UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN, E INNOVACIÓN TECNOLÓGICA

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADA EN EL ESTÁNDAR ISO 27001 PARA LA EMPRESA EJEPROY CIA. LTDA.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

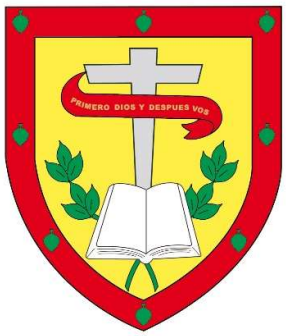
AUTOR: CHRISTIAN FERNANDO AGUILAR CORONEL

DIRECTOR: ING. JUAN PABLO CUENCA TAPIA MSC.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN, E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERIA EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO:

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADA EN EL ESTÁNDAR ISO 27001 PARA LA EMPRESA EJEPROY CIA. LTDA.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR: CHRISTIAN FERNANDO AGUILAR CORONEL

DIRECTOR: ING. JUAN PABLO CUENCA TAPIA MSC.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Christian Fernando Aguilar Coronel portador(a) de la cédula de ciudadanía Nº **0103997755**. Declaro ser el autor de la obra: "**Diseño de un sistema de gestión de seguridad de la información (SGSI) basada en el estándar ISO 27001 para la empresa EJEPROY CIA. LTDA.**", sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **26 de marzo de 2025**

F: .....

Christian Fernando Aguilar Coronel

C.I. **0103997755**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente trabajo de investigación fue desarrollado **por Christian Fernando Aguilar Coronel** con número de cédula **0103997755** con el tema: **"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADA EN EL ESTÁNDAR ISO 27001 PARA LA EMPRESA EJEPROY CIA. LTDA."**, bajo mi supervisión.

JUAN PABLO CUENCA TAPIA

ING. JUAN PABLO CUENCA Msc.
DOCENTE TUTOR

Dedicatoria

Dedico este trabajo con profunda gratitud a mi Esposa Viviana y a mi hijo Christian Sebastián cuyo sacrificio y amor incondicional han sido el pilar fundamental para alcanzar esta meta, una de las más importantes de mi vida. Su apoyo inquebrantable no solo hizo posible continuar mi educación, sino que también me inspiró a seguir adelante con determinación y compromiso.

A los dos, mi dedicatoria por ser las personas más importantes en este logro.

Agradecimiento

Expreso mi más sincero agradecimiento a mi docente tutor, Ing. Juan Pablo Cuenca, por su invaluable guía, paciencia y orientación a lo largo de este proceso, brindándome el conocimiento y apoyo necesario para alcanzar esta gran meta en mi vida. A su vez también a todos los docentes que estuvieron en cada ciclo académico impartiendo sus conocimientos y enseñanzas.

Resumen

Ejeproy Cía. Ltda., se encuentra situada en Cuenca - Ecuador dedicada a ejecutar proyectos de construcción, al momento enfrenta una creciente necesidad de gestionar y proteger de una manera efectiva la información critica que maneja en el desarrollo de sus actividades. La naturaleza de sus operaciones implica el manejo de información confidencial que incluyen datos financieros, contratos, especificaciones técnicas de proyectos, datos personales, en general información sensible en el manejo. El incumplimiento de normativas, la exposición a ciberataques o pérdida de datos, podría afectar gravemente en su reputación como empresa y causar pérdidas económicas muy significativas. Cabe mencionar que es de suma importancia y en general el diseño de un SGSI que se encuentre enfocado a la norma ISO/IEC 27001 y políticas locales vigentes. Las amenazas y la necesidad imperante por tener una protección adecuada los datos, se encuentra impulsando a muchas más organizaciones a considerar de forma urgente el diseño y posterior implementación de estos sistemas para salvaguardar sus activos de información, Por lo tanto, es imprescindible realizar un diseño que evalué e identifiqué las brechas de manera continua. Este sistema debe garantizar que Ejeproy Cía. Ltda. cuente con las medidas necesarias para proteger la información y cumpla con los requisitos regulatorios y normativos vigentes, promoviendo cultura de seguridad.

Palabras clave: Activos de información; confidencialidad; disponibilidad; integridad

Abstract

Ejeproy Cia. Ltda. is a company located in Cuenca-Ecuador. This company is dedicated to create projects in the construction área, at this time their in a great need of a good project to manage their most valuable information of how they develop their activities in construction. Their main source of operation is to handle confidential information that include, financial data, contracts, techniques in construction personal information. Ciber attacks, exposure or lost of data, could affect severly the companies reputation, causing them financial losts in a great scale. It is very important to invention that desing of SGSI that goes under the norm ISO/IEC 27001 and local lays, forces the company to have a major protection control of all their data, so it is very important to have a unique desing that they can implement in the future for posible threats. This system should give the company the proper tools to be protected against ever attack and this way protect every data the have in there possession, and at the some time obeying the law and policies imposed to them as a major company, showing a secure handling of data.

Keywords: Information assets; confidentiality; availability; integrity

DESING OF A SYSTEM FOR SECURITY MANAGEMENT OF INFORMATION (SGSI) BASED ON STANDARDS OF ISO 27001 FOR THE COMPANY EJEPROY CIA. LTDA.

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADA EN EL ESTÁNDAR ISO 27001 PARA LA EMPRESA EJEPROY CIA. LTDA.

Introducción

En un entorno donde los datos actualmente son los activos más valiosos en las empresas, la necesidad en establecer los mecanismos más eficientes y eficaces para la protección de datos muestra una relevancia innegable. Según Oca (2019), en esta era donde todo se encuentra digitalizado la seguridad de la información no solo es una opción de estrategia, sino la necesidad imperante que nos permite garantizar la competitividad y sostenibilidad de las organizaciones. En el mundo informático específicamente en Latinoamérica donde la creciente cantidad de ciberdelincuencia y amenazas cibernéticas como son, ataques a las infraestructuras tecnológicas, robo de datos, manipulación de datos, ciberataques como otras vulnerabilidades se debería exigir de manera oportuna las implementaciones y medidas necesarias que se ajusten y que salvaguarden la integridad, disponibilidad y confidencialidad del activo más importante hoy en día para las empresas la información (Pruna et al., 2020).

Actualmente Ejeproy Cía. Ltda., que se encuentra dentro del sector de la construcción enfrenta grandes desafíos en el contexto donde la gestión de datos, digitalización de los procesos y manejo de información sensible son partes fundamentales en el desarrollo de sus operaciones, desde el manejo de datos de clientes, información financiera, contratos, planos de ejecución de proyectos y obras, la empresa administra un significativo volumen de datos mismo que requieren de una protección rigurosa. Además Paguay (2020), nos indica que el no contar con un enfoque de manera estructurada para tener asegurada la información, la empresa tiene un riesgo significativo de tener pérdidas económicas relevantes, posibles sanciones en el ámbito legal al no tener cumplimiento de las normativas vigentes en Ecuador desde 2021 y la normativa ISO 27001 que obliga a las empresas a tener cultura de seguridad en las organizaciones (Cabezas Mena & Lucas Franco, 2023).

Para poder mitigar los riesgos, según Falcón Huallpa & Martínez Zambrano (2023), la adopción de un SGSI que se encuentre basado en la normativas internacionales y locales da un enfoque de solución estratégica. Como menciona Ramos Pachón et al. (2024), esta normativa internacional ayuda de manera estructurada a gestionar riesgos de seguridad, mismos que establecen políticas, procedimientos y control permitiendo asi la defensa de manera efectiva de la información. Como indica Tandazo Tipan (2022), la funcionalidad de operaciones tiene que estar enmarcada en las directrices establecidas asegurando

efectivamente el resguardo de los datos siendo primordial adoptar este sistema y normativas.

El propósito de este estudio es diseñar un SGSI que este alineado conforme a las exigencias que requiere EJEPROY CIA. LTDA., permitiendo robustecer su posición en seguridad de la información. En este sentido Mera Amores (2022) menciona que en todo esto se tendrá que analizar las vulnerabilidades actuales, se definirán las estrategias y se establecerán controles que se encuentren alineados con la normativa.

La estructura de este documento como menciona Gelvez Araque & Neiva Márquez (2021), está diseñada para proporcionar un análisis de manera integral del proceso de diseño del SGSI. Se realizará una evaluación integral del estado actual de Ejeproy Cía. Ltda., identificando brechas, riesgos y áreas de mejora con las normativas vigentes nacionales e internacionales (Rubio Ganchala & Terán Suárez 2023). Luego se desarrollará una guía de implementación que incluya políticas, procedimientos y controles de seguridad alineados con la normativa internacional y las normativas legales aplicables, asegurando la coherencia con la cultura de seguridad empresarial. Posteriormente según lo indicado por Salazar Lazo & Ávila Correa (2024), se elaborará un informe técnico final con los resultados del diagnóstico, las recomendaciones propuestas y el plan de acción a seguir, proporcionando a la alta dirección datos certeros que serán necesarios para contar con una seguridad de manera integral.

En conclusión, este estudio busca proporcionar una guía clara y estructurada para que EJEPROY CIA. LTDA. pueda fortalecer su seguridad de manera efectiva. La adopción mediante el SGSI no solo permitirá a la empresa cumplir con normativas y estándares internacionales, sino que también la dotará de una ventaja competitiva dentro de un mundo tecnológico exigente en términos de protección de datos y ciberseguridad.

Materiales y métodos

Para el desarrollo del (SGSI) en EJEPROY CIA. LTDA., se empleará un enfoque estructurado compuesto por cinco fases principales.

1.- Fase de Inicio

Definir el Alcance del SGSI

- Identificar las áreas, procesos y activos críticos de Ejeproy que estarán dentro del alcance del SGSI.

- Establecer los límites físicos, organizativos y tecnológicos del sistema.

Consolidar el aval del nivel gerencial.

- Consolidar el respaldo de la alta gerencia a través de una normativa que establezca la protección de los datos.
- Asignar recursos necesarios (tiempo, personal y presupuesto).

Formar el Equipo del SGSI

- Designar un líder del proyecto y formar un equipo multidisciplinario responsable de la implementación y gestión.

2.- Fase de Evaluación

Realizar una Evaluación de Madurez Inicial

- Evaluar la situación actual en procesos de seguridad de manera general en EJEPROY.

Reconocer y catalogar activos de información.

- Crear un inventario con activos de información (hardware, software, datos, personal, etc.).
- Establecer la importancia de cada activo para los procesos del negocio.

Realizar un Análisis de Riesgos

- Analizar los riesgos usando una metodología adecuada (por ejemplo, OCTAVE, MAGERIT o ISO 27001).
- Identificar amenazas, vulnerabilidades e impacto de los riesgos en activos.

3.- Fase de Planificación

Establecer un Tratamiento de Riesgos

- Diseñar un plan para tratar los riesgos (evitar, transferir, mitigar o aceptar).
- Priorizar las medidas basadas en el control y evaluación de riesgos.

Definir Políticas y Procedimientos en Seguridad

- Documentar las políticas de seguridad alineadas con los objetivos estratégicos de EJEPROY.
- Crear procedimientos para la tramites de incidentes, continuidad y control de acceso.

4.- Fase de Implementación

Implementar medidas de protección.

- Aplicar medidas de protección por medio de la normativa ISO 27001 y anexo A mediante planes y tratamiento de eventos y riesgos.

- Establecer herramientas tecnológicas para proteger la información (firewalls, encriptación, etc.).

Capacitar al Personal

- Sensibilizar y capacitar a los usuarios sobre la importancia de tener una cultura general de seguridad.
- Asegurarse de que entiendan y se cumplan las políticas y procedimientos establecidos.

5.- Fase de Monitoreo

Gestionar Incidentes de Seguridad

- Establecer un procedimiento para el manejo de incidentes que permita detectar, abordar y prevenir futuras vulnerabilidades ante situaciones críticas.

Desarrollo

Conceptos relacionados

Confidencialidad: La confidencialidad significa que los datos de las empresas u organizaciones se encuentren de manera privada o secreta (Lorenzo, 2023). Mediante esto se puede impedir que los datos sean intercambiados, ya sea esto de una manera accidental o de una manera intencional y así asegurarse que la información que se envía llegue de manera íntegra sin ser modificada a su destino final, es decir igual a la que fue enviada (Guaña Moya, 2023). La clave para que la información sea confidencial es estar netamente seguros que personal no autorizado o que no tenga permisos tengan acceso a la información de la organización (Coronel Suárez et al., 2022).

Integridad: Nos asegura que nuestros datos se encuentren completos, precisos y sin modificaciones indebidas durante su almacenamiento, de tal manera que realmente sean confiables en su procesamiento y transmisión (Utrilla, 2020). Toda modificación indebida de los registros puede comprometer su confiabilidad y generar errores operativos.

Disponibilidad: La disponibilidad es la que garantiza que la información y sistemas se encuentren con todos los accesos que lo requieran las 24 horas del día. Este principio es crucial para tener continuidad en el negocio. Los fallos en la disponibilidad pueden afectar la operatividad y continuidad de una empresa (Sánchez & Ureta, s. f.).

Activos de información: Son recursos que las empresas utilizan para almacenar, procesar y transmitir datos valiosos. Los mismos pueden ser el hardware, software, propiedad intelectual, bases de datos, documentos físicos y el conocimiento personal. La gestión de

manera adecuada de estos activos es crucial para el aseguramiento de los datos y la prevención de vulnerabilidades. (Macias et al., 2023).

Gestión de riesgos: El manejo de riesgos sigue un procedimiento estructurado que permite reconocer, analizar y reducir amenazas que pueden comprometer directamente la privacidad, exactitud y accesibilidad de la información (Contreras Olea, 2022).

Norma ISO/IEC 27001: Determina las directrices para el desarrollo del SGSI, mediante su enfoque permite a las empresas identificar los riesgos, tener controles y políticas garantizando el avance y mejora (Brito Perez & Francisco Ferreras, 2022).

Cultura de seguridad: Implementar programas de capacitación continúa fomentando las buenas prácticas como son el reconocimiento de correo electrónico fraudulente, el uso de contraseñas seguras, y el manejo responsable de información sensible entre otras buenas prácticas que se manejen dentro de las empresas (Marchand Niño, 2020).

Trabajos relacionados

(Isaza Giraldo, 2023), realizó un SGSI para esal asociación esperanza viva (ASESVI), como resultado de la ausencia de un modelo de seguridad y la deficiencia en el resguardo de la información se debe realizar un tratamiento de los datos, mismos que se encuentran usados de manera inadecuada. También la falta de políticas y cultura de seguridad que hacen que se encuentren mucho más expuestos ante eventos adversos como la ciberdelincuencia. La falta de estas medidas de seguridad hace que esta empresa se encuentre vulnerable las cuales podrían tener consecuencias legales.

(Busto Pérez de Mendiguren, 2024), presenta el modelado y ejecución vigente con normativa ISO, dentro de la corporación TRADUX destacando que los objetivos de este negocio son la triada CIA. La seguridad de datos sensibles en las empresas son aspectos críticos ya que la omisión de esta puede derivar en consecuencias legales, financieras y operativas graves las cuales pueden desencadenar y comprometer la continuidad del negocio. En este contexto, las empresas enfrentan el desafío de contar con una seguridad efectiva de los datos identificando riesgos asociados y así poder gestionarlos de manera efectiva eficiente y sostenible. Como respuesta ante estas necesidades se diseña e implementa el SGSI obteniendo como resultado una buena estructura de políticas asegurando los principales activos de la empresa, la posterior auditoría realizada al final de la implementación que consigue mejorar de manera significativa el estado inicial en el que se encontró la empresa, creando un plan de formación y tratamiento riguroso de la

información en los empleados y que debe estar enmarcada en normativas internacionales vigentes.

(Banda Yánez & Morejón Armijo, 2022), desarrolla un sistema de SGSI para la agrupación Marista con sede en Ecuador, misma que enfrenta el requerimiento para adoptar estrategias y herramientas que sean efectivas para poder cuidar los datos y sus sistemas, en los cuales se incluye información con datos personales y de finanzas de sus empelados como también de centros educativos que están dentro de la organización a escala nacional. Actualmente no disponen de un sistema y peor aún con un área especializada en el monitoreo y gestión para garantizarla privacidad y seguridad de la información, también carece de capacitación para su personal y capacitaciones en políticas de seguridad de datos. El primer paso antes de poder realizar una interacción se inicia con un análisis de la estructura y situación actual de seguridad, realizando auditorias con inspecciones establecidos en la normativa ISO y utilizando la metodología de brechas GAP, en la cual esta técnica permite evaluar a la norma. Los resultados que se obtienen muestran brechas de seguridad existentes y a partir de esto se define acciones y estrategias que garanticen de manera efectiva una integración del SGSI.

(Limones Zambrano & Peralta Peralta, 2023), desarrolla una investigación y una comparativa de normativas entre Ecuador y Uruguay. En ecuador es imperante que se tenga activa y en vigencia dicha ley para que se regule tanto a instituciones nacionales como extranjeras que conservan y tratan datos personales. La normativa en Ecuador está vigente desde el año 2021 en el registro oficial N.459, esto como un derecho constitucional dentro del Ecuador. La ley ecuatoriana plantea a futuro en 2 años específicamente implementar medidas técnicas y jurídicas en el ámbito público y privado, de esta manera encaminar a las organizaciones a salvaguardar los datos personales de toda la población.

(Guzmán Calderón, 2021), desarrolla un trabajo de seguridad en una empresa que ofrece servicios de control eléctricos para vigilancia y obtención de información en el sector petrolero e industrial. Siempre con la visión de mejorar y mitigar frente a eventos de seguridad. Este diseño tiene una vital importancia dada la relevancia del sistema, se trabaja con marcos de referencia como es el NIST y el COBIT 2019, estos permiten controlar y gestionar de mejor manera los datos. Se detecta tras un análisis inicial que la organización es altamente vulnerable ante eventos de seguridad y respuesta ante eventos adversos son prácticamente nulos que en caso de consumarse el fallo en la seguridad se

puede afectar gravemente el cumplimiento de los servicios a los clientes y afectar la operatividad y continuidad del negocio.

(Ventura Rios & Varona Pérez, 2023), desarrollan un diseño de seguridad para Arfusog empresa dedicada a recolectar desechos sólidos no aprovechables a través de rutas preestablecidas, en esta empresa se puede recalcar la falta de un SGSI teniendo en cuenta que desde la alta dirección se pretende proteger la información de una manera íntegra y segura. Dada la importancia de este sistema se contará con responsables para salvaguardar los activos de la empresa de una manera oportuna ante un evento adverso. Después del trabajo realizado se encuentra que casi el 90% de los empleados desconocen de la seguridad de los datos y peor aún de conocimiento de las normas que rigen en estos sistemas de seguridad. Luego de la aplicación del diagrama de Pareto se identifica falta de conocimiento de la normativa local vigente e internacional debido a la inexistencia de una matriz de riesgos y la mayoría de personal maneja de manera empírica la seguridad de los datos. Después de este análisis se establece reglamentos y metodologías para controlar la disponibilidad de los recursos informáticos de la organización y se lo haga de una manera controlada quedado establecidos los riesgos y con la normativa internacional vigente ISO 27001.

(Lopez Aguirre, 2022), desarrolla el trabajo de titulación para ingeniero de sistemas diseñando un sistema de seguridad en una empresa constructora llamada Málaga, la misma que tiene dentro de sus activos información datos críticos propios y de clientes. Con este trabajo se identificará los potenciales riesgos para la organización como amenazas y vulnerabilidades en manejo de datos. Posterior a la ejecución ISMS que sirve para supervisar y blindar la información como indica la norma ISO dependiendo de tres fases vitales para tener formalizados los objetivos de manera inequívoca como son: apertura de la información, la clasificación y la decencia. Estando ya asegurados con las normativas correspondientes se tiene a todo el personal preparado y capacitado ante peligros y riesgos inminentes que se pueden dar dentro de la empresa, teniendo que ejecutarse en caso de que surja un evento de seguridad o ataque, debe ejecutarse los procesos y políticas preestablecidos en estos eventos para seguridad de toda la empresa y de cada área haciendo posible la recuperación inmediata y en el menor tiempo posible para no ocasionar perdidas que puedan afectar el correcto desarrollo de la misma.

(Avila Torres & Cuenca Tapia, 2021), desarrollan este estudio analizando los riesgos en EMAPAL-EP, utilizando la metodología MAGERIT 3.0 para detectar amenazas y reducir vulnerabilidades en su infraestructura. La investigación resalta la importancia de tener

medidas adecuadas para prevenir incidentes que puedan comprometer las operaciones. Este proceso esta desarrollado en 5 etapas claves y a partir de esos resultados se diseña un plan de acción que busca fortalecer la seguridad y minimizar las amenazas dando continuidad a los procesos operativos. La aplicación de MAGERIT en la organización permite gestionar los riesgos mediante estándares internacionales facilitando la toma de decisiones estratégicas para la protección de sus datos.

Resultados y discusión

Ejeproy Cía. Ltda. es una organización radicada en Cuenca-Ecuador, opera en el sector de la construcción y están establecidos desde el 03 de octubre del año 2003 como una empresa de ejecución en ingeniería y como empresa consultora de proyectos. Su experiencia en este mercado le ha permitido abarcar una amplia gama en proyectos de construcción como actividad principal, desde urbanizaciones modernas, edificios funcionales e institucionales, naves industriales y bodegas, transformando en realidad las ideas propuestas. Cuenta con un equipo de especialistas altamente calificados con gran trayectoria en la industria y demás áreas afines como es la gestión, ingeniería de diseño, fiscalización, planificación y construcción de infraestructuras en general.

Este trabajo tiene como finalidad diseñar un SGSI a través de los siguientes aspectos.

1) Alcance y contexto del SGSI, define la aplicabilidad y los límites del sistema dentro de la organización como identifica los activos y áreas que tendrán la cobertura del SGSI.
2) La alta dirección tendrá el compromiso de establecer políticas de seguridad, invertir en recursos tecnológicos, humanos y financieros.
3) Evaluar e identificar los riesgos para detectar las posibles vulnerabilidades y amenazas que podrían afectar a la organización.
4) Implementación de regulaciones y salvaguardas de protección, estos lineamientos establecidos son los que garantizaran que la organización pueda tener continuidad del negocio ante incidentes adversos.
5) Capacitación y concientización del personal, el factor humano es esencial en toda organización de esta manera se garantiza que los empleados estén capacitados y comprometidos garantizando así el correcto funcionamiento del sistema.

Este diseño fue desarrollado siguiendo una estructura técnica y académica basada en la LOPDP vigente en territorio ecuatoriano y la normativa ISO/IEC 27001:2022,

desarrollándose bajo un enfoque metodológico de manera estructurada considerando el impactó de la seguridad informática en Ejeproy Cía. Ltda.

Fase de inicio

Definir alcance del SGSI

Se definen a continuación los procesos, áreas y activos críticos de Ejeproy Cía. Ltda.

Administración-Finanzas:

Nóminas y gestión contable de la empresa, procesamiento de datos financieros, información y documentación bancaria, pagos a proveedores, pagos a personal, recepción de pagos de clientes y facturación.

Proyectos:

Manejo de información en monitoreo y ejecución de obras, planificación incluyendo planos, costos y cronogramas en la ejecución de proyectos.

Recursos Humanos:

Almacenamiento de datos personales de empleados, cumplimiento en normativas laborales, evaluación del desempeño y contratación del personal.

Atención a clientes:

Manejo de información contractual especificaciones de carácter técnico y comunicación con clientes, detalles de proyectos.

Logística y Proveedores:

Coordinación de materiales, insumos y contratistas, este proceso incluye registro de proveedores, inventarios y gestión de órdenes de compra.

Áreas críticas

Oficinas administrativas:

En este espacio se procesan contratos, registros laborales, documentación financiera los cuales requieren acceso controlado a la información y medidas de protección para archivos digitales y físicos.

Centro de datos y servidores:

Infraestructura donde se almacenan servidores, bases de datos, dispositivos y equipos de comunicaciones, dispositivos de respaldo, monitoreo y políticas de acceso restringido.

Departamento de ingeniería y diseño de proyectos:

Departamento donde se diseñan y manejan planos y modelos estructurales de los proyectos a realizarse o en ejecución.

Compras y logística:

Controles de distribución e inventario de materiales que son utilizados en los proyectos de construcción.

Gerencia:

La gerencia realiza evaluaciones del desempeño y manejo del personal, presupuestos, análisis de costos para los proyectos a desarrollarse, planes estratégicos, financieros, reportes de estándares de calidad y normativas legales de cumplimiento.

Presidencia:

Es el nivel más alto dentro de la estructura organizativa y es la que responde a la dirección general de toda la empresa, con información sensible como análisis e inversiones de viabilidad financiera, acuerdos y contratos con socios estratégicos y clientes.

Activos críticos de la información

Activos digitales:

- Bases de datos contables y financieras.
- Documentación y contratos electrónicos.
- Diseños y planos almacenados en ordenadores.
- Software ERP y gestión de proyectos.
- Comunicación interna y correos electrónicos del dominio ejeproy.com

Activos físicos:

- Infraestructura de sistemas de comunicación y redes.
- Controles de vigilancia y acceso físico en oficinas.
- Servidores, computadores y dispositivos de almacenamiento de información.
- Documentación impresa de proyectos y contratos.

Activos Humanos:

- Contratistas y proveedores que tienen acceso a datos.
- Colaboradores con privilegios sobre información sensible.
- Usuarios que tengan privilegios administrativos sobre redes y sistemas.
- Usuarios con acceso, manejo de redes y sitio web.

Compromiso de la alta dirección

El éxito que tenga el SGSI en la empresa EJPROY CIA. LTDA. depende en gran escala del liderazgo y compromiso que tenga la alta dirección, garantizando de esta manera que la integración del SGSI esté dentro de la estrategia de la empresa con las siguientes políticas.

Dirección y respaldo estratégico:

- Serán aprobadas las políticas que estén aplicadas en toda la estructura organizativa de la empresa.
- Serán alineados los objetivos estratégicos del SGSI con toda la organización asegurando de esta manera la integración de cada uno y de todos los procesos que se involucran dentro de este sistema.

Asignación de los recursos.

- Destinar de manera íntegra los recursos necesarios como son financiero, tecnológicos y humanos para el correcto funcionamiento del sistema.
- Implementar soluciones y herramientas tecnológicas para reforzar el monitoreo de amenazas, control de accesos, cifrado de datos que refuercen la seguridad pudiendo ser la implementación de dispositivos de firewall y de seguridad perimetral con los que actualmente no cuenta la empresa.

Cumplimiento normativo legal vigente.

- Establecer el marco de gestión de los riesgos asegurando de esta manera que se implementen los controles necesarios para reducir las vulnerabilidades existentes.
- Tener garantizado y regulados los estándares que rigen en la actualidad el desarrollo de un SGSI.

Cultura de seguridad.

- Tener implementados canales de comunicación para gestionar de manera inmediata eventos adversos que puedan presentarse.
- Promover cultura de seguridad en cada departamento.

Supervisión y mejora continua.

- Aplicando ajustes de mejoras basadas en incidentes y auditorias.
- Actualizándose al entorno tecnológico y normativo con las políticas y controles en caso de tener cambios en los mismos.

Formación del equipo SGSI

Responsable del SGSI: Actividades en el rol del responsable dirigir y mantener el sistema.

Tabla 1

Cuadro del equipo responsable del SGSI en Ejeproy. Cía. Ltda.

ELEMENTO	AREA CORRESPONDIENTE
Líder del proyecto.	Dirección de seguridad de la información/Gestión de proyectos.
Comité de seguridad.	Seguridad de la información/Auditoria y cumplimiento.
Gestión de riesgos.	Departamento de seguridad de la información/Gestión corporativa de riesgos.
Infraestructura y seguridad tecnológica.	Departamento de TI /Operaciones tecnológicas
Cumplimiento legal.	Departamento Legal/ Seguridad de la información y cumplimiento normativo.
Concienciación y capacitación.	Recursos humanos/Seguridad de la información.

Fuente: fuente propia.

Fase de evaluación.

Realizar evaluación de madurez inicial.

Tabla 2

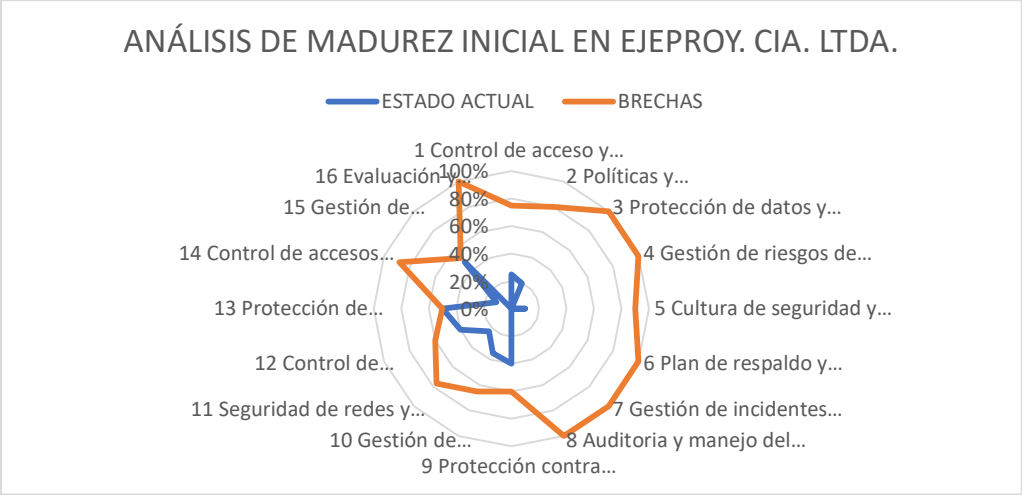
Niveles de controles de madurez Ejeproy Cía. Ltda.

ID	PROCESOS	ESTADO ACTUAL	BRECHAS
1	Control de acceso y gestión de identidades	25%	75%
2	Políticas y procedimientos de seguridad	20%	80%
3	Protección de datos y gestión de información sensible	0%	100%
4	Gestión de riesgos de seguridad de la información	0%	100%
5	Cultura de seguridad y capacitación del personal.	10%	90%
6	Plan de respaldo y recuperación ante desastres	0%	100%
7	Gestión de incidentes de seguridad	0%	100%
8	Auditoria y manejo del SGSI	0%	100%
9	Protección contra software malicioso (malware)	40%	60%
10	Gestión de incidentes de seguridad	35%	65%
11	Seguridad de redes y comunicaciones	23%	77%
12	Control de dispositivos y almacenamiento de extraíbles	40%	60%
13	Protección de infraestructura tecnológica	50%	50%
14	Control de accesos fijos	12%	88%
15	Gestión de proveedores y terceros	48%	52%
16	Evaluación y cumplimiento normativo	0%	100%

Fuente: fuente propia.

Figura 1

Grafica radial del análisis de madurez Ejeproy Cía. Ltda.



Fuente: fuente propia.

Análisis de procedimientos y políticas de seguridad.

- Ejeproy no tiene políticas básicas de seguridad, tampoco están formalmente documentadas ni con marco estructurado con normativa.
- En Ejeproy no cuenta con responsabilidades ni roles definidos en seguridad.

Control de acceso y gestión de identidades.

- Se cuenta con controles de acceso básicos, pero no se tiene una gestión de manera robusta de privilegios y usuarios.
- Para el acceso a sistemas críticos no se realiza la autenticación multifactorial.

Protección de datos y gestión de información sensible.

- En la situación actual no se tiene implementado las técnicas de cifrado en la protección de los datos que son sensibles y se encuentran en reposo o en tránsito.
- El almacenamiento de la información se encuentra en dispositivos sin medidas de seguridad robustas.

Gestión de riesgos de seguridad.

- No se tiene registros de amenazas y vulnerabilidades en los activos informáticos.
- No existe planificación de tratamiento de riesgos ni medidas de mitigación que estén documentadas.

Recuperación y respaldo ante desastres.

- No se cuenta con redundancia para respaldo de datos de servidores críticos ni almacenamiento en la nube.

- No se tiene ningún programa de restauración de datos en caso de ocurrir algún incidente.

Capacitación y cultura de seguridad del personal.

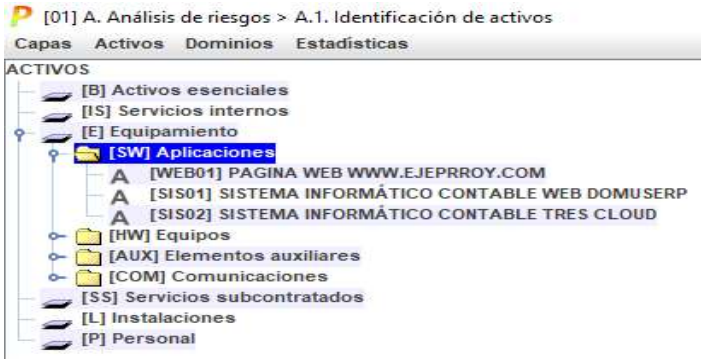
- Se han realizado capacitaciones básicas y concienciación sobre posibles ataques como malware, ransomware, phishing entre otras amenazas cibernéticas.
- Los empleados no están familiarizados con políticas de seguridad y manejo de información confidencial.

Identificar activos de la información.

En este proceso se identifican todos los activos con los que cuenta la empresa.

Figura 2

Identificación de activos



Fuente: fuente PilarBasic

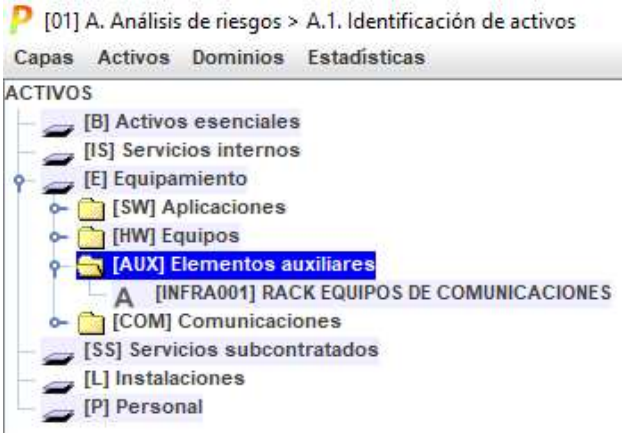
Figura 3

Identificación de activos

Fuente: fuente PilarBasic

Figura 4

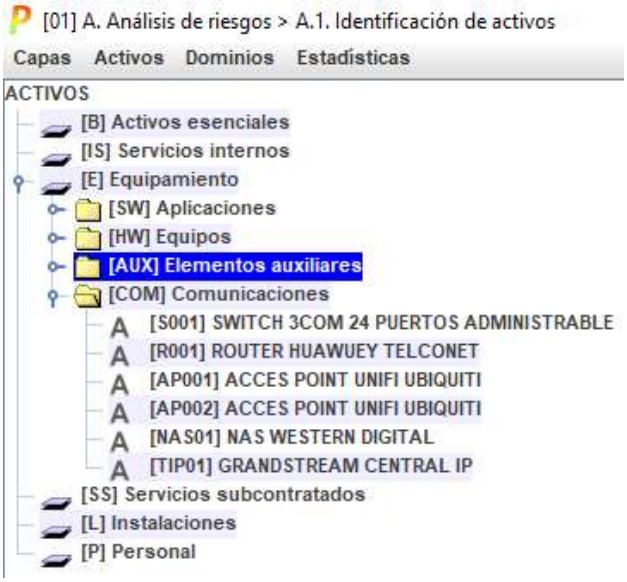
Identificación de activos



Fuente: fuente PilarBasic

Figura 5

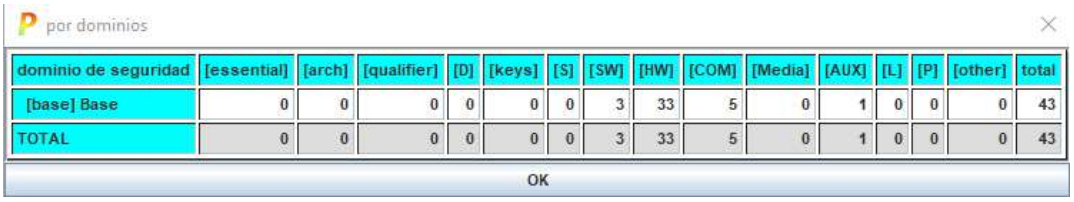
Identificación de activos



Fuente: fuente PilarBasic

Figura 6

Identificación de activos



dominio de seguridad	[essential]	[arch]	[qualifier]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[other]	total
[base] Base	0	0	0	0	0	0	3	33	5	0	1	0	0	0	43
TOTAL	0	0	0	0	0	0	3	33	5	0	1	0	0	0	43

Fuente: fuente PilarBasic

Realizar análisis de los riesgos.

En Ejeproy. Cía. Ltda., se realiza un estudio de riesgos evidenciando que la empresa enfrenta altos riesgos como accesos no autorizados, robo o perdida de información, ataques de malware o ransomware, errores humanos, fallas en infraestructura, incumplimiento normativo, phishing y suplantación, fugas de información. Para reducir estas vulnerabilidades es primordial fortalecer los controles de seguridad.

Tabla 3

Análisis de riesgos Ejeproy Cía. Ltda. Basado en ISO/IEC 27001

ANÁLISIS DE RIESGOS EJEPROY CIA. LTDA. BASADO EN ISO/IEC 27001

ACTIVO DE LA INFORMACIÓN	AMENAZA	PROBABILIDAD (1-5)	IMPACTO (1-5)	CALCULO DEL RIESGO (P * I)	NIVEL DEL RIESGO
INFORMACIÓN FINANCIERA Y CONTABLE	ACCESO NO AUTORIZADO	4	5	20	CRITICO
INFORMACIÓN FINANCIERA Y CONTABLE	ROBO O PERDIDA DE INFORMACIÓN	3	4	12	ALTO
INFORMACIÓN FINANCIERA Y CONTABLE	ATAQUES DE MALWARE	5	5	25	CRITICO
DATOS PERSONALES DE EMPLEADOS Y CLIENTES	ACCESO NO AUTORIZADO	5	4	20	CRITICO
DATOS PERSONALES DE EMPLEADOS Y CLIENTES	PHISHING Y SUPLANTACIÓN	5	5	25	CRITICO
PLANOS Y DOCUMENTOS DE PROYECTOS	FUGAS DE DATOS POR TERCEROS	2	3	6	MEDIO
PLANOS Y DOCUMENTOS DE PROYECTOS	ROBOS DE INFORMACIÓN	3	4	12	ALTO
INFRAESTRUCTURA TECNOLOGICA REDES Y SERVIDORES	ATAQUE DE MALWARE	5	5	25	CRITICO
INFRAESTRUCTURA TECNOLOGICA REDES Y SERVIDORES	FALLAS DE INFRAESTRUCTURA	4	4	16	CRITICO
SISTEMAS DE GESTION DOMUSERP Y TRES CLOUD	INCUMPLIMIENTO NORMATIVO	3	5	15	CRITICO
SISTEMAS DE GESTION DOMUSERP Y TRES CLOUD	ERRORES HUMANOS	4	3	12	ALTO
CORREOS ELECTRÓNICOS CORPORATIVOS	PHISHING Y SUPLANTACIÓN	4	3	12	ALTO
CORREOS ELECTRÓNICOS CORPORATIVOS	ROBO DE INFORMACIÓN	3	4	12	ALTO
PROVEEDORES CON ACCESO A DATOS	FUGAS DE INFORMACIÓN	3	4	12	ALTO
PROVEEDORES CON ACCESO A DATOS	CUMPLIMIENTO NORMATIVO	3	5	15	CRITICO
REGISTROS DE ACCESO FISICOS Y LOGICOS	ACCESO NO AUTORIZADO	3	3	9	MEDIO
REGISTROS DE ACCESO FISICOS Y LOGICOS	ROBO DE CREDENCIALES	4	4	16	CRITICO

Fuente: fuente propia.

RIESGO= PROBABILIDAD X IMPACTO

Tabla 4

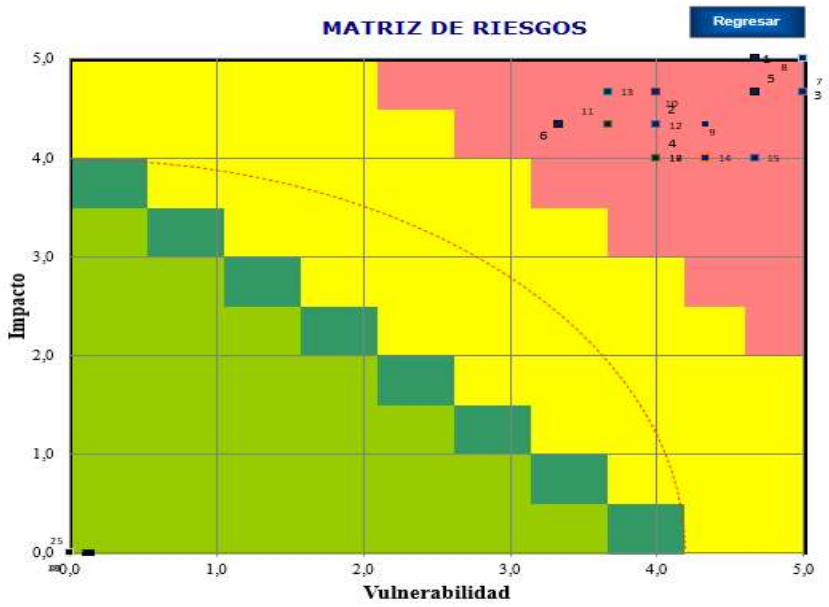
Tabla de análisis de riesgos ISO/IEC 27001

RIESGOS	NIVEL	MEDIDAS APLICAR
RIESGO CRITICO	15-25	IMPLEMENTAR CONTROLES INMEDITAS, AUTENTICACIÓN MULTIFACTOR, AUDITORIAS
RIESGO ALTO	10-14	APLICAR MEDIDAS CORRECTIVAS URGENTES, POLITICAS DE ACCESO, MONITOREO CONTINUO
RIESGO MEDIO	5-9	MITIGAR CON PILITICAS DE SEGURIDAD Y CAPACITACION AL PERSONAL
RIESGO BAJO	1-4	CONTROLAR Y MONITOREAR SIN ACCIONES URGENTES

Fuente: fuente propia.

Figura 7

Matriz de riesgos Ejeproy Cía. Ltda.



Fuente: fuente propia.

Fase de planificación.

Tabla 5

Establecer tratamiento de los riesgos en Ejeproy Cía. Ltda.

Activo de información	Amenaza	Cálculo del riesgo	Nivel del riesgo	Tratamiento del riesgo
Información financiera y contable	Acceso no autorizado	20	CRITICO	Mitigar (Implementar controles de acceso y monitoreo en tiempo real)
Información financiera y contable	Robo o perdida de información	12	ALTO	Reducir (Aplicar cifrado de datos y copias de seguridad)
Información financiera y contable	Ataques de malware o rasomware	25	CRITICO	Mitigar (Antivirus avanzado y segmentación de red)
Datos personales de empleados y clientes	Acceso no autorizado	20	CRITICO	Mitigar (Autenticación multifactor y control de privilegios)
Datos personales de empleados y clientes	Phishing y suplantación	25	CRITICO	Mitigar (Capacitación en ciberseguridad y simulaciones de ataques)
Planos y documentos de proyectos	Fuga de datos por terceros	6	MEDIO	Transferir (Implementar acuerdos de confidencialidad y control de accesos)
Planos y documentos de proyectos	Robo de información	12	ALTO	Reducir (Establecer control de accesos y cifrado de documentos)
Infraestructura tecnológica redes y servidores	Ataque de malware	25	CRITICO	Mitigar (Firewall, segmentación de red y monitoreo constante)
Infraestructura tecnológica redes y servidores	Fallas en infraestructura	16	CRITICO	Mitigar (Implementar redundancia y respaldo automatizado)

Fuente: fuente propia.

Tabla 6

Establecer tratamiento de los riesgos en Ejeproy Cía. Ltda.

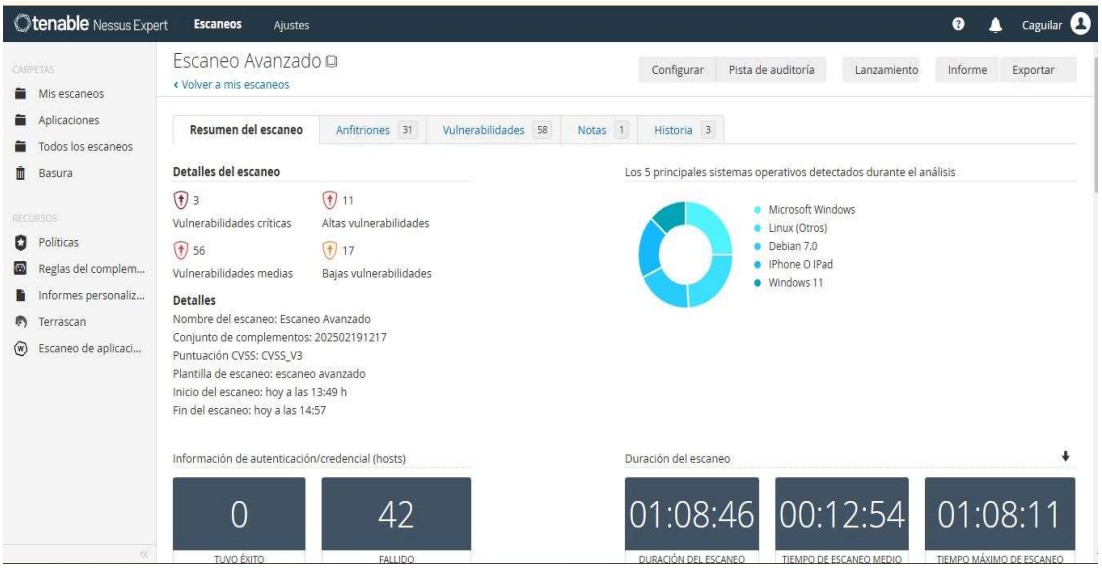
Sistemas de gestión domuserp y tres cloud	Incumplimiento normativo	15	CRITICO	Mitigar (Alinear políticas con ISO 27001 y ley de protección de datos personales)
Sistemas de gestión domuserp y tres cloud	Phishing y suplantación	12	ALTO	Reducir (Aplicar autenticación multifactor y monitoreo de accesos)
Correos electrónicos corporativos	Phishing y suplantación	12	ALTO	Reducir (Filtros antispam y capacitación en seguridad)
Correos electrónicos corporativos	Robo de información	12	ALTO	Reducir (Monitoreo de correos y uso de cifrado)
Proveedores con acceso a datos	Fugas de información	12	ALTO	Reducir (Establecer acuerdos de seguridad en contratos)
Proveedores con acceso a datos	Incumplimiento normativo	15	CRITICO	Mitigar (Revisar contratos y exigir cumplimiento normativo)
Registros de accesos físicos y lógicos	Acceso no autorizado	9	MEDIO	Transferir (Control Biométrico y auditorias de accesos)
Registros de accesos físicos y lógicos	Robo de credenciales	16	CRITICO	Mitigar (Monitoreo continuo y doble autenticación)

Fuente: fuente propia.

En este plan de establecimiento de los riesgos permite a Ejeproy cumplir con las normativas locales e internacionales vigentes mitigando y priorizando las amenazas críticas.

Figura 8

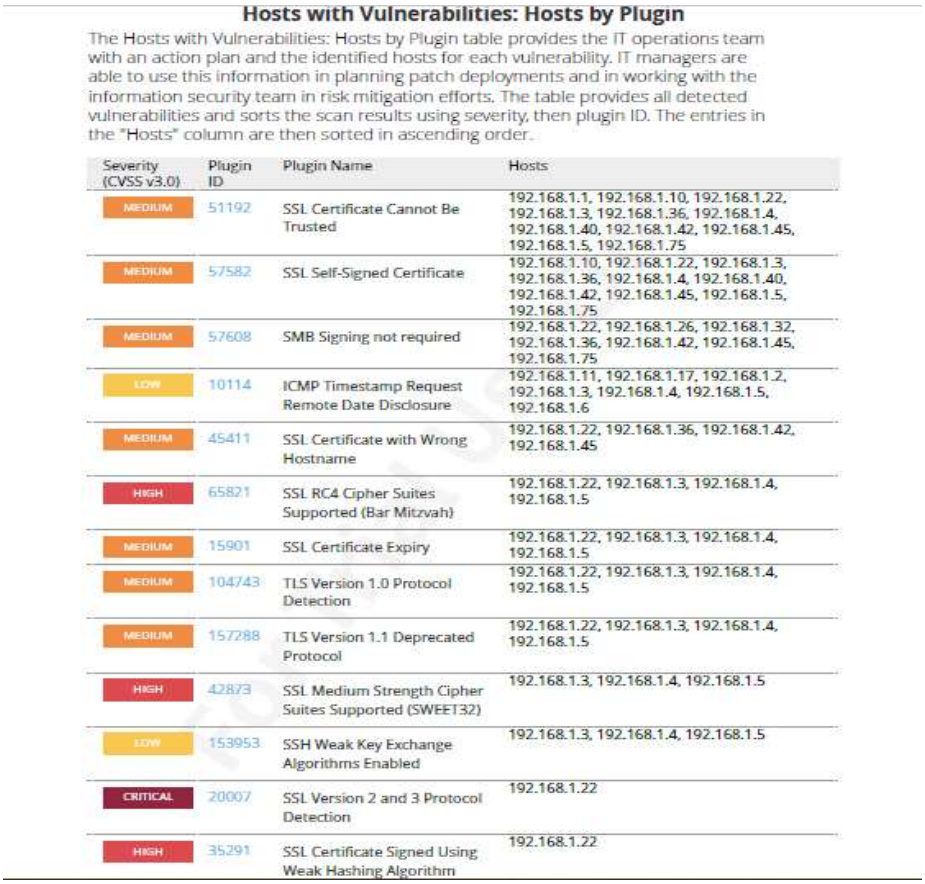
Análisis de vulnerabilidades real realizado en la empresa Ejeproy. Cía. Ltda. con la herramienta Tenable Nessus.



Fuente: Tenable Nessus

Figura 9

Análisis de vulnerabilidades por host



Hosts with Vulnerabilities: Hosts by Plugin

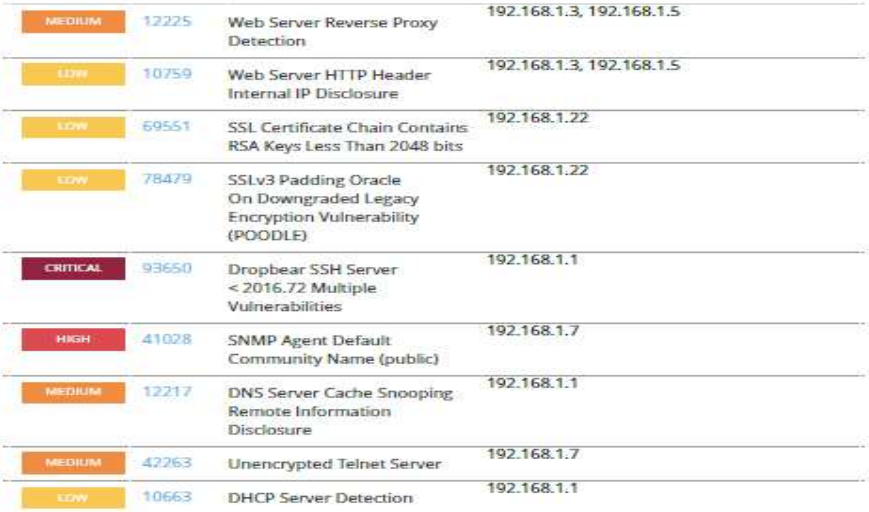
The Hosts with Vulnerabilities: Hosts by Plugin table provides the IT operations team with an action plan and the identified hosts for each vulnerability. IT managers are able to use this information in planning patch deployments and in working with the information security team in risk mitigation efforts. The table provides all detected vulnerabilities and sorts the scan results using severity, then plugin ID. The entries in the "Hosts" column are then sorted in ascending order.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Hosts
MEDIUM	51192	SSL Certificate Cannot Be Trusted	192.168.1.1, 192.168.1.10, 192.168.1.22, 192.168.1.3, 192.168.1.36, 192.168.1.4, 192.168.1.40, 192.168.1.42, 192.168.1.45, 192.168.1.5, 192.168.1.75
MEDIUM	57582	SSL Self-Signed Certificate	192.168.1.10, 192.168.1.22, 192.168.1.3, 192.168.1.36, 192.168.1.4, 192.168.1.40, 192.168.1.42, 192.168.1.45, 192.168.1.5, 192.168.1.75
MEDIUM	57608	SMB Signing not required	192.168.1.22, 192.168.1.26, 192.168.1.32, 192.168.1.36, 192.168.1.42, 192.168.1.45, 192.168.1.75
LOW	10114	ICMP Timestamp Request Remote Date Disclosure	192.168.1.11, 192.168.1.17, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.6
MEDIUM	45411	SSL Certificate with Wrong Hostname	192.168.1.22, 192.168.1.36, 192.168.1.42, 192.168.1.45
HIGH	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	192.168.1.22, 192.168.1.3, 192.168.1.4, 192.168.1.5
MEDIUM	15901	SSL Certificate Expiry	192.168.1.22, 192.168.1.3, 192.168.1.4, 192.168.1.5
MEDIUM	104743	TLS Version 1.0 Protocol Detection	192.168.1.22, 192.168.1.3, 192.168.1.4, 192.168.1.5
MEDIUM	157288	TLS Version 1.1 Deprecated Protocol	192.168.1.22, 192.168.1.3, 192.168.1.4, 192.168.1.5
HIGH	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	192.168.1.3, 192.168.1.4, 192.168.1.5
LOW	153953	SSH Weak Key Exchange Algorithms Enabled	192.168.1.3, 192.168.1.4, 192.168.1.5
CRITICAL	20007	SSL Version 2 and 3 Protocol Detection	192.168.1.22
HIGH	35291	SSL Certificate Signed Using Weak Hashing Algorithm	192.168.1.22

Fuente: Tenable Nessus

Figura 10

Análisis de vulnerabilidades por host



MEDIUM	12225	Web Server Reverse Proxy Detection	192.168.1.3, 192.168.1.5
LOW	10759	Web Server HTTP Header Internal IP Disclosure	192.168.1.3, 192.168.1.5
LOW	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	192.168.1.22
LOW	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	192.168.1.22
CRITICAL	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	192.168.1.1
HIGH	41028	SNMP Agent Default Community Name (public)	192.168.1.7
MEDIUM	12217	DNS Server Cache Snooping Remote Information Disclosure	192.168.1.1
MEDIUM	42263	Unencrypted Telnet Server	192.168.1.7
LOW	10663	DHCP Server Detection	192.168.1.1

Fuente: Tenable Nessus

Definir políticas de seguridad.

Política 1: Política de seguridad.

- Solamente el personal autorizado puede tener acceso a la información crítica de la empresa.
- En accesos a sistemas sensibles se debe aplicar autenticación multifactorial (MFA) a todo el personal que tenga permisos de acceso a estos sistemas.
- La información debe ser protegida y clasificada según el nivel de sensibilidad que tenga.

Política 2: Seguridad de datos sensibles.

- De ser el caso se garantizará la modificación y supresión de información confidencial de trabajadores, usuarios y aliados comerciales en derecho fundamental.
- Todos los datos personales que maneja Ejeproy deben ser almacenados de manera segura y cifrada.
- Antes de recolectar datos personales de cualquier persona o empleado la empresa debe obtener el consentimiento explícito de cada persona para el tratamiento de sus datos.

Política 3: Política de control de accesos.

- Se gestionará accesos a los sistemas solo a través de roles y privilegios definidos concedidos a cada usuario por departamento.
- Se deberá aplicar autenticación multifactorial (MFA) en los accesos a la información sensible.
- Cada 6 meses se revisarán los accesos concedidos a cada usuario para revocar privilegios innecesarios de ser el caso.

Política 4: Recuperación ante eventos adversos.

- Se contará con pruebas constantes de restauración de datos.
- Se realizarán copias cifradas de la información crítica de la empresa.
- De presentarse alguna eventualidad el equipo SGSI definirá los lineamientos a seguir de acuerdo a sus funciones.

Procedimientos

Procedimiento 1: Gestión de incidentes.

1. **Detección:** Reportar de manera inmediata al departamento de TI si se detecta algún tipo de incidente.
2. **Registro:** Se llevará un registro en bitácora documentando el incidente en un sistema de gestión de eventos.
3. **Clasificación:** Se identificará la criticidad y el impacto del incidente.
4. **Respuesta**: Las medidas correctivas se tomarán de manera inmediata para contener el incidente.

Procedimiento 2: Continuidad del negocio.

1. **Análisis de impacto:** Tener identificados los sistemas críticos y el tiempo de recuperación de los mismos
2. **Estrategias de respaldo:** Implementar copias de seguridad con almacenamiento en la nube y copias cifradas de los datos en medios extraíbles.
3. **Plan de respuesta:** En caso de surgir un incidente tener definidas las personas responsables y el plan a ejecutarse.
4. **Pruebas y simulación:** Realizar pruebas de recuperación antes desastres una vez al año.

Procedimiento 3: Procedimiento de control de accesos.

1. **Solicitud de acceso:** Para conceder acceso a un usuario se tendrá que solicitar mediante correo electrónico y con su debida justificación.
2. **Autorización:** Solo mediante autorización de gerencia o responsable de TI se puede aprobar acceso a información sensible.
3. **Implementación:** Según el principio de menor privilegio se asignarán los permisos a los usuarios.
4. **Monitoreo:** Cada seis meses se realizarán auditorias de acceso a los sistemas.

Procedimiento 4: Protección de datos.

1. **Recolección de información**: Al momento de solicitar información personal se solicitará carta de consentimiento explicito.
2. **Almacenamiento seguro:** Los datos serán cifrados y se almacenarán en servidores que tengan control de acceso.
3. **Derechos de los titulares:** Se tendrán mecanismos habilitados para que los clientes puedan tener acceso a consultar, modificar o eliminar sus datos.

4. **Reportes de cumplimiento:** Se generarán reportes sobre el manejo de datos personales anualmente.

Fase implementación.

En Ejeproy Cía. Ltda., se deben tener implementados los controles de seguridad que estén alineados con planes para tratar los riesgos y la normativa ISO/IEC 27001.

Control de seguridad de la normativa ISO según anexo A.

Organizados en 4 categorías que detallaremos a continuación.

Tabla 7

Controles de seguridad según el anexo A

Categoría	Controles principales	Aplicación en Ejeproy. Cía. Ltda.
Controles organizacionales.	Gestión de seguridad de proveedores, gestión de accesos, respuesta ante incidentes.	Aplicación de auditorias periódicas y autenticación multifactorial (MFA)
Controles de personas	Capacitación en concienciación, en seguridad, seguridad en contratación.	Programas de capacitación en simulaciones de phishing y ciberseguridad.
Controles físicos.	Control de seguridad en centro de datos, control en accesos físicos.	Implementación de video vigilancia de áreas críticas y acceso biométrico.
Controles tecnológicos.	Monitoreo de redes, cifrado, firewalls, copias de seguridad.	Aplicación de segmentación de red, cifrado de datos sensibles, firewalls avanzados.

Fuente: fuente propia.

Puesta en marcha de salvaguardas en Ejeproy Cía. Ltda.

Gestión de identidades.

- Aplicación multifactor (MFA) en todos los sistemas que se usan en la empresa.
- Usar registros de las auditorias para detectar y rastrear accesos e intentos sospechosos.

Protección de cifrado y datos.

- Implementación de seguridad TLS/SSL para cifrar los datos en tránsito.
- Restricción mediante token de acceso a datos personales.
- Uso de cifrado AES 256 para protección de datos en reposo.

Protección contra amenazas y seguridad en redes.

- Segmentar la red para tener aisladas las áreas más críticas de la empresa.
- Uso de antivirus avanzados y sistemas de anti malware en todos los equipos.
- Implementación de firewalls de última generación utilizando herramientas de monitoreo y prevención de accesos no autorizados (IDS/IPS)

Gestión en incidentes de seguridad.

- Implementación de una plataforma de monitoreo en tiempo real de SIEM, este sistema interpreta y centraliza datos relevantes de seguridad.
- Establecimiento de un CSIRT como responsable de la administración y resolución de respuesta en eventos de ciberseguridad.
- En caso de tener ciberataques contar con protocolos establecidos de respuesta rápida.

Respaldo y recuperación de datos.

- Realizar pruebas de recuperación de datos cada tres meses.
- Tener redundancia de servidores críticos e implementación de alta disponibilidad (HA).
- Realizar copias de seguridad diarias en entornos de la nube y entornos locales.

Tabla 8

Soluciones tecnológicas para protección de datos en Ejeproy. Cía. Ltda.

Herramientas	Función	Aplicación en Ejeproy. Cía. Ltda.
Cifrado TLS/SSL y AES 256	Protección de datos en tránsito y en reposo)	Aplicado en comunicaciones y bases de datos.
SIEM (Azure centinel, IBM, Splunk.)	Monitoreo de eventos de seguridad en tiempo real	Detectar ataques avanzados y amenazas.
Antivirus (Kaspersky, CrowdStrike, SentinelOne)	Protección contra ransomware, y malware	Detectar y eliminar endpoints y amenazas.
Firewalls (Palo alto, Aruba, Fortinet)	Filtrar el tráfico no autorizado	Protección contra ataques de red.
Back up en la nube (Google cloud, Azure, AWS)	Recuperación de datos y respaldo seguro	Protección ante ciberataques y ante fallos.
Control de acceso (Azure AD, Okta)	Gestión de identidades y autenticación MFA	Seguridad en el acceso a los sistemas.

Fuente: fuente propia.

Capacitar al personal.

Se sensibilizará a los empleados sobre la importancia de proteger de manera íntegra los datos de la empresa, tratando los siguientes temas que se detallaran a continuación:

Módulo 1: Aspectos claves sobre la protección de datos.

- Consecuencias de ataques casos reales.
- Impacto de ciberataques y brechas de seguridad en la empresa.
- Conceptos claves de la triada CIA.

Formato: Videos explicativos y presentación interactiva.

Duración: 1 hora.

Módulo 2: Cumplimiento normativo.

- Medidas obligatorias de seguridad en el tratamiento de información personal.
- Políticas de almacenamiento, recolección y eliminación de información personal.
- Responsabilidades institucionales y garantía para los usuarios sobre sus datos.

Formato: Análisis de los casos mediante talleres prácticos

Duración:2 horas

Módulo 3: Gestión de contraseñas y seguridad en los accesos.

- Protección de dispositivos corporativos y personales contra los accesos no autorizados.
- Uso de autenticación multifactor (MFA)
- Políticas de gestión de accesos y creación de contraseñas seguras.

Formato: Taller interactivo y realizar una evaluación de conocimientos adquiridos.

Duración: 2 horas

Módulo 4: Prevención de ataques cibernéticos y phishing.

- Prácticas seguras de uso documentos digitales y correo corporativo.
- Como actuar en casos de recibir algún intento de phishing.
- Reconocer sitios web maliciosos y correos electrónicos fraudulentos.

Formato: Talleres prácticos mediante simulaciones de ataques.

Duración: 3 horas.

Módulo 5: Plan de respuesta y gestión en incidentes.

- Responsabilidades y roles de los empleados en respuesta ante incidentes.
- Obtener un flujo de reportes de incidentes en Ejeproy Cía. Ltda.
- Que se tiene que hacer en caso de detectar ataques cibernéticos o brechas de seguridad.

Formato: Pruebas de respuesta ante incidentes en un entorno controlado.

Duración: 3 horas.

Seguimiento y evaluaciones del programa de capacitación en Ejeproy Cía. Ltda.

Métodos a evaluar:

- Encuestas para mejorar en futuras capacitaciones mediante la retroalimentación.
- Simulaciones de ataques de phishing para medir la respuesta ante este tipo de incidentes.

- Realizar pruebas de conocimiento al finalizar cada módulo.

Reentrenamiento y monitoreo:

- Análisis de todos los incidentes para realizar mejoras continuas en futuras capacitaciones.
- Cada seis meses se tendrá que realizar un reentrenamiento obligatorio en temas de seguridad cibernética.
- Enviar reportes de capacitación y cumplimiento a la alta dirección.

Fase de monitoreo

Gestionar incidentes.

Metodología de respuesta ante incidentes según lineamientos de ISO/IEC 27001

Tabla 9

Administración de incidentes Ejeproy Cía. Ltda.

ID	Fase	Descripción	Acciones claves	Responsables	Tiempo de respuesta
1	Identificación	Detectar incidentes de seguridad en sistemas y redes.	Monitoreo con SIEM en tiempo real, reportes del usuario y alertas automáticas.	Equipo de seguridad y equipo de TI	Inmediato
2	Registro	Documentar cada incidente con detalles de alcance e impacto.	Categorización del incidente y registro en la base de datos de incidentes.	Área de seguridad de la información.	30 minutos
3	Análisis	Evaluar el impacto y determinar la causa raíz.	Identificación de vulnerabilidades explotadas, revisión de logs y análisis forenses.	Analista de seguridad.	1 – 2 horas
4	Contención	Limitar la propagación del incidente para minimizar los daños.	Bloqueos de cuentas comprometidas, aplicación de parches de seguridad, aislamiento de equipos afectados.	Equipo de TI	2 – 4 horas
5	Erradicación	Eliminar la amenaza y restaurar los sistemas comprometidos.	Desinfección del malware, restablecimiento de configuraciones seguras, actualización de software.	Equipo de seguridad y equipo de TI	4 – 8 horas
6	Recuperación	Restaurar la operación correcta y normal de los sistemas.	Pruebas de integración del sistema, revisión de backups, monitoreo después del incidente	Administradores de sistemas	8 – 24 horas
7	Lecciones aprendidas	Evaluar los incidentes para mejorar la seguridad.	Identificación de mejoras de procesos y controles de seguridad, revisión del informe del incidente.	Comité de seguridad.	48 horas

Fuente: fuente propia.

Conclusiones

El desarrollo del diseño SGSI en EJEPROY. CIA. LTDA. ha sido realizado bajo un proceso fundamental y estratégico para fortalecer y proteger los datos de la empresa. Este diseño esta basado en la LOPDP de Ecuador y la norma ISO/IEC 27001. Este sistema ha permitido el análisis, detección, evaluación y mitigación de los riesgos relacionados con la protección de la información, garantizando la continuidad de las operaciones y cumplimiento normativo vigente nacional e internacionalmente.

Por medio de los análisis de riesgos estructurados, se han identificado amenazas citicas como vulnerabilidades en la gestión de datos personales, ataques de malware, accesos no autorizados, fugas de información, fallos en seguridades SSL. En respuesta a estos riesgos se han implementado controles de seguridad alineados con las normativas vigentes incluyendo segmentación de redes, cifrado de datos, autenticación multifactor (MFA), firewalls de última generación y procesos de gestión ante incidentes que permitan a Ejeproy Cía. Ltda. Tener una respuesta efectiva y rápida ante alguna eventualidad de amenaza cibernética. También se ha priorizado de manera directa la capacitación del personal mediante programas de ciberseguridad asegurando de esta manera que los empleados cumplan y comprendan los procedimientos y políticas de seguridad establecidos en este (SGSI). Dentro de las capacitaciones se han realizado simulaciones de ataques y las pruebas necesarias de respuesta ante incidentes garantizando que los empleados estén capacitados y puedan actuar ante algún tipo de incidente de seguridad.

El diseño de este SGSI desde una perspectiva estratégica permite a EJEPROY. CIA. LTDA. reforzar la protección de la información de manera eficiente y puntual, ya que al encontrarse completamente vulnerable según los análisis de madurez inicial obtenidos mejorara la confianza de socios comerciales, empleados, clientes y proveedores. En conclusión, este diseño representa para EJEPROY. CIA. LTDA. un modelo integral de gestión de seguridad alineados a normativas locales e internacionales vigentes, minimizando los riesgos y teniendo políticas claras asegurando así un entorno digital confiable y seguro para el futuro de la empresa.

Referencias bibliográficas

Avila Torres, R. A., & Cuenca Tapia, J. P. (2021). Análisis y evaluación de riesgos: Aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. Dominio de las Ciencias, 7(Extra 4), 78.

Banda Yánez, L. F., & Morejón Armijo, V. E. (2022). Propuesta de diseño de un SGSI para la Agrupación Marista del Ecuador utilizando como marco de referencia la ISO27001. Escuela de Posgrado Newman - EPN. https://repositorio.epnewman.edu.pe/handle/20.500.12892/476

Brito Perez, V. M., & Francisco Ferreras, J. F. (2022). Implementación de un sistema de gestión de seguridad basado en la norma ISO 27001, para la protección de la información en el Centro Médico Siglo 21 en el periodo septiembre—Diciembre, 2022. [Thesis, Universidad Abierta para Adultos. Escuela de Postgrado]. https://rai.uapa.edu.do/handle/123456789/2537

Busto Pérez de Mendiguren, E. (2024). Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa TRADUX. https://openaccess.uoc.edu/handle/10609/150577

Cabezas Mena, D. F., & Lucas Franco, G. S. (2023). Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación española desde un enfoque de ciberseguridad y delitos informáticos [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/25114

Contreras Olea, G. A. (2022). Análisis comparativo entre las metodologías de gestión de riesgos de los Sistemas de Gestión de Seguridad de la Información (SGSI): Magerit y Octave. [bachelorThesis, Babahoyo: UTB-FAFI. 2022]. http://dspace.utb.edu.ec/handle/49000/12551

Coronel Suárez, I. A., Quirumbay Yagual, D. I., Coronel Suárez, I. A., & Quirumbay Yagual, D. I. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Científica y Tecnológica UPSE (RCTU), 9(2), 97-109. https://doi.org/10.26423/rctu.v9i2.672

Falcón Huallpa, E., & Martínez Zambrano, E. J. (2023). Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, para el Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil" (Quito—Ecuador). Escuela de Posgrado Newman - EPN. https://repositorio.epnewman.edu.pe/handle/20.500.12892/741

Gelvez Araque, A. F., & Neiva Márquez, J. A. (2021). Análisis diferencial del SGSI actual de la caja de compensación de Comfiar de Arauca y los requisitos de la norma ISO 27001:2013. https://hdl.handle.net/20.500.12494/43666

Guaña Moya, E. J. (2023). La importancia de la seguridad informática en la educación digital: Retos y soluciones. RECIMUNDO: Revista Científica de la Investigación y el Conocimiento, 7(1), 609-616.

Guzmán Calderón, D. D. (2021). Diseño de un programa de gestión de seguridad de la información para una empresa del sector industrial [masterThesis, Quito: Universidad de las Américas, 2021]. http://dspace.udla.edu.ec/handle/33000/13781

Isaza Giraldo, H. G. (2023). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2022, para la Esal Asociación Esperanza Viva (ASESVI). https://hdl.handle.net/20.500.12494/54002

Limones Zambrano, J. M., & Peralta Peralta, J. A. (2023). Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación Uruguaya desde un enfoque de ciberseguridad y delitos informáticos [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/25184

Lopez Aguirre, J. E. (2022). Implementación del SGSI, basado en la ISO/IEC 27001 para dar tratamiento al riesgo en una empresa constructora. https://repositorio.usil.edu.pe/entities/publication/73d88f8d-7990-4b64-a4dd-cedf62ad00f9

Lorenzo, L. A. J. (2023). Planificar la implementacion del sistema de gestion de seguridad de la informacion basado en la norma iso/iec 27001:2023 para la integridad, confidencialidad y disponibilidad de su informacion en la empresa automatisoft S.A.C. http://repositorio.upci.edu.pe/handle/upci/843

Macias, M. M. M., Macias, R. W. M., Navarrete, M. L. I., & Navarrete, J. A. I. (2023). Normas y estándares en auditoría: Una revisión de su utilidad en la seguridad informática. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5(4), 584-599. https://doi.org/10.59169/pentaciencias.v5i4.700

Marchand Niño, W. R. (2020). Cultura de seguridad de información en la protección de activos informáticos en la Universidad Nacional Agraria de la Selva, 2018- 2020. http://repositorio.uncp.edu.pe/handle/20.500.12894/6838

Mera Amores, I. F. (2022). Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: Empresa ALTAC. https://repositorio.puce.edu.ec/handle/123456789/27444

Oca, L. T.-M. de, Medina-León, A., Nogueira-Rivera, D., & Serrate-Alfonso, A. (2019). Evaluación del sistema de seguridad de la información para empresas de proyectos. Ciencias Holguín, 25(3), 1-15.

Paguay, A. V. B. (2020). Influencia de las Tecnologías de Información en los procesos contables de las organizaciones. REVISTA DE INVESTIGACIÓN SIGMA, 7(01), Article 01. https://doi.org/10.24133/sigma.v7i01.1845

Pruna, F. X. J., Jeada, P. V. Y., & Jumbo, J. L. C. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. REVISTA CIENTÍFICA ECOCIENCIA, 7(1), Article 1. https://doi.org/10.21855/ecociencia.71.303

Ramos Pachón, L. R., Del Rio Flórez, L. E., & Regalado Ortiz, J. M. (2024). Diseño y construcción de una guía práctica para la transición en la Norma ISO 27001:2013 a ISO 27001:2022 aplicada a la empresa Soluciones Globales S.A.S. https://hdl.handle.net/20.500.12495/13803

Rubio Ganchala, C. J., & Terán Suárez, D. A. (2023). Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación Argentina desde un enfoque de ciberseguridad y delitos informáticos [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/25186

Salazar Lazo, C., & Ávila Correa, B. (2024). Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales. 593 Digital Publisher CEIT, 9(1), 88-102.

Sánchez, J. A. G., & Ureta, J. S. (s. f.). LA SEGURIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN CLÍNICA.

Tandazo Tipan, A. A. (2022). Plan de seguridad informática aplicando la norma iso-27001 para la protección de activos informáticos en la empresa “Rav” [bachelorThesis]. https://dspace.uniandes.edu.ec/handle/123456789/15140

Utrilla, A. A. R. (2020). SEGURIDAD INFORMATICA: TECNOLOGIA DE DEFENSA EN PROFUNDIDAD Y PENTESTING. https://repositorio.uvm.edu.ve/handle/123456789/504

Ventura Rios, V., & Varona Pérez, M. E. (2023). Diseño de un sistema de gestión de seguridad de la información (SGSI) para la asociación ARFUSOG, recolectora de residuos sólidos de la ciudad de Sogamoso, mediante el uso de herramientas de gestión de proyectos. http://repository.unad.edu.co/handle/10596/56243