores, proveedores y entidades involucradas o vinculadas a la empresa financiera.

3. Referencias normativas

En la implementación del SGSI estará sustentado en la ISO/IEC 27001:2013, cuya norma apoya a la organización para que pueda utilizar las mejores técnicas de seguimiento y control, involucrando recursos tecnológicos y humanos. Para que esto ocurra es necesaria una adecuada formación de todos los empleados de la organización, generando así conciencia por parte de los empleados, todas las capacitaciones deben quedar registradas. Este proceso auxilia en la evaluación de los estándares que están

siendo puestos en práctica por los empleados, identificando y evaluando las vulnerabilidades, riesgos y amenazas que puedan ocurrir y sus niveles de impacto en la organización. Esta norma incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Con una alta dirección comprometida y una formación eficaz de los empleados, es posible reducir la cantidad de amenazas que aprovechan las vulnerabilidades potenciales.

4. Contexto de la organización

En vista de los problemas presentados anteriormente, la propuesta del SGSI tiene como finalidad la adopción de un plan, donde se pretende crear una comisión integrada por los siguientes miembros: coordinación general de tecnologías de la información, miembros de seguridad y tecnologías de la información y las comunicaciones, y el gerente de seguridad de la información y las comunicaciones, así como el gerente de la empresa de consultoría financiera en Lima.

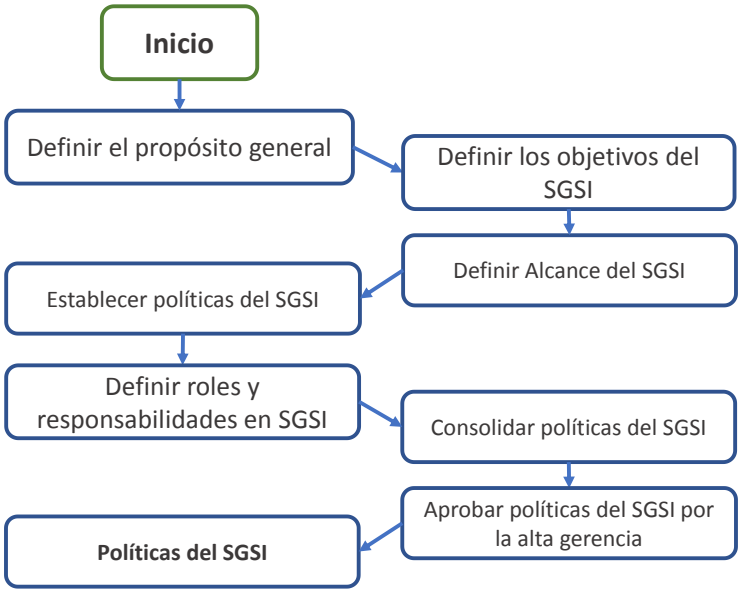
Realización de varias reuniones y actividades con este comité, definiéndose finalmente la siguiente planificación prevista:

- Capacitación en ISO/IEC 27001:2013 para los involucrados en la planificación e implementación del SGSI;
- Creación del alcance y política del SGSI;
- Identificación de activos en los sectores relacionados con el alcance;
- Identificación de riesgos relacionados con el alcance;
- Realización de análisis de riesgos;
- Clasificación de la información;
- Creación de la declaración de aplicabilidad;
- Creación de nuevos controles y documentación de los existentes a través de procedimientos, políticas y manuales;
- Creación de indicadores;
- Realización de reuniones de análisis crítico y auditorías internas;
- Sensibilización de todos los implicados en el SGSI de la organización.

5. Liderazgo

La política de seguridad de la información será dirigida por la alta gerencia, donde se buscará la protección contra diversos tipos de amenazas para garantizar la continuidad del negocio, reducir los riesgos, visando preservar la disponibilidad, integridad, confidencialidad, autenticidad y resguardo de la información generada, procesada y almacenada en la empresa, con el fin de ampliar las oportunidades de mejora en el SGSI. De este modo, establecer la política de seguridad de la información que abarque a los funcionarios, ocupantes de cargos comisionados o encargados, prestadores de servicios, becarios y partes interesadas en el SGSI, con el fin de cumplir con los siguientes elementos: confidencialidad, integridad, disponibilidad. A continuación, el esquema a seguir para la aprobación de las políticas:

Figura 6
Camino para la aprobación de las políticas del SGSI en la empresa financiera.



Una vez aprobada la política de la empresa financiera, se requiere la necesidad de cumplir con SGSI organizacional, cuyas funciones y responsabilidades generales se deben tener los miembros y la gerencia para la seguridad de la información y los activos:

- Garantizar la seguridad de los sistemas de información, infraestructura, aplicaciones, productos, servicios, redes de telecomunicaciones y otros recursos utilizados por la empresa, que ayudan en la creación, recopilación, procesamiento, almacenamiento, transmisión, análisis y disposición de la información.

- Seguir y aplicar las medidas especificadas en la política de seguridad de la información organizacional de la empresa financiera.
- Seguir y aplicar las medidas de protección de datos especificadas en la política de protección de datos.
- Seguir cumplir las medidas de fuga de datos especificadas en la Política de fuga de datos.
- Asegurar que todas las políticas de seguridad de la información sean de libre acceso para todos los miembros y colaboradores de la empresa.
- Asegurar que todas las políticas de seguridad de la información de la empresa estén siendo debidamente aplicadas y seguidas por todos los colaboradores y miembros.
- Garantizar que las políticas de seguridad de la información se revisen y mejoren periódicamente.
- Asegurar el cumplimiento de las políticas de seguridad de la información con las normas ISO/IEC 27001:2013.

Es obligatorio adherirse a todas las políticas, normas, procedimientos, lineamientos y prácticas de la empresa financiera, relacionadas con la seguridad de la información. Los requisitos únicos pueden requerir desviaciones menores de esta política u otras de seguridad de la información relacionadas. Sin embargo, corresponde a la dirección decidir sobre estas posibles desviaciones. Así que, los intentos de eludir, subvertir, eliminar o modificar cualquier control de seguridad de la información para eludir o evadir cualquier filtrado, monitoreo u otros controles de seguridad están estrictamente prohibidos y sujetos a sanciones. Esta política de seguridad de la información se aplica a los siguientes procesos realizados:

- La gestión y acceso al código fuente de los sistemas desarrollados por la empresa; tales como gestión y acceso a bases de datos;
- Todas las tecnologías utilizadas por la empresa financiera, que estén asociadas a la creación, recolección, procesamiento, almacenamiento, transmisión, análisis y disposición de información relacionada con los procesos planteados en el ítem anterior.
- Todos los sistemas de información, infraestructura, aplicaciones, productos, servicios, redes de telecomunicaciones y recursos relacionados con los procesos mencionados en el numeral al inicio.

- Todos los becarios, empleados, consultores, proveedores y entidades involucradas o vinculadas al laboratorio.

6. Planificación de acciones para abordar riesgos y oportunidades

La seguridad de la información en la empresa tuvo un nivel de madurez regular, ya que no existe una política de seguridad de la información, solo se atiende una situación de seguridad de la información cuando existe una anomalía en las actividades. Debido a esto, se realizó una serie de acciones a emprender respecto a la seguridad de la información.

- Difusión que, es responsabilidad de cada colaborador proteger la información y los recursos de procesamiento de la información, los accesos al sistema son analizados frecuentemente para que se registren las ocurrencias con el fin de detectar eventos o acciones que indiquen fallas de seguridad en los procesos.
- Contar con un plan de contingencia en caso de cortes de energía, utilizando equipos para alimentar el servidor de la empresa.
- El sector de tecnologías de la información debe estar compuesto por un servidor de respaldo, que normalmente cubren el soporte técnico a la empresa financiera, donde el coordinador participe en la decisión de nuevos servicios y productos que involucren al sector.
- Controla el acceso a los ambientes físicos de la empresa
- La limpieza se llevará a cabo con frecuencia en los equipos.
- Resguardar conmutadores de red para que no tengan la puerta abierta en la empresa, lo que permite el acceso a la red interna de la empresa con riesgo de ataque dentro de la propia red
- Revisión de computadoras sin licencia del sistema operativo
- Controlar el control de acceso a internet, y se puede acceder a sitios web inapropiados, se pueden realizar descargas de cualquier tipo de archivos maliciosos en las computadoras, y chequear el estado de las copias de seguridad comprobándose después de su finalización, y se debe realizar a diario.
- El personal de TI debe contener plan de actividades; el equipo y la infraestructura, donde se monitoree las copias de seguridad se almacenan en el propio servidor.

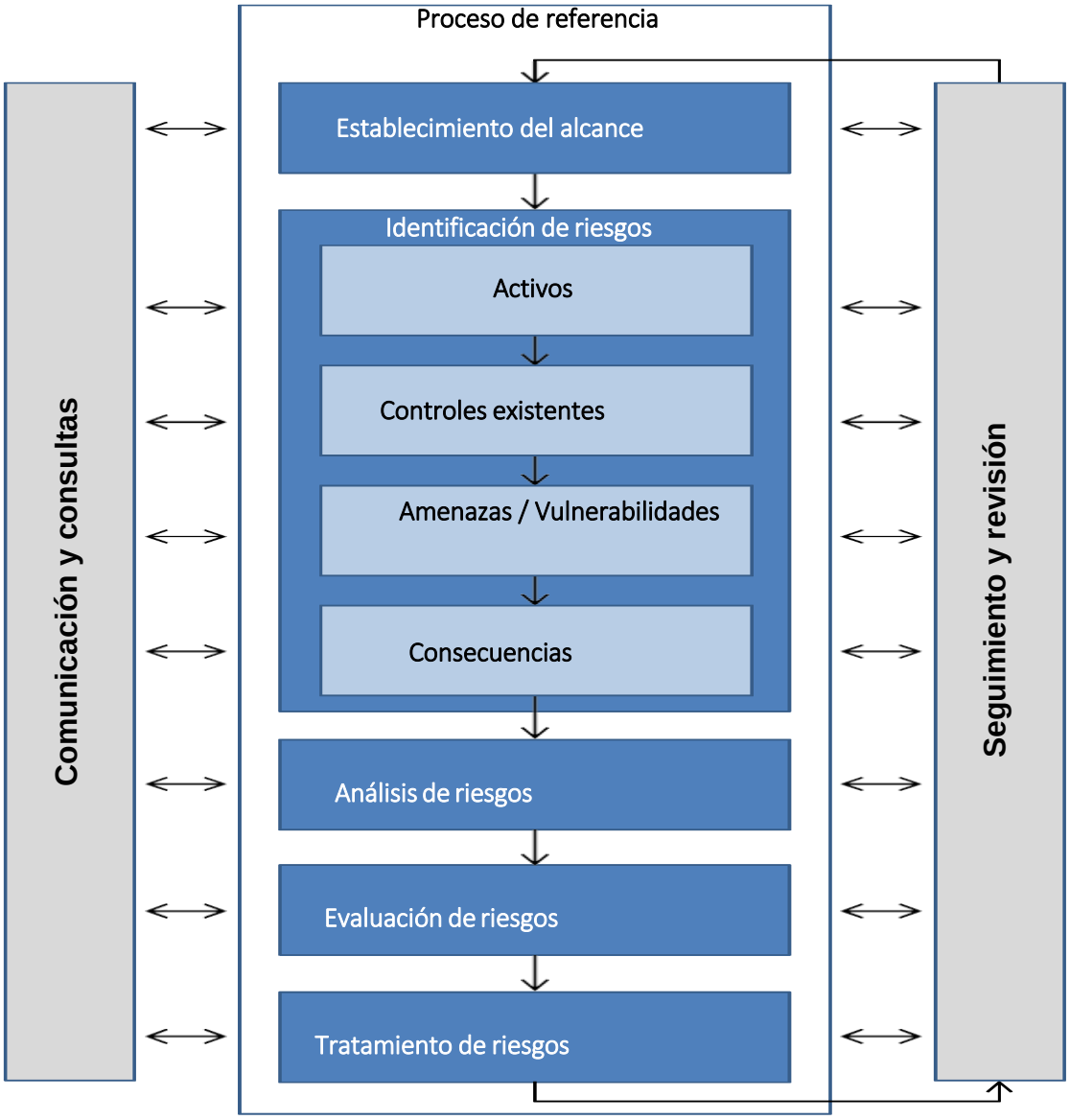
- Luego de realizar los chequeos y visitas in situ, se debe realizar un plan integral política de seguridad, donde se abordarán los puntos de mayor registro de ocurrencia y reforzando la importancia de la seguridad de la información con los empleados.

La gestión de riesgos representa el conjunto de actividades que está en el centro del SGSI se crea una estructura para que la empresa financiera monitoree los niveles de seguridad de la información. Esto se hace a través de revisiones periódicas de los niveles de riesgo antes y después de que se implementen los controles de seguridad. Sin embargo, como se ve a continuación, la eficacia del proceso de gestión de riesgos depende de que la organización sea capaz de realizar varias actividades importantes, que incluyen:

- Reconocer exactamente cuál es la información de la organización;
- Definir cómo esta información se relaciona entre sí;
- Identificar dónde se almacena esta información;
- Identificar las características de los medios de almacenamiento, como amenazas y vulnerabilidades;
- Conciliar el grado de control que tiene sobre la información y los medios de almacenamiento con sus necesidades de visibilidad de la situación de cada bloque de información;
- Ser capaz de evaluar consistentemente el impacto de la pérdida de información;

El modelo de apoyo aquí propuesto busca presentar estas acciones directamente en la fase de planificación de la ISO/IEC 27001:2013. Con eso, la organización puede diseñar mejor un método más realista frente al escenario externo, consciente de las dificultades que trae consigo (Figura 7).

Figura 7
Proceso de referencia para la gestión de riesgos.



Nota. Elaborado en base a la teoría de la ISO/IEC 27001:2013

7. Apoyo

Aquí se estará proporcionando recursos, competencia, comunicación y el aseguramiento de la información documentada. Entre los aspectos que se les debe prestar apoyo están:

a) Seguridad en los recursos humanos

- **Antes de la contratación**. Asegúrese de que los empleados y las partes externas comprendan sus responsabilidades y se ajusten a las funciones para

las que han sido seleccionados, así como los términos y condiciones de contratación.

- **Durante el compromiso**. Asegúrese de que los empleados y las partes externas conozcan y cumplan con sus responsabilidades en materia de seguridad de la información, responsabilidades en la empresa, concientización, educación y capacitación en seguridad de la información, y los procesos disciplinarios
- **Cierre y cambio del compromiso**. Protección de los intereses de la organización como parte del proceso de cambio o cierre de la contratación. Responsabilidades para el cierre o cambio de la contratación.

b) Identificación y gestión de activos

Para ello, se deben realizar reuniones y entrevistas en los sectores para identificar activos y actividades relacionadas con el alcance del SGSI. El resultado debe ser registrado y categorizado. Además, clasificar por nivel de confidencialidad, etiquetas de identificación, criterios de clasificación, restricción de acceso, debido transporte y disposición. De este modo, la empresa financiera ha de utilizar el siguiente modelo para realizar la clasificación de la información:

- **Externa**. La información con esta clasificación puede ser accedida por cualquier persona pública.
- **Interno**. Solo los miembros de la empresa pueden acceder y administrar la información con esta clasificación.
- **Confidencial**. Solo los miembros o equipos específicos de la empresa financiera pueden acceder y administrar la información con esta clasificación.

En los procesos de gestión y acceso al código fuente de los sistemas desarrollados por la empresa financiera, así como a la base de datos, debe intervenir la respectiva codificación de la información y sus respectivas clasificaciones.

A continuación, la gestión de los activos de la empresa financiera debe contener:

- Responsabilidad por activos. Se prepara un inventario de activos, propietario, uso aceptable, devolución de activos

- Clasificación de la información. Asegurar que la información recibe un nivel adecuado de protección, de acuerdo a su importancia para la organización.
- Etiquetado y tratamiento de la información.
- Tratamiento de los activos. Los procedimientos para el tratamiento de los activos deben desarrollarse e implementarse de acuerdo con el esquema de clasificación de la información adoptado por la organización.
- Manejo de medios. Impedir la divulgación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios.

c) Sensibilización al SGSI

Asegurar que los empleados realicen sus actividades laborales de acuerdo con la política de seguridad de la información del instituto, contribuyendo a la eficacia del SGSI. Así que, con la adopción de esta propuesta, los empleados tendrán:

- Conocimiento de la política de seguridad de la información de la institución, en un lenguaje sencillo, claro y objetivo;
- Recibir capacitación para conocer la importancia y la necesidad de tener una seguridad de la información sólida y eficaz, para que vea que las cosas simples, como bloquear su computadora cuando no está, son extremadamente importantes para mantener la seguridad;
- Realizar respaldo de datos periódicamente;
- Instalar y actualizar el antivirus en todas las computadoras de la institución;
- Ejecutar análisis antivirus en el sistema, en medios extraíbles;
- Mayor conciencia de los servidores en cuanto al uso y creación de claves de acceso a los sistemas, red e internet;
- Estar al tanto de los órganos superiores de los aspectos involucrados en el monitoreo del uso de Internet, creando reglas institucionales de correo electrónico;
- Contar con un sector local responsable para reportar en casos de incidentes de seguridad de la información;
- Toda área restringida deberá contar con una advertencia, los empleados deberán portar un gafete de identificación;

- Los visitantes serán registrados a la entrada y salida, de ser posible acompañados por alguien de la institución;
- Ampliar el monitoreo electrónico para rastrear las acciones de los empleados y visitantes.

8. Operación

Tiene como propósito llevar a cabo la planificación y control operativo, evaluación de riesgos y tratamiento de los mismos.

Luego de clasificar la información, es necesario conocer qué amenazas a la información están sujetas a riesgos, por lo que se debe realizar un análisis misma. Por ser un método simple y fácil de entender, se opta por el método cualitativo para el análisis de riesgos, cuya lista de activos de información se ubican sus amenazas encontradas, tal como se expresa en la Tabla 4.

En este sentido, para completar esta tabla, se deben seguir los siguientes pasos:

- El primer paso, es evaluar el valor de la consecuencia; es decir, el impacto si la amenaza se materializa. Se define un valor de 1 a 5, donde 1 es el riesgo más bajo y 5 el riesgo más alto, para cada amenaza.
- En el segundo paso, se hace lo mismo, ahora para la columna probabilidad de ocurrencia, que indica con qué frecuencia ocurre la amenaza.
- En el tercer paso, se calcula la medida del riesgo multiplicando (valor de la consecuencia X probabilidad de ocurrencia), este valor indica el grado de riesgo de la amenaza.
- Finalmente, en la columna de orden de amenazas, se ordenan las amenazas de acuerdo a la medida de riesgo previamente calculada. Para ilustrar mejor el análisis descrito anteriormente, siga la tabla utilizada en el desarrollo de este trabajo. Para preservar la empresa estudiada, la siguiente tabla contiene datos ficticios.

Tabla 4
Método cualitativo para el análisis de riesgos.

Amenazas	Valor de consecuencia	Probabilidad de ocurrencia	Medida de riesgo	Orden de amenaza
Amenaza A				
Amenaza B				
Amenaza C				
Amenaza D				
Amenaza E				

Nota. Elaborado en base a las normas ISO/IEC 27001:2013.

En el análisis y evaluación es responsabilidad del comité de seguridad de la información. La tabla anterior sigue el modelo sugerido por la norma ISO/IEC 27001:2013, siendo suficiente para el estándar, ya que incluye la posibilidad de crear una tabla a medida, según las necesidades organizativas.

Los controles fueron extraídos de la norma con base en las orientaciones proporcionadas por los requisitos de la norma ISO/IEC 27001:2013, entre otros factores, con el mismo grado de importancia, también se obtienen en cuenta durante la elección de los controles, como la clasificación de la información, el análisis de riesgos, el costo de implementación de los controles, las necesidades de la empresa y las demandas futuras, donde a partir de los riesgos identificados en la actividad anterior, se realizará un análisis que dará como resultado una hoja de cálculo que contendrá la descripción, probabilidad, impacto, y las respectivas acciones (tratamiento).

Una obtenido lo anterior, se declaración de aplicabilidad, donde se crea una hoja de cálculo para gestionar la declaración de aplicabilidad del SGSI, informando cuál de las secciones y controles se están utilizando, en su caso, con qué propósito y cómo se controla este elemento, a través de políticas, procedimientos, manuales, registros, entre otros. Una vez hecho esto, todo estará listo para la redacción del texto de la política de seguridad de la información, así como la creación de documentos para controlar el SGSI.

9. Evaluación del desempeño

Seguimiento, medición, análisis y evaluación de auditoría interna y revisión por la dirección, en el cual se debe llevar:

a) Indicadores

Para monitorear y medir el desempeño de los objetivos y metas del SGSI.

b) Reuniones de revisión y auditorías internas. Determinar un período de tiempo para la realización de revisiones y auditorías internas, discutiendo la siguiente información:

- Acciones de seguimiento de reuniones y auditorías anteriores;
- Análisis SGSI;
- Desempeño relacionado con la efectividad del SGSI;
- Resultado de las evaluaciones de riesgos y estado de los planes de tratamiento de riesgos;
- Cambios en temas internos y externos que puedan afectar el SGSI;
- Identificación de sugerencias de mejora.

c) Monitorear y analizar críticamente el SGSI

Reúne las prácticas necesarias para evaluar la eficiencia y eficacia del sistema de gestión y presenta los resultados para el análisis crítico por parte de la gerencia. La política de seguridad se utiliza para comparar y lograr el desempeño con las pautas definidas. Requisitos de la norma ISO 27001 para este paso:

- Realizar procedimientos de seguimiento y análisis crítico.
- Realizar revisiones periódicas de la eficacia del SGSI (incluido el cumplimiento de la política y los objetivos del SGSI, y la revisión de los controles de seguridad), teniendo en cuenta los resultados de las auditorías de seguridad de la información, los incidentes de seguridad de la información, los resultados de la eficacia de las mediciones, las sugerencias y los comentarios de todas las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información.
- Revisar los análisis/evaluaciones de riesgos a intervalos planificados y revisar los riesgos residuales y los niveles de riesgo aceptables identificados.
- Llevar a cabo auditorías internas del SGSI a intervalos planificados.
- Llevar a cabo una revisión de gestión del SGSI de forma regular para garantizar que el alcance siga siendo adecuado y que se identifiquen mejoras en los procesos del SGSI.
- Actualizar los planes de seguridad de la información para tomar en cuenta los resultados de las actividades de monitoreo y revisión.

- Registrar acciones y eventos que puedan tener un impacto en la efectividad o desempeño del SGSI.

10. Mejora

Esta sección forma parte de la fase de mejora del ciclo de la implementación, y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua. Así que, realizar acciones correctivas y preventivas, con base en los resultados de la auditoría interna del SGSI y la revisión de la gerencia u otra información relevante, para lograr la mejora continua.

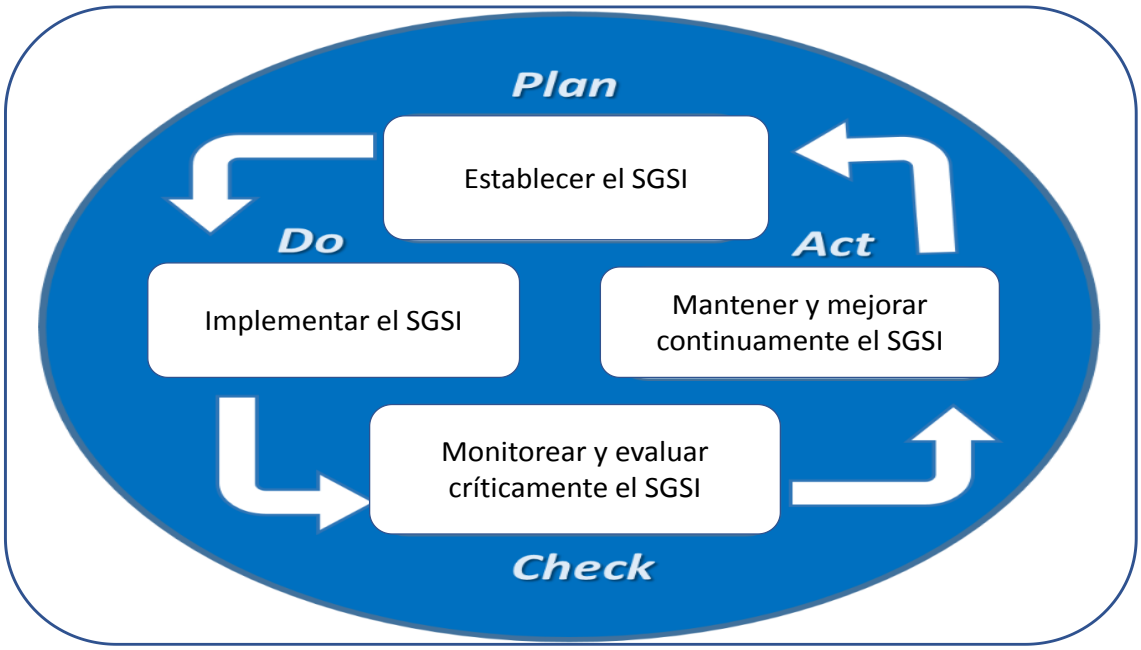
- Requisitos de la norma ISO 27001 para este paso:
- Implementar las mejoras identificadas en el SGSI.
- Tomar las acciones preventivas y correctivas apropiadas.
- Aplicar las lecciones aprendidas de las experiencias de seguridad de la información de otras organizaciones y las de la propia organización.
- Comunique las acciones y mejoras a todas las partes interesadas con un nivel de detalle adecuado a las circunstancias y, si corresponde, obtenga un acuerdo sobre cómo proceder.
- Asegurar que las mejoras alcancen los objetivos previstos.

Pasos a seguir para la implementación de la propuesta de basada en la norma ISO/IEC 27001:2013

Es un sistema de gestión empresarial[1] enfocado en la seguridad de la información, que incluye todo el enfoque organizacional utilizado para proteger la información corporativa y sus criterios de confidencialidad, integridad y disponibilidad. De este modo, SGSI incluye estrategias, planes, políticas, medidas, controles y diversos instrumentos utilizados para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

La norma ISO 27001 adopta el modelo PDCA (Plan-Do-Check-Act) para describir la estructura de un SGSI. La siguiente imagen, junto con una descripción de cada uno de los pasos, probablemente lo ayudará a familiarizarse un poco más con el concepto.

Figura 8
Descripción de los pasos basados en el modelo PDCA (Plan-Do-Check-Act).



En resumen, se tienen los siguientes pasos generales:

a) **Establecer el SGSI**. Representa el escenario que da vida al SGSI. Sus actividades deben establecer políticas, objetivos, procesos y procedimientos para la gestión de la seguridad de la información. Son los instrumentos estratégicos fundamentales para que la organización integre su seguridad de la información en las políticas y objetivos globales de la organización.

b) **Implementar el SGSI**. Consiste en implementar y operar la política de seguridad, controles/medidas de seguridad, procesos y procedimientos.

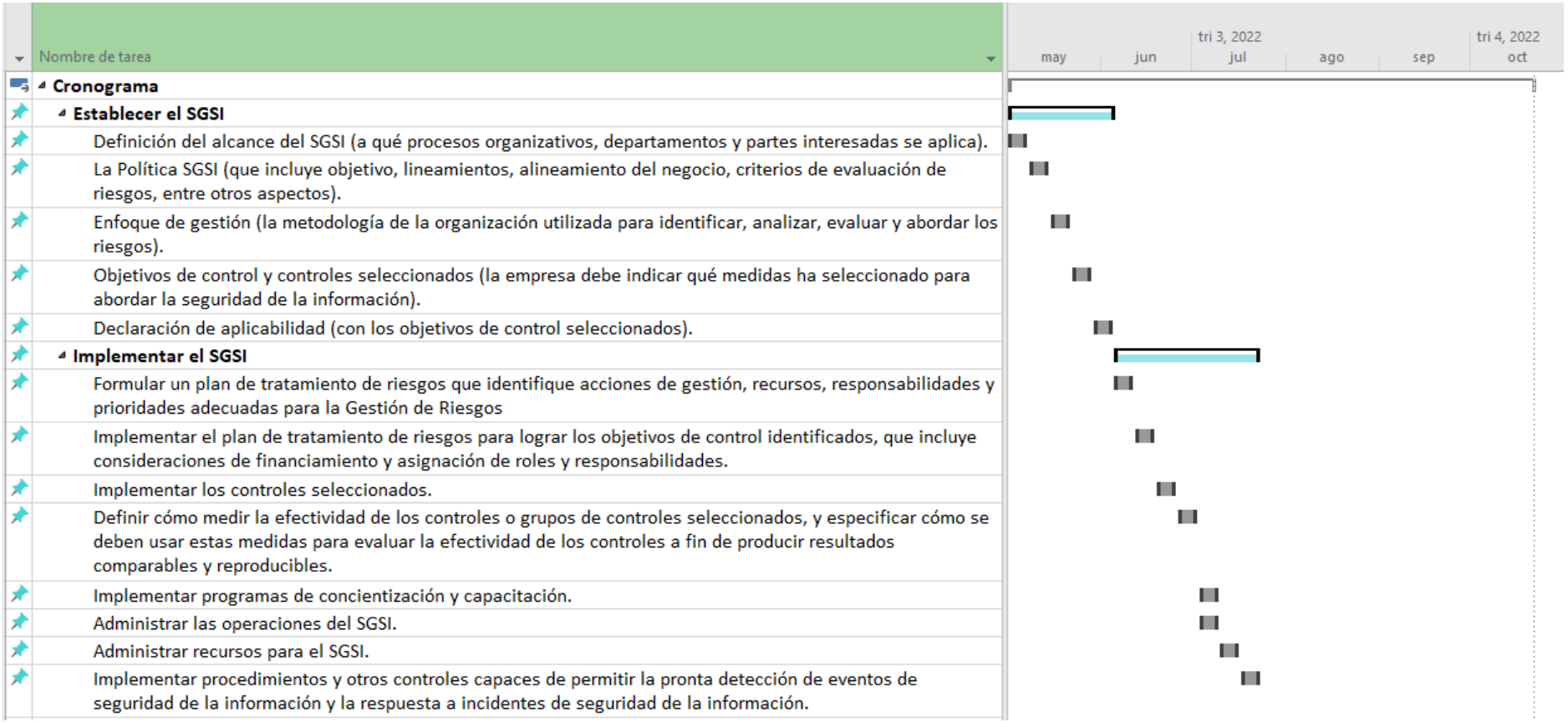
c) **Monitorear y analizar críticamente el SGSI**. Reúne las prácticas necesarias para evaluar la eficiencia y eficacia del sistema de gestión y presenta los resultados para el análisis crítico por parte de la gerencia. La política de seguridad se utiliza para comparar y lograr el desempeño con las pautas definidas.

d) **Mantener y mejorar continuamente el SGSI**. Realizar acciones correctivas y preventivas, con base en los resultados de la auditoría interna del SGSI y la revisión de la gerencia u otra información relevante, para lograr la mejora continua del SGSI.

En la siguiente figura, se muestra el cronograma tentativo con las actividades para la implementación de la propuesta basada en la norma ISO/IEC 27001:2013:

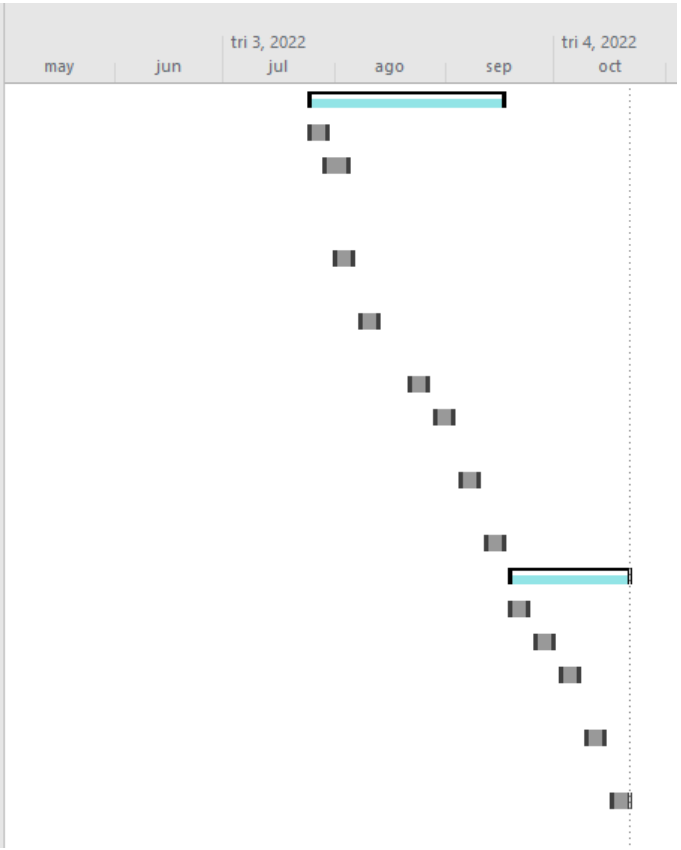
Figura 9

Cronograma para la implementación de la propuesta basada en la norma ISO/IEC 27001:2013



Continuación de la tabla anterior…

Nombre de tarea
Monitorear y evaluación crítica del SGSI
Realizar procedimientos de seguimiento y análisis crítico.
Realizar revisiones periódicas de la eficacia del SGSI (incluido el cumplimiento de la política y los objetivos del SGSI, y la revisión de los controles de seguridad), teniendo en cuenta los resultados de las auditorías de seguridad de la información
Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información.
Revisar los análisis/evaluaciones de riesgos a intervalos planificados y revisar los riesgos residuales y los niveles de riesgo aceptables identificados.
Llevar a cabo auditorías internas del SGSI a intervalos planificados.
Llevar a cabo una revisión de gestión del SGSI de forma regular para garantizar que el alcance siga siendo adecuado y que se identifiquen mejoras en los procesos del SGSI.
Actualizar los planes de seguridad de la información para tomar en cuenta los resultados de las actividades de monitoreo y revisión.
Registrar acciones y eventos que puedan tener un impacto en la efectividad o desempeño del SGSI.
Mantener y mejorar continuamente el SGSI
Implementar las mejoras identificadas en el SGSI.
Tomar las acciones preventivas y correctivas apropiadas.
Aplicar las lecciones aprendidas de las experiencias de seguridad de la información de otras organizaciones y las de la propia organización.
Comunique las acciones y mejoras a todas las partes interesadas con un nivel de detalle adecuado a las circunstancias y, si corresponde, obtenga un acuerdo sobre cómo proceder.
Asegurar que las mejoras alcancen los objetivos previstos.



Nota. Elaboración propia en base a la teoría del ISO/IEC 27001:2013

3.4. Contrastación de hipótesis

Seguidamente se enuncian las suposiciones

H $_{investigador}$: Un sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001:2013 beneficiará a la empresa de consultoría financiera de Lima, 2021 protegiendo la información sensible.

H $_{Nula}$: Un sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001:2013 no beneficiará a la empresa de consultoría financiera de Lima, 2021 protegiendo la información sensible.

Para darle respuesta a la comprobación de la suposición planteada, se recurrió a través del análisis de las respuestas del cuestionario y de la observación directa. En tal sentido, se formularon dos preguntas para medir el grado de relevancia para la resolver los inconvenientes en lo referido a la seguridad de la información en la empresa, requiriendo un conjunto de políticas para el resguardo, protección y el minimizar los ataques cibernéticos, tal como se expresa en la siguiente tabla, donde la P19 está relacionada nivel de importancia en la política de seguridad de la información, y la P20 es referida al requerimiento de la organización de un SGSI que ayude a prevenir los riesgos de ciberataques.

Tabla 5

Resultados del cuestionario para la pregunta 19 y 20.

Grado	Nivel	P19		P20	
		fi	%	fi	%
Sin importancia	1	0	0%	0	0%
	2	0	0%	0	0%
	3	1	6%	0	0%
	4	2	11%	2	11%
Mucha importancia	5	15	83%	16	89%
Total		18	100%	18	100%

Nota. Resultados de la encuesta aplicada para la P19 (¿Cuál es el nivel de importancia con respecto a la seguridad de la información?) y P20 (¿Considera usted que, su organización requiere urgentemente un sistema de gestión de seguridad de la información (SGSI) que ayude a prevenir los riesgos de ciberataques?)

Si bien algunos encuestados expresaron alto grado de conciencia de la necesidad de buenas prácticas de seguridad de la información, se demuestra la necesidad de ajustes, mayor alineación de acciones para atender las demandas. Asimismo, predominantemente de los evaluados se inclinaron por las respuestas altas, indicando que la organización requiere urgentemente un SGSI que ayude a prevenir los riesgos de ciberataques, así como la protección de activos informáticos, y resguardo de los mismos. Por consiguiente, se rechaza la suposición nula, y se acepta la planteada por el investigador; es decir, "*Un sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001:2013 beneficiará a la empresa de consultoría financiera de Lima, 2021 protegiendo la información sensible"*.

IV. DISCUSIONES

Como se expone, este trabajo estuvo dirigido al diseño de un SGSI basado en la norma ISO/IEC 27001:2013 para una empresa consultora, la cual no cuenta con ningún o pocos controles de seguridad. En este modo, los resultados señalan la importancia de generar una propuesta para implementar un sistema de gestión de seguridad de la información (SGSI) para cualquier institución u organización, siguiendo la norma internacional ISO/IEC 27001:2013, ya que constituye en el conjunto de medidas reactivas y preventivas que permiten resguardar, así como proteger los activos informáticos, asegurando la disponibilidad, integridad y confidencialidad de la misma, y ayudando a mantener la continuidad de las operaciones en momentos de contingencia o de tratamiento ante la ocurrencia de un ciberataque.

El presente estudio logró desarrollarse mediante la evaluación de la variable sistema de gestión de seguridad de la información (SGSI) y sus dimensiones “planeación”, “ejecución (do)”, “verificación (check)” y “acción (act)”, los cuales lograron describir todos los elementos necesarios para la obtención de los objetivos de la investigación. Con respecto al objetivo general planteado en la investigación, se demostró que implementar un sistema de gestión de seguridad de la información (SGSI) robusto, según la Norma ISO/IEC 27001:2013, permite disminuir los riesgos ante ataques cibernéticos.

Ante los resultados anteriores, se encontró que la mayoría de los servidores desconocen la política de seguridad de la información de la institución. Por lo que es posible inferir que el comportamiento de los servidores, en relación a la seguridad de la información, está directamente ligado al desconocimiento de la política de la institución, lo que provoca que se tomen algunas actitudes equivocadas. Con ello, se constató que la política de seguridad de la información es de suma importancia para la empresa consultora, ya que define reglas que se deben seguir, facilitando el trabajo realizado. Está totalmente vinculado a los objetivos de la empresa, todos los empleados deben tener acceso a él y será revisado en un período determinado, de manera que se puedan realizar ajustes para la mejora continua.

Si se compara con el trabajo investigativo de Rincón (2020), donde se encontró similitudes, ya que concluye que la implementación del SGSI brindará mayor

protección a los activos de la empresa, favoreciendo la continuidad de la operación, neutralizando amenazas y creando confianza a clientes nuevos en el uso de los servicios y productos ofrecidos. Además, la presente investigación concuerda con el hecho de que la implementación de un SGSI basado en la norma internacional ISO/IEC 27001:2013 ayuda a brindar mayor protección a los activos informáticos, proporcionando mayor confiabilidad en los procesos y productos desarrollados por la empresa.

Asimismo, la investigación de Ordoñez y Castro (2017) encontró que un conjunto de deficiencias y vulnerabilidades en el cumplimiento del estándar o norma internacional NTCISO-IEC 27001:2013, debido a que nunca habían considerado la seguridad en sus procedimientos y carecían del conocimiento sobre el tema, reflejándose en las encuestas efectuadas a la gerencia y a los colaboradores, donde se obtuvieron respuestas negativas en relación al cumplimiento y conocimiento de los controles de la norma. En este sentido, en la presente investigación también se utilizó la tormenta de ideas (brainstorm) con el personal supervisor y los colaboradores, lográndose obtener los principales inconvenientes que presentan en la empresa consultora, siendo el punto de partida para la creación de mecanismos técnicos para proteger y resguardar los datos informativos a través de los módulos PDCA, dentro del el marco referencial necesario para diseñar de manera óptima un SGSI adecuado para la empresa.

Por otro lado, en el trabajo de investigación Vargas et al. (2017), donde los resultados evidenciaron la carencia de conocimientos de buenas prácticas en seguridad de la información, así como la ausencia de políticas de seguridad, y cuyos riesgos son principalmente por la carencia de conocimiento de buenas prácticas de seguridad de la información; asimismo, se recomendó formalizar el sistema de seguridad a través de la documentación de los programas, políticas y procedimientos, orientados por las normas ISO 27001. De la misma manera, la presente investigación concordó con la recomendación de implementar un sistema de gestión de seguridad de la información (SGSI) basado en la norma internacional ISO/IEC 27001:2013.

Mediante el desarrollo del SGSI se pretende mejorar y cubrir sus deficiencias, con el fin de proteger su activo más importante que es la información, se espera cumplir con los tres pilares de seguridad de la información, confidencialidad, integridad y disponibilidad. Es necesario sensibilizar al grupo de trabajo de la institución con capacitaciones, habilitaciones, charlas de capacitación, para conocer los procesos de

gestión de la información y sus activos informáticos. La información cobra cada vez más importancia para las organizaciones, por ello, la importancia de su protección es cada vez más indiscutible. La falta de conocimiento a menudo lleva a las personas a cometer comportamientos inadecuados. Esta política de seguridad también se puede utilizar como ayuda para anticipar el riesgo y garantizar la continuidad del servicio.

Al comparar con la investigación de Benítez (2019), cuyos hallazgos indicaron que para mantener los índices de seguridad de la información es necesario el uso controlado e inspeccionado del servicio de Internet en la compañía, así como la implementación de un SGSI, gracias al cual se minimizó de manera significativa los incidentes técnicos, así como se redujo el tiempo de respuesta en el responsable de TI y en el usuario. Mientras que, la presente investigación se encontró dentro de las malas prácticas el envío de información sensible a través de sitios web o correos electrónicos comerciales (como Gmail, Yahoo, Hotmail) y el no usar VPN corporativos para el trabajo remoto, y que la implementación de un SGSI contribuiría a asegurar la continuidad de las operaciones.

Por otro lado, Armas (2018) encontró que, al carecerse de medidas de seguridad guiados y documentados, ocurren irregularidades en perjuicio del resguardo de la información de la empresa, y que mediante un plan de acción sustentado en normas prediseñadas y adaptadas permitiría la identificación de puntos relevantes para una mejor gestión y análisis de riesgos; por consiguiente, se recomendaría implementar el SGSI para minimizar los riesgos e instalar de un comité de seguridad de la información. De la misma manera, la presente investigación concordó con la recomendación de conformar un equipo de detección y respuesta ante ciberataques mental para mantener el control de los eventos y alertas de seguridad en tu empresa y la certeza de tener un equipo enfocado las 24 horas del día en este tema.

Asimismo, Yana (2018) también evidenció que, al igual que la presente investigación, cuando no se cuenta con una política y estandarizada en el resguardo y protección de la información dentro cualquier empresa, siempre pueden ocurrir desviaciones que pueden incurrir en inconvenientes con la información confidencial. Es por ello que, un plan de acción planteado para un diseño y uso con una política integral dentro del SGSI, en el cual se instituyen criterios para su control, implementación, seguimiento y optimización continua.

La realización de este trabajo proporcionó un mayor conocimiento sobre las normas y procedimientos abordados en la norma ISO/IEC 27001:2013 de acuerdo con la propuesta de creación de un SGSI. Durante el período de análisis realizado, se encontró que el normal funcionamiento de la empresa depende cada vez más de sus sistemas de información, lo que intensifica la necesidad de maximizar su seguridad. Se percibió que existe una preocupación por la seguridad de la información, a pesar de no tener una política de seguridad definida, y con mecanismos deficientes en la difusión y concientización hacia las vulnerabilidades encontradas. Al tratarse de una empresa que brinda servicios de consultora financiera, la información es considerada un elemento crítico, por lo que es necesario que todos los empleados conozcan la política de seguridad de la información de la institución, sin embargo, una mejor práctica para resolver este problema, incluso frente a toda la complejidad.

La propuesta presentada pretende reducir la incidencia de numerosas amenazas a la seguridad de la información, así como crear una cultura organizacional de seguridad. Con la implementación de la propuesta del SGSI se espera que la empresa consultora obtenga: un aumento de la conciencia interna sobre la seguridad de la información; una optimización de los planes y procesos de gestión de la información, a través de la estandarización de los procesos; definición de responsabilidades por los activos; compromiso con la aplicación de la política, entre otras ventajas. Así que, se esperan buenos resultados de este trabajo con la implementación del SGSI, a través de los resultados obtenidos del cuestionario se nota que aun sin conocer las políticas de seguridad de la institución, tratan a la seguridad como algo muy importante para realizar su trabajo diario.

Finalmente, es de resaltar que, la implementación del SGSI en la empresa estudiada no generaría inversiones directas, lo que no garantiza que otras organizaciones también implementarán el PSI de forma gratuita, pero sí que, con el estudio de las normas y estándares conocidos y su adecuada adecuación a la realidad de la empresa, la inversión puede ser pequeña y absorbida por la organización. La oportunidad de utilizar un ambiente de producción como el de la empresa consultora en este estudio, mostró las dificultades que encuentran las pequeñas empresas en la implementación de la propuesta, demostrándose que para alcanzar un nivel de seguridad deseable no siempre es necesario contar con un alto inversiones, sino una cuidadosa selección de controles

basada en la clasificación de la información y el análisis de riesgos. Como el ISO/IEC 27001:2013 es parte integral de un SGSI, se puede considerar que la implementación de políticas de seguridad de la información es un paso importante hacia la creación de un plan de acción.

CONCLUSIONES

Los resultados obtenidos en la presente investigación permitieron llegar a las siguientes conclusiones:

Primera

A través de este trabajo fue posible generar una propuesta en cuanto a la gestión de seguridad de la información, evidenciándose que la misma constituye una necesidad relevante y de urgencia para la mejora en la protección y resguardo de la información. También se percibió la necesidad de algunas mejoras en algunos procesos, como la realización de copias de seguridad, la protección de equipos tecnológicos y la creación de una política y seguridad. Se puede concluir que la implementación de una política de seguridad de la información es de gran importancia, ya que el uso de estándares normativos en los procesos internos, facilitarían la gestión, y la realización de capacitaciones sobre protección de la información, siendo posible para reducir el costo de los incidentes y las altas pérdidas de información.

Segunda

A partir de la tormenta de ideas con los especialistas entrevistados se logró efectuar un inventario de los eventos de violaciones a la ciberseguridad, un diagrama de Pareto con la frecuencia de estos eventos y un diagrama de Ishikawa con las principales causa-raíz identificadas, lográndose identificar los diferentes tipos de eventos ocurridos, tales como hackeo de identidad, robo de información, infección con código malicioso, infección con malware, acceso indebido a sistemas, acceso indebido a información y detección de exploits. Además, se identificaron seis (6) tipos de causas-raíz: malas prácticas de los empleados, malas prácticas de la empresa, errores en capacitación, errores en la contratación, deficiencias en los sistemas y deficiencias en las políticas de la empresa. Todo esto conllevaron a diagnosticar que, la empresa consultora presenta deficiencias y vulnerabilidades en su política y gestión de su información.

Tercera

Se logró identificar los mecanismos técnicos que permitan implementar un sistema de gestión de seguridad de la información (SGSI), el cual debe constar de 4 etapas: 1)

planeación", 2) ejecución (do)", 3) verificación (check)" y 4) acción (act), los cuales definieron los objetivos, alcance y límites de la políticas de acción optimizado, así consiste la manera más idónea para una eventual implementación del SGSI y conformar un equipo de detección y respuesta, que ayudarán a tener las directrices claras y lineamientos a seguir para responder de manera rápida, oportuna y eficiente ante un ciberataque, cuya verificación consistió ser entendido y aplicado por todos los colaboradores o empleados, para brindar resultados positivos, y con revisión periódica para identificar si se requieren tomar nuevas acciones correctivas.

Cuarta

La propuesta de implementación de un sistema de gestión de seguridad de la información (SGSI) bajo la Norma ISO/IEC 27001:2013 en la empresa donde se desarrolló este estudio, permitirá resguardar y proteger los activos informáticos, asegurando la disponibilidad, integridad y confidencialidad de la misma, y ayudando a mantener la continuidad de las operaciones en momentos de contingencia o de tratamiento ante la ocurrencia de un ciberataque.

RECOMENDACIONES

Los resultados obtenidos en la actual investigación permitieron sugerir las siguientes recomendaciones:

Primera

Realizar esfuerzos para impulsar una cultura corporativa de ciberseguridad, que concientice a los colaboradores de los riesgos que conlleva no seguir las normas de seguridad a la hora de trabajar con activos informáticos; evitar las malas prácticas de los empleados como envío de información sensible a través de sitios web o correos electrónicos comerciales, el uso de contraseñas débiles o la ausencia de contraseñas, no usar VPN corporativos para el trabajo remoto y el no encriptar las bases de datos. Es por ello que, se debe implementar la propuesta diseñada y elaborada para establecer una política integral en materia del SGSI en base a la norma ISO/IEC 27001:2013.

Segunda

Capacitar al personal de la empresa en ciberseguridad, y considerar también la contratación de personal especializado en mitigar daños y pérdidas por ciberataques, ya sea como personal contratado permanente, o como asesores externos que brinden consultorías especializadas en todos los aspectos de la-gestión de la seguridad

Tercera

Considerar robustecer los sistemas de respaldo, adquiriendo discos duros portátiles, servidores físicos y en la nube (cloud), y equipos VPN para uso corporativo, así como la actualización de software (antivirus, antispam y firewalls) y sistemas operativos.

Cuarta

Implementar la propuesta del sistema de gestión de seguridad de la información (SGSI) bajo la Norma ISO/IEC 27001:2013 que se ha desarrollado en este estudio, siguiendo el cronograma de trabajo y monitoreando el avance de las actividades o tareas propuestas, que incluya la conformación de un equipo de detección y respuesta ante ciberataques mental para mantener el control de los eventos y alertas de seguridad en tu empresa y la certeza de tener un equipo enfocado las 24 horas del día en este tema.

Finamente, para trabajos futuros, también pueden definirse en el sentido de buscar comprender cómo la empresa puede lograr su modernización, dado el escenario actual. Por tal razón, se sugiere la replicación de este trabajo, para buscar remediar las limitaciones que esta investigación pudo haber tenido durante su ejecución. Validar los mecanismos a través de más casos de estudio; asimismo, evaluando la aplicabilidad de los mecanismos identificados o incluso nuevos mecanismos de seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2017). *El proyecto de investigación*. 7º Edición. Venezuela: Episteme.

Armas, A. y. (2018). *Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016.* Perú: Universidad Nacional Santiago Antunez.

Benitez, C. (2019). *Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza.* Perú: Universidad tecnologica del Perú.

Cano, J. (2011). *-La-Gerencia-de-laSeguridad-de-la-Informacion-Evolucion-yRetos-Emergentes.* Isaca.

Deloitte Latan. (27 de agosto de 2021). *Ciber Riesgos y Seguridad de la Información en América Latina y El Caribe. Tendencia 2019*. Obtenido de file:///C:/Users/Usuario/Documents/CHRISTIAN%20L%C3%93PEZ/Cyber%20Survey%20LATAM%20-%20Per%C3%BA%20.pdf

ESET. (2020). *ESET Security Report de 2020*. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

EY. (2020). *Encuesta Global sobre Seguridad de la Información*. Obtenido de https://www.ey.com/es_pe/giss

Galindo, C. (2014). *La firma electrónica avanzada y su certificación. En: Seguridad de la información.* Guatemala: Universidad San Carlos de Guatemala, .

Hernández, R. y Mendoza, C. (2018). *Metodología de la Investigación. Las rutas de cuantitativa, cualitativa y mixta*. McGraw Hill, México.

ISO27000. (09 de septiembre de 2021). *SGSI*. Obtenido de https://www.iso27000.es/sgsi.html

Isotools. (27 de agosto de 2021). *Sistemas de Gestión de Riesgos y Seguridad*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Miranda, K. (2013). *Guía Metodológica para implementar un Sistema de Gestión de Seguridad.* Peru: Universidad de Piura.

NQA Organismo de Certificación Global. (2020). *ISO 27001: Sistemas de gestión de seguridad de la información.* Perú.

NTP-ISO/IEC 17799: Norma Técnica Peruana. (2015). *NTP-ISO/IEC 17799: Norma Técnica Peruana.* Peru: SGSI.

Ordoñez, L. y Castro J. (2017). *Diseño de un sistema de gestión de seguridad de la información para la empresa SISELCOM S.A.S. bajo la norma ISO 27001:2013.* . Bogota: Universidad Piloto de Colombia.

Purdy, G. (2010). *ISO 31000: 2009—setting a new standard for risk management.* usa: . Risk analysis, 30(6), 881-886.

Rincón, C. (2020). *Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la Norma Internacional ISO/IEC 27001:2013 para la compañía ESSENSALE S.A.S.* Bogota: Universidad Nacional a Distancia.

Rueda, A. y Castillo, J. (2017). *Diseñar Un Sistema De Gestión De Seguridad De La Información Para El Colegio Agroindustrial De Puerto Nuevo Del Municipio De Simacota (Santander), Basado En La Norma 27001: 2013.* Colombia: Universidad Abierta y a Distancia.

Vargas, J.; Mandoòn, Y. y Sánchez, G. (2017). *Diseño de un sistema de gestión de seguridad de la información de los registros de los usuarios de la biblioteca Chaid Neme, basado en la norma NTC-ISO-IEC 27001:2013.* Colombia: Univeridad Francisco de Paula Santander.

Yana, W. (2018). *Propuesta de un sistema de gestión de seguridad de la información, aplicando la metodología MAGERIT para el Gobierno Regional Puno Caso: Proyecto especial Camélidos Sudamericanos – PECSA, 2.* Lima: Telesup.

ANEXOS

Anexo 1: Matriz de análisis de datos

<table>
<tr><td colspan="7">Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013</td></tr>
<tr><th>PROBLEMA GENERAL</th><th>OBJETIVO GENERAL</th><th>HIPOTESIS GENERAL</th><th>VARIABLE</th><th>DIMENSIONES</th><th>INDICADORES</th><th>METODOLOGIA</th></tr>
<tr><td>¿De qué manera la propuesta de un sistema de Gestión de Seguridad de la Información según la Norma ISO/IEC 27001:2013 beneficia a una Empresa de Consultoría Financiera de Lima, 2021?</td><td>Generar una propuesta para implementar un sistema de gestión de seguridad de la información (SGSI) para una Empresa de Consultoría Financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013</td><td rowspan="4">Un sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001:2013 beneficiará a una empresa de consultoría financiera de Lima, 2021 protegiendo la información sensible.</td><td rowspan="4">Sistema de Gestión de Seguridad de la Información (SGSI)</td><td>Planeación</td><td>• Análisis de la situación actual
• Políticas de seguridad
• Análisis de riesgo</td><td rowspan="4">Método: Analítico-sintético e hipotético-deductivo.
Tipo: Aplicada y De Campo.
Enfoque: Mixto (cualitativo – cuantitativo).
Nivel: Descriptivo y explicativo.
Diseño: No experimental
Corte: Transversal.
Población: La población estuvo representada por los procesos llevados a cabo en la consultora para el respaldo y protección de su información; así como los 18 servidores.</td></tr>
<tr><td>PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td><td></td><td></td></tr>
<tr><td>¿Cuál es el diagnosticar la situación problemática sobre deficiencias en el sistema de gestión de seguridad de la información en una empresa de consultoría financiera en Lima, 2021?</td><td>Diagnosticar la situación problemática sobre deficiencias en el sistema de gestión de seguridad de la información en una empresa de consultoría financiera en Lima, 2021.</td><td>Ejecución (Do)</td><td>• Implementación del SGSI
• Control de riesgos</td></tr>
<tr><td>¿Cuáles son los mecanismos técnicos que permitan optimizar el sistema de gestión de seguridad de la información en una empresa de consultoría financiera en Lima, 2021?</td><td>Identificar los mecanismos técnicos que permitan optimizar el sistema de gestión de seguridad de la información en una empresa de consultoría financiera en Lima, 2021.</td><td>Verificación (Check)</td><td>• Verificación de implementación del SGSI
• Verificación del control de riesgos</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Acción (Act)</td><td>• Acciones</td></tr>
</table>

¿Cuál es la propuesta sobre el sistema de gestión de seguridad de la información bajo la Norma ISO/IEC 27001:2013 para aumentar la protección de la información en una empresa de consultoría financiera en Lima, 2021.	Efectuar una propuesta sobre un sistema de gestión de seguridad de la información (SGSI) bajo la Norma ISO/IEC 27001:2013 para aumentar la protección de la información en una empresa de consultoría financiera en Lima, 2021.				preventivas • Acciones correctivos	**Muestra**: La muestra estuvo representada por los procesos llevados a cabo en la consultora para el respaldo y protección de su información; así como los 18 servidores de la empresa consultora. **Técnica de recolección de datos**: Encuesta y la observación. **Instrumentos:** cuestionario y observación directa de campo. **Métodos de análisis de datos**: Análisis y estadística descriptiva.

Anexo 2: Instrumento de recolección de datos

Título de la investigación: "Propuesta de un sistema de gestión de seguridad de la información para una empresa de consultoría financiera en Lima, 2021, según la norma ISO/IEC 27001:2013"

Estimado Colaborador: Después de haber sido informado adecuadamente sobre el propósito científico de nuestro cuestionario, agradeceremos su colaboración respondiendo cada una de las preguntas del presente cuestionario. Para ello, lea detenidamente cada ítem y sírvase marcar con un aspa "X" un solo recuadro de datos y dar respuesta a las preguntas formuladas:

1 ¿Cuál es el nivel de conocimiento de las políticas de seguridad de la información que existen en la empresa? En una escala del 1 al 5.

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

No se Lo se totalmente

2 - Si tiene algún conocimiento sobre la política de seguridad de la información de la empresa, ¿cómo califica el conocimiento?

- ☐ Comprensión fácil
- ☐ Comprensión intermedia
- ☐ Comprensión difícil
- ☐ No tengo conocimiento

3 - ¿Ha recibido alguna capacitación sobre seguridad de la información?

Sí ☐ No ☐ No tengo conocimiento ☐

4 - Antes de iniciar sus actividades profesionales en la empresa, ¿todo usuario recibe orientación en materia de seguridad de la información y toma conocimiento de las normas existentes?

Sí ☐ No ☐ No tengo conocimiento ☐

5 - En su opinión, ¿los usuarios de la empresa conocen las normas de seguridad de la información existentes?

Sí ☐ No ☐ No tengo conocimiento ☐

6- ¿La elección de sus contraseñas siguió alguna política de seguridad de la información de la empresa?

Sí ☐ No ☐ No tengo conocimiento ☐

7 - ¿El cambio de contraseña es periódico?

Sí ☐ No ☐ No tengo conocimiento ☐

8 - ¿Existe un requisito por parte de los sistemas para una contraseña fuerte?

Sí ☐ No ☐ No tengo conocimiento ☐

9 - ¿Cuenta con respaldo de los archivos necesarios para realizar su trabajo?

Sí ☐ No ☐ No tengo conocimiento ☐

10 - ¿Existen reglas para el uso de Internet?

Sí ☐ No ☐ No tengo conocimiento ☐

11 - ¿El uso de Internet es monitoreado por algún organismo de TI?

Sí ☐ No ☐ No tengo conocimiento ☐

12 - ¿Existen reglas para el uso del correo electrónico empresa?

Sí ☐ No ☐ No tengo conocimiento ☐

13 - ¿Tu computadora tiene protección antivirus?

Sí ☐ No ☐ No tengo conocimiento ☐

14 - ¿Ejecutas el antivirus antes de ejecutar cualquier archivo presente en cualquier medio removible (pendrives, HD, DVD, CD-ROM)?

Sí ☐ No ☐ No tengo conocimiento ☐

15 - ¿Existe un procedimiento para reportar un incidente de seguridad de la información?

Sí ☐ No ☐ No tengo conocimiento ☐

16 - ¿Las áreas de acceso restringido contienen una advertencia?

Sí ☐ No ☐ No tengo conocimiento ☐

17 - ¿Se registra la entrada y salida de visitantes? *

Sí ☐ No ☐ No tengo conocimiento ☐

18 - ¿Se monitorean las acciones de los empleados y visitantes? *

Sí ☐ No ☐ No tengo conocimiento ☐

19 - ¿Cuál es el nivel de importancia con respecto a la seguridad de la información?

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sin importancia Mucha importancia

20. - ¿Considera usted que, su organización requiere urgentemente un sistema de gestión de seguridad de la información (SGSI) que ayude a prevenir los riesgos de ciberataques?

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sin importancia Mucha importancia

PREGUNTAS DIAGNOSTICAS:

a.- ¿Cuáles han sido los principales eventos de violaciones a la ciberseguridad que se han presentado en la empresa durante el año 2021?

Resp.: _____

b.- ¿Cuáles cree usted que son las principales causa-raíz de los inconvenientes en las deficiencias de la protección de la información?

Resp.: _____

c.- ¿Cuáles cree usted que son principales mecanismos técnicos que permitan implementar un SGSI en una empresa de consultoría financiera en Lima

Resp.: _____

d.- ¿Qué recomendaciones daría usted para efectuar una propuesta para implementar un Sistema de Gestión de Seguridad de la información (SGSI) bajo la Norma ISO/IEC 27001:2013?

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICAFACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA De Sistemas e Informatica

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS:

"Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de consultoría Financiera En Lima, 2021, Segun la Norma ISO/IEC 27001:2013"

PRESENTADO POR (Tesista): Bach Espinoza Melendez Juan carlos Y Lopez Torres, CHRISTIAN Brayan

I. DATOS GENERALES DEL EXPERTO NRO: .....

1.1. Apellidos y Nombres : Flores Eulogio, Rossino Arnaldo

1.2. Grado Académico : Maestro

1.3. Cargo e Institución donde Labora: Universidad Peruana de Ciencias

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado			X		
2. OBJETIVIDAD	Está expresado en conducta observable				X	
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología			X		
4. ORGANIZACION	Existe organización Lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones				X	
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.				X	

II. OPCION DE APLICABILIDAD : Alta

III. PROMEDIO DE VALORACIÓN: Muy Bueno

IV. RECOMENDACIÓNES : Ninguna

Firma del experto:

Fecha: 13/07/2022

DNI: 10561280

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICAFACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA de Sistemas e Informatica

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de consultoría Financiera en Lima, 2021, Segun la Norma ISO/I.EC 27001: 2013"

PRESENTADO POR (Tesista): Bach Espinoza Melendez, Juan carlos y Lopez Torres, christian Brayan

I. DATOS GENERALES DEL EXPERTO NRO: .....

1.1. Apellidos y Nombres : Hermoza achante, Ruben EDgar

1.2. Grado Académico : Maestro

1.3. Cargo e Institución donde Labora: Universidad Peruana de Ciencias

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACION	Existe organización Lógica					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.				X	

II. OPCION DE APLICABILIDAD : Alta

III. PROMEDIO DE VALORACIÓN: Muy Bueno

IV. RECOMENDACIÓNES :

Firma del experto:

Fecha: 12/07/22 DNI: 42057740

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICAFACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA de Sistemas e Informática

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS:
"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORIA FINANCIERA EN LIMA, 2021, SEGÚN LA NORMA ISO/IEC 27001-2013"

PRESENTADO POR (Tesista): Bach
ESPINOZA MELENDEZ JUAN CARLOS

I. DATOS GENERALES DEL EXPERTO NRO: .....

1.1. Apellidos y Nombres : QUISPE AYQUIPA CESAR ANTONIO

1.2. Grado Académico : MG. EN INVESTIGACIÓN Y DOCENCIA UNIVERSITARIA

1.3. Cargo e Institución donde Labora:

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado			X		
2. OBJETIVIDAD	Está expresado en conducta observable				X	
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				X	
4. ORGANIZACION	Existe organización Lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones			X		
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.				X	

II. OPCION DE APLICABILIDAD : ALTO

III. PROMEDIO DE VALORACIÓN: MUY BUENO

IV. RECOMENDACIÓNES : Ninguno

Firma del experto:

Fecha: 18/07/22

DNI: 42425585

Anexo 3: Base Datos

	CUESTIONARIO																
No.	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	**Total**
1	1	1	2	2	2	2	1	1	2	3	2	2	2	1	3	2	**29**
2	2	3	3	3	2	3	3	3	3	3	2	2	1	1	1	2	**37**
3	3	2	3	3	3	2	3	3	2	3	2	2	3	2	2	3	**41**
4	3	3	2	3	3	2	2	2	3	3	2	2	1	1	2	1	**35**
5	3	2	2	3	2	3	1	1	2	2	2	1	1	1	1	2	**29**
6	2	2	3	3	3	1	2	2	1	3	2	2	2	1	1	2	**32**
7	2	3	3	2	2	3	2	1	1	1	2	1	1	2	2	1	**29**
8	3	2	2	2	2	3	2	3	2	2	2	3	2	2	1	1	**34**
9	2	1	2	1	2	1	2	1	1	2	2	1	1	2	3	2	**26**
10	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	**17**
Vi	0.56	0.60	0.41	0.61	0.36	0.69	0.49	0.76	0.56	0.61	0.09	0.41	0.45	0.25	0.61	0.41	
K	16																
∑Vi	7.87																
Vt	39.49																
α	**0.85**																

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

α = Alfa de Cronbach

K = Número de Ítems

Vi = Varianza de cada ítems

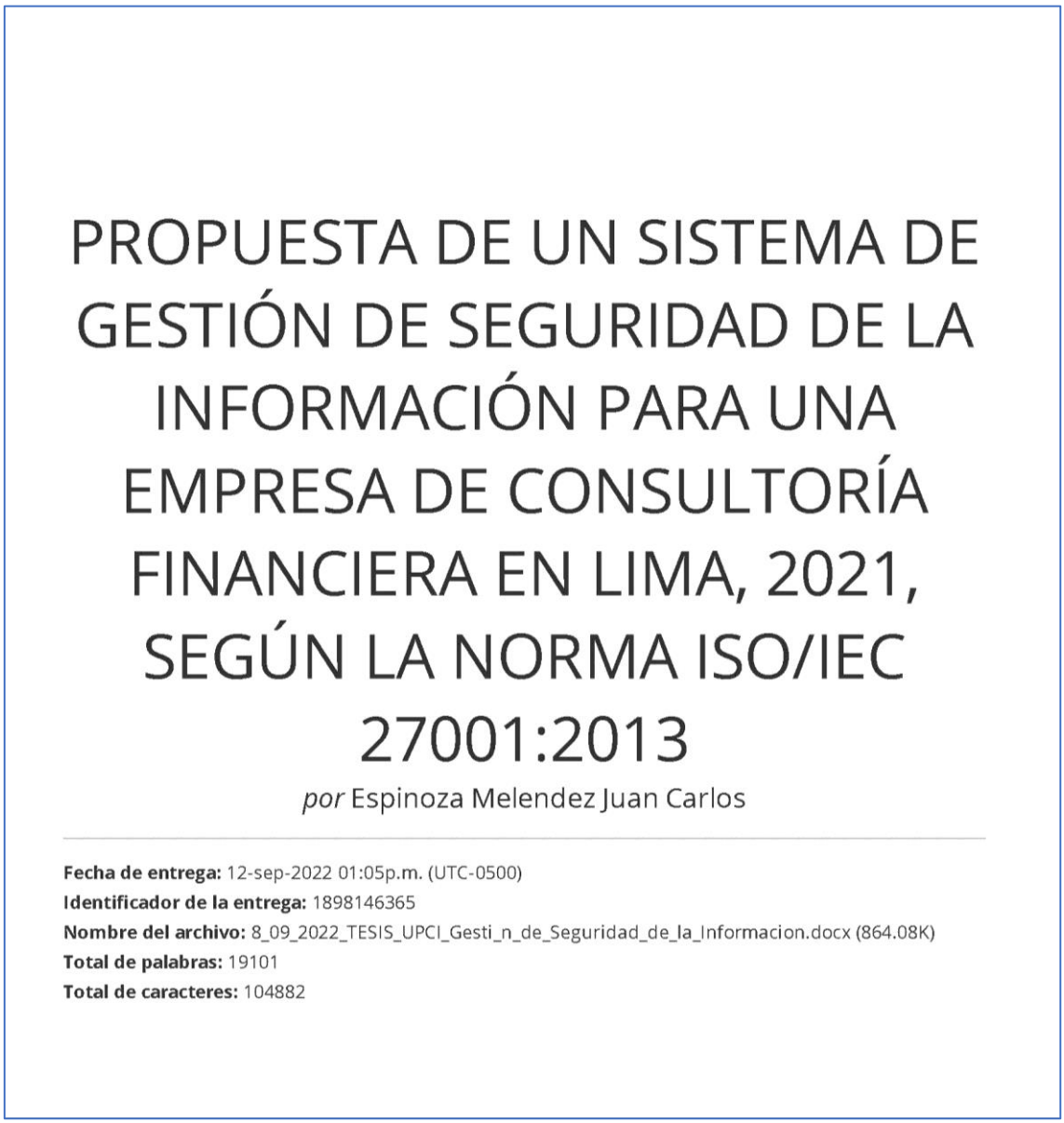
Vt = Varianza total

SI=3

NO=2

No tengo conocimiento=1

Anexo 4: Evidencia de similitud digital



PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA FINANCIERA EN LIMA, 2021, SEGÚN LA NORMA ISO/IEC 27001:2013

por Espinoza Melendez Juan Carlos

Fecha de entrega: 12-sep-2022 01:05p.m. (UTC-0500)
Identificador de la entrega: 1898146365
Nombre del archivo: 8_09_2022_TESIS_UPCI_Gesti_n_de_Seguridad_de_la_Informacion.docx (864.08K)
Total de palabras: 19101
Total de caracteres: 104882

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA FINANCIERA EN LIMA, 2021, SEGÚN LA NORMA ISO/IEC 27001:2013

INFORME DE ORIGINALIDAD

3%	2%	0%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	2%
2	repositorio.upci.edu.pe Fuente de Internet	<1%
3	repository.unad.edu.co Fuente de Internet	<1%
4	core.ac.uk Fuente de Internet	<1%
5	blog.netdatanetworks.com Fuente de Internet	<1%
6	Submitted to Universidad Señor de Sipan Trabajo del estudiante	<1%
7	bibliotecavirtualoducal.uc.cl Fuente de Internet	<1%
8	repositorio.ulasamericas.edu.pe Fuente de Internet	<1%

9	vsip.info Fuente de Internet	<1 %
10	hdl.handle.net Fuente de Internet	<1 %
11	es.scribd.com Fuente de Internet	<1 %
12	repositorio.ucv.edu.pe Fuente de Internet	<1 %
13	centrodeconocimiento.ccb.org.co Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Anexo 5. Autorización de publicación en repositorio

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Espinoza Melendez Juan Carlos

DNI: 48511404 Correo electrónico: 48511404m@gmail.com

Domicilio: Jiron Necochea 2021 - Villa María Del Triunfo

Teléfono fijo:9 - Teléfono celular: 939834194

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: FACULTAD DE CIENCIAS E INGENIERIA

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (X)

Título del Trabajo de Investigación / Tesis:

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA UNA UNA EMPRESA DE CONSULTORIA FINANCIERA EN LIMA 2021, SEGÚN LA NORMA ISO/IEC 27001:2013

3.- OBTENER:

Bachiller ( ) Titulo (X) Mg ( ) Dr ( ) PhD ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) indicada en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):
(X) Sí, autorizo el depósito total.
( ) Sí, autorizo el depósito y solo las partes:
( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los 19 días del mes de NOVIEMBRE de 2022

Firma

Huella digital

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: LOPEZ TORRES CHRISTIAN BRYAN

DNI: 77382754 Correo electrónico: CH.LOPEZTORRES@GMAIL.COM

Domicilio: Mz B1 LT 12 3er Sector Derecho Urb Antonia Moreno de Caceres - Ventanilla

Teléfono fijo: 6221224 Teléfono celular: 940442857

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: FACULTAD DE CIENCIAS E INGENIERIA

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (x)

Título del Trabajo de Investigación / Tesis:

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA UNA UNA EMPRESA DE CONSULTORIA FINANCIERA EN LIMA 2021, SEGÚN LA NORMA ISO/IEC 27001:2013

3.- OBTENER:

Bachiller ( ) Titulo (X) Mg ( ) Dr ( ) PhD ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) TESIS indicada en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):
(X) Sí, autorizo el depósito total.
( ) Sí, autorizo el depósito y solo las partes: _____
( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los 19 días del mes de NOVIEMBRE de 2022

Huella digital

Firma