UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Facultad de Ciencias Administrativas, Contables y Comercio
Carrera de Gestión de la Información Gerencial

TRABAJO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del título de:

Licenciada En Gestión de la Información Gerencial

Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información, Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social Manta, 2024

(Estudio de caso).

AUTORA:

Saltos García Martha Isabel

MANTA-ECUADOR

2024

Tema

Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información, Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social, Manta, 2024

(Estudio de caso)

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1 Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Carrera de Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas Contables y Comercio de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular – Estudio de Caso bajo la autoría de la estudiante **Saltos García Martha Isabel**, legalmente matriculado/a en la Carrera de Gestión de la Información Gerencial, período académico 2024_2, cumpliendo el total de 240 horas (96 horas Fase de Diseño y 144 horas Fase de Resultado), cuyo tema del trabajo es **"Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información, Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social Manta, 2024 (Estudio de caso)".**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 20 de diciembre de 2024

Lo certifico,

Lic. Oswaldo Waldemar Mero Delgado
Docente Tutor
Área: Administrativas Contables y Comercio

Autoría

Yo, Martha Isabel Saltos García, con cédula de identidad N° 1315499275, perteneciente a la carrera de Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas, Contables y Comercio, egresada de la Universidad Laica Eloy Alfaro de Manabí, declaro que el siguiente estudio de caso titulado: "Normas ISO 27000 para mejorar el Sistema de Gestión de la Información, Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social IESS de los Esteros, 2024 (Estudio de Caso).", es de mí autoría.

De esta manera, reconozco que los aprendizajes adquiridos en estos años son únicamente obtenidos de la Universidad Laica Eloy Alfaro de Manabí.

Saltos García Martha Isabel

C.I 1315499275

Dedicatoria

Dedico esta investigación bajo la modalidad estudio de caso:

A Dios, por ser el inspirador para cada uno de mis pasos dados en mi convivir diario, misma que me fortalece mi espiritualidad, fe, esperanza y amor.

A mis padres, Ing. Leonardo Saltos Chica y Lic. Nancy García López por ser los guías en el sendero de cada acto que realizo hoy, mañana y siempre, como hija y como profesional llevando en mi corazón y en mi memoria los valores, principios y moral inculcados durante mi existencia.

A mis hermanos, José Antonio y Carlos Alberto Saltos García, por ser el incentivo para seguir adelante con mis anhelos de ser una profesional en esta sociedad mantense mantense, manabita y ecuatoriana

Martha Isabel Saltos García

Agradecimiento

Extiendo mi agradecimiento a la Universidad Laica Eloy Alfaro de Manabí, especialmente a la Carrera Gestión de Información Gerencial, de la Facultad de Ciencias Administrativas, Contables y Comercio, por permitir ser parte de este templo del conocimiento y saberes dentro de las áreas administrativas.

A la Facultad Ciencias Administrativas, Contables y Comercio por acogerme como estudiante para la preparación académica dentro el mágico mundo en el área administrativo y por ende a la Carrera de Gestión de la Información Gerencial por ofrecerme los conocimientos en el campo amplio de la Gestión de la Información, herramientas académicas y tecnológicas necesarios para mi crecimiento profesional y personal, recibida con base sólida, la cual seguiré construyendo mi futuro en el desempeño profesional.

A los docentes de la Carrera mencionada un reconocimiento desde mi corazón por cada vivencia de conocimiento y sabiduría compartida dentro de las aulas de clases, las cuales han contribuido al desempeño como estudiante convirtiéndose en herramienta para un futuro mejor en mi desarrollo profesional.

Finalmente, un agradecimiento especial a mi Tutor Lic. Oswaldo Waldemar Mg, por acompañarme con dedicación y paciencia en cada etapa de esta investigación, destacando su orientación y apoyo constante, como base fundamental para lograr la finalización de esta investigación con éxito.

Srta. Martha Isabel Saltos García

Índice

Introducción

Hoy en día las empresas públicas y privadas deben aplicar la Norma ISO 27000 para cumplir con los estándares establecidos y a su vez lograr su mejora continua llevando a cabo los protocolos del sistema de gestión de seguridad de la información de manera que permita garantizar el cumplimiento correcto de sus objetivos para las organizaciones; por ello, esta investigación lleva como tema Normas ISO 27000 para mejorar la gestión de la seguridad de la información en el departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social IESS de los Esteros.

El interés para realizar el trabajo de investigación es conocer cómo se establece la norma ISO 27000 de manera eficiente en el departamento de Talento Humano tomando en cuenta sus puntos relevantes para mejorar la gestión de seguridad de la información. Asimismo, esta norma ayudará al IESS a fortalecer su sistema de gestión de seguridad de la información para mejorar su eficiencia y por ende lograr sus objetivos de manera efectiva.

Como finalidad de este estudio de caso es fortalecer las habilidades y destrezas a los servidores públicos para así examinar la Norma 27000 lo que proporcionará un enfoque sistemático, estructurado para identificar, gestionar y mitigar los riesgos que enfrenta el departamento de Talento Humano. Por otro lado, el objetivo de este estudio es, analizar las Normas ISO 27000 para mejorar la gestión de la seguridad de la información en el departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social IESS de los Esteros.

En base a los componentes de esta investigación es de enfoque cualitativa y cuantitativa, asimismo su alcance es netamente descriptivo y exploratorio basado en un tipo de investigación bibliográfico y de campo. Además, en su diseño se enlaza los métodos de análisis, síntesis inductivo y deductivo, en el cual se complementa con técnicas y herramientas que permiten recoger la información a través de la observación, entrevista semiestructurada y

la encuesta realizada a la población del lugar de los hechos basado en el muestreo estratificado.

La distribución de este trabajo de investigación estudio de caso esta efectuada en el diseño fase 1 y análisis de resultados fase 2 respectivamente; por tanto, su estructura de la distribuye de la siguiente forma: en el diseño corresponde tema, introducción, antecedentes investigativos, justificación, objetivos, marco conceptual y metodológico los cuales son considerados mediante la descripción de teorías como la de la observación para fundamentar explícitamente sus variables tanto dependiente como independiente; en la siguiente sección, se exponen los hallazgos de la investigación como resultados obtenidos, análisis de resultados, conclusiones, recomendaciones, referencias, anexos y propuestas de solución, todo esto obtenido mediante la información obtenida una vez aplicada la técnicas y analizado sus datos.

Por otro parte, el análisis de resultados revela una comprensión variada entre los colaboradores sobre la importancia de establecer buenas prácticas para implementación del SGSI (Sistema de Gestión de Seguridad de la Información). De esta manera también se señala la necesidad de continuar trabajando para mejorar su eficacia y garantizar la protección de la información.

Asimismo, se evidencia que dentro del estudio proporciona una visión clara para mejorar la seguridad de la información en el departamento de Talento Humano. Al implementar las recomendaciones se logra un nivel de seguridad más alto y proteger los activos de información de la organización.

Antecedentes Investigativos

En la era digital, la gestión efectiva de la seguridad de la información se convierte en una prioridad crítica para las organizaciones, especialmente en el sector público, donde la protección de datos es fundamental. El Instituto Ecuatoriano de Seguridad Social (IESS) de los Esteros enfrenta importantes desafíos en la protección de la información gestionada por su departamento de Talento Humano, esta área es responsable de manejar datos sensibles tanto personales y laborales de miles de empleados y afiliados.

El IESS, de Manta es una organización pública y autónoma con justicia privada y solidaridad, la Constitución de 2008 consolida el IESS y a través del Artículo 34 que establece el Seguro Social como un derecho indispensable de todos los ciudadanos en el marco de los cambios realizados por el gobierno, un cambio relevante ocurrió el 20 de octubre de 2010, cuando, a través de la Resolución del Consejo Directivo N° 334 se amplió la cobertura del seguro de salud. Este cambio incluyó a las sucursales del IESS, personas retiradas relacionadas con sus hijos menores de 18 años y cónyuge, incrementando significativamente el número de beneficiarios.

Las normas ISO 27000, y en particular la ISO/IEC 27001, proporcionan un marco robusto para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Estas normas internacionales son reconocidas por su capacidad para ayudar a las organizaciones a gestionar la seguridad de los activos de información de manera sistemática y eficiente.

El presente estudio de caso se centra en analizar cómo la adopción y aplicación de las normas ISO 27000 pueden mejorar el SGSI del departamento de Talento Humano del IESS de los Esteros en el año 2024. A través de este análisis, se pretende identificar las amenazas y vulnerabilidades principales, evaluar la efectividad del sistema actual, y plantear recomendaciones basadas en estándares internacionales reconocidos. Asimismo, se evaluará

el rol de la capacitación del personal y las barreras para la implementación de las normas ISO 27000, que proporciona una visión integral de los beneficios y desafíos asociados con el fortalecimiento de la seguridad de la información en este entorno.

La investigación se basa en una revisión exhaustiva de las normas ISO 27000 para fortalecer el Sistema de Gestión de Seguridad de Información. se llevará a cabo un análisis detallado del entorno actual de seguridad en el departamento de Talento Humano, con el objetivo de Identificar las debilidades existentes y posteriormente diseñar un plan de acción alineados con las recomendaciones y buenas prácticas de ISO 27000.

Luego de revisar diversos proyectos de investigación; se determinan estudios que sirven de guía para el desarrollo del presente trabajo de Estudio de Caso. A continuación, se realiza un breve análisis de las investigaciones desarrolladas en relación con este estudio de caso:

En Europa, en Asturias (Comunidad Autónoma de España), Álvarez (2017) desarrolla una investigación con tema “Implementación ISO 27001-Empresa Ficticia”, contiene como objetivo: Implantar un plan director de seguridad en una empresa de acuerdo a las normas ISO 27001 e ISO 27002, para cumplir con este trabajo se emplea una metodología de tipo observacional, descriptiva, donde destacan una correcta implementación de este modelo, se realiza mediante fases, empleando metodologías de gestión en proyectos.

Se confirma como resultado mediante la evaluación que se aplica, es fructífera la implementación de las Normas ISO 27001, puesto que la estimación inicial evaluó los puntos de forma obligatoria, superando en un 80% el control de los accesos y mejora los servicios competentes en los aspectos de seguridad. Para concluir el enfoque principal de la implementación fue la ISO 27001, y así proteger la confidencialidad, integridad de los datos e información que cuenta la organización.

En Cajamarca-Perú, Chugden Romero (2022) desarrolla una investigación titulada “Modelo de seguridad informática aplicando la norma ISO 27001 para proteger los activos de información de la empresa PROTALENT SAC Cajamarca, 2022”, donde se evidencia como problemática que no cuentan con el control de seguridad y confidencialidad; el objetivo de la investigación fue desarrollar un modelo de seguridad de la informática utilizando la norma ISO 27001 aplicado a la empresa, recurriendo una metodología de enfoque mixto de tipo correlacional- explicativo, método inductivo–deductivo de diseño no experimental.

Los resultados indican que es necesario implementar controles efectivos de seguridad de la información basados en la norma ISO 27001, para mitigar los riesgos identificados, además, para optimizar los procesos de la empresa Protalent S.A.C, es fundamental reducir las quejas y mejorar la eficiencia operativa. Esto requiere la aplicación de evaluaciones previas y posteriores, lo que permite medir el impacto y contribuir de manera significativa a la correcta adaptación de la norma ISO 27000.

En Ecuador- Santo Domingo, Sampedro Guamán et al., (2019) efectúan una investigación titulada “Percepción de seguridad de la información en las pequeñas y medianas empresas en Santo Domingo”, el objetivo fue analizar las consecuencias que tiene el uso de los sistemas informáticos, con el enfoque de la aplicabilidad de Normas Internacionales ISO, aplicando una metodología de tipo transversal, descriptiva; obteniendo como resultado que para proteger uno de los activos más valiosos con los que cuenta las PyMES, que es la información tanto física como digital. El estudio culminó con la generación de datos estadísticos sobre la seguridad de la información, orientados a que los empresarios a minimizar los problemas en sus entidades y organizaciones y a fortalecer la protección de sus activos más valiosos.

El estudio de Camargo (2017), denominado “Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil – CNSC (Comisión Nacional del Servicio Civil) basado en la norma ISO27000 e ISO 27001” tiene como objetivo asegurar, mantener la total confidencialidad de la información que maneja recibe y guarda en la entidad, evitando la posible pérdida por las amenazas del medio. La gestión de la seguridad de la información aplicando la norma ISO 27000 e ISO 27001 en las tecnologías de la Comisión Nacional del Servicio Civil (CNSC) en Bogotá capital de Colombia, en la cual se utilizó la metodología de análisis y gestión de riesgos de los sistemas de información donde se detectó los activos críticos y el impacto que se originan en la entidad.

Los resultados de la investigación por Camargo (2017) evidenciaron varias conclusiones clave relacionadas con la gestión de la seguridad de la información en el área tecnológica de la Comisión Nacional del Servicio Civil (CNSC). Entre ellos los más relevantes se destacan: La falta de controles y políticas de seguridad en la cual el análisis reveló que la CNSC enfrenta un alto nivel de riesgo debido a la ausencia de controles de seguridad adecuados, prácticas insuficientes en la gestión de riesgos y la carencia de una política de seguridad formalmente aprobada y respaldada por los directivos.

Este trabajo de investigación concluye que la aplicación de la norma ISO/IEC 27001 evidencia que el CNSC enfrenta un alto riesgo debido a la ausencia de controles, la falta de prácticas adecuadas del recurso humano y la carencia de una política de seguridad aprobada por los directivos lo cual dificulta su implementación y cumplimiento.

Ponce (2023), en su estudio de investigación llamado “Sistema de gestión de seguridad de la información para la Protección de datos en una inmobiliaria, Lima 2022” desarrollado en la Universidad César Vallejo, Trujillo, Perú. Su propósito general fue optimizar la seguridad de datos en una inmobiliaria en la ciudad de Lima durante el año 2022 logrado gracias a la propuesta de implementar un SGSI. El tipo de la investigación fue aplicada y de diseño pre experimental. Contaron con una muestra poblacional de 8 instituciones (entre públicas y privadas), las que se evaluaron gracias a una encuesta de satisfacción. Concluye con que el nivel de riesgo de seguridad de la información se aplacó en un 60.00%, las estimaciones que se obtuvieron en las operaciones estadísticas antes y después de implementar la salida fueron de 4.47 y 1.37 puntos. Esto demuestra que un SGSI eleva al máximo la seguridad de los datos de una compañía inmobiliaria en la ciudad de Lima durante el año 2022.

El estudio realizado en Ecuador en el cantón Babahoyo, Guamán (2022), desarrolla una investigación titulada “Análisis y diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing, aplicando la Norma ISO 27001. En la empresa Data-Fiber”, aplicar operabilidad en toda la empresa, donde empleen web, para mejorar las necesidades del cliente servidor. Como resultado se resalta que el uso de la web por parte del usuario o cliente, debe incluir la definición clara de responsabilidades y derechos compartidos.

Vegas (2019), desarrolló una tesis titulada “Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001”. Tuvo como propósito principal el diseño de un SGSI para las actividades académicas de la Universidad Nacional de Piura de acuerdo con la NTP ISO/IEC 27001. Este estudio es de tipo aplicado, recolectó información cuantitativa y cualitativa, de diseño no experimental, aplicó la técnica de encuestas para la recolección de datos, aplicando como instrumento un cuestionario.

Concluyó con que, al encontrar un porcentaje bajo de cumplimiento del 39%, que demuestra que hay desgano relacionado a la seguridad de la información dentro la organización, lo cual se debe a que hay controles básicos en el funcionamiento de la seguridad de la información; pero que aún no se encuentran documentados ni se ha sensibilizado ni capacitado al personal sobre su uso y tampoco hay procedimientos y métricas para medir el cumplimiento de dichos controles, por lo que es fundamental implantar un SGSI.

Definición del Caso de Estudio

El caso de estudio se desarrolla en el Instituto Ecuatoriano de Seguridad Social (IESS), entidad cuya organización y funcionamiento se basa en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia, enfatiza su aplicación en el Sistema del Seguro General Obligatorio que forma parte del Sistema Nacional de Seguridad Social del Ecuador.

En la actualidad se encuentra en una etapa de transformación en la que se está realizando la planificación y elaboración de planes estratégicos para los diferentes servicios sustentados en la Ley de Seguridad Social vigente. Además, la aplicación de estos planes convertirá a la Institución en una fase seguradora moderna y técnica, con personal capacitado que atenderá con eficiencia, oportunidad y amabilidad a todas personas que solicite los servicios y prestaciones que ofrece.

Por otra parte, se destaca que, la constante competencia entre organizaciones surge la necesidad de analizar los diversos factores que emergen en su entorno debido a un cambio rotundo; por lo tanto, es sustancial que adopten nuevas estrategias para obtener ventaja competitiva en el mercado, favoreciendo los productos o servicios que ofrecen a los clientes. En tal escenario, una de las opciones más seguras para lograr buenos resultados es efectuar un Plan de Gestión para Seguridad de la información que esté basado a la norma ISO 27000 que permita fortalecer la mejora de Sistema de Gestión de la Seguridad de la información y su enfoque de gestión de riesgo (Advisory, 2019).

Valencia Duque (2021), Indica que la seguridad de la información es crucial para las organizaciones, y la norma ISO/IEC 27000 ofrece un marco integral para proteger los activos de información y cumplir con las regulaciones. Por otra parte, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en esta norma ayuda a gestionar los riesgos tecnológicos y garantizar la confidencialidad, integridad y disponibilidad de los datos,

mejorando la resiliencia organizacional frente a amenazas cibernéticas y asegurando el cumplimiento legal.

De igual manera, un Sistema de Gestión de Seguridad de la Información es una forma de trabajar, mediante el cual una organización asegura la protección o resguardo de información y la confianza de los clientes. Para conseguir aquello la organización, planifica, mantiene y mejora continuamente el desempeño de sus procesos bajo un esquema de eficiencia y eficacia que le permite lograr mejores innovaciones, también proporciona herramientas para el monitoreo de acciones correctivas y mejora continua.

Sin embargo, una de las problemáticas que enfrenta el departamento de Talento Humano es la escasez de experiencia interna, lo que representa un obstáculo significativo; por otro lado, la complejidad de la norma, abarca una amplia gama de actividades, desde la identificación de riesgos hasta la gestión de incidentes, requiere un conocimiento especializado que el personal sin la formación adecuada podría no poseer. Esta carencia podría dificultar la correcta implementación y mantenimiento del sistema, lo que resalta la necesidad urgente de capacitación continua y el fortalecimiento de las competencias del equipo para asegurar el éxito del SGSI y la protección efectiva de la información.

La falta experiencia interna en el departamento tiene un impacto negativo en varios aspectos del proceso de gestión de la seguridad de la información; es decir, dificulta la correcta identificación de riesgos, la evaluación adecuada de los controles existentes y la implementación de medidas efectivas para salvaguardar la información confidencial. Asimismo, este vacío de conocimiento puede generar fallas en la anticipación de amenazas potenciales, lo que aumenta la vulnerabilidad de la organización frente a incidentes de seguridad.

Por tanto, es fundamental evaluar los efectos del Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27000 en el Instituto Ecuatoriano de Seguridad Social- IESS

de los Esteros, utilizando una combinación de metodologías cualitativa y cuantitativa. Este enfoque integral permitirá explorar diversos aspectos claves, que se materializan mediante las siguientes interrogantes:

¿Qué conceptos claves define la Norma ISO 27000 y cómo pueden contribuir a optimizar el Sistema de Gestión de Seguridad de la Información?

¿Cuáles son las vulnerabilidades y amenazas más relevantes de seguridad de la información que enfrenta el departamento de Talento Humano del IESS de los Esteros?

¿Cuáles serían las principales barreras para la implementación de las normas ISO 27000 en el Departamento de Talento Humano del IESS de Manta y cómo pueden superarse?

¿Cuál es el impacto de la capacitación y concienciación del personal en la mejora de la seguridad de la información en el Departamento de Talento Humano del IESS de Manta, con las Normas ISO 27000?

Objetivos del Estudio de Caso

Objetivo General

Analizar las Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información en el Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social de Manta.

Objetivo Especifico

- Definir conceptualmente sobre la Norma ISO 27000 para mejorar el Sistema de Gestión de Seguridad de la Información.
- Identificar las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta el departamento de Talento Humano del IESS de los Esteros.
- Determinar las principales barreras para la implementación de las normas ISO 27000 en el Departamento de Talento Humano del IESS de Manta y cómo pueden superarse.
- Diagnosticar el impacto de la capacitación y concienciación del personal en la mejora de la seguridad de la información en el departamento de Talento Humano del IESS de los Esteros bajo el marco de la Normas ISO 27000.

Justificación del Estudio

El presente trabajo de investigación hace mención sobre las Normas ISO 27000 para mejorar el sistema de gestión de seguridad de la información en el departamento de Talento Humano de la Institución Ecuatoriano de Seguridad Social de los Esteros, está investigación ha sido seleccionada por la relevancia que tiene la Norma ISO 27000, es la de gestionar los riesgos de seguridad de la información, puesto que todas las organizaciones trabajan en la diferenciación, la ejecución de este sistema permitirá fortalecer los procesos mediante la mejora continua e innovación en los procedimientos.

La importancia de esta investigación radica en la mejora del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27000. Este estándar internacional constituye una herramienta clave que permitirá a la institución establecer una estructura sólida y competitiva en sus procesos; a su vez, promoverá la mejora continua del sistema de gestión y optimizando la eficiencia del departamento de Talento Humano. Como resultado, de logrará una mayor satisfacción del cliente y un cumplimiento más efectivo de los objetivos y metas organizacionales.

Asimismo, el estudio es factible porque se sustenta efectivamente con los recursos bibliográficos y tecnológicos para la búsqueda de información. Además, con el apoyo del encargado de Talento Humano y su subordinado, se obtendrá la información necesaria para los procedimientos. Además, la relevancia de la investigación radica en que se realizará un análisis de la Norma ISO 27000 del Sistema de Gestión de Seguridad de la Información para mejorar la competitividad y productividad, trascendiendo en la rentabilidad de las entidades.

El impacto social del estudio es concientizar a las organizaciones del entorno, sobre los beneficios de aplicar un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27000. Esta norma reconocida internacionalmente proporciona un marco estructurado para proteger la información sensible, asegurando la confidencialidad, integridad y

disponibilidad de los datos. La implementación de esta norma no solo ayuda a cumplir con las necesidades y expectativas del cliente, sino que también favorece la mejora del desempeño administrativo y operativo. Al establecer procesos claros de gestión de riesgos y medidas de seguridad, se garantiza la eficacia y eficiencia de la organización, creando un entorno más seguro y confiable, tanto para los empleados como para los usuarios finales. De esta forma el estudio promueve una mayor conciencia sobre la importancia de seguridad de la información en la sociedad y su impacto positivo en el desarrollo organizacional.

Marco conceptual

Normas ISO 27000

La Norma ISO 27000

La autora de la revista Sussy Bayona (2022), indica que la norma ISO 27000 es uno de los estándares que se están respaldados con la seguridad de la información que existen dentro de alguna empresa u organización, su diseño está desarrollado con el ciclo Deming, conocido como PDCA que ayuda a establecer requisitos para mejorar continuamente el desenvolvimiento de este sistema dentro de la empresa.

Baena et al. (2019) posteriormente deduce que alrededor del mundo, existen diversos factores que afectan el sistema de la información, lo cual genera la necesidad de implementar normas que brinden protección al sistema. Por ello se implementan las normas ISO 27000, que son estándares de seguridad para las organizaciones, estas Norma 27000 permiten la ejecución de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo la metodología del ciclo Deming o PDCA.

De acuerdo a las opiniones dadas por los dos autores se explica de manera clara que las Normas ISO 27000 es una herramienta decisiva para el sistema de gestión de seguridad de la información, recalcando su base en el ciclo PDCA. Mientras que Sussy Bayona (2022), se enfoca más en la mejora continua interna, Baena et al. (2019) ofrecen una perspectiva más amplia sobre la necesidad global de estas normas. Juntas, estas visiones facilitan una comprensión exhaustiva de la importancia y aplicación de ISO 27000 en el contexto actual de la seguridad de la información.

Importancia de la Norma ISO 27000

De acuerdo a EXCELENCIA (2020) la Importancia de la Norma ISO 27000 se basa en el cumplimiento del Reglamento General de Protección de Datos en las Organizaciones. Sin embargo, es fundamental tener presente que la Norma ISO 27000 se centra en la identificación y gestión de riesgos asociados con la seguridad de la información y ayuda a las organizaciones a tomar medidas preventivas y reducir el impacto potencial de los riesgos.

En la actualidad se está tratando de adoptar el modelo de proceso PDCA (Planear-Hacer-Chequear-Actuar), el mismo que toma como insumos los requerimientos y expectativas de la seguridad de la información de las partes interesadas, generando satisfacción de requerimientos para la seguridad de la información. Villacis Miguel Leopoldo (2016)

Por otra parte, según los autores EXCELENCIA (2020) y Villacis Miguel Leopoldo (2016) corroboro lo siguiente la Norma ISO 27000 como un instrumento integral para la gestión de la seguridad de la información. Se destaca su importancia en el desempeño regulatorio, especialmente en relación con la protección de datos, y su enfoque en la gestión de riesgos. Además, la adopción del modelo PDCA sugiere un compromiso con la mejora continua y la adaptabilidad a las necesidades cambiantes de seguridad.

Objetivo de la Norma ISO 27000

Como afirma el autor de la revista Salvador (2019) a inicios de la norma ISO 27001 en 2005 y la segunda versión de la ISO 17799, cuyo número de referencia fue cambiado por el ISO/IEC 27002:2005 en Julio 2007, avanza el reglamento de Gestión de Seguridad de la información, esto es realizado de manera continua, donde ha surgido una amplia gama de estándares, conocidos hoy como ISO/IEC 27000.

“Tiene como objetivo definir requisitos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados y

proporcionales, protegiendo así la información, es recomendable para cualquier empresa grande o pequeña". (SlideShare, 2016).

Con base a lo expuesto los dos autores Salvador (2019) y (SlideShare, 2016) mencionan que el Objetivo de la Norma ISO 27000 es efectuar una gestión de seguridad de la información, siendo efectivo y eficiente. Además, es importante destacar que un sistema de gestión de seguridad de la información (SGSI) es un entorno de trabajo que permite a las organizaciones definir y establecer políticas, procedimientos y controles para proteger su información y minimizar los riesgos vinculados con la seguridad. Por otra parte, el objetivo del SGSI es asegurar la disponibilidad, integridad y confidencialidad de la información.

Barreras para la implementación de la Norma ISO 27000

González y Pérez (2020) Señalan que la complejidad de la norma y la falta de entendimiento de su alcance son problemas comunes para las organizaciones que intentan adoptar la ISO 27000, especialmente cuando se implementa por primera vez. A continuación, se mencionan las principales barreras para la implementación de la Norma ISO 27000.

- Falta de compromiso de la alta dirección
- Resistencia al cambio organizacional
- Falta de credibilidad por parte de las partes interesadas externas
- Falta de comprensión y diferencias de opciones sobre la competencia

En base a lo indicado se deduce que la implementación exitosa de la Norma ISO 27000 requiere un enfoque integral que aborda tanto los aspectos teóricos como humanos. Al superar las barreras mencionadas, las organizaciones pueden beneficiarse de una mayor seguridad de cumplimiento dentro de la Institución. Además, es importante tomar en cuenta los procedimientos de la Norma ISO 27000 para reducir los riesgos de seguridad, caso contrario

afectaría a la organización como la fuga de información sino cuenta con un control de seguridad y confidencialidad.

Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión

Sanabria Estrada et al., (2019) conceptualiza los sistemas de gestión como métodos mediante los cuales, la organización planifica, ejecuta, controla y delimita las actividades preventivas, para cumplir tanto con la misión organizacional, como con las metas y los objetivos planificados estratégicamente, facilitando el suministro de productos o servicios, que satisfagan los requisitos de las partes interesadas.

Diana (2017) indica que los Sistemas de Gestión son modelos que se fundamentan en Normas internacionales reconocidas y aprobadas, que facilitan a las organizaciones una optimización de sus procesos basados en un ciclo de mejora continua. Para proponer Sistemas de Gestión, las Organizaciones de Normalización reúnen a expertos con el fin de compartir conocimientos y desarrollar estándares internacionales voluntarios relevantes para el mercado, que apoyen la innovación y aporten soluciones a los retos globales.

Ambos autores se enfocan en visiones distintas que a su vez son complementarias de los sistemas de gestión. En el caso de Sanabria Estrada et al., (2019) menciona que la visión más enfocada a la aplicación práctica de las empresas, son los sistemas en la cual ayudan a cumplir con los objetivos internos y satisfacer las partes interesadas. Por otra parte, la autora Diana (2017) indica que el concepto se centra más en una perspectiva más amplia, recalcando el contexto internacional, la regularización y el impacto global de estos sistemas mencionados.

Seguridad de la Información

Según Gómez (2007) la seguridad de la información es la disciplina que abarca los sistemas de protección física, la prevención de accidentes o la prevención de actividades desleales por parte de los empleados de una organización o empresa.

De esta manera los tres pilares fundamentales de la seguridad de la información son:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Dussan (2020) define que la seguridad de la información se trata de un grupo de componentes interconectados que colaboran en conjunto para recolectar, procesar, guardar y compartir información, con el propósito de respaldar la voluntad de la alta gerencia, la coherencia y el control en la empresa.

De acuerdo a Gómez (2007) y Dussan (2020) corroboran que la seguridad de la información nos indica que es una herramienta indispensable para las organizaciones que buscan alcanzar el éxito en el competitivo entorno empresarial actual. Al proporcionar información precisa, oportuna y accionable, un Sistema de Gestión de la información empodera a la gerencia para tomar decisiones estratégicas acertadas, mejorar la coherencia operativa y mantener un control efectivo sobre las operaciones de la empresa.

Seguridad de la Información en una Organización

Una organización o empresa debe estar consciente que la información es un activo importante o primordial en la continuidad del negocio, por lo cual deberá establecer medidas que apoyen a garantizar su integridad, disponibilidad y confidencialidad; sin embargo muchas de las empresas u organizaciones se centran únicamente en la aplicación de la seguridad física, dejando de lado otros aspectos de relevancia que están ligados directamente al manejo y gestión de la información, lo cual se denomina la “seguridad de la información” (Hallberg y Hunstad, 2005).

El autor del sitio web Miguel Angel Parra Martinez (2019), relata que esta norma ISO 27000 tiene muchas posibilidades en la cual se permite ayudar en los aspectos relevantes a considerar en la separación de funciones de actividades a través de la seguridad de la información y el tratamiento de datos bien ejecutado. Esto hace que la seguridad de la información sea aún más importante para las empresas u organizaciones que lo utilizan.

Hallberg y Hunstad (2005) y Miguel Angel Parra Martinez (2019) muestra un enfoque evolutivo de la seguridad de la información desde el conocimiento básico de su importancia hasta la ejecución de estándares específicos como ISO 27000. Por otro lado, se destaca la necesidad de un enfoque holístico que vaya más allá de la mera seguridad física, abarcando aspectos de gestión, sistema de datos y separación de funciones. Asimismo, la creciente importancia de la seguridad de la información en el ámbito empresarial es un tema central, reflejando la evolución de las inquietudes y prácticas en este campo a lo largo del tiempo.

El Sistema de Gestión de Seguridad de la Información

Como menciona López (2023) el Sistema de Gestión de Seguridad de la Información es un conjunto de políticas que sirven para la administración y protección de la información. Para poder se implementado debe estar desarrollado bajo algún marco de seguridad como es el

estándar de la ISO/IEC 27001, reconocido internacionalmente, aprobado desde 2005 por la International Organization for Standardization y por la Comisión International Electrotechnical Commission. La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI según el Ciclo de Deming PDCA (Plan, Do, Check, Act) con un enfoque en la mejora continua.

Según Regina (2019), el apoyo para la adopción de un Sistema de Gestión de Seguridad de la Información se basa en la norma ISO 27000, que es un conjunto de estándares internacionales relacionados con la Seguridad de la Información. Esta norma proporciona una serie de pautas de mejores prácticas para establecer, preservar y mejorar, al tiempo que estandariza estos procedimientos para regular los Sistemas de Gestión de Seguridad de la Información (SGSI).

Como análisis general acerca de lo que menciona López (2023) y Regina (2019) deduzco que un Sistema de Gestión de Seguridad de la Información se basa en un conjunto integral de políticas y procedimientos que son más bien diseñados para administrar y proteger eficazmente los activos de la información de una empresa. Sin embargo, también se señala que el enfoque de esta norma se basa en sí un ciclo de Deming en la cual proporciona un marco para la mejora continua del sistema, es importante tomar en cuenta que la Norma ISO 27000 proporciona un marco de referencia completo y coherente para la gestión de la seguridad de la información. Ofrece un conjunto de directrices y mejores prácticas que las organizaciones

Amenazas y vulnerabilidades de seguridad de la información

Méndez (2021) lo define como la posibilidad de que una amenaza encuentre las vulnerabilidades de los activos y dañe a la organización; considerada como la combinación de la probabilidad de un evento y sus consecuencias. El riesgo determina lo que podría pasarles a

los diferentes activos de la información si estos no son protegidos de manera adecuada. Es importante saber de cada activo que es lo que se va a proteger, así como saber en qué medida las características están en peligro, es decir, analizar el sistema.

Además, una de las principales amenazas y vulnerabilidades que se exponen hoy en día las empresas son:

Amenazas de Malware: Los programas maliciosos constituyen una de las principales amenazas cibernéticas que enfrentan las empresas. Dentro de este grupo, existen diversas formas de amenazas, siendo las más comunes las siguientes:

Virus: Los virus informáticos son programas diseñados para infiltrarse en un dispositivo y causar alteraciones en su rendimiento. Para que un virus logre infectar un sistema, se requiere la acción de un usuario, ya sea de forma intencional o accidental.

Gusanos: Son tipos de malware más prevalentes que afectan los equipos y sistemas de las empresas, ya que no necesitan la acción directa del usuario ni la alteración de archivos para infectar un dispositivo. Su objetivo principal es replicarse y propagarse a través de la red, infectando tantos dispositivos como sea posible. Representan un riesgo significativo para las redes empresariales, ya que la infección de un solo equipo puede afectar rápidamente toda la infraestructura en poco tiempo.

Vulnerabilidades del sistema

Todos los sistemas y aplicaciones informáticas presentan algún tipo de defecto en su diseño, estructura o código que crea vulnerabilidades. Aunque estos fallos sean mínimos, pueden ser suficientes para exponer el sistema y la información a riesgos, actuando como un punto de acceso para ataques tanto internos como externos. Las vulnerabilidades más comunes suelen originarse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.

Como análisis general del autor Méndez señala que el riesgo se refiere a la probabilidad que una amenaza aproveche las debilidades de los activos de una organización, causando daños; es decir, este concepto se basa en la combinación de la probabilidad de que ocurra un incidente y sus consecuencias. Por consiguiente, para gestionar el riesgo de manera efectiva, es crucial identificar qué activos deben ser protegidos y evaluar en qué medida están expuestos a posibles amenazas. Este análisis permite comprender mejor el sistema y tomar medidas adecuadas para prevenir o mitigar los daños.

Capacitación y Concienciación

Larota Cuito (2024) Proporcionar capacitación y concienciación al personal sobre las nuevas medidas de seguridad implementadas. Asegurar que comprendan su papel y responsabilidad en la seguridad de la información. Se debe realizar un recorrido por las normas ISO que refuerzan esa implementación de la norma ISO 27001 enfocada a las buenas prácticas referentes a los controles y protección de datos para los servicios de los proveedores y trabajadores.

La formación y sensibilización del personal en seguridad de la información pueden asistir a las organizaciones en la mitigación de riesgos cibernéticos y garantizar el cumplimiento de las normativas de protección de datos.

- Reducción de costos
- Mejora de la reputación corporativa
- Cumplimiento de la norma
- Reducción de las vulnerabilidades a los ciberataques
- Creación de una cultura de seguridad

De acuerdo a lo mencionado por Larota Cuito (2024) se destaca la importancia de ofrecer capacitación y sensibilización al personal sobre las medidas de seguridad adoptadas en la organización, asegurándose de que comprendan su rol en la protección de la información. Esto implica un enfoque en las normativas ISO, especialmente la ISO 27001, que promueve las buenas prácticas en el control y protección de datos, tanto para los servicios de proveedores como para los empleados. La educación y la conciencia sobre la seguridad de la información son herramientas clave para reducir los riesgos cibernéticos y asegurar que la organización cumpla con las normativas de protección de datos vigentes.

Marco Metodológico

El presente estudio se basa en un enfoque cualitativo y cuantitativo para investigar las características singulares de la gestión de seguridad de la información en el Instituto Ecuatoriano de Seguridad Social IESS de los Esteros bajo al marco de la norma ISO/IEC 27000. La metodología adoptada será de naturaleza descriptiva debido a que facilita la recopilación de información de diversas fuentes bibliográficas y la exploración de situaciones o poblaciones determinadas.

Esta investigación utiliza un alcance descriptivo y exploratorio, detallando y especificando los componentes del estudio, lo cual permite comprobar las vulnerabilidades de seguridad de la información en el área de Talento Humano en el IESS de los Esteros.

Por ende, con esta metodología se coordina y alcanza los objetivos propuestos acerca de información ISO/ SGSI y estructura estándar internacional ISO/IEC 27000 para determinar los requisitos y normativas que permitan el establecimiento, operación, supervisión y revisión de un SGSI (Sistema de Gestión de Seguridad de la información) en el IESS.

Participantes

Las unidades básicas del objeto de estudio lo conforman 52 empleados del departamento de Talento Humano. Este grupo incluye tanto al personal directivo, que posee un amplio conocimiento de los procesos y actividades necesarias para los operarios del área, como al personal operativo, que se encarga de manipular la información necesaria para llevar a cabo sus funciones específicas. Asimismo, el personal directivo también desempeña un papel crucial en la toma de decisiones estratégicas.

En el desarrollo de la presente investigación se procede a trabajar directamente con los participantes, en este caso el personal administrativo. La metodología consiste en la adquisición y recopilación de datos la cual se adhiere a los principios de seguridad de la

información establecidos en las Normas ISO 27000, garantizando la protección de activos de información sensibles durante todo el proceso de investigación. Por lo tanto, al ser una población de cincuenta y dos no es necesario extraer la muestra porque es un tipo de muestra no probabilística.

Métodos

El método de investigación a utilizar es el **deductivo** que implica la generación de una estrategia para el planteamiento de la propuesta de solución al fenómeno, hecho, suceso, según Torres (2021), este método que lingüísticamente significa conducir o extraer, se basa en el razonamiento, permite pasar de principios generales a hechos particulares. Es decir, una vez al comprobar y verificar que un principio es válido, se comienza a aplicarlo en contextos particulares. Por otra parte, también utilice el **método inductivo** para evaluar y mejorar el sistema de gestión de seguridad de la información (SGSI) existente en la empresa, con el objetivo de aumentar la satisfacción del personal y optimizar los procesos, todo ello basado en la norma ISO 27000

Muestreo estratificado: La población se divide en estratos (por ejemplo, por edad, sexo o ubicación) y se selecciona una muestra aleatoria de cada estrato. Este método es eficiente cuando se quiere asegurar que la muestra represente adecuadamente la variedad de la población total. Este método se emplea para asegurar que la muestra represente apropiadamente la diversidad de la población total, especialmente cuando hay subgrupos sustanciales con características o atributos distintos.

Técnicas de la investigación

Observación

Para llevar a cabo el estudio se procede a utilizar la técnica de observación, en el lugar donde se desarrollan las actividades de gestión administrativa, con el fin de comprender en profundidad un fenómeno sin utilizar datos numéricos. Esta técnica permite tomar información y su posterior análisis necesarios para el correcto desarrollo del estudio. Asimismo, se utilizará un listado de verificación (Check list) alineado con los objetivos de la investigación que guiará al encuestado a responder las preguntas de forma secuencial sin desviarse del propósito del estudio.

Adicionalmente se empleará el análisis de documentos para obtener información relevante para la investigación. Este enfoque permitirá comprender el desarrollo y las particularidades de los procesos además de proporcionar datos que corroboren o cuestionen las respuestas del entrevistado.

Encuestas

Mediante el instrumento de encuesta, se maneja el formulario de Google (Forms) a través de la cuenta de correo, donde se ingresaron trece preguntas. De acuerdo con la encuesta esta técnica de investigación estará dirigida al personal administrativo para conocer qué tipo de estrategias son las utilizadas para desarrollar la actividad y conocimientos de los mismos, en la cual es un medio accesible para la obtención de resultados del sistema aplicado en la institución y verificada los requerimientos adquiridos para sus usuarios. La encuesta tiene como objetivo identificar las estrategias implementadas en el departamento de Talento Humano y evaluar el conocimiento del personal sobre las buenas prácticas de seguridad de la información. además, busca determinar la efectividad de las medidas adoptadas y cómo estas

contribuyen a cumplir con los requisitos y expectativas de los usuarios dentro de la organización.

Análisis de datos

En general el análisis de datos basado en la Norma ISO 27000 permite realizar una evaluación detallada y objetiva del SGSI, identificando tanto los puntos fuertes como las áreas de mejora. El proceso no solo optimiza la seguridad de la información, sino que también asegura que el sistema de gestión esté alineado con las mejores prácticas internacionales, garantizando una protección adecuada y el cumplimiento de los requisitos normativos. Asimismo, para hacer una simulación de datos se manejará la aplicación de Excel en el cual se podrá obtener información y grandes cantidades de datos. Además, la herramienta de Excel ayuda a gestionar eficientemente los datos y a tomar decisiones basadas en evidencia.

Resultados Obtenidos

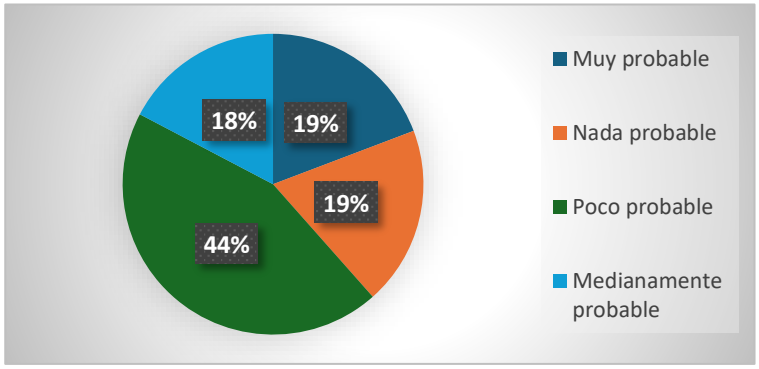
Tabla: 1

¿Tiene conocimiento de la norma ISO 27000?

Alternativas	Frecuencia	Porcentaje
Muy probable	10	19%
Nada probable	10	19%
Poco probable	23	44%
Medianamente probable	9	18%
Total	52	100%

Nota: Conocimiento de la Norma ISO 27000

Gráfico: 1



Interpretación y Análisis

Los resultados de la encuesta indican que 10 personas consideran muy probable que tenga conocimiento sobre la norma ISO 27000 que equivale a 19%; como también coinciden con 10 participantes restantes como nada probable que corresponde a 19%, mientras que 23 de los encuestados la califica como poco probable que corresponde un 44% y finalmente, nueve de los participantes que pertenecen un 18% evaluaron como medianamente probable.

El personal administrativo considerado de acuerdo a los porcentajes tanto 44% y 18% que refleja poco probable y medianamente probable respectivamente, en no tener conocimiento sobre la Norma ISO 27000, es necesario fortalecer sobre temas que se inserten sobre la norma y la seguridad de la información para identificar los estándares y protocolos que servirán como apoyo para que las organizaciones cumplan sus objetivos de manera efectiva.

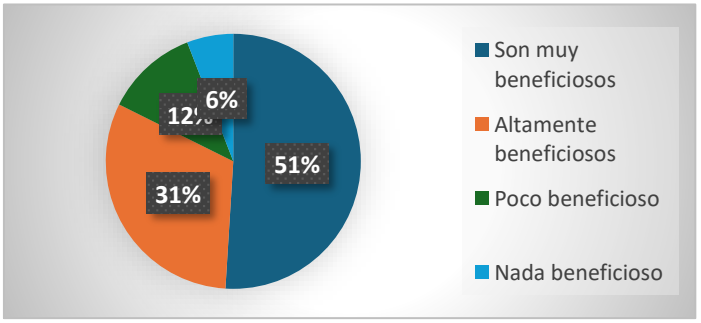
Tabla 2

¿Qué nos dice la norma ISO 27000 sobre los recursos humanos?

Alternativas	Frecuencia	Porcentaje
Son muy beneficiosos	27	51%
Altamente beneficioso	16	31%
Poco beneficioso	6	12%
Nada beneficioso	3	6%
Total	52	100%

Nota: Norma ISO 27000 sobre los recursos humanos.

Gráfico: 2



Interpretación y Análisis

En el análisis de resultados se muestra que 27 participantes consideran que los recursos humanos son muy beneficiosos, por otro lado, 16 de los encuestados lo califican como altamente beneficiosos que corresponde el 31%; no obstante, seis participantes perciben que los recursos humanos que comprende a 12%; y tres de los encuestados indican que la norma ISO 27000 no es nada beneficioso en este ámbito.

En cuanto la Norma ISO 27000 indica que los recursos humanos deben concientizar al respecto con alto nivel de conocimiento sobre el dominio de la Norma ISO para fortalecer las debilidades y destrezas que permita identificar los roles y responsabilidades mientras se define aspectos tales como el cumplimiento de los estándares establecidos por la Norma ISO como la confidencialidad, integridad y seguridad. Por consiguiente, el 12% y 6 % señala poco beneficioso y nada beneficioso respectivamente, debe sumarse a las reglas establecidas en la ISO 270000 para llevar un mejor sistema de gestión de seguridad de la información.

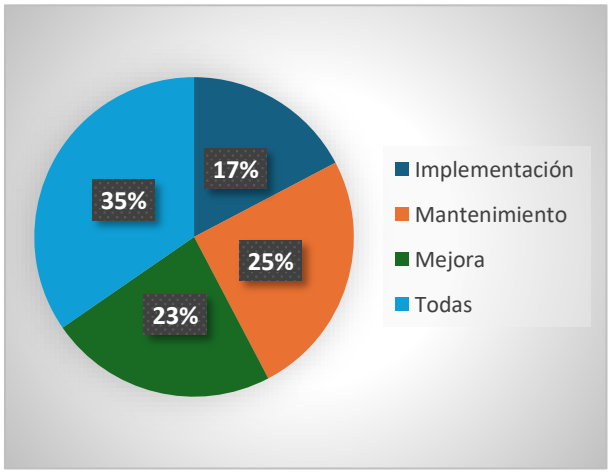
Tabla 3

¿Qué aspectos se consideran en las Norma ISO 27000?

Alternativas	Frecuencia	Porcentaje
Implementación	9	17%
Mantenimiento	13	25%
Mejora	12	23%
Todas	18	35%
Total	52	100%

Nota: Aspectos que se consideran en la norma ISO 27000

Gráfico 3



Interpretación y Análisis

Los resultados indican que nueve de los encuestados reconocen que la norma ISO 27000 va más allá de una simple implementación con un porcentaje significativo de 17%; por otra parte, 13 de los encuestados que corresponden a 25% destacan la importancia del mantenimiento continuo; mientras que, 12 participantes identifican la mejora como un aspecto clave que comprende un 23%; y finalmente, 18 colaboradores consideran que la Norma ISO no ofrece una visión clara de los aspectos específicos que deberían se prioritarios, que corresponden a un 37%.

Dentro de los aspectos de la Norma ISO 27000 a considerar por los servidores públicos con mayor importancia, es la implementación para priorizar los procesos que se lleven a cabo en el departamento de Talento Humano, considerando como parte equitativo de los demás aspectos que se mencionan.

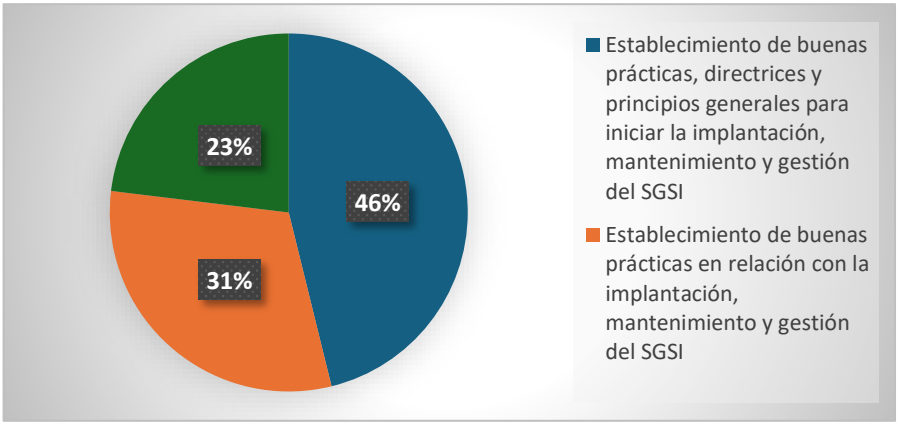
Tabla 4

¿Cuál es la finalidad de la Norma ISO 27000?

Alternativas	Frecuencia	Porcentaje
Establecimiento de buenas prácticas y principios generales para iniciar la implementación	24	46%
Establecimiento de buenas prácticas en relación con la implementación	16	31%
Establecimiento de buenas prácticas de gestión en relación con la implementación	12	23%
Total	52	100%

Nota: Finalidad de la norma ISO 27000

Gráfico: 4



Interpretación y Análisis

En el esquema se determina que 24 colaboradores comprende la importancia del establecimiento de buenas prácticas y principios generales para iniciar la implementación lo que representa 46%; Por el contrario, 16 de los participantes que equivale 31% reconocen la existencia del establecimiento de buenas prácticas en relación con la implementación; además, y para finalizar, 12 de los participantes indica la necesidad fortalecer el establecimiento de buenas prácticas de gestión en relación con la implementación que corresponde el 23%.

La finalidad de la Norma ISO 27000 cumplen ciertos porcentajes en relación al establecimiento de buenas prácticas y principios generales para iniciar la implementación, tomando en cuenta la falta de conocimiento y otros aspectos en contra a actividades proactivas, llegue a perjudicar los sistemas de gestión de seguridad de la información dentro del departamento de Talento Humano.

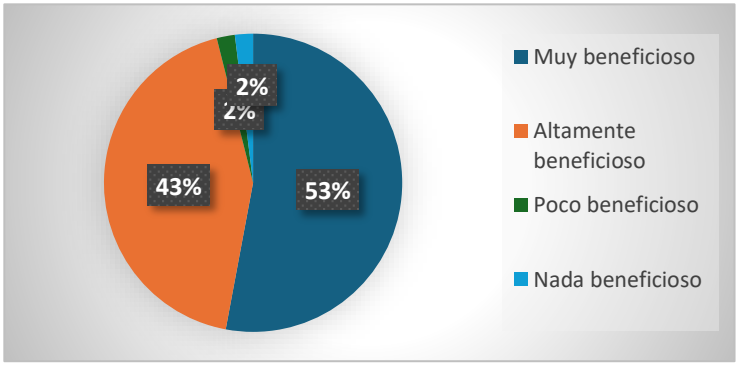
Tabla 5

¿Es beneficioso aplicar las normas ISO 27000 dentro de un sistema de gestión de seguridad de la Información?

Alternativas	Frecuencia	Porcentaje
Son muy beneficiosos	27	53%
Altamente beneficioso	23	43%
Poco beneficioso	1	2%
Nada beneficioso	1	2%
Total	52	100%

Nota: Beneficios de las normas ISO 27000 dentro de un SGSI

Gráfico: 5



Interpretación y Análisis

Según la gráfica, 27 participantes consideran que un sistema de gestión de seguridad de la información es muy beneficioso que corresponde al 53%; mientras que, 23 encuestados lo perciben como altamente beneficioso que representa un 43%; no obstante, dos de los colaboradores opinan que la ISO 27000 son poco beneficios y nada beneficioso los cuales coincidencia cada uno con el 2%.

Un sistema de gestión de seguridad de la información garantiza la protección de los datos y recursos organizacionales, en la cual proporciona un marco estructurado para gestionar riesgos, fortalecer la seguridad y cumplir con estándares internacionales. Asimismo, existe una gran extensión sobre la importancia de los beneficios de la Norma ISO 27000, los cuales coinciden con un porcentaje del 2% donde se refleja la necesidad de mayor sensibilización o capacitación para que comprendan su impacto positivo de la norma en la seguridad y gestión de la información

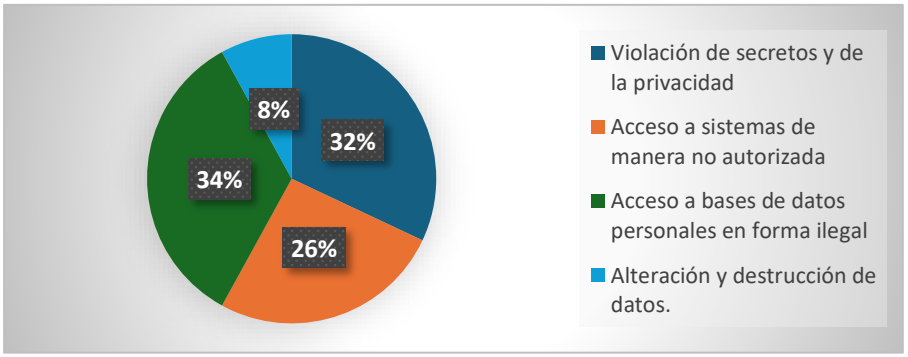
Tabla 6

¿Cuáles son las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta el Departamento de Talento Humano del IESS de los Esteros?

Alternativas	Frecuencia	Porcentaje
Violación de secretos y de la privacidad	17	32%
Acceso a sistemas de manera no autorizada	14	26%
Acceso a bases de datos personales en forma ilegal	17	34%
Alteración y destrucción de datos	4	8%
Total	52	100%

Nota: Principales amenazas y vulnerabilidades de seguridad de la información

Gráfico: 6



Interpretación y Análisis

De acuerdo con los resultados,17 participantes identifican la violación de secretos y de la privacidad como su principal preocupación en materia de seguridad, que representa un 32%; por otro lado,14 de los encuestados señala el acceso no autorizado a los sistemas que equivale al 26%; finalmente, 17 de los encuestados que equivale al 34% identificaron al acceso a bases de datos personales de forma ilegal como otras amenazas; Sin embargo, cuatro colaboradores indican que la alteración y destrucción de datos son esencial para el funcionamiento de la organización que representa un 8%.

El personal encuestado indica que el 34% y 8% enfatizan la urgencia de reforzar las medidas de seguridad. Además, se resalta que la alteración o destrucción de datos compromete el funcionamiento de la organización, subrayando la importancia de garantizar la integridad de la información para mantener la operatividad.

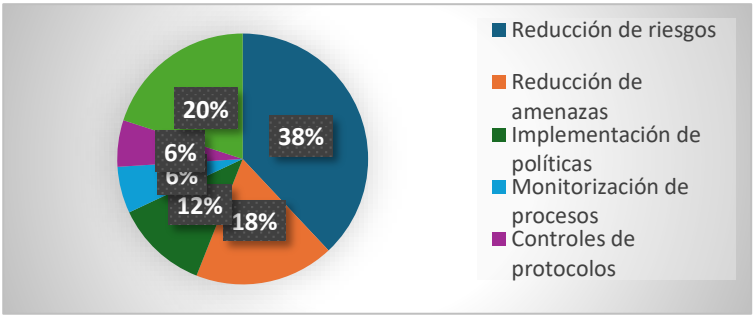
Tabla 7

¿Cuáles son las principales razones por lo que una organización debería establecer y mantener un SGSI?

Alternativas	Frecuencia	Porcentaje
Reducción de riesgos	20	38%
Reducción de amenazas	10	18%
Implementación de políticas	6	12%
Monitorización de procesos	3	6%
Controles de protocolos	3	6%
Protección de datos	10	20%
Total	52	100%

Nota: Principales razones por lo que una organización debería establecer y mantener un SGSI

Gráfico: 7



Interpretación y Análisis

El análisis de resultados indica que 30 participantes resaltan la importancia de la reducción de riesgos y amenazas como las principales razones para establecer un SGSI con un porcentaje de 38% y 18%; al contrario, seis de los participantes destaca la implementación de políticas como un aspecto clave que corresponde al 12%; mientras que, seis de los colaboradores es decir, el 12% evaluaron al monitorización de procesos y el control de protocolos como un factor fundamental; y finalmente 10 de los encuestados que equivale al 20% considera la protección de datos como una de las razones principales para implementar un SGSI.

La reducción de riesgos y amenazas, junto con la protección de datos, son las principales razones para implementar un SGSI, seguido de la importancia de sus políticas y la monitorización de procesos y controles. Además, se pretende mejorar los protocolos del sistema de gestión de la información para conllevar el éxito correcto dentro de la organización cumpliendo con los principios establecidos.

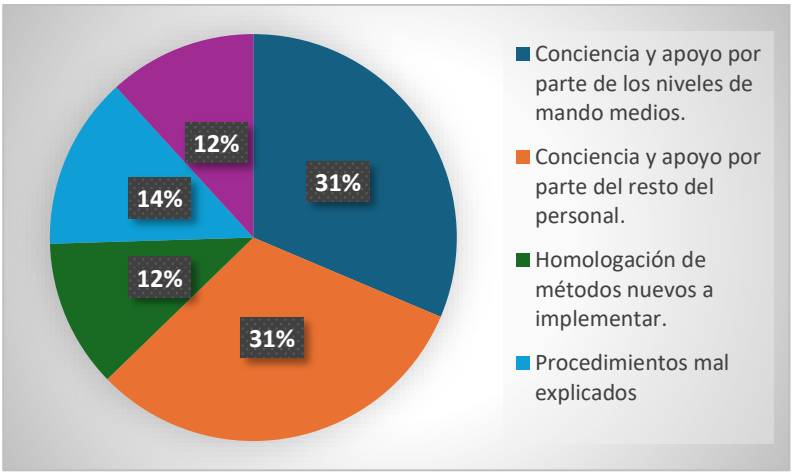
Tabla 8

¿Cuáles serían las principales barreras para la implementación de las normas ISO 27000 en el Departamento de Talento Humano del IESS de los Esteros y cómo pueden superarse?

Alternativas	Frecuencia	Porcentaje
Conciencia y apoyo por parte de los niveles de mando medios.	16	31%
Conciencia y apoyo por parte del resto del personal.	17	31%
Homologación de métodos nuevos a implementar.	6	12%
Procedimientos mal explicados	7	14%
Formatos inadecuados para registrar la información necesaria	6	12%
Total	52	100%

Nota: Principales barreras para la implementación de las normas ISO 27000

Gráfico: 8



Interpretación y Análisis

La gráfica muestra que, 16 participantes identifican la falta de conciencia y apoyo por parte de los niveles de mando medio como la principal barrera, que equivale 31%; sin embargo, 17 encuestados que corresponde al 31% considera fundamental contar con la conciencia y apoyo del resto del personal.; por otra parte, seis de los colaboradores señala la homologación de métodos nuevos a implementar como una barrera importante, que equivale el 12%; mientras que, siete de los encuestados que corresponde al 14% calificaron los procedimientos mal explicados como un obstáculo significativo; mientras que seis de los participantes consideran que los formatos son inadecuados para registrar la información necesaria que representa el 12%.

La falta de conciencia y apoyo de los mandos medios se presenta como una barrera clave, evidenciando una desconexión entre los niveles de gestión superior y el personal operativo. Esta situación puede dificultar la implementación exitosa de las iniciativas y en los mandos medios que desempeña un papel crucial en la coordinación y aceptación de las políticas por parte de los equipos. Además, se observa una carencia de alineación y coordinación en la adopción de nuevas políticas y procesos, así como la necesidad de optimizar los recursos y herramientas disponibles para asegurar una correcta ejecución y documentación de la información dentro de la organización.

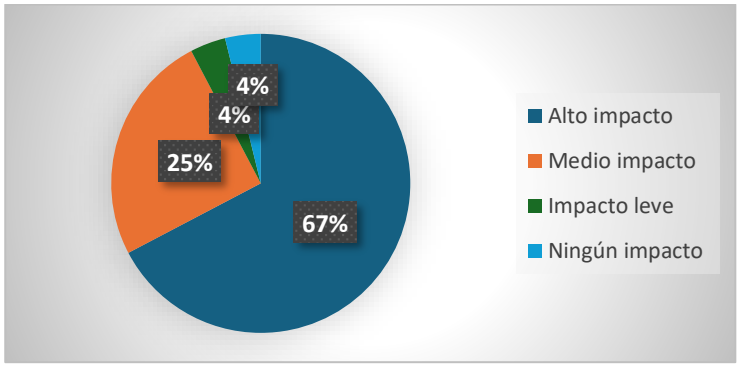
Tabla: 9

¿Qué impactos pueden sufrir los procesos y la reputación de una organización al no cumplir con los requisitos de seguridad de la información?

Alternativas	Frecuencia	Porcentaje
Alto impacto	34	67%
Medio impacto	14	25%
Impacto leve	2	4%
Ningún impacto	2	4%
Total	52	100%

Nota: Impactos de los procesos en la organización

Gráfico: 9



Interpretación y Análisis

De acuerdo a los resultados previstos se indica que 34 de los participantes que representa el 67% lo considera como un alto impacto; por el contrario, 14 encuestados que corresponde un 25% lo evalúa como medio impacto; mientras que, cuatro de los colaboradores, con un pequeño porcentaje de 4% se identifica un impacto leve; Asimismo, 2 de los colaboradores que equivale a 2% lo valoran como ningún impacto, aunque reconocen la importancia de la seguridad de la información.

La seguridad de la información tiene un alto impacto en la organización, lo que refleja una fundamental valoración. Sin embargo, los procesos y la reputación de una organización pueden sufrir riesgos al no cumplir con los requisitos de seguridad de la información. Estas desventajas incluyen posibles brechas de seguridad, pérdidas de datos, sanciones legales y daño a la confianza de clientes y socios, lo que subraya la necesidad de una gestión adecuada y constante actualización en la seguridad de la información.

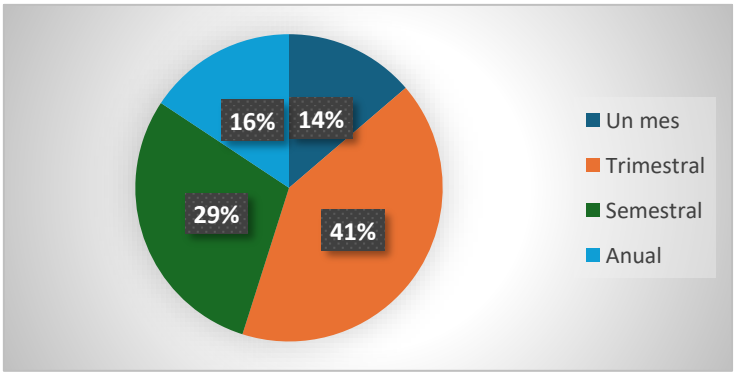
Tabla 10

¿Con qué frecuencia una organización debe realizar evaluación de riesgos de seguridad de la información conforme a ISO 27000?

Alternativas	Frecuencia	Porcentaje
Un mes	7	14%
Trimestral	22	41%
Semestral	15	29%
Anual	8	16%
Total	52	100%

Nota: Evaluación de riesgos de seguridad de la información conforme a ISO 27000

Gráfico: 10



Interpretación y Análisis

En el gráfico se señalan que siete de los participantes destacan la importancia de realizar evaluaciones mensuales de riesgos para garantizar la efectividad de un Sistema de Gestión de Seguridad de la Información lo que representa 14%; mientras que, 22 de los participantes opinan que la evaluación debería realizarse de manera trimestral que comprende el 41%; Por otro lado, 15 de los encuestados que corresponden al 29% consideran que la evaluación debería llevarse a cabo cada seis meses; y finalmente, ocho de los colaboradores indican que las evaluaciones anuales son adecuadas, lo que equivale al 16%.

Según norma ISO 27000, las evaluaciones de riesgos deben ser periódicas adaptarse a los cambios y amenazas en el entorno. Aunque la frecuencia ideal puede variar según el contexto y el riesgo, los resultados sugieren que tanto una evaluación mensual como semestral son prácticas adecuadas, dependiendo del nivel de la información manejada y los recursos disponibles.

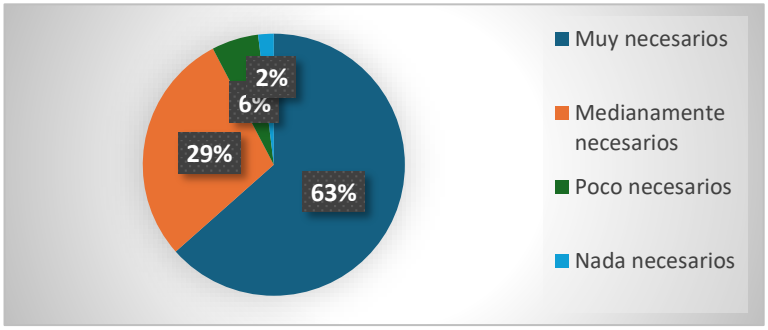
Tabla 11

¿Los recursos (humanos, tecnológicos, financieros) son necesarios para cumplir con los estándares de seguridad de la información establecidos en ISO 27000?

Alternativas	Frecuencia	Porcentaje
Muy necesario	33	63%
Medianamente necesario	15	29%
Poco necesario	3	6%
Nada necesario	1	2%
Total	52	100%

Nota: Estándares de seguridad de la información establecidos en ISO 27000

Gráfico: 11



Análisis e Interpretación

En base a los resultados, se observa que 33 participantes recalcan que los recursos (humanos, tecnológicos y financieros) son muy necesarios que equivale 63%; Por el contrario, 15 de los participantes que corresponden a 29% evaluaron como medianamente necesarios; sin embargo, tres de los encuestados califican los recursos como poco necesarios que comprenden el 6%; y para concluir, un participante, lo que representa el 2%, considera que estos recursos no son nada necesarios.

Los recursos humanos, tecnológicos y financieros son fundamentales para el éxito de la organización, destacando su relevancia en el cumplimiento de los estándares de seguridad de la información establecidos en ISO 27000. En este sentido, se considera necesarios para cumplir con dichos estándares establecidos por la Norma ISO 27000. En este contexto, se reconocen como indispensables para garantizar la implementación efectiva y sostenida de estos estándares.

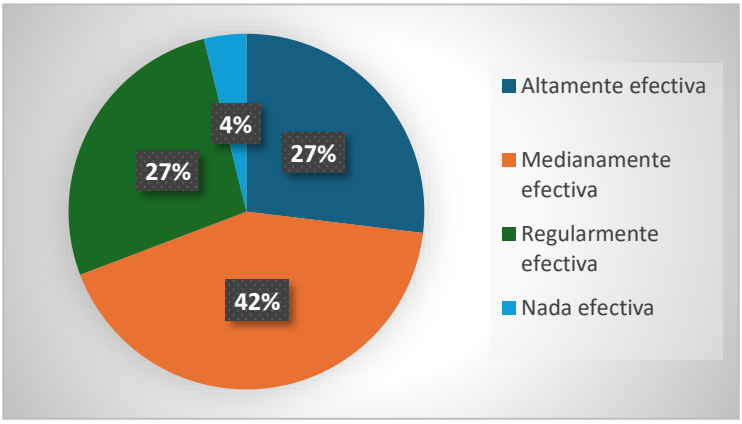
Tabla: 12

¿Qué nivel de efectividad es la implementación actual del SGSI en el Departamento de Talento Humano del IESS de los Esteros?

Alternativas	Frecuencia	Porcentaje
Altamente efectiva	14	27%
Medianamente efectiva	22	42%
Regularmente efectiva	14	27%
Nada efectiva	2	4%
Total	52	100%

Nota: Implementación de Sistema de Gestión de Seguridad de la Información

Gráfico: 12



Interpretación y Análisis

Según los resultados de la encuesta, 14 de los participantes, lo que representa el 27% evaluaron que la Implementación del Sistema de Gestión de Seguridad de la Información es altamente efectiva que corresponden al 27%; Por otro lado, 22 de los participantes, lo que equivale al 42%, lo calificaron que la implementación es medianamente efectiva. Mientras tanto,14 de los encuestados lo que representa el 27%, es regularmente efectiva; por último, dos de los colaboradores que corresponde a un 4% lo considera como nada efectiva.

La implementación actual del SGSI tiene como base la identificación de los controles de seguridad que implica un proceso estructurado que abarca desde la planificación inicial hasta la autoría final y a su vez cumplir con las medidas de seguridad adecuada para así lograr una mejora continua efectiva.

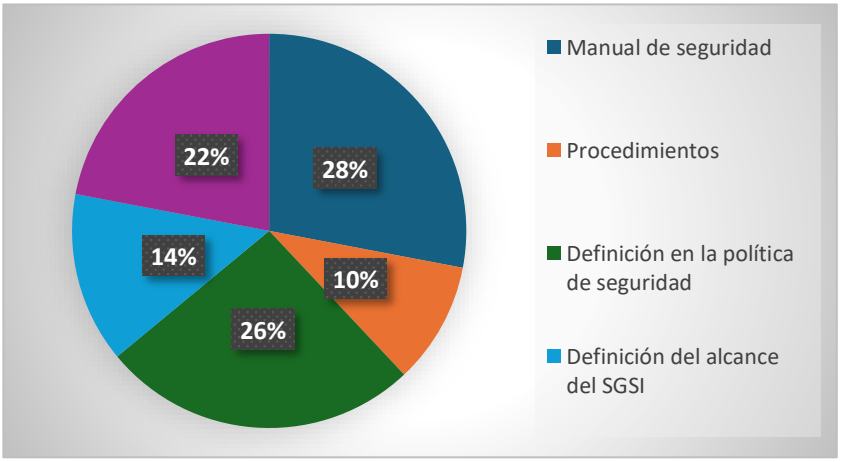
Tabla 13

¿Qué temas de capacitación y concienciación del personal en la mejora de la seguridad de la información en el Departamento de Talento Humano del IESS de los Esteros, con las Normas ISO 27000?

Alternativas	Frecuencia	Porcentaje
Manual de seguridad	15	28%
Procedimientos	6	10%
Definición en la política de seguridad	13	26%
Definición del alcance del SGSI	7	14%
Programas de concientización sobre la seguridad de la empresa	11	22%
Total	52	100%

Nota: Capacitación y concienciación de la seguridad de la información con las Normas ISO 27000

Gráfico: 13



Análisis e Interpretación

De acuerdo a los resultados, se observa una distribución equilibrada entre los diferentes temas de capacitación y concienciación. Esto indica que 15 de los participantes lo que equivale al 28% lo cual consideran importante contar con un manual de seguridad, mientras que, seis de los encuestados califican los procedimientos como un aspecto fundamental que corresponde al 10%; Asimismo, 13 colaboradores indican tener conocimiento sobre la definición establecida en la política de seguridad lo que representa el 26%; Sin embargo, siete de los participantes conocen sobre la definición del alcance del SGSI que corresponde al 14%; y finalmente 11 de los encuestados que corresponde a 22% recalcaron sobre la calidad de los programas de concientización sobre la seguridad de la empresa.

La importancia de contar con un manual de seguridad, procedimientos claros y un buen conocimiento sobre la política de seguridad ayudará a una correcta implementación en el departamento de Talento Humano. Asimismo, una parte significativa del personal indica que el manual de seguridad de la información es una herramienta clave en la que se reconoce como instrucciones bien definidas para asegurar la efectividad y una estructura sólida de normas y procesos claros para gestionar adecuadamente la seguridad en la organización. Es por esta razón que es importante que la implementación no solo garantice la seguridad de la información, sino que también promueva la capacitación continua del personal, fortaleciendo sus habilidades y destrezas, esto permitirá al equipo responder eficazmente a posibles amenazas, adaptarse a los cambios tecnológicos y a su vez asegurar el cumplimiento de los estándares establecidos, fomentando una cultura organizacional comprometida con la seguridad y la mejora continua de la organización.

Análisis de Resultados

De acuerdo con los resultados, se evidencia una brecha significativa en el conocimiento sobre la norma ISO 27000 entre el personal administrativo. Aunque algunos demuestran cierta familiaridad con la norma, la mayoría refleja desconocimiento o incertidumbre al respecto. Esta falta de comprensión podría dificultar el apoyo necesario para la implementación eficiente de un Sistema de Gestión de Seguridad de la Información (SGSI), lo que comprometería la capacidad de la organización para proteger y garantizar la seguridad de sus activos de información.

Es fundamental, por lo tanto, priorizar la capacitación en temas relacionados con la norma y la seguridad de la información. De este modo, al fortalecer el conocimiento sobre los estándares y protocolos que promueve la ISO 27000, la organización no solo mejorará su capacidad para proteger los activos de información, sino que también cumplirá con las normativas aplicables. Asimismo, esto permitirá garantizar una gestión más segura y eficiente de sus recursos.

Según el autor del sitio web Miguel Angel Parra Martinez (2019), relata que esta norma ISO 27000 tiene muchas posibilidades en la cual se permite ayudar en los aspectos relevantes a considerar en la separación de funciones de actividades a través de la seguridad de la información y el tratamiento de datos bien ejecutado. Esto hace que la seguridad de la información sea aún más importante para las empresas u organizaciones que lo utilizan.

Asimismo, Ecuador, Ministerio de Telecomunicaciones (2020) corrobora que el Sistema de Gestión de Seguridad de la Información es: “El elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional” El SGSI pretende salvaguardar la confidencialidad, integridad y disponibilidad de la información.

A partir del análisis realizado, se evidencia que la efectividad del SGSI depende en gran medida del grado de capacitación y conciencia del personal. Abordar las brechas de conocimiento existentes es fundamental para que las organizaciones comprendan y apliquen de manera adecuada los principios y estándares de la norma ISO 27000. Al alinear las percepciones y conocimientos del personal con los objetivos del SGSI, se pueden diseñar estrategias de formación que refuercen las competencias necesarias para proteger los activos de información y cumplir con las normativas vigentes.

En este sentido, se destacan que las principales amenazas y vulnerabilidades identificadas en el Departamento de Talento Humano del IESS incluyen la violación de secretos y la privacidad, el acceso no autorizado a los sistemas y el acceso ilegal a bases de datos personales. Además, algunos consideran que la alteración y destrucción de datos son aspectos críticos para el funcionamiento de la organización. Estas preocupaciones subrayan la importancia de fortalecer las medidas de seguridad de la información para proteger los activos y garantizar la integridad de los procesos organizacionales.

A raíz de estos resultados se refleja que las principales preocupaciones en materia de seguridad de la información, como la violación de secretos y la privacidad, el acceso no autorizado a sistemas y bases de datos personales, están alineadas con los riesgos destacados en el Departamento de Talento Humano del IESS. Asimismo, aunque en menor medida, se reconoce la alteración y destrucción de datos como una amenaza significativa para el funcionamiento de la organización. Estos hallazgos subrayan la necesidad de implementar medidas de seguridad sólidas que salvaguarden la información crítica y respalden la integridad de los procesos organizacionales.

De igual manera, una de las principales amenazas internas es la Insatisfacción laboral para que los empleados descontentos pueden buscar venganza filtrando información confidencial, la falta de conciencia como lo había mencionado anteriormente la falta de

conocimiento sobre las políticas de seguridad y las buenas prácticas que puede llevar a acciones que comprometan la seguridad de la información. Como amenazas externas son los ataques a terceros como brecha de seguridad en proveedores de servicios que pueden comprometer la información del IESS.

Según ISO/IEC 27000 et al., (2018) menciona que la seguridad de la información consiste en la aplicación y gestión de los controles apropiados que implica la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito comercial sostenido y continuidad, y reducir al mínimo las consecuencias de los incidentes de seguridad de la información. Se logra mediante la aplicación de un conjunto de aplica controles, seleccionados a través del proceso de gestión de riesgos y gestionarse a través de un SGSI, incluidas las políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información.

En conclusión, el análisis de la información presentada revela una preocupación generalizada por parte de los encuestados. Los participantes en la encuesta identificaron de manera clara los principales riesgos a los que se enfrentan las organizaciones, mientras que el autor, según Según ISO/IEC 27000 et al., (2018), refuerza la importancia de contar con un sistema de gestión de seguridad para los riesgos. Según la norma ISO 27000, un SGSI implica la aplicación y gestión de controles apropiados para garantizar la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implementación de políticas, procesos, procedimientos y tecnologías que protegen los activos de información.

De acuerdo con los hallazgos, los resultados de la gráfica ponen en evidencia barreras clave para la implementación de la norma ISO 27000, destacando áreas que requieren atención para cumplir con los requisitos específicos de la norma. La falta de conciencia y apoyo por parte de los niveles de mando medio y del resto del personal son señaladas como las principales barreras, lo que indica la necesidad de fomentar una cultura organizacional alineada

con los principios de la norma. Además, aspectos como la homologación de nuevos métodos, procedimientos mal explicados y formatos inadecuados reflejan obstáculos operativos que impactan en la gestión de la información.

Estos hallazgos refuerzan la necesidad de abordar tanto las barreras culturales como operativas para garantizar que los principios fundamentales de la norma, como la confidencialidad, integridad y disponibilidad de la información, sean comprendidos y aplicados en todos los niveles. La implementación efectiva de la norma ISO 27000 requiere superar estas limitaciones mediante estrategias de capacitación integral, procesos claros y recursos que fortalezcan la seguridad de la información en la organización, alineando las percepciones y acciones del personal con los estándares establecidos.

Por lo tanto, una organización o empresa debe estar consciente que la información es un activo importante o primordial en la continuidad del negocio, por lo cual deberá establecer medidas que apoyen a garantizar su integridad, disponibilidad y confidencialidad; sin embargo muchas de las empresas u organizaciones se centran únicamente en la aplicación de la seguridad física, dejando de lado otros aspectos de relevancia que están ligados directamente al manejo y gestión de la información, lo cual se denomina la “seguridad de la información” (Hallberg y Hunstad, 2005).

En este sentido, de acuerdo con lo señalado por (Hallberg y Hunstad, 2005), la información debe considerarse un activo crucial para la continuidad del negocio, lo que implica la necesidad de garantizar su integridad, disponibilidad y confidencialidad mediante un enfoque integral de seguridad de la información. Este enfoque supera la visión limitada que tienen muchas organizaciones, que suelen centrarse únicamente en medidas de seguridad física, dejando de lado aspectos críticos relacionados con la gestión y protección de la información.

Los resultados muestran una distribución equilibrada en cuanto a la percepción y conocimiento sobre los diferentes aspectos de la capacitación y concienciación en seguridad de la información. Se destaca la importancia de contar con un manual de seguridad, lo que refleja la necesidad de directrices claras que guíen las prácticas de seguridad dentro de la organización. Asimismo, aunque se reconoce la relevancia de los procedimientos, se observa que no todos los involucrados han comprendido completamente su importancia, lo que sugiere que es necesario un mayor enfoque en su capacitación. A pesar de que existe conocimiento sobre la política de seguridad, algunos aún no tienen claridad sobre el alcance del SGSI, lo que resalta una brecha que debe abordarse para una implementación más efectiva. Además, aunque se valora la concientización sobre seguridad, se considera que la calidad de los programas puede mejorarse para garantizar que todos estén plenamente informados y comprometidos con las prácticas de seguridad.

En este contexto, la necesidad de una capacitación integral en materia de seguridad de la información. Bien al implementar programas de capacitación diseñados a medida, se puede mejorar significativamente el nivel de conocimiento y conciencia de los empleados, y fortalecer la seguridad de la información de la institución. Además, las amenazas que se presenta en la seguridad informática son todos los elementos o acciones de manera premeditada que se hacen para atentar contra la información de datos.

Además, las amenazas que se presenta en la seguridad informática son todos los elementos o acciones de manera premeditada que se hacen para atentar contra la información (datos), estas se presentan cuando existen vulnerabilidades internas y externas que se utiliza en diferentes situaciones como perjudicar o robar información. Las vulnerabilidades se dan desde el usuario con el uso incorrecto de la tecnología, falta de capacitaciones a personal, contraseñas obsoletas, etc. Para un sistema seguro se establece una serie de estándares, protocolos, métodos, reglas y técnicas. Tigse Jorge Luis (2020)

En base a lo mencionado tanto por el autor como en los resultados obtenidos, se resalta la importancia de la capacitación como una herramienta clave para mejorar la seguridad de la información. Al invertir en programas de capacitación de calidad, las organizaciones pueden reducir el riesgo de incidentes de seguridad, proteger sus activos y cumplir con los requisitos legales. Esto subraya la necesidad de priorizar la formación del personal para garantizar que estén preparados para enfrentar riesgos, aplicar buenas prácticas y contribuir al cumplimiento de los estándares establecidos en la gestión de la seguridad de la información.

A partir de los resultados obtenidos de la encuesta, se reflejan diversas percepciones sobre la efectividad de la implementación del Sistema de Gestión de Seguridad de la Información. Una parte significativa considera que es medianamente efectiva, lo que indica que, aunque se han logrado avances, aún existen aspectos por mejorar. Otros la califican como altamente efectiva, lo que evidencia reconocimiento hacia los esfuerzos realizados en seguridad de la información. Sin embargo, un grupo más pequeño señala que la implementación es regularmente efectiva o incluso nada efectiva, destacando la necesidad de fortalecer ciertos procesos y ajustar estrategias para garantizar que el sistema cumpla con los objetivos esperados.

En consecuencia, el nivel de efectividad de un Sistema de Gestión de Seguridad de la Información en la institución es un proceso complejo que exige una evaluación exhaustiva y adaptada a las necesidades específicas. Es fundamental considerar factores internos como auditorías recientes, indicadores clave de desempeño, historial de incidentes de seguridad, y otros aspectos relevantes. Este enfoque integral permite identificar áreas de mejora, garantizar el cumplimiento de los objetivos del sistema y fortalecer la protección de los activos de información.

Con respecto Pierce, B. Sweeney (2005) indica que el estándar ISO 27000 proporciona orientación sobre la elaboración y uso de medidas para evaluar la eficacia de un SGSI, siendo

estas aplicadas a la medición de controles o grupos de controles, sin embargo, no describen ni especifican cómo medir y evaluar la efectividad de los controles, sólo se limitan a exigir su evaluación y cumplimiento.

En conclusión, la evaluación de la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) constituye un desafío significativo, en la cual requiere un análisis detallado y continuo. Aunque el SGSI presenta aspectos positivos, es esencial profundizar en su evaluación mediante el uso de herramientas avanzadas que permitan medir con precisión la eficiencia de los controles implementados. Tal como sugiere Pierce, B. Sweeney (2005), este enfoque no solo optimiza el funcionamiento del sistema, sino que también facilita la identificación de áreas de mejora, garantizando una protección más robusta de los activos de información y el cumplimiento efectivo de los estándares establecidos.

Conclusiones

Al finalizar el presente trabajo se concluye lo siguiente:

O.E. 1. Definir conceptualmente sobre la Norma ISO 27000 para mejorar el Sistema de Gestión de Seguridad de la Información.

Luego de una exhaustiva revisión de la literatura se destacan la relevancia de evaluar el conocimiento del personal sobre la norma ISO 27000 y la implementación de un SGSI como elementos clave para fortalecer la seguridad de la información en la organización. Este análisis subraya que la capacitación continua es fundamental para garantizar que el personal esté alineado con los estándares establecidos, mejorando su comprensión y habilidades para proteger eficazmente los activos de información. Además, permite identificar áreas de mejora en los programas de formación, promoviendo una cultura de seguridad sólida y asegurando el cumplimiento de las normativas aplicables. Esto refuerza la capacidad de la organización para enfrentar riesgos y salvaguardar la integridad, confidencialidad y disponibilidad de la información.

O.E.2. Identificar las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta el departamento de Talento Humano del IESS de los Esteros.

De acuerdo con la identificación de las amenazas y vulnerabilidades especificas del Departamento de Talento Humano del IESS de los Esteros, señala que una de las principales amenazas internas es la insatisfacción laboral que puede llevar a los empleados a filtrar información confidencial, además la usencia de conciencia y el déficit de conocimiento sobre las políticas de seguridad y las buenas prácticas generan acciones que comprometen la seguridad de la información. Por otro lado, las amenazas externas incluyen ataques a terceros, como brecha de seguridad en proveedores de servicios que también ponen a riesgos la información del IESS.

O.E.3. Determinar las principales barreras para la implementación de las normas ISO 27000 en el Departamento de Talento Humano del IESS de Manta y cómo pueden superarse.

Los resultados destacan la importancia de la norma ISO 27000 para gestionar la seguridad de la información mediante sus pilares clave: confidencialidad, integridad y disponibilidad. Aunque se reconoce su valor, muchas organizaciones aún priorizan la seguridad física, dejando de lado aspectos esenciales de la gestión de la información. Esto subraya la necesidad de un enfoque integral que considere la información como un activo crítico para la continuidad del negocio y fomente su protección efectiva en todos los niveles.

O.E.4. Diagnosticar el impacto de la capacitación y concienciación del personal en la mejora de la seguridad de la información en el departamento de Talento Humano del IESS de los Esteros bajo el marco de la Normas ISO 27000.

Para concluir, la capacitación integral en seguridad de la información es esencial para mitigar vulnerabilidades internas y externas, reducir riesgos y proteger los activos organizacionales. Esto refuerza el cumplimiento de estándares y fortalece la conciencia y competencias del personal, asegurando una gestión más segura y eficiente de la información.

Recomendaciones

O.E.1. Definir conceptualmente sobre la Norma ISO 27000 para mejorar el Sistema de Gestión de Seguridad de la Información.

Se recomienda implementar programas de capacitación continua y evaluaciones periódicas sobre la norma ISO 27000 y el SGSI, con el fin de mantener al personal actualizado y alineado con los estándares de seguridad de la información. Esto fortalecerá su capacidad para proteger los activos informáticos, identificar posibles áreas de mejora y fomentar una cultura de seguridad robusta en la organización. Además, es crucial invertir en recursos y herramientas adecuadas para garantizar la efectividad de estas capacitaciones y asegurar el cumplimiento normativo.

O.E.2. Identificar las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta el departamento de Talento Humano del IESS de los Esteros.

Es fundamental implementar un programa integral de capacitación y concienciación sobre seguridad de la información dirigido a todos los empleados del Departamento de Talento Humano del IESS de los Esteros, con el fin de reducir los riesgos derivados de la falta de conocimiento y conciencia. Además, se debe fortalecer la comunicación interna sobre las políticas de seguridad y las buenas prácticas. Para mitigar las amenazas externas, es crucial establecer políticas de seguridad que incluyan evaluaciones periódicas de los proveedores de servicios y garantizar que estén alineados con los estándares de seguridad establecidos. También se deben implementar mecanismos de control y monitoreo para detectar y prevenir filtraciones de información, tanto internas como externas.

O.E.3. Determinar las principales barreras para la implementación de las normas ISO 27000 en el Departamento de Talento Humano del IESS de Manta y cómo pueden superarse.

Se sugiere que las organizaciones adopten un enfoque integral de seguridad de la información que no solo priorice la seguridad física, sino que también integre los principios de la norma ISO 27000, enfocándose en la confidencialidad, integridad y disponibilidad de la información. Es crucial sensibilizar a todos los niveles organizacionales sobre la importancia de tratar la información como un activo estratégico, asegurando su protección mediante políticas claras y formación continua. Además, se recomienda realizar evaluaciones periódicas de riesgos y actualizar los protocolos de seguridad para mantenerse alineados con las mejores prácticas y mitigar amenazas emergentes.

O.E.4. Diagnosticar el impacto de la capacitación y concienciación del personal en la mejora de la seguridad de la información en el departamento de Talento Humano del IESS de los Esteros bajo el marco de la Normas ISO 27000.

Es recomendable que la organización establezca programas de formación continua en seguridad de la información para todo el personal. Esto ayudará a aumentar la conciencia y las habilidades del equipo, reduciendo así los riesgos tanto internos como externos y mejorando la protección de los activos de información. Además, se debe realizar un seguimiento regular para asegurar que se cumplan los estándares de seguridad y ajustar las prácticas frente a nuevas amenazas.

Referencias

Advisory, R. (2019). Ciber Riesgos y Seguridad de la Información en América Latina &. *Deloitte*.

Alvarez. (2017). IMPLEMENTACION DE POLITICAS SEGURIDAD BASADAS EN EL MODELO ISO 27001 EN LA EMPRESA MEDIOS DE COMUNICACIÓN DIGITAL INFORMATE PAJÁN. Jipijapa, Manabí, Ecuador: Unesum.

Álvarez. (2017). Implementacion de politicas seguridad basadas en el modelo iso 27001 en la empresa medios de comunicación digital informate Paján. Jipijapa, Manabí, Ecuador : UNESUM.

Ascanio et al. (2015). Implementacion de politicas seguridad basadas en el modelo iso 27001 en la empresa medios de comunicación digital infórmate paján. jIPIJAPA, mANABÍ, eCUADOR: unesum.

Baena. (2019). Importancia de la Norma ISO/IEC 27000 en la implementación de un Sistema de Gestión de la Seguridad de la Información. Dialnet.

Bayona, S. (Abril de 2022). Diseño del plan de gestión para la seguridad de la información basada en las Normas ISO 27000 en la empresa Bamarex S.A.

Blazic, B. &. (2008). Un enfoque de modelación económica de la información. *Revista Internacional de Gestión de la Información*.

Camargo. (2017). Diseño de un sistema de gestión de la seguridad de la informacion (SGSI) en el área tecnológica de la comision nacional del servicio civil - CNSC basado en la norma ISO27000 e ISO27001 . UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA , Lima-Perú : UNAD.

Cuito, L. (2024). Propuesta de un sistema de gestión de seguridad de la información basado en la norma ntp iso/iec 27001:2014 para proteger los activos de información de la municipalidad distrital de chamaca. Perú .

Duque, V. (2021). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Scielo Portugal*.

Dussan. (2020). Políticas de seguridad informática. Ambato, Ecuador.

Estrada, S. (2019). Diseño de un Sistema de Gestión de Seguridad y Salud en el trabajo, aplicando la Norma ISO 45001:2018, para la Universidad Laica Eloy Alfaro de Manabí, Campus Manta. Manta, Manabí, Ecuador.

Excelencia. (2020). Serie ISO 27000 Escuela. Europea de Excelencia ISO/IRC.

Gómez, A. (Marzo de 2007). Diseño de una política de seguridad de la información basada en la Norma ISO 27000 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior. Quito, Ecuador.

González y Pérez. (2020). Barreras en la implementación de la ISO 27000 en organizaciones públicas y privadas. *Revista de Seguridad Organizacional*.

Guamán, M. (2022). Implementacion De politicas seguridad basadas en el modelo ISO 27001 En La Empresa Medios De Comunicación Digital Infórmate Paján. Jipijapa, Manabí, Ecuador : UNESUM.

Hallberg y Hunstad. (2005). Diseño de una política de seguridad de la información basada en la Norma ISO 27002:2013, para el sistema de botones de seguridad del ministerio del interior. *Magister en tecnologías de la información con mención en seguridad de redes y comunicación*, 25. Quito, Ecuador.

Hallo, T. (2020). Implementacion De politicas seguridad basadas en el modelo ISO 27001 En La Empresa Medios De Comunicación Digital Informate Paján. Jipijapa , Manabí, Ecuador : Unesum.

López, A. (2023). Un Sistema de Gestión de la Seguridad de la Información o SGSI. *Artículo sobre el Sistema de Gestión de la Seguridad de la Información o hashtag#SGSI como parte de la formación de cumplimiento en materia de seguridad hashtag#GRC hashtag#Seguridad hashtag#Ciberseguridad hashtag#ISO27001*.

Luis, T. J. (2020). Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho S.A. Facultad de Ingeniería en Sistemas.

Matamoros, B. L. (2005). Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autencidad, responsabilidad no repudio y fiabilidad pueden ser también consideradas.

Méndez, M. (2021). Diseño de un sistema gestión de seguridad de información para proteger los activos de información del servicio de administración tributaria de la zona norte del Perú . Universidad Privada del Norte, Perú .

Miguel Angel Parra Martinez. (2019). Análisis de seguridad basado en la Norma ISO 27000. (A. D. 27000.

Miguel, C. R. (2012). Universidad Politécnica Salesiana sede Cuenca. Carrera de Ingeniería en sistemas. Ecuador.

Normaiso 27001. (2020). Implementar ISO 27001 paso a paso - 1 como hacer un Analisis

Pierce, B. Sweeney,. (2005). Modelo para la evaluación de desempeño de los controles de un SGSI basado en. Medellín , Colombia .

Ponce, A. (2023). Sistema de gestión de seguridad de la información para la Protección de datos en una inmobiliaria. Universidad César Vallejo, Trujillo, Perú., Lima.

Quintero, D. M. (2017). Sistemas de Gestión en Seguridad y Salud en el Trabajo (SG-SST). *Diagnóstico y análisis para el sector de la construcción*. Colombia.

Regina. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. Contribuciones a La Economía, Junio.

Romero, C. (2022). IMPLEMENTACION DE POLITICAS SEGURIDAD BASADAS EN EL MODELO ISO 27001 EN LA EMPRESA MEDIOS DE COMUNICACIÓN DIGITAL INFÓRMATE PAJÁN. Jipijapa, Manabí, Ecuador.

Salvador. (Abril de 2019). Diseño del plan de gestión para la seguridad de la información basada en las normas iso 27000 en la empresa Bamarex S.A.

Sampedro Guamán et al. (2019). Implementacion De politicas seguridad basadas en el modelo IS 27001 en la empresa medios de comunicación digital infórmate Paján. Jipijapa, Manabí, Ecuador: UNESUM.

SlideShare. (2016). “Sistema para el compartimiento de archivos usando la norma iso 27000 para digitalizar y centralizar la información administrativa y académica del colegio Dr. trajano naranjo iturralde”.

Telecomunicaciones, M. d. (2020). Guía para la implementación del esquema gubernamental de seguridad de la informaciòn. Ecuador.

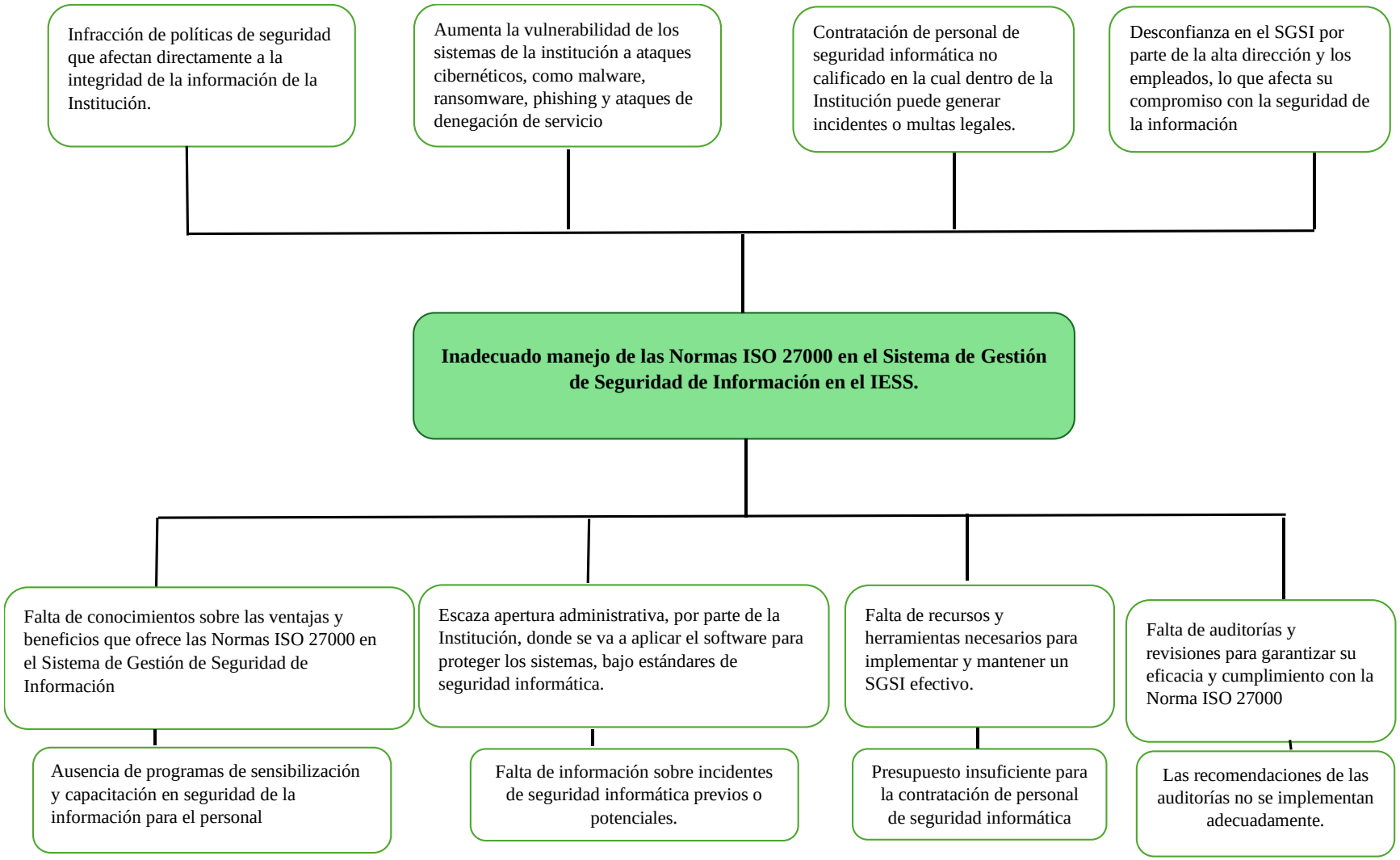
Torres. (2021). Sistema de gestión de seguridad de la información, para la gestión del riesgo de la información de una empresa comercializadora de Lubricantes en la ciudad de chiclayo.

Vegas, I. (2019). Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001 (Tesis de pregrado). Universidad Nacional de Piura, Piura, Perú.

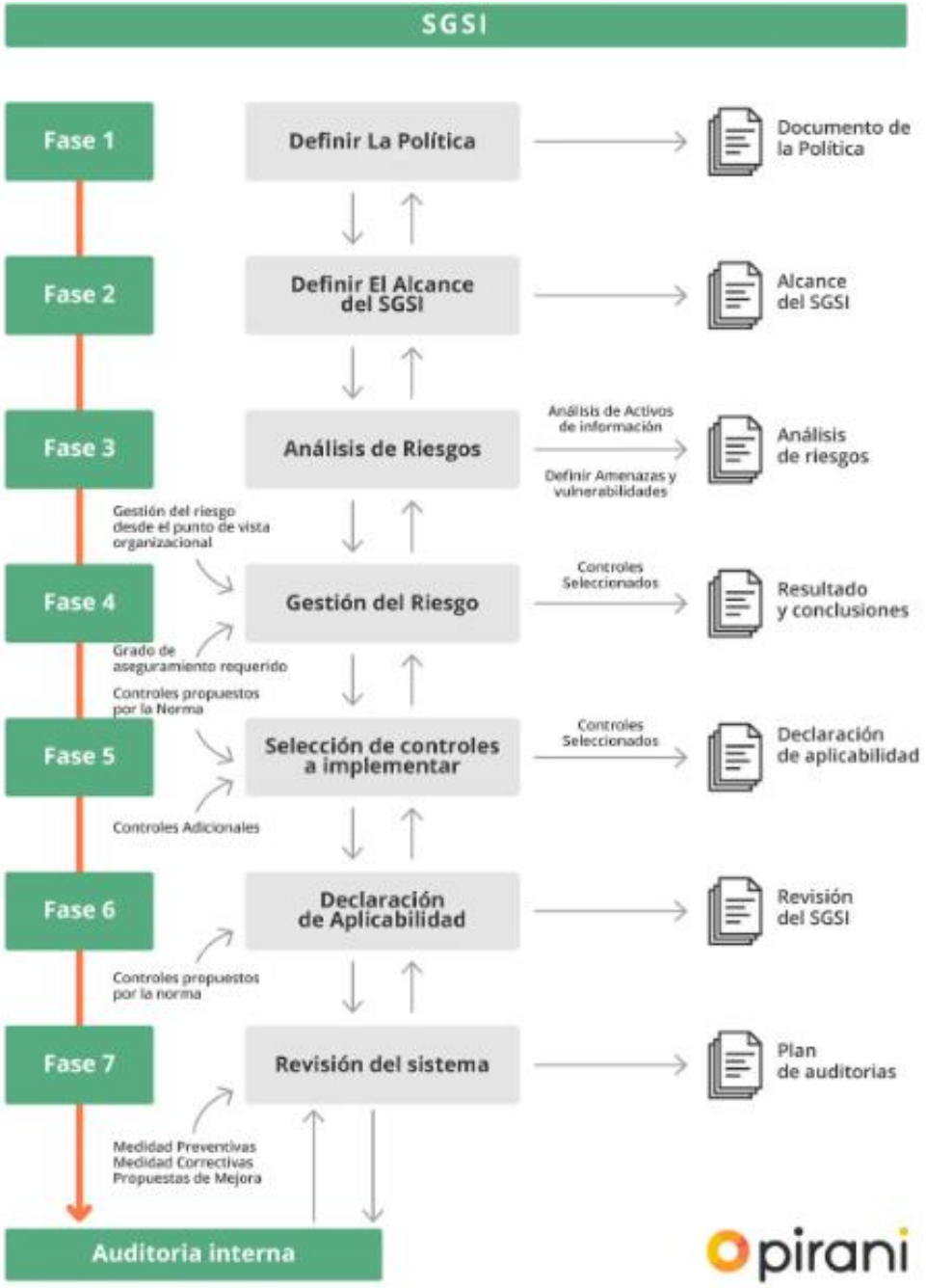
Villacis Miguel Leopoldo. (2016). Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) Basado en la Norma ISO 27001:2013 para la Red Corporativa de la Empresa Ecuatronix. Ingeniería Electrónica. 18. Quito, Ecuador.

Anexos

Árbol de Problema



Anexo 1: Guía para el Sistema de Gestión de Seguridad de la Información



Pasos que debes seguir para elaborar un Sistema de Gestión de Seguridad de la Información

Anexo 2: Evaluación de Riesgo

CALIFICACION DEL RIESGO	DESCRIPCIÓN
Muy alto (7-9)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir estos riesgos y mitigar los riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir el riesgo y los riesgos de mitigación deberían implementarse lo antes posible.
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir los riesgos y mitigar los peligros deberían incluirse en los planes y presupuestos futuros.
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir aún más el riesgo o mitigar los peligros junto con otras mejoras de seguridad y mitigación.

Clasificación y Valoración del riesgo

Anexo 3: Valoración del Riesgo

(Ejemplo)

Elementos de activos de información	Valor de los activos
C: confidencialidad	4
I: integridad	2
D: disponibilidad	1
Amenaza	3
Vulnerabilidad	3

El valor del riesgo para este caso es calculado de la siguiente forma:

Valor del riesgo por la confidencialidad: 4 x 3 x 3 = 36

Valor del riesgo por la integridad: 2 x 3 x 3 = 18

Valor del riesgo por la disponibilidad: 1 x 3 x 3 = 9

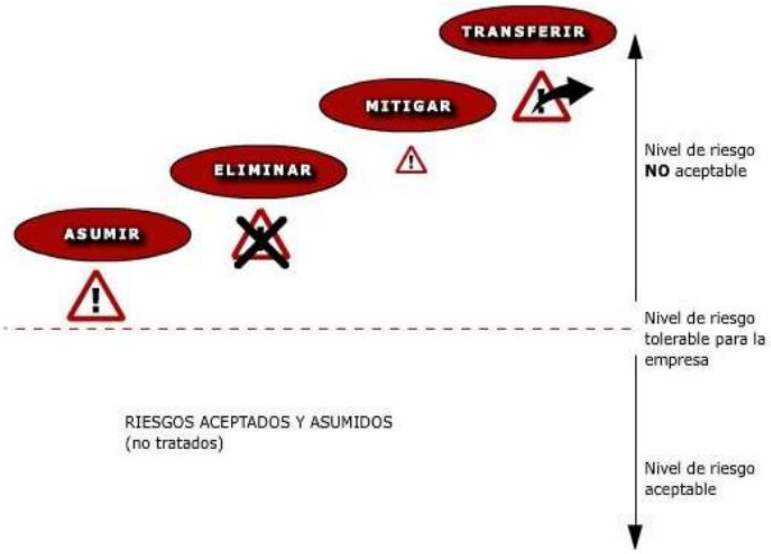
Ejemplo del cálculo para la valoración del riesgo

Anexo 4: Probabilidades de los niveles de Riesgos

	AMENAZA								
	1			2			3		
	VULNERABILIDAD								
ACTIVOS DE INFORMACIÓN	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

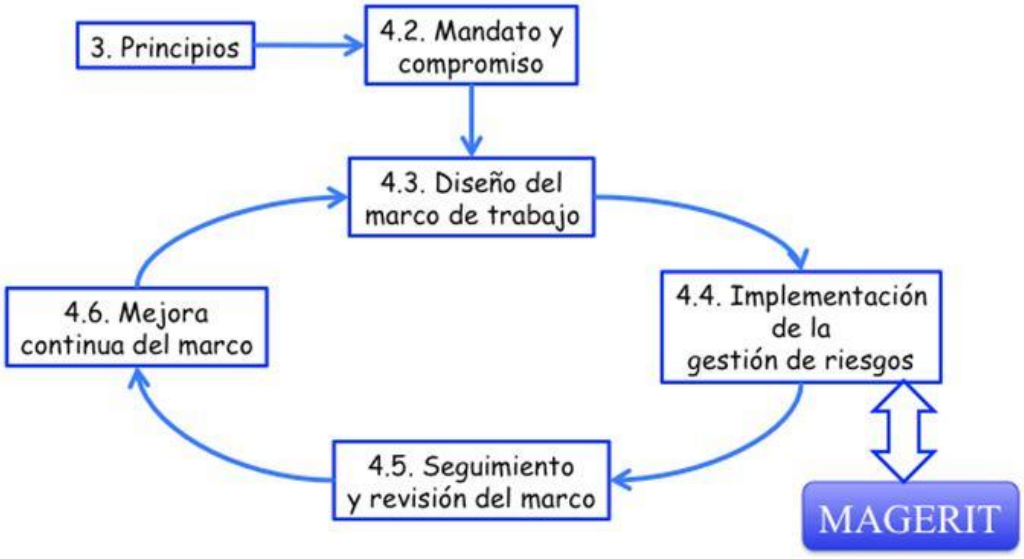
Niveles de Riesgos

Anexo 5: Medidas de mitigación para el tratamiento de riesgos



Tratamiento del Riesgos en un Sistema de Seguridad de la Información

Anexo 6: MAGERIT



Metodología de Análisis y Gestión de Riesgos del Sistema de Información

Anexo 5: Declaración de Aplicabilidad ISO 27001

		Activo 1				
A9	**Control de Acceso**	Implementado	Aplica a los riesgos del activo	Coste de implementacion Aceptable	Coste de mantenimiento Aceptable	Justificacion o comentarios
9.1.1	Política de control de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.1.2	Acceso a las redes y a los servicios de red	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.1	Registro y baja de usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.2	Provisión de acceso de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.3	Gestión de privilegios de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.4	Gestión de la información secreta de autentificación de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.5	Revisión de los derechos de acceso de usuario	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.6	Retirada o ajuste de los derechos de acceso	SI/NO	SI/NO	SI/NO	SI/NO	

Modelo de declaración de Aplicabilidad ISO 27001

Anexo 7: Fotografía de la técnica del instrumento aplicado

Entrevista en el Departamento de Talento Humano

Anexo: 8 Ficha de observación aplicada en el departamento de Talento Humano

Lista de verificación para la observación directa

Objetivo: Analizar las Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información en el Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social de Manta.

Datos generales

Nombre del Observador: ……

Ficha de Observación: …….

Hora de Inicio: …….

Hora de Finalización: …….

Lugar de Observación: …….

N°	Observaciones	SI	NO
1.	¿Cumple con el nivel de efectividades la implementación actual del SGSI en el Departamento de Talento Humano del IESS de los Esteros?		
2.	¿Qué impactos podría sufrir una organización al no cumplir con los requisitos de seguridad de la información?"		
3.	¿Tiene conocimiento de la norma ISO 27000?		
4.	¿La norma ISO 27000 tiene como finalidad establecer un marco para la gestión de la seguridad de la información?		
5.	¿Se consideran aspectos como la confidencialidad, integridad y disponibilidad de la información en la norma ISO 27000?		
6.	¿Los recursos (humanos, tecnológicos, financieros) son necesarios para cumplir con los estándares de seguridad de la información establecidos en ISO 27000?		
7.	¿Es beneficioso aplicar las normas ISO 27000 dentro de un sistema de gestión de seguridad de la Información?		
8.	¿Existen barreras en el Departamento de Talento Humano del IESS de los Esteros para la implementación de las normas ISO 27000, y se pueden identificar posibles soluciones para superarlas?		

9.	¿Conoce de las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta el Departamento de Talento Humano del IESS de los Esteros?		
10.	¿Se están abordando adecuadamente los temas de capacitación y concienciación del personal en el Departamento de Talento Humano del IESS de los Esteros en relación con las Normas ISO 27000 para mejorar la seguridad de la información?		

Anexo 9: Encuesta

Encuesta sobre la ISO 27000

El objetivo principal es "Demostrar el aporte de las Normas ISO 27000 para mejorar el Sistema de Gestión de Seguridad de Información en el Departamento de Talento Humano del Instituto Ecuatoriano de Seguridad Social de Manta". A través de esta herramienta, se busca identificar las áreas de mejora, las brechas existentes y las oportunidades para fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI).

La propuesta metodológica que hemos desarrollado es altamente adaptable y puede ser fácilmente ajustada para una encuesta online utilizando herramientas como Google Forms.

Marque con una (x) solo una de las alternativas de cada ítem presentado a continuación

1. **¿Qué nivel de efectividad es la implementación actual del SGSI en el Departamento de Talento Humano del IESS de los Esteros?**

- ◯ Altamente Efectiva
- ◯ Medianamente efectiva
- ◯ Regularmente efectiva
- ◯ Nada efectiva

2. **¿Qué impactos pueden sufrir los procesos y la reputación de una organización al no cumplir con los requisitos de seguridad de la información?**

- ◯ Alto impacto
- ◯ Medio impacto
- ◯ Impacto leve
- ◯ Ningún Impacto

3. **¿Tiene conocimiento de la norma ISO 27000?**

- ◯ Muy probable
- ◯ Nada probable
- ◯ Poco probable
- ◯ Medianamente probable

4. **¿Cuál es la finalidad de la norma ISO 27000?**

- ◯ Establecimiento de buenas prácticas, directrices y principios generales para iniciar la implantación, mantenimiento y gestión del SGSI

Preguntas aprobadas y validadas por el Lcdo. Oswaldo Mero Docente de la Carrera de gestión de la Información Gerencial de la Facultad de Ciencias Administrativas, Contables y Comercio de la Universidad Laica Eloy Alfaro de Manabí (ULEAM).

Propuesta de Solución

Tema: Guía detallada de la norma ISO 27000 para el Sistema de Gestión de Seguridad de la Información en el Instituto Ecuatoriano IESS de los Esteros.

Introducción

En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo tanto, es necesario que toda organización que busca excelencia en los servicios o productos que ofrece, adopte un Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. Para cubrir estas necesidades la ISO (Organización Internacional para la Estandarización).

Justificación

El presente instrumento tiene como objetivo presentar una guía detallada de la norma ISO 27000 para el Sistema de Gestión de Seguridad de la Información en el Instituto Ecuatoriano IESS de los Esteros. A través de este estudio, buscamos establecer un conjunto de políticas, procesos y controles que en sí permitan proteger la información, cumplir con los requerimientos legales y regulatorios.

Para dar solución a los requerimientos del Instituto Ecuatoriano de Seguridad Social del IESS de los Esteros se ha propuesto realizar una guía detallada de un Sistema de Gestión de Seguridad de la Información, el cual permite garantiza el proceso de gestión de la seguridad dirigido a preservar la disponibilidad, confidencialidad, integridad y la autenticación de la información y así evitar o disminuir los riegos de amenazas vigentes actualmente. El SGSI será establecido acorde a la normativa de la ISO 27000.

Objetivo general

Elaborar una guía exhaustiva que permita a las organizaciones implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y eficaz, alineado con los requisitos de la norma ISO 27000.

Objetivos Específicos

- Proporcionar instrucciones paso a paso para llevar a cabo una evaluación de riesgos de seguridad de la información conforme a la ISO 27000, identificando los controles necesarios para mitigar los riesgos.
- Determinar el alcance para la aplicación del estándar ISO 27000 en el Instituto Ecuatoriano de Seguridad Social del IESS de los Esteros.
- Diseñar un Sistema de Gestión de Seguridad de la Información para mantener y mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación.

Metodología

La elaboración de la guía detallada de la norma ISO 27000 para el Sistema de Gestión de Seguridad de la Información se lleva a cabo con las siguientes fases.

Definición de la Política

La política de seguridad es un requisito de la norma ISO 27000 y considera los objetivos de la seguridad de la información de la organización (Normaiso 27001, 2020).

- La política de seguridad establece el marco general y los objetivos de seguridad de la información de la organización.
- Considera los requerimientos legales y contractuales relativos a la seguridad de la información.

- Está alineada con el contexto estratégico de gestión del riesgo, será proporcionada y coherente.
- Establece los criterios de evaluación del riesgo
- Está aprobada por la dirección.

Definición del Alcance

En base a la sección de alcance de la norma ISO 27000 se establece:

- Objetivo de la norma
- Tipos de organizaciones a lo que se aplica; y
- Las secciones de la norma que son denominadas cláusulas que contiene los requisitos que deben cumplir una organización para que se certifique que es conforme con ella es decir que si cumple.

La norma ISO 27000 está diseñada para ser aplicable a cualquier tipo de organización, independientemente del tamaño, la complejidad, el sector industrial, el propósito o la madurez, su organización puede implementar y mantener un SGSI que cumpla con la norma ISO 27000.

Análisis de riesgo

Frente a una amenaza potencial se establece un análisis en base a los parámetros de la frecuencia y el valor de la vulnerabilidad (Normaiso 27001, 2020). El análisis de riesgos es un proceso en el cual se tomarán en cuenta los niveles de impactos. La metodología sugiere un proceso para el análisis de riesgos, que consiste en:

- Identificación de activos
- Análisis de amenazas
- Análisis de vulnerabilidades
- Definición de controles

Identificación de activos

En esta fase, se realizó la identificación de los activos críticos relacionados con los procesos internos de la organización. Un activo se define como cualquier recurso que tenga un valor esencial para el funcionamiento y la continuidad de la entidad. Para asegurar su protección y disponibilidad, se utilizó la metodología MAGERIT. La clasificación de estos activos se detalla en la tabla, de acuerdo con el segundo apartado de la metodología, conocido como Catálogo de Elementos.

Tipos de Activos	Descripción
Datos/Información	Se refiere a información relevantes de la organización. Ejemplo: Informes, guías, procesos, etc.
Servicios	Mantenimiento de computadoras, soporte. Sistema financiero, herramientas tecnológicas, base de datos, etc.
Software	Sistema financiero, herramientas tecnológicas, base de datos, etc.
Hardware	La parte, infraestructura de la institución, por ejemplo: servidor, computadoras
Redes de comunicación	Son aquellos servicios de comunicación como: Teléfonos y celular.
Soporte de información	Se refiere al medio físico o tecnológico que es utilizado para almacenar y respaldar datos.

Equipamiento auxiliar	Son dispositivos o herramientas para apoyar un equipo o sistema principal para su funcionamiento, estos son los siguientes: Computadora (teclado y mouse) componentes electrónicos (cables, adaptador y cargadores.
Instalaciones	Se basa a los espacios físicos, estructuras donde se encuentra los sistemas de información, como vehículos
Personal	Es un miembro de la organización donde trabaja ejemplo: usurarios, secretaria, técnicos etc.

Elaboración propia, información basada en el Departamento de Talento Humano

Identificar los riesgos donde se debe considerar:

- La identificación de los activos que están dentro del alcance del SGSI y a sus responsables directos.
- La identificación de amenazas en relación a los activos.
- La identificación las vulnerabilidades.
- La identificación de los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Identificación de amenazas y vulnerabilidades

Como se explicó anteriormente, los activos de una organización son su principal valor y, por lo tanto, están expuestos a diversas amenazas. En sí estás amenazas pueden aprovechar vulnerabilidades en los sistemas, aplicaciones o datos para causar daños, como pérdidas de información o interrupciones en los servicios. Es fundamental identificar y evaluar

Metodología de Análisis de Riesgos MAGERIT

Es una metodología creada por el Ministerio de Administraciones Públicas de España, diseñada para llevar a cabo análisis de riesgos y gestionar su mitigación. Esta metodología define los pasos necesarios para analizar el estado de los riesgos y las acciones para controlarlos, asegurando que el proceso se mantenga gestionado en todo momento.

MAGERIT persigue los siguientes objetivos.

Directos:

- Concienciar a los responsables de la organización de información de la existencia de riesgos y de la necesidad de gestionarlo.
- Proporcionar un enfoque estructurado para evaluar los riesgos asociados al uso de las tecnologías de la información y las comunicaciones.
- Ayudar a descubrir y planificar el tratamiento pertinente para mantener los riesgos a bajo control.

Indirecto

- Capacitar a la organización para afrontar procesos de evaluación, auditoría, certificación o acreditación, según sea necesario en cada situación.

Es fundamental tener en cuenta que la metodología MAGERIT se alinea con los criterios de valoración de activos establecidos por la norma ISO/ICE 27001, como la disponibilidad, integridad y confidencialidad. Además, también incluyen aspectos derivados de estos criterios, como la seguridad. Cabe resaltar que la aplicabilidad de estos criterios puede variar según las necesidades específicas de cada caso.

Gestión de riesgo

Se describe la metodología a utilizar para la gestión de riesgos con el objetivo de tomar decisiones correctas según los riesgos derivados de las tecnologías de la información, así como el inventario de activos de la organización y la valoración de estos, considerando la confidencialidad, integridad y disponibilidad de la información. Además, se realiza un análisis de amenazas y una valoración de los riesgos, estimando así los riesgos a los que está expuesta la organización.

De acuerdo al estudio de caso, el objetivo demostrar el aporte de las Normas ISO 27000 y elaborar una guía exhaustiva que permita a las organizaciones implementar y mantener un Sistema de Gestión de Seguridad de Información. En este trabajo de estudio se indican los resultados de la experiencia aplicando las fases de metodologías de análisis y evaluación de riesgo con el diseño o aplicación del instrumento, como cuestionarios aplicados a los administradores, entrevista al personal del área de Talento Humano, usuarios y testeo, que permitieron establecer el diagnóstico de seguridad en una organización; aplicando luego una lista de chequeo basada en los estándares, para verificar la existencia de controles de seguridad en los procesos organizacionales. Finalmente, según los resultados del análisis y evaluación de los riesgos, los autores se proponen los controles de seguridad adecuados para que sean integrados posteriormente dentro de un SGSI que responda a las necesidades de seguridad informática de la organización de estudiada.

La metodología se compone de algunas secciones principales:

- Evaluación de riesgos
- Tratamiento de riesgos
- Selección de controles
- Declaración de aplicabilidad

Evaluación de riesgos

Una vez calculado el valor de riesgo asociado a cada amenaza que podría impactar un activo de información, el siguiente paso es establecer criterios claros sobre lo que se considera un nivel de riesgo aceptable. Esto implica definir qué niveles de riesgo pueden ser asumidos sin necesidad de intervención adicional y cuáles requieren la implementación de medidas específicas para su tratamiento.

A continuación, se establece cuatro categorías de riesgo que servirán para determinar las acciones necesarias en función de las puntuaciones asignadas previamente en la tabla de valores de riesgo que se encuentra en el apartado de anexo.

A partir de los resultados obtenidos en el análisis de riesgo, el siguiente paso consiste en determinar las acciones necesarias para reducir los distintos niveles de riesgo. Estas acciones, según la norma ISO 27001, se conocen como controles de seguridad de la información.

Tratamiento de riesgos

Después de identificar y evaluar los riesgos, el siguiente paso en la gestión de riesgos es desarrollar un plan de respuesta adecuado.

Asimismo, la evaluación de riesgos permite a la organización identificar primero los riesgos que considera inaceptables. El principal objetivo de la gestión de riesgos es gestionar y abordar estos riesgos inaceptables mediante acciones específicas en esta etapa.

Por cada riesgo identificado en su evaluación de riesgos, debe aplicar criterios coherentes para determinar si debe:

- Aceptar el riesgo o
- Tratar el riesgo

Las opciones de tratamiento de riesgos disponibles suelen ser una de las siguientes:

- Reducir el riesgo, con la aplicación de contramedidas o salvaguardas especificadas controles de la norma.
- Evitar el riesgo, dejando de realizar la actividad que produce el riesgo.
- Transferir el riesgo, a un tercero. Ejemplo: Una aseguradora o una tercerización de servicios.
- Aceptar el riesgo, que consiste en asumir la responsabilidad de correr dicho riesgo.

La decisión de aceptar un riesgo debe contar con la aprobación formal de la alta dirección de la organización. Esta opción suele adoptarse cuando el costo de implementar el control necesario supera el valor del propio activo.

En base a lo mencionado previamente, es importante tener en cuenta los cuatro tipos o categorías de decisiones para abordar el tratamiento de riesgos, los cuales se establecen de la siguiente forma en la cual se visualiza en el Anexo N°3.

Riesgo transferible: En este caso, el riesgo es transferido a otra organización debido a su naturaleza crítica, que requiere atención prioritaria o inmediata. Asimismo, podría darse la situación de que el riesgo esté cubierto por algún tipo de seguro asociado.

Riesgo Mitigable*:* De acuerdo a la situación, el riesgo puede ser mitigado mediante la implementación de controles de seguridad específicos, dada su alta gravedad.

Riego Eliminable: En este caso, lo más común es retirar el activo que expone a la organización a riesgos que no se puede justificar.

Riesgos Asumible: En esta situación, el riesgo asociado al activo se considera aceptable por la organización, lo que implica que no se implementará medidas para reducirlo o eliminarlo continuamente estas amenazas y vulnerabilidades para proteger los activos de la organización.

Valoración de riesgos del SGSI

La evaluación de riesgos se lleva a cabo una vez que se ha elaborado un inventario de activos de información, identificando las categorías de importancia de dichos activos y estableciendo los criterios para analizar amenazas y vulnerabilidades.

Asimismo, el nivel de riesgo se puede calcular aplicando una fórmula que considera los valores asignados al “valor de los activos de información, la “escala de las amenazas” y el “nivel de vulnerabilidad”.

C: Valor del riesgo por la confidencialidad

I: Valor del riesgo por la integridad

D: Valor del riesgo por la disponibilidad

Valor del riesgo = “Valor del activo” x “Amenazas” x “Vulnerabilidades”

En base a la información obtenida es posible calcular y determinar el nivel de riesgo asociado a cada activo.

Una vez realizada la valoración de los riesgos, se debe decidir si se acepta el riesgo o si es necesario reducirlo. Para ello, es importante definir un valor mínimo como límite para la aceptación del riesgo. Por otro lado, el nivel límite establecido es 4, es decir, se aceptarán los riesgos cuyos valores sean inferiores a este nivel, mientras que para los riesgos superiores se tomarán medidas específicas.

Una vez analizado el cuadro previo, concluimos que los riesgos aceptados corresponden a aquellos con baja probabilidad de ocurrencias y un impacto mínimo en caso de presentarse. A continuación, se incluye una tabla que la encontramos en el Anexo N°3 con los niveles de riesgos correspondientes.

Asimismo, aquellos riesgos con niveles menores a 4 como se indica en la tabla anterior, son aquellos que se van a aceptar. Como se puede observar son aquellos con una valoración mínima para no afectar la funcionalidad de la organización.

Selección de controles a implementar

Es un paso crucial en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basada en ISO 27000. La norma proporciona un amplio catálogo de controles, pero no todos son obligatorios. La elección de los controles adecuados dependerá de un análisis de riesgos específicos para cada organización

A continuación, encontramos 11 dominios de cobertura de la norma, como son:

- Políticas de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Gestión de las comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes en seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

Declaración de Aplicabilidad

Es un documento que contiene definidos los objetivos de los controles en la organización relacionados con la seguridad de la información; así como los procedimientos de aplicación de los controles, con la finalidad de evaluar las brechas de seguridad en cada dominio o ámbito de seguridad de la información. La ISO 27000 define una lista de controles y objetivos de control que sirven de guía para definir cuáles son incluidos o excluidos en esta evaluación.

Revisión del Sistemas

Es fundamental para identificar las fortalezas y debilidades de la seguridad de la información de una organización y, por ende, para elaborar una guía efectiva basada en ISO 27000. Esta revisión permite alinear los controles de seguridad con los riesgos específicos de la organización.

Pasos para realizar una revisión de sistemas:

- Definir el alcance
- Recopilación de información
- Evaluar el cumplimiento
- Evaluar la eficacia
- Identificar el riesgo
- Recomendar controles

Conclusión

Para finalizar al adoptar la norma ISO 27000 en el IESS de los Esteros constituye una inversión estratégica que generará beneficios a largo plazo, tanto la institución como para sus afiliados. Asimismo, al seguir este marco de referencia internacional, el IESS se posiciona como una institución líder en seguridad de la información, fortaleciendo su reputación y contribuyendo al desarrollo de un sistema de seguridad social más seguro y confiable.