UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27001 PARA LA EMPRESA SITEC S.A."

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

Línea de investigación: Producción industrial y tecnología sostenible

AUTOR:

Jessica Fernanda Chiquito Caiza

DIRECTOR:

Ing. Fabián Geovanny Cuzme Rodríguez, Msc

Ibarra – Ecuador 2026

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004148357		
APELLIDOS Y NOMBRES:	Chiquito Caiza Jessica Fernanda		
DIRECCIÓN:	Pimampiro		
EMAIL:	jfchiquitoc@utn.edu.ec / ferchiquitoo97@gmail.com		
TELÉFONO FIJO:	xxxxxx	**TELÉFONO MÓVIL:**	0989087634

DATOS DE LA OBRA	
TÍTULO:	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27001 PARA LA EMPRESA SITEC S.A
AUTOR (ES):	CHIQUITO CAIZA JESSICA FERNANDA
FECHA:DD/MM/AAAA	09/02/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO EN TELECOMUNICACIONES
DIRECTOR:	ING. FABIÁN GEOVANNY CUZME RODRÍGUEZ, MSC
ASESOR:	ING. JAIME ROBERTO MICHILENA CALDERÓN, MSC

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 09 días del mes de febrero de 2026

EL AUTOR:

Chiquito Caiza Jessica Fernanda

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 09 de febrero de 2026

ING. FABIÁN GEOVANNY CUZME RODRÍGUEZ, MSC

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) ……. Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ Validar únicamente con FirmaEC ……

Ing. Fabián Geovanny Cuzme Rodríguez, Msc

C.C.: 1311527012

DEDICATORIA

Con amor dedico este trabajo a mi madre, pilar fundamental de mi vida, quien me inspiró y me impulsó constantemente a terminar mi carrera. A mi hijo que es el motor de mis días dándome la fuerza necesaria para seguir adelante y concluir este proceso académico.

A mi hermana y sobrino, por acompañarme en mis noches de desvelo y brindarme siempre alientos para no rendirme.

Finalmente, a mi amiga Katherine quien me apoyo de manera incondicional durante mi embarazo mientras finalizaba mi malla curricular.

Chiquito Caiza Jessica Fernanda

AGRADECIMIENTO

Agradezco a Dios por el don de la vida y ser mi fortaleza en cada una de las etapas de mi proceso académico. A mi madre por su apoyo incondicional por brindarme siempre lo necesario y por ayudarme con el cuidado de mi hijo mientras yo cumplía con mis responsabilidades universitarias.

Expreso mi sincero agradecimiento a mi director de trabajo de titulación Fabián Cuzme por brindarme sus conocimientos, orientarme con profesionalismo y ser mi guía fundamental para alcanzar permitieron esta etapa académica. De igual forma agradezco a mi asesor y coordinador de carrera Jaime Michelena quien comprendió que además de ser estudiante soy madre de familia, brindándome siempre su apoyo, compresión y valiosos consejos durante este proceso.

Chiquito Caiza Jessica Fernanda

RESUMEN EJECUTIVO

El presente trabajo propone un plan de seguridad para la gestión de riesgos en la empresa SITEC S.A, quien es proveedor de servicio de Internet (ISP), utilizando como marco principal la metodología Magerit 2013 con la norma ISO 27001. Este enfoque metodológico proporciona una guía sistemática y estructurada para identificar, evaluar y mitigar las amenazas potenciales que afectan a las infraestructuras críticas de la empresa. En la empresa se brinda servicios de internet, están expuestos a una variedad de riesgos que incluyen ataques cibernéticos, fallas de hardware o software y desastres naturales. La adecuada gestión de riesgos permite proteger los activos físicos o tecnológicos, también garantiza la continuidad operativa y la calidad de los servicios que se ofrece a los clientes.

El sistema de seguridad desarrollado se fundamenta en el análisis de los activos de la empresa, como servidores, dispositivos de red, sistemas de alimentación interrumpida y sistemas y materiales. Para la realización del análisis se utilizaron herramientas especiales como Mitratec que permite identificar, clasificar y analizar ataques cibernéticos, AEIS SBC permite controlar, proteger y asegurar las comunicaciones y OSware, que permitieron identificar las vulnerabilidades y evaluar el nivel ante amenazas. Los datos recopilados se integraron a una matriz de riesgo que prioriza las amenazas según su impacto, potencial y la probabilidad de ocurrencia, con esto se realiza la implementación de medidas. Los resultados obtenidos constan de la identificación de vulnerabilidades críticas y la propuesta de controles de seguridad. Este estudio resalta la importancia de un sistema de gestión de seguridad de la información en la empresa SITEC S.A asegurando los activos de la empresa y asegurar la confianza del cliente.

Palabras clave: activos críticos, Gestión de riesgos, Magerit, ISP, proveedor de internet, ISO27001.

ABSTRACT

This study presents a comprehensive security plan for risk management at SITEC S.A., an Internet Service Provider (ISP), based primarily on the MAGERIT 2013 methodology aligned with the ISO/IEC 27001 standard. This structured and systematic approach enables the identification, assessment, and mitigation of potential threats to the company's critical infrastructure. As an ISP, SITEC S.A. faces a wide range of risks including cyberattacks, hardware or software failures, and natural disasters making effective risk management essential not only to protect physical and technological assets but also to ensure business continuity and service quality for its customers.

The proposed security framework is grounded in a detailed analysis of the company's key assets, such as servers, network devices, uninterruptible power supply systems, and associated software and hardware components. Specialized tools were employed during the assessment phase: Mitratec for identifying, classifying, and analyzing cyber threats; AEIS SBC for securing and monitoring communications; and OSware for vulnerability detection and threat level evaluation. The collected data was consolidated into a risk matrix that prioritizes threats based on their potential impact, likelihood of occurrence, and overall risk level, thereby guiding the implementation of tailored security controls.

The outcomes of this study include the identification of critical vulnerabilities and the proposal of specific, actionable security measures. Ultimately, this work underscores the strategic importance of implementing an Information Security Management System (ISMS) at SITEC S.A. to safeguard organizational assets and reinforce customer trust.

Keywords: Critical assets, Risk management, MAGERIT, ISP, Internet service provider, ISO/IEC 27001.

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE FIGURAS

Capítulo I: Antecedentes

1.1. Tema

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27001 PARA LA EMPRESA SITEC S.A.

1.2. Problema

En los últimos años el crecimiento de ataques informáticos plantea un nuevo panorama a la forma de prevenir incidentes, aunque ya se brinda mayor atención a la seguridad de la información aún no es prioridad en las diferentes empresas en el Ecuador. Un reporte del Observatorio de Derechos Digitales alertó que Ecuador atraviesa una ola de ciberataques sin precedentes en el país, lo que genera preocupación entre ciudadanos y empresas (Gutiérrez, 2022). Dado que las empresas se apoyan cada vez más en la información como un recurso fundamental para mejorar la calidad y el valor de sus productos y servicios, la preservación de la información confidencial se convierte en una estrategia esencial para asegurar la continuidad y el éxito a largo plazo. Ecuador ocupa el segundo puesto de los países más atacados por piratas informáticos, en particular el ransomware, también conocido como secuestro de datos. En primer lugar, está Brasil con 603 mil ataques. Le sigue Ecuador, con 212 mil en el último año, y luego está México, con 102 mil ataques. Este tipo de ataques cibernéticos afecta a empresas, que son extorsionadas a cambio de desbloquear la información obtenida por los ciberdelincuentes, o que no sea entregada a otras compañías. (Ocasio, 2023).

La norma ISO 27001 se centra en la mitigación de los riesgos que ponen en peligro la integridad, la confidencialidad y la disponibilidad de los activos de información de una entidad.

La empresa SITEC S.A se enfrenta a la creciente amenaza de perdida de información, acceso no autorizado, alteración o robo de información sensible. Esta información incluye datos confidenciales de los clientes, propiedad intelectual, datos financieros y cualquier otro activo de información crítica. La falta de un sistema de gestión de seguridad de la información eficiente y de políticas y procedimientos documentados expone a la empresa a riesgos significativos, incluyendo:

- La violación de la confidencialidad: exposición de información sensible por personas no autorizadas.

- Integridad de la Información: la información puede ser alterada de manera no autorizada.

- Disponibilidad de la Información: la falta de un plan de protección de la información de seguridad podría resultar en interrupciones operativas y la perdida de acceso a datos críticos.

- Repercusiones Legales y Regulatorias: la empresa podría enfrentar sanciones legales y financieras si no cumple con las leyes y regulaciones de seguridad de la información. (Samaniego Mena & Ponce Ordóñez, 2021)

Por ello entonces se va a establecer un sistema de gestión de seguridad de la información que cumpla con la norma ISO 27001 y documentar políticas y procedimientos de seguridad para abordar estos riesgos y garantizar la protección de la información sensible de la empresa SITEC S.A y sus clientes. La implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO 27001 es esencial para abordar esta problemática de manera efectiva y mitigar los riesgos asociados con la seguridad de la información.

1.3. Objetivos

1.3.1. Objetivo General

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 para la empresa SITEC S.A.

1.3.2. Objetivos Específicos

- Realizar un estudio sobre los aspectos de seguridad informática para determinar los lineamientos a seguir en la realización del sistema de gestión de seguridad de la información.
- Establecer el análisis de los riesgos físicos y lógicos de la infraestructura de la red de la empresa, a través de un estudio de campo.
- Diseñar las políticas de seguridad basados en un análisis previo de las normas ISO 27001 y los resultados obtenidos de las vulnerabilidades que tiene la empresa.
- Establecer un cronograma de aplicabilidad de los controles seleccionados para los activos encontrados asegurando la adecuada integración y gestión de medidas de seguridad.

1.4. Alcance

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 en la empresa SITEC S.A, siguiendo los requisitos detallados en la norma ISO 27001. Este proceso abarcará desde una evaluación de los riesgos y vulnerabilidades presentes en la infraestructura de la red hasta la formulación y ejecución de políticas de seguridad específicas para la empresa. Además, se llevará a cabo un análisis detallado de los aspectos críticos de la seguridad de la información para identificar los

requisitos particulares de SITEC S.A. La implementación del SGSI no solo se centrará en mitigar riesgos, sino que también resultará en la creación de un entorno seguro y confiable para la gestión de información sensible, abordando de manera efectiva aspectos como la confidencialidad, integridad y disponibilidad de los activos de información de SITEC.

Figura 1

Fases del Sistema Gestión de Seguridad de la Información

Nota: El Sistema de Gestión de Seguridad de la Información (SGSI) es un marco de trabajo diseñado para gestionar de manera integral la seguridad de la información en una organización.

Se tiene como objetivo entregar el diseño de implementación del SGSI y llevar a cabo la implementación de los controles. Se realizará las siguientes fases para la implementación del SGSI en base a la figura numero dos:

En la Fase1 (Definición de la política), se establece los principios y objetivos de seguridad de la información, lo cual implica identificar los activos críticos y establecer criterios de evaluación. Así cumpliendo los objetivos uno y tres.

Para la Fase 2 (Definición del Alcance del SGIS), se delimita el alcance del sistema de seguridad de la información y se identifican los activos y procesos a proteger. Con esto se cumple los objetivos uno,

Continuando con la Fase 3 (Análisis de Riesgos), se identifican y evalúan los riesgos de seguridad mediante el análisis de amenazas, vulnerabilidades e impactos. Aquí es donde se aplica la metodología MAGERIT para realizar un análisis de los riesgos y sus implicaciones. Cumpliendo con los objetivos uno y dos.

Después en la Fase 4 (Gestión de Riesgos), se desarrollan estrategias para mitigar los riesgos identificados y se establecen planes de acción para su tratamiento. Con esto se cumple el objetivo dos.

En esta Fase 5 (Selección de Controles a Implementar), se encarga de seleccionar los controles de seguridad más adecuados para mitigar los riesgos identificados. Aquí se utiliza la metodología MAGERIT para priorizar y seleccionar los controles más apropiados. Cumpliendo con el objetivo cuatro.

La Fase 6 (Aplicabilidad), se desarrolla un cronograma detallado para la implementación de los controles. Se enfoca en integrar los controles de seguridad en los procesos y sistemas de la organización. Y con esto cumplir con el objetivo cuatro.

Finalmente, en la Fase 7 (Revisión del SGSI), se evalúa periódicamente el desempeño del sistema y se realizan mejoras continuas. Se llevan a cabo revisiones periódicas del SGSI para evaluar su eficacia y actualizarlo según sea necesario. Así se cumple con los objetivos tres y cuatro.

1.5. Justificación

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) a nivel nacional establece requisitos que las empresas de telecomunicaciones deben cumplir para

operar adecuadamente. La ley orgánica de telecomunicaciones dicta que el Ministerio responsable de las Telecomunicaciones y de la Sociedad de la Información, como autoridad principal, debe definir políticas y planes para el desarrollo de la sociedad de la información. (ARCOTEL, 2018)

La correcta gestión de la información es vital para el funcionamiento eficiente de la red de datos, por lo que la empresa SITEC S.A deben adherirse a políticas específicas para proporcionar un servicio de Internet eficiente. Para garantizar la continuidad del servicio, SITEC S.A utiliza bases de datos que protegen la información ante posibles fallos o eventos disruptivos, minimizando así las pérdidas económicas y la insatisfacción de los usuarios. (Cichonski, 2020)

Además, cada proveedor de servicios de Internet (ISP) tiene un plazo definido para desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo y preparar la documentación necesaria para auditorías. Esto implica organizar actividades y contar con equipos especializados en cada área para cumplir con las normativas de ARCOTEL. La implementación del SGSI es fundamental para establecer normas adaptadas a las distintas necesidades de seguridad del ISP, asegurando la integridad de la información. (ARCOTEL, 2018)

Este proyecto contribuye directamente al logro de varios Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas, destacando la importancia de garantizar la seguridad y la continuidad de las operaciones en el entorno digital, especialmente en el ámbito empresarial. Se fortalece la infraestructura de seguridad de la información, abordando así el ODS 9 (Industria, Innovación e Infraestructura) al promover la adopción de tecnologías seguras y resilientes.

Además, al proteger la información sensible de la empresa y sus clientes, el proyecto contribuye al ODS 16 (Paz, Justicia e Instituciones Sólidas) al fortalecer la seguridad

cibernética y prevenir amenazas que podrían afectar la estabilidad y confianza en las instituciones empresariales. Asimismo, al diseñar políticas basadas en análisis previos y verificar su cumplimiento para el mejoramiento constante de la seguridad. (Affairs, 2023)

En la ley de protección de datos personales se tiene el Cumplimiento Normativo: donde se garantiza un marco normativo sólido. Cumplir con esta norma demuestra el compromiso de la empresa con las mejores prácticas en seguridad de la información, lo cual es esencial para cumplir con las regulaciones de protección de datos.

Confidencialidad y Privacidad: El SGSI se centra en garantizar la confidencialidad de la información, un aspecto clave en la protección de datos personales. Estableciendo políticas y procedimientos específicos, la empresa puede asegurar que la información personal esté resguardada de accesos no autorizados y uso indebido.

Evaluación de Riesgos y Vulnerabilidades: La evaluación de riesgos físicos y lógicos en la infraestructura de red, como se propone en el proyecto, contribuye directamente a identificar y abordar posibles amenazas a la seguridad de los datos personales. Esto es esencial para cumplir con los requisitos de protección de datos, que a menudo exigen evaluaciones periódicas de riesgos.

Diseño de Políticas de Seguridad: El proyecto propone diseñar políticas de seguridad basadas en análisis de normas ISO 27001 y vulnerabilidades específicas de la empresa. Este enfoque permite adaptar las políticas para cumplir con requisitos específicos de protección de datos.

Verificación del Cumplimiento: La verificación del cumplimiento de las políticas de seguridad, como se propone en el proyecto, es esencial para garantizar que las medidas implementadas sean efectivas y estén alineadas con las regulaciones de protección de datos.

El Código Orgánico Integral Penal (COIP) de Ecuador, que es un marco legal integral que aborda diversas cuestiones, incluida la protección de datos y la seguridad de la información.(Barrezueta, 2021)

Protección de Datos Personales: El COIP reconoce la importancia de proteger los datos personales de los individuos. La implementación del SGSI según ISO 27001 en SITEC S.A contribuirá directamente a proteger la información personal de clientes, empleados y otras partes interesadas, al establecer medidas de seguridad adecuadas y mitigar los riesgos asociados con posibles violaciones de privacidad.

Prevención de Delitos Informáticos: El COIP aborda los delitos informáticos, y la implementación de un SGSI ayuda a prevenir y gestionar posibles incidentes de seguridad informática. Al establecer políticas, procedimientos y controles, la empresa SITEC S.A puede reducir la probabilidad de incidentes como accesos no autorizados, alteración de datos y otros delitos informáticos que podrían infringir las disposiciones del COIP.

Responsabilidad Empresarial: El COIP establece responsabilidades para las empresas en la protección de datos y la seguridad de la información. Implementar un SGSI demuestra la diligencia debida de la empresa para proteger la información y cumplir con las responsabilidades legales relacionadas con la seguridad de la información.

Cooperación con Investigaciones: En caso de que ocurra un incidente de seguridad, la empresa SITEC S.A, al contar con un SGSI, estará en una mejor posición para cooperar con las investigaciones legales. La documentación clara de políticas y procedimientos, junto con la capacidad de realizar auditorías internas, facilita la colaboración con las autoridades y el cumplimiento de las obligaciones legales.

Sanciones y Penalidades: El COIP establece sanciones y penalidades para las violaciones a la privacidad y la seguridad de la información. La implementación del SGSI

busca prevenir estas violaciones, reduciendo así el riesgo de enfrentar consecuencias legales y económicas (Taplin, 2019).

CAPITULO II Fundamentación Teórica

En este capítulo, se realiza una revisión de los temas fundamentales que contextualizan y respaldan el proyecto. Se comienza con las Normativas de Telecomunicaciones, abarcando los marcos regulatorios y las directrices que gobiernan el sector. El objetivo es entender las normas y estándares específicos que afectan el ámbito de las telecomunicaciones, identificando las responsabilidades y requisitos legales que deben cumplir las entidades del sector. La investigación se extiende a una comprensión profunda de un Sistema de Gestión de Seguridad de la Información (SGSI), analizando las metodologías, prácticas y estándares reconocidos internacionalmente que guían la implementación efectiva de estos sistemas. Se exploran los principios fundamentales de la seguridad de la información y su aplicación en un entorno organizacional.

Se conceptualiza un Proveedor de Servicios de Internet (ISP), examinando su función, estructura y responsabilidades en la provisión de servicios de conectividad. Se analizan las mejores prácticas y los requisitos asociados con la prestación de servicios de Internet, así como los desafíos y consideraciones específicas para los proveedores en el contexto actual.

El Marco Legal se convierte en otro elemento crucial de la investigación, abordando las regulaciones y legislaciones que impactan directamente el ámbito de las telecomunicaciones, la seguridad de la información y la prestación de servicios de Internet. Se busca entender las obligaciones legales, los protocolos de cumplimiento y las posibles implicaciones legales para asegurar que el proyecto se desarrolle en conformidad con las normativas vigentes.

2.1. Sistema de Gestión de Seguridad de la Información

En esta sección se describe, se detalla el propósito y se explica el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI); además, se mencionan los sistemas de gestión que pueden integrarse con el SGSI.

2.1.1 Definición de SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para gestionar información sensible de una empresa, asegurando su protección a través de la implementación de políticas, procedimientos y controles. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando riesgos y asegurando la continuidad del negocio.(Humphreys, 2007)

La Norma ISO/IEC 27001 es un enfoque sistemático y estructurado para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma internacional proporciona un marco para gestionar de manera efectiva la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos.

La metodología de la ISO/IEC 27001 sigue el ciclo PDCA:

Plan (Planificar): Establecer los objetivos y procesos necesarios para proporcionar resultados de acuerdo con la política de seguridad de la información de la organización.

Do (Hacer): Implementar los procesos según lo planificado.

Check (Verificar): Monitorear y medir los procesos y productos frente a las políticas, objetivos y requisitos, e informar sobre los resultados.

Act (Actuar): Tomar acciones para mejorar continuamente el desempeño del SGSI

2.1.2 ¿Para qué sirve un SGSI?

Un Sistema de Gestión de Seguridad de la Información (SGSI) se utiliza para proteger la información sensible de una organización, asegurando su confidencialidad, integridad y disponibilidad. Ayuda a gestionar los riesgos relacionados con la seguridad de la información mediante la implementación de medidas y controles adecuados. Además, garantiza el cumplimiento de leyes, regulaciones y estándares internacionales, como el ISO/IEC 27001. Un SGSI mejora la confianza y reputación de la organización al mostrar un fuerte compromiso con

la seguridad, contribuye a la continuidad del negocio, optimiza la eficiencia operativa y define claramente las responsabilidades, promoviendo la transparencia. También permite la revisión y mejora continua de las políticas, procedimientos y controles de seguridad, adaptándose a nuevas amenazas y cambios en el entorno.

2.1.3 ¿Cómo se implementa un SGSI?

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se realiza a través de varias fases definidas, cada una con un propósito específico para asegurar la protección adecuada de la información dentro de una organización. En la figura 2 se observa las fases del proceso de implementación de un SGSI:

Figura 2

Fases del Sistema de Gestión de Seguridad de la Información

Nota. Adaptado de (*IEC*, 2024)

Definir la Política: En esta primera fase, se establece la política de seguridad de la información, que guiará todas las actividades y decisiones relacionadas con la seguridad dentro de la organización.

Definir el Alcance del SGI: En esta fase, se determina qué áreas, sistemas, procesos y activos de la organización estarán cubiertos por el Sistema de Gestión de Seguridad de la Información.

Análisis de Riesgo: Aquí se identifican y evalúan los riesgos que pueden afectar la seguridad de la información. Este análisis permite entender las posibles amenazas y vulnerabilidades.

Gestión de Riesgo: Basado en el análisis de riesgos, se desarrollan estrategias y medidas para gestionar y mitigar los riesgos identificados, asegurando la protección de la información.

Selección de Controles a Implementar: En esta fase, se seleccionan e implementan los controles necesarios para mitigar los riesgos de seguridad de la información. Estos controles pueden ser técnicos, administrativos o físicos.

Aplicabilidad: Se asegura que los controles y procedimientos seleccionados sean aplicables y adecuados para los riesgos específicos y el contexto de la organización.

Revisión SGSI: Finalmente, se lleva a cabo una revisión del SGSI para evaluar su efectividad y eficiencia, y realizar los ajustes necesarios para mejorar continuamente el sistema.

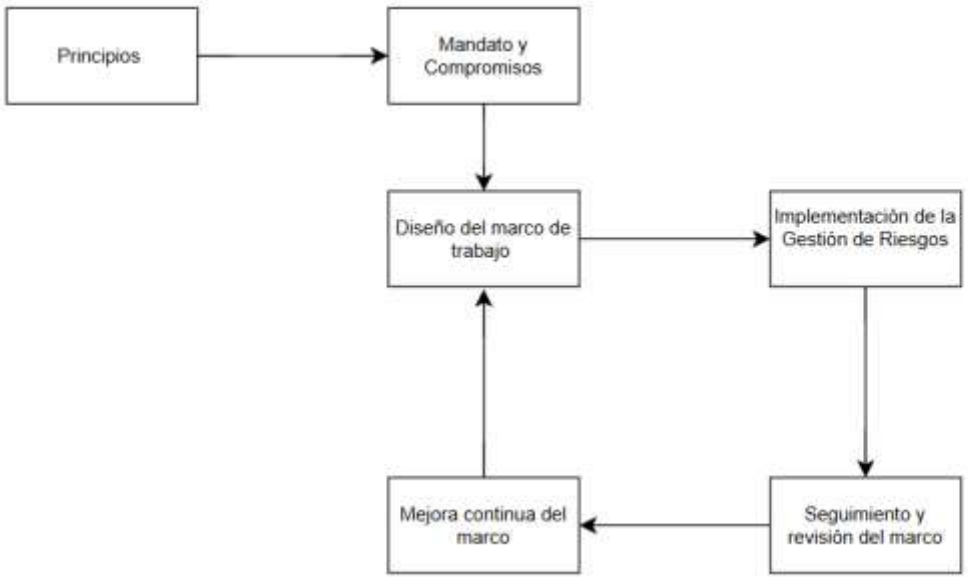
2.2 Metodología para la gestión de riesgos

La Norma ISO/IEC 27001 no especifica métodos concretos a seguir para el análisis de riesgos, lo que permite a las organizaciones elegir la metodología que mejor se adapte a sus necesidades y contexto.

En el libro "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)" (2012), se presenta una metodología desarrollada en España específicamente para la identificación y gestión de riesgos en los sistemas de información. Esta metodología destaca por su flexibilidad y capacidad de adaptación a distintos tipos de organizaciones, independientemente de su tamaño o sector siguiendo los pasos como se muestra a continuación en la figura 3.

Figura 3

Metodología de Análisis y Gestión de Riesgo



Nota. Adaptada de (Amutio Gómez, 2012)

MAGERIT aborda el análisis y gestión de riesgos de manera integral, considerando tanto los aspectos técnicos como organizativos, lo que incluye la identificación de activos, amenazas, vulnerabilidades y el análisis de impactos potenciales. Su proceso estructurado facilita la implementación a través de fases claramente definidas: inventario de activos, análisis de riesgos, evaluación de controles existentes y diseño de un plan de tratamiento de riesgos.

Además, MAGERIT proporciona una amplia gama de documentación y herramientas de apoyo, incluyendo plantillas y guías prácticas, lo que simplifica su aplicación. La metodología permite evaluaciones tanto cuantitativas como cualitativas de los riesgos, lo que ayuda a las organizaciones a medir los riesgos en términos de probabilidades y consecuencias, así como a utilizar evaluaciones más subjetivas basadas en la experiencia y juicio experto.

MAGERIT promueve la mejora continua en la gestión de riesgos, mediante la revisión y actualización periódica del análisis de riesgos y la implementación de nuevas medidas de control según sea necesario. Esta orientación hacia la mejora continua asegura que las organizaciones puedan adaptarse a nuevas amenazas y cambios en el entorno, manteniendo la seguridad de sus sistemas de información aplicando las fases de la metodología de análisis de riesgo como se muestra a continuación en la figura 4:

Figura 4

Fases del Proceso de la metodología de análisis de riesgo

Nota. Adaptado de (*IEC, 2024*)

PILAR, que significa "Procedimiento Informático Lógico para el Análisis de Riesgos", es una herramienta desarrollada por el Centro Criptológico Nacional (CCN) para implementar la metodología MAGERIT, destinada al análisis y gestión de riesgos en sistemas de información. Utilizada ampliamente en la administración pública española, PILAR permite realizar análisis de impacto y continuidad de operaciones tanto cuantitativos como cualitativos, gestionando eficientemente los activos de TI y actualizándose regularmente para mantener su eficacia. Además, facilita el cumplimiento de normativas de seguridad como el Esquema Nacional de Seguridad (ENS) y la ISO/IEC 27001. (INNOTEC, 2023)

2.3 Marco Legal

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001 se enmarca en un conjunto de leyes, regulaciones y estándares internacionales que aseguran la protección y gestión adecuada de la información. El marco legal que regula los servicios de Internet y la seguridad de la información en Ecuador está compuesto por una serie de leyes y normativas diseñadas para proteger tanto a los usuarios como a las empresas que operan en el entorno digital. A continuación, se destacan algunos de los principales componentes del marco legal relevante:

Constitución de la Republica del Ecuador

La Constitución de la República del Ecuador, publicada en el Registro Oficial No. 449 el 22 de octubre de 2008, es la norma superior sobre cualquier otra normativa jurídica. Esta constitución establece los lineamientos para la organización del Estado, define la existencia de Ecuador y determina quiénes deben gobernar. Además, principios fundamentales de derechos y deberes relacionados con la protección de la información y la privacidad de los ciudadanos, sirviendo como base para la creación de leyes y regulaciones que afectan a los servicios de telecomunicaciones y a los proveedores de servicios de Internet. Esta ley tiene como objetivo garantizar que las empresas, incluidos los proveedores de servicios de Internet (ISP), cumplan

con normas estrictas sobre la recolección, almacenamiento y procesamiento de datos personales, respetando los derechos de los ciudadanos ecuatorianos. Los ISP, en consecuencia, no solo deben ofrecer servicios de conectividad, sino también proteger la confidencialidad, integridad y disponibilidad de la información de los usuarios. Las normativas, como la ISO 27001 para la gestión de seguridad de la información, están alineadas con los principios constitucionales, promoviendo la implementación de medidas de ciberseguridad que resguarden la privacidad y seguridad de los datos personales. (ASAMBLEA NACIONAL DEL ECUADOR, 2008)

Ley Orgánica de Protección de Datos Personales (LOPDP)

Esta ley, promulgada en 2021, establece el marco legal para la protección de los datos personales en Ecuador. La LOPDP regula la recolección, almacenamiento, procesamiento y transferencia de datos personales, garantizando los derechos de los titulares de los datos. Las empresas de internet deben cumplir con los principios de legalidad, consentimiento, transparencia, y seguridad en el manejo de los datos personales. Los Proveedores de Servicios de Internet (ISP) y otras entidades que manejan datos personales están obligados a implementar sistemas de seguridad que garanticen la confidencialidad y el uso adecuado de dicha información. Entre los principios claves de la ley se encuentran la legalidad, el consentimiento informado, la transparencia y la seguridad en el tratamiento de datos. Los ISP, al igual que otras empresas, deben cumplir con estos principios para proteger los datos de los usuarios, evitando el uso indebido o la comercialización de la información sin el consentimiento explícito del titular. La ley otorga a los ciudadanos varios derechos, como el derecho de acceso, rectificación, eliminación y portabilidad de sus datos, asegurando un control total sobre su información. También incluye un régimen sancionatorio para quienes no cumplan con las normativas, aunque estas disposiciones entrarán en vigor dos años después de la promulgación de la ley.

Código Orgánico Integral Penal (COIP)

El COIP incluye disposiciones relacionadas con los delitos informáticos y la protección de los sistemas de información. Las empresas de internet deben asegurar que sus SGSI están diseñados para prevenir, detectar y responder a incidentes de seguridad que podrían constituir delitos informáticos según el COIP. El Código Penal es una herramienta del Estado utilizada para sancionar o imponer penas a quienes sean encontrados culpables de cometer un delito tipificado en la ley. El antiguo código ha sido modificado por varias leyes, incluyendo la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial Suplemento No. 577 el 17 de abril de 2002.

El COIP establece sanciones para quienes cometan delitos informáticos, como el robo de información o la extorsión mediante el uso de datos. Las empresas que no aseguren adecuadamente sus sistemas de gestión de seguridad de la información (SGSI) podrían ser responsables si no previenen, detectan o responden a estos delitos de manera efectiva. Es por esto por lo que la implementación de un SGSI conforme a la norma ISO 27001 es esencial para los ISPs, garantizando el cumplimiento de las normativas y la protección de la información sensible de los usuarios. El COIP ha sido actualizado para incluir nuevas normativas que fortalecen la lucha contra los delitos informáticos, con la promulgación de reformas específicas como la Ley Orgánica Reformatoria al COIP para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos en 2021. Esta reforma introduce figuras como el sexting no consentido y otras formas de ciberacoso, que son sancionadas severamente.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta ley regula las actividades relacionadas con el comercio electrónico y la utilización de firmas electrónicas en Ecuador. Establece la necesidad de garantizar la seguridad, confidencialidad e integridad de los datos en las transacciones electrónicas, lo que es

fundamental para las empresas de internet. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se publicó en el Registro Oficial Suplemento No. 577 el 17 de abril de 2002. Esta ley tiene como objetivo regular la información que se transmite a través de las redes de telecomunicaciones, abarcando el comercio electrónico y la protección de los usuarios.

La ley en Ecuador regula los mensajes de datos, firmas electrónicas, servicios de certificación, contratos electrónicos y telemáticos, y servicios electrónicos a través de redes de información, incluyendo el comercio electrónico y la protección de usuarios. Los mensajes de datos están sujetos a las leyes de propiedad intelectual y deben ser conservados en su formato original, manteniendo su accesibilidad e integridad. Se establece la confidencialidad y reserva de los datos, penalizando las infracciones. La creación y uso de bases de datos requieren el consentimiento del titular, respetando la privacidad y confidencialidad. La procedencia de los mensajes se asume correcta salvo prueba en contrario. Violaciones a la intimidad y acceso no autorizado a servidores son sancionados con prisión, así como el aprovechamiento ilícito de servicios públicos y la apropiación fraudulenta mediante sistemas informáticos. La suplantación de identidad y la revelación ilegal de bases de datos también conllevan penas de prisión. La interceptación ilegal de datos y ataques a la integridad de sistemas informáticos están severamente penalizados, especialmente si afectan servicios públicos o la seguridad ciudadana.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta ley regula las actividades relacionadas con el comercio electrónico y la utilización de firmas electrónicas en Ecuador. Establece la necesidad de garantizar la seguridad, confidencialidad e integridad de los datos en las transacciones electrónicas, lo que es fundamental para las empresas de internet. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se publicó en el Registro Oficial Suplemento No. 577 el 17

de abril de 2002. Esta ley tiene como objetivo regular la información que se transmite a través de las redes de telecomunicaciones, abarcando el comercio electrónico y la protección de los usuarios.

La ley en Ecuador regula los mensajes de datos, firmas electrónicas, servicios de certificación, contratos electrónicos y telemáticos, y servicios electrónicos a través de redes de información, incluyendo el comercio electrónico y la protección de usuarios. Los mensajes de datos están sujetos a las leyes de propiedad intelectual y deben ser conservados en su formato original, manteniendo su accesibilidad e integridad. Se establece la confidencialidad y reserva de los datos, penalizando las infracciones. La creación y uso de bases de datos requieren el consentimiento del titular, respetando la privacidad y confidencialidad. La procedencia de los mensajes se asume correcta salvo prueba en contrario. Violaciones a la intimidad y acceso no autorizado a servidores son sancionados con prisión, así como el aprovechamiento ilícito de servicios públicos y la apropiación fraudulenta mediante sistemas informáticos. La suplantación de identidad y la revelación ilegal de bases de datos también conllevan penas de prisión. La interceptación ilegal de datos y ataques a la integridad de sistemas informáticos están severamente penalizados, especialmente si afectan servicios públicos o la seguridad ciudadana. Los servicios de certificación desempeñan un papel crucial, ya que garantizan la validez y autenticidad de las firmas electrónicas y los mensajes de datos. Estos servicios están regulados por organismos acreditados que deben cumplir con altos estándares de seguridad, como lo establece el reglamento de la ley.

2.4 Proveedor de Servicios de Internet

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 es esencial para los Proveedores de Servicios de Internet (ISP), ya que estos manejan grandes datos sensibles y operan en un entorno expuesto a riesgos de ciberseguridad. Los ISP son responsables de la conectividad de millones de usuarios y

empresas, por lo que la protección de la confidencialidad, integridad y disponibilidad de la información que gestionan es crucial para garantizar la seguridad de sus servicios.

La norma ISO 27001 proporciona un marco estandarizado que ayuda a los ISP a identificar, gestionar y mitigar riesgos asociados con la seguridad de la información, permitiendo así que implementen políticas, procedimientos y controles que mejoren la resiliencia ante amenazas cibernéticas. Además, cumplir con esta norma no solo protege a los ISP contra posibles incidentes de seguridad, sino que también asegura el cumplimiento de normativas legales nacionales e internacionales, como las leyes de protección de datos personales y la regulación de telecomunicaciones. Al adoptar un SGSI conforme a la ISO 27001, los ISP no solo fortalecen su infraestructura de seguridad, sino que también mejoran la confianza de sus clientes y su reputación en el mercado, diferenciándose en un entorno cada vez más competitivo.

Un Proveedor de Servicios de Internet (ISP, por sus siglas en inglés) es una empresa u organización que ofrece servicios de acceso a Internet a individuos, empresas y otras entidades. Los ISPs proporcionan una variedad de servicios, incluyendo conexiones de banda ancha (DSL, cable, fibra óptica y 5G), conexiones satelitales, servicios de correo electrónico, hosting de sitios web, registro de dominios, servicios de seguridad (como firewalls y VPNs), servicios de Voz sobre IP (VoIP) y, en algunos casos, servicios de televisión y entretenimiento. Las funciones principales de un ISP incluyen la provisión de conexiones a Internet, mantenimiento y soporte técnico, monitoreo de la red, gestión del ancho de banda, cumplimiento normativo y provisión de direcciones IP. Ejemplos de ISPs conocidos incluyen AT&T, Comcast Xfinity, BT Group y Orange, que operan en diversas regiones del mundo, proporcionando conectividad esencial en la era digital.(Greene & Smith, 2020)

2.3.1 Principales Proveedores de Servicios de Internet

Según el último informe de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), el mercado de proveedores de servicios de Internet (ISP) en Ecuador está dominado por unos pocos actores principales, quienes compiten intensamente por la cuota de mercado a continuación se muestra en la figura 5 cada uno de los proveedores y su porcentaje en el mercado.

Figura 5

Porcentajes de proveedores de internet en el mercado

Nota. Adaptado de (ARCOTEL, 2018)

Corporación Nacional de Telecomunicaciones (CNT)

La empresa estatal del Ecuador lidera el mercado de proveedores de servicios de Internet (ISP) con una participación del 36%. CNT ofrece una amplia gama de soluciones de conectividad tanto para hogares como para empresas, destacándose por su extensa cobertura en todo el territorio nacional. Su liderazgo en el mercado se debe en parte a su capacidad para brindar servicios de Internet en áreas remotas y urbanas, asegurando la inclusión digital a nivel nacional y apoyando el desarrollo económico del país.

Consorcio Ecuatoriano de Telecomunicaciones (Conecel) S.A.

Operado bajo la marca Claro y perteneciente a América Móvil, es el segundo mayor proveedor de servicios de Internet en Ecuador, con una participación del 30% del mercado. Claro ofrece tanto servicios de Internet móvil como fijo, destacándose por su amplia red de cobertura y la calidad de su servicio. La empresa es reconocida por su capacidad de ofrecer conectividad robusta en diversas regiones del país, lo que la convierte en una opción clave para usuarios que buscan un servicio confiable en diversas áreas geográficas.

Telefónica S.A.

Con una participación del 20% en el mercado ecuatoriano, Movistar, parte del Grupo Telefónica, ocupa el tercer lugar entre los proveedores de servicios de Internet en el país. Movistar ofrece tanto servicios de Internet móvil como fijo, distinguiéndose por su constante innovación tecnológica y por sus ofertas competitivas que buscan satisfacer las necesidades de un mercado cada vez más exigente. La compañía es reconocida por su enfoque en brindar conectividad de calidad y por mantenerse a la vanguardia en la implementación de nuevas tecnologías para mejorar la experiencia del usuario.

Netlife S.A.

Con el 10% de la cuota de mercado, Netlife ha logrado posicionarse como un jugador destacado gracias a su especialización en tecnología de fibra óptica. Esta empresa se ha caracterizado por ofrecer velocidades de conexión muy altas, convirtiéndose en una opción preferida en áreas urbanas donde la demanda de Internet de alta velocidad es mayor. El crecimiento de Netlife ha sido significativo, y su enfoque en la calidad del servicio y la expansión de su infraestructura de fibra óptica le ha permitido consolidarse como uno de los principales actores en el mercado de Internet en Ecuador.

Otros Proveedores

Con una participación del 4% en el mercado, los proveedores más pequeños de servicios de Internet en Ecuador se especializan en nichos específicos y ofrecen soluciones personalizadas. Estos incluyen tanto empresas regionales como locales que, aunque compiten con grandes operadores, buscan diferenciarse mediante una atención más cercana al cliente, servicios adaptados a las necesidades locales y precios competitivos. Estas compañías juegan un papel importante en áreas geográficas donde los proveedores más grandes no siempre tienen presencia, aportando variedad y flexibilidad al mercado de telecomunicaciones. Entre estos proveedores se encuentra la empresa SITEC S.A., que forma parte de este 4% de otros proveedores.

2.3.2 Importancia de planes de seguridad para los ISP

Los Proveedores de Servicios de Internet (ISP) desempeñan un papel importante en la infraestructura de la conectividad global. A medida que la dependencia de Internet continúa creciendo, también aumenta la necesidad de seguridad de planes para proteger tanto a los proveedores como a los usuarios finales. Se tienen varios ámbitos en los que se marcan a continuación:

Protección contra amenazas cibernéticas

Los ISP son objetivos frecuentes de ciberataques debido a su papel central en la transmisión de datos. Las amenazas cibernéticas, como los ataques DDoS (Distributed Denial of Service), el malware, y las intrusiones, pueden interrumpir los servicios y causar pérdidas significativas. Según "Cybersecurity for Dummies" de Joseph Steinberg (2021), los planes de seguridad efectivos ayudan a los ISP a identificar, prevenir y mitigar estas amenazas mediante la implementación de medidas como firewalls, sistemas de detección de intrusos y protocolos de respuesta rápida. (Steinberg, 2019)

Protección de datos personales

La privacidad y protección de datos personales es una preocupación creciente para los usuarios de Internet. Los ISP manejan grandes volúmenes de datos sensibles, y cualquier brecha de seguridad puede resultar en la exposición de información personal. El libro "Data Privacy and Security" de David Wright y Paul De Hert (2020) subraya que los planes de seguridad robustos son vitales para garantizar la confidencialidad, integridad y disponibilidad de los datos, cumpliendo además con las normativas de protección de datos como el GDPR (Reglamento General de Protección de Datos).(Salomon, 2020)

Confianza del cliente y reputación

La confianza del cliente es fundamental para el éxito de los ISP. Los incidentes de seguridad pueden erosionar esta confianza y dañar la reputación de un proveedor. "Managing Cyber Risk in the Financial Sector" de Ruth Taplin (2019) destaca que los planes de seguridad no solo protegen los activos del ISP sino que también mejoran la percepción de seguridad entre los clientes, lo que es esencial para mantener y atraer usuarios.(Taplin, 2019)

Cumplimiento Normativo

Los ISP tienen una amplia gama de regulaciones y normativas que varían según la región. El incumplimiento de estas leyes puede resultar en sanciones severas y daños reputacionales. El texto "Cybersecurity Law" de Jeff Kosseff (2022) explora cómo los planes de seguridad ayudan a los ISP a mantenerse en conformidad con las leyes vigentes, evitando multas y asegurando operaciones continuas.(Kosseff, 2022)

Innovación y Adaptación

La seguridad no es estática. Los planes de seguridad deben evolucionar constantemente para adaptarse a las nuevas amenazas y tecnologías. El libro "The Art of Cyberwarfare" de Jon DiMaggio (2022) enfatiza que los ISP deben invertir en investigación y desarrollo continuo en ciberseguridad para mantenerse un paso adelante de los atacantes.(DiMaggio, 2022)

CAPITULO III: METODOLOGIA

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 en la empresa SITEC S.A. requiere un enfoque metodológico riguroso y estructurado. Este capítulo se detalla los procedimientos y técnicas empleados para llevar a cabo el proyecto. La metodología adoptada se basa en principios y prácticas reconocidas internacionalmente, asegurando que el SGSI sea efectivo y cumpla con los estándares de calidad y seguridad establecidos.

3.1 Metodología de Investigación

En esta sección se explica la metodología de investigación utilizada para la implementación del SGSI y el análisis de riesgo. Se tiene un enfoque cualitativo y cuantitativo se realizará mesas de trabajo con el gerente técnico, se utilizarán herramientas de análisis de riesgos y evaluación de controles de seguridad. En herramientas tenemos Magerit para la evaluación de riesgos, identificando las amenazas y vulnerabilidades de la infraestructura. Y la norma ISO 27001 para guiar la implementación del SGSI asegurando la confidencialidad, integridad y disponibilidad de la información.

3.2 Definición del Alcance, Objetivos y Funciones

Se delimitará el alcance del SGIS especificando los activos más críticos y procesos de la empresa SITEC S.A. Los activos evaluados serán Hardware, software, Personal y Bases datos.

Se implementará un SGIS conforme a la norma ISO 27001 para la empresa SITEC S.A y se realizará el análisis de riesgo físicos y lógicos, diseñar las políticas de seguridad, establecer un cronograma de implementación de controles.

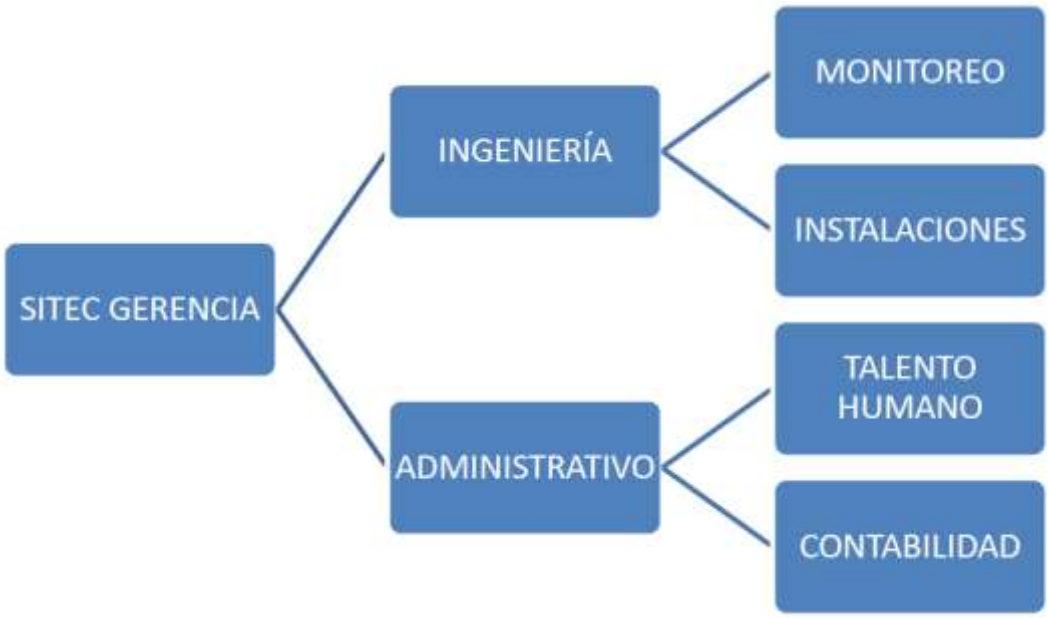
3.3 Estructura Organizacional

Para comprender el contexto en el que se implementará el SGSI, es fundamental analizar la estructura organizacional de SITEC S.A. La empresa cuenta con una estructura

jerárquica que facilita la gestión y coordinación de las actividades relacionadas con la seguridad de la información. La Figura 6 presenta el diagrama de flujo organizacional, donde se observa que SITEC GERENCIA es el nodo principal, conectado directamente a los departamentos de Ingeniería y Administrativo. Desde Ingeniería se deriva una relación bidireccional con Instalaciones y un vínculo hacia Monitoreo. Administrativo, a su vez, tiene conexiones hacia Talento Humano y Contabilidad. Este esquema jerárquico y funcional es esencial para la implementación efectiva del SGSI, ya que permite una distribución clara de responsabilidades y una comunicación eficiente entre los diferentes departamentos.

Figura 6

Estructura Organizacional de la empresa SITEC S.A



Nota. Adaptado de la Empresa SITEC S.A

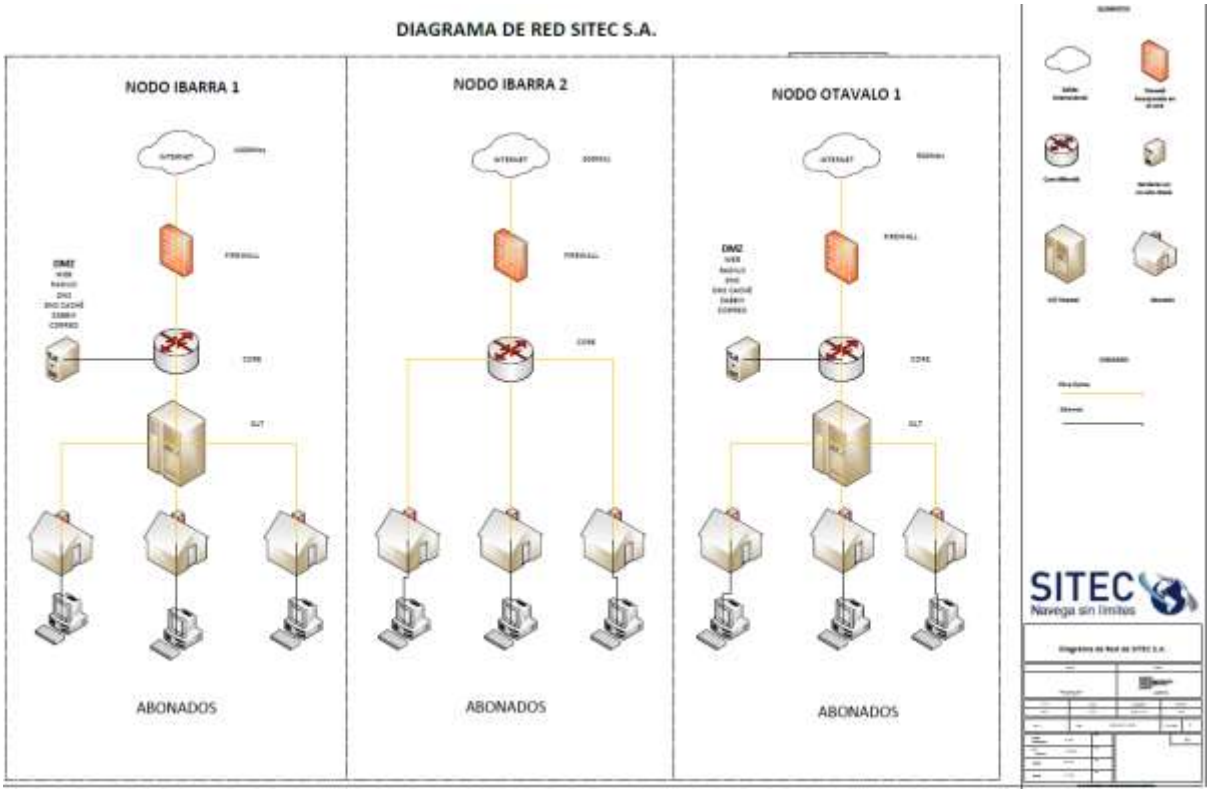
3.4 Diagrama Operacional de la Red

La infraestructura de red de la empresa SITEC S.A. es un componente crítico para la implementación del SGSI. La Figura 7 muestra el diagrama de red de la empresa, que se divide en tres nodos principales: Nodo Ibarra 1, Nodo Ibarra 2 y Nodo Otavalo 1. Cada nodo

representa una sección de la red con diferentes configuraciones de seguridad y distribución de servicios para los abonados.

Figura 7

Diagrama de Red de la Empresa SITEC S.A



Nota. Fuente empresa SITEC S.A.

Los nodos Ibarra 1 y Otavalo 1 tienen una estructura similar. Ambos están conectados a Internet con una velocidad de 1000 Mbps para Ibarra 1 y 300 Mbps para Otavalo 1. La conexión de cada uno pasa primero por un firewall, que protege la red antes de llegar a la DMZ (Zona Desmilitarizada). En la DMZ se alojan servicios críticos como Web, Radius, DNS, DNS Caché, Jabber y Correo. A continuación, la conexión llega al dispositivo central o "Core", que se enlaza con un equipo OLT (Optical Line Terminal) de Huawei, encargado de distribuir la señal de fibra óptica a los abonados, representados por casas y computadoras conectadas.

El Nodo Ibarra 2 es más sencillo, pues solo cuenta con una conexión a Internet de 1000 Mbps, protegida por un firewall y gestionada a través de un dispositivo Core. Este Core conecta directamente a los abonados, sin incluir una DMZ ni OLT visibles en la estructura del nodo.

En el margen derecho del diagrama, se muestra una leyenda que identifica los elementos de la infraestructura: firewall, Core (Mikrotik), servidores en DMZ, OLT Huawei, y los abonados. También indica los tipos de conexión utilizados: fibra óptica para la distribución principal y Ethernet para conexiones internas.

3.5 Identificación de Activos

Mediante una reunión con el Gerente Técnico de la empresa SITEC S.A, se llevó a cabo la elaboración de un listado detallado de los activos de la empresa. Este proceso permitió identificar y clasificar los recursos tecnológicos y financieros, facilitando así una visión clara de sus elementos críticos y el estado actual de sus activos y pasivos. La identificación de estos componentes es fundamental para evaluar los riesgos asociados y establecer un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001.

A continuación, en la Tabla 1 se presentan los activos y sus respectivas descripciones, las cuales fueron identificados durante el análisis detallado en el Anexo 1:

Tabla 1

Lista de Activos Hardware identificados en la reunión con la empresa SITEC S.A.

Nombre Activo	Descripción
OLT Huawei (Optical Line Terminal)	Software propietario Huawei utilizado para gestionar la transmisión de datos entre la red de acceso de fibra óptica y red troncal.
Switch Cisco Borde	Dispositivo utilizado para la conmutación de datos en la red.

Router MikroTik	Se tiene tres de borde, uno de proveedor y dos de corporativos. Equipos de control de red LAN y acceso a la red WAN.
Switch POE (Power over Ethernet)	Dispositivo de trasmisión de datos que suministra energía eléctrica a los dispositivos conectados a través del mismo cable Ethernet como las cámaras de seguridad o puntos de accesos inalámbricos.
Servidor Core i7	Servidor con Proxmox - DNS Cache en Debian: Servidor configurado para consultas DNS, mejorando el rendimiento y reducido el tiempo de respuesta en la red. - Monitoreo Zabbix: Monitoreo de la infraestructura de la red. - Radius en Debían: Servidor de autentificación y autorización al acceso de la red. - Telefonía Issabel basado en Linux: Gestiona las llamadas VoIP.
Baterias gel	Respaldo de energía su propósito es tener encendida el nodo mientras no exista energía eléctrica y mientras se enciende el generador.
Inversor 3kva	Cambiar la energía de las baterías 12v o 24v a 110v
ATS (Automatic Transfer Switch)	Mecanismo para prender automáticamente la energía por generador.

Generador 6500kva	Sirve para generar energía y mantener los nodos encendidos
Onus (Optical Network Units)	Dispositivo por donde los clientes acceden a internet.
Vehiculo	Realizar trabajos en campo
ONT (Optical Network Terminal)	Software de propietario Huawei utilizado para conectar los usuarios a través de la red óptica.
Cable de Fibra óptica	Se utiliza para la transmisión de datos a largas distancias de la red.
Patchcord	Cable de conexión utilizado para interconectar algunos dispositivos dentro de la red.
NAP (Network Access Point)	Dispositivo para conectar los usuarios a la red.
ODF (Optical Distribution Frame)	Dispositivo que facilita la gestión de las conexiones óptica y asegura que la señal se redirija correctamente.
Mangas	Elemento de protección para cables dentro de la infraestructura de la red.
Rack de Piso y pared	Estructuras utilizadas para montar y organizar los dispositivos de red como switches, routers y servidores.
Gabinete metálico de piso y poste	Es un armario de seguridad donde se almacenan equipos electrónicos como servidores o switches.
Splitter óptico	Dispositivo utilizado para dividir una señal de fibra óptica en varias señales.

Barra Tensora	Estructura utilizada para soportar y tensar cables.

Nota: La tabla 1 muestra los activos identificados durante la reunión con el representante de la empresa SITEC S.A.

Activos de nómina

Estos activos de nómina se refieren al recurso humano de la empresa, que desempeña un papel clave en la administración, mantenimiento y operación de los sistemas tecnológicos. A continuación, en la Tabla 2 se detalla el listado del nombre del personal, el cargo que ocupa y en que sucursal se encuentra trabajado. Listado que fue identificado durante el análisis detallado en el Anexo 1.

Tabla 2

Lista de Activos de nómina identificados en la reunión con la empresa SITEC S.A

Nombre	**Cargo**	**Sucursal**
León Gudiño Susana del Rocío	Gerente General / Administración	Matriz
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	Matriz
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	Matriz
Rodríguez Stalyn	Técnico	Ibarra/Otavalo
Vallejo Fabricio	Técnico	Ibarra/Otavalo
Romero Roberth	Técnico Externo	Ibarra
Jácome Roberto	Técnico Externo	Otavalo

3.4 Análisis de Riesgos

Para iniciar el análisis de riesgos, se realizará las valoraciones de los activos siguiendo la metodología MAGERIT, evaluando el valor, el impacto y la probabilidad de afectación. Estos valores los detallamos en la Tabla 3 y en la Tabla 4, donde los valores se clasificarán en una escala del 1 al 5, que va desde muy bajo hasta muy alto. Estos valores se expresarán de manera tanto cualitativa como cuantitativa. Lo que nos permitirá calcular el nivel de riesgo de cada activo. Esta clasificación servirá como base para guiar las acciones de mitigación correspondientes.

- **Valor (Importancia del activo) e Impacto (Evalúa las consecuencias de la pérdida o daño del activo)**

Tabla 3

Valoraciones Cualitativas y Cuantitativas para el valor y el impacto de los activos de la empresa.

Valor Cualitativo	Valor Cuantitativo
MA: Muy alto	**5**
A: Alto	**4**
M: Medio	**3**
B: Bajo	**2**
MB: Muy bajo	**1**

- **Probabilidad (Que una amenaza ocurra)**

Tabla 4

Valoraciones Cualitativas y Cuantitativas para la probabilidad de los activos de la empresa

Valor Cualitativo	Valor Cuantitativo
MA: prácticamente seguro	**5**
A: Probable	**4**
M: Posible	**3**
B: Poco Probable	**2**
MB: Muy Raro	**1**

3.4.1 Valoración de Activos

Las valoraciones de los activos se llevarán a cabo aplicando la metodología MAGERIT. Para la asignación de los valores de cada activo, se tomarán en cuenta los datos presentados en el Anexo1 y se utilizarán las Tablas 3 y 4 mencionas anteriormente. Cada activo será valorado en términos de valor, impacto y probabilidad, empleando un enfoque de cualitativo como cuantitativo, lo que nos permitirá determinar de manera estructurada el valor de cada activo en función de los criterios establecidos. En la Tabla 5 se mostrará a detalle cada asignación de valores para cada activo y activo personal de la empresa.

Tabla 5

Listado de asignación de valores para los Activos en la empresa SITEC S.A

Activo	Valores Cualitativos			Valores Cuantitativos		
	Valor	**Impacto**	**Probabilidad**	**Valor**	**Impacto**	**probabilidad**
OLT Huawei (Optical Line Terminal)	MA	MA	A	5	5	4
Switch Cisco Borde	MA	A	M	5	4	3
Router MikroTik	MA	A	A	5	4	4
Switch POE (Power over Ethernt)	M	M	M	3	3	3
Servidor Core i7	MA	MA	A	5	5	4
Baterias gel	MA	MA	A	5	5	4
Inversor 3kva	A	A	M	4	4	3
ATS (Automatic Transfer Switch)	A	A	M	4	4	3
Generador 6500kva	MA	A	M	5	4	3
Onus (Optical Network Units)	MA	MA	A	5	5	4
Vehiculo	MA	M	MA	5	3	5
ONT (Optical Network Terminal)	MA	MA	MA	5	5	5

Cable de Fibra óptica	MA	MA	A	5	5	4
Patchcord	MA	M	B	5	3	2
NAP (Network Access Point)	MA	M	B	5	3	2
ODF (Optical Distribution Frame)	MA	A	M	5	4	3
Mangas	MA	M	B	5	3	2
Rack de Piso y pared	MA	A	B	5	4	2
Gabinete metálico de piso y poste	MA	M	M	5	3	3
Splitter óptico	MA	M	B	5	3	2
Barra Tensora	MA	M	B	5	3	2

Activos de nómina

Por otra parte, la Tabla 6 lista a los activos de nómina que se refiere a personal de la empresa son partes claves para el funcionamiento de la empresa, incluyendo gerente general, administración, presidente, gerencia técnica, secretario, encargado de regulación, técnicos y técnicos externos. Para cada uno de los activos, se asignan los valores cualitativos como cuantitativos correspondientes, los cuales se detallan en la Tabla 3 y 4.

Tabla 6

Listado de asignación de valores para los Activos de nómina en la empresa SITEC S.A

Nombre	Cargo	Valores Cualitativos			Valores Cuantitativos		
		Valor	Impacto	Probabilidad	Valor	Impacto	Probabilidad
León Gudiño Susana del Rocío	**Gerente General / Administración**	MA	MA	M	5	5	3
Obando Villada Carlos Mario Fernando	**Presidente / Gerencia Técnica**	MA	MA	A	5	5	4
León Gudiño Marcelo Wladimir	**Secretario, Encargado de Regulación**	A	A	A	4	4	4
Rodríguez Stalyn	**Técnico**	A	M	M	4	3	3
Vallejo Fabricio	**Técnico**	A	M	M	4	3	3
Romero Roberth	**Técnico Externo**	M	M	B	3	3	2
Jácome Roberto	**Técnico Externo**	M	M	B	3	3	2

3.4.3 Nivel de riesgo de cada uno de los activos

Utilizando la metodología de MAGERIT para el análisis de riesgo, la valoración, el impacto y la probabilidad de los activos se realiza una escala cualitativa que permite clasificar los niveles de riesgos. Con esto facilitar la interpretación y gestión de los riesgos, se emplean colores que representan visualmente los diferentes niveles de riesgos de los activos. A continuación, el listado de colores:

- Rojo (MA – Muy Alto)
- Naranja (A – Alto)
- Amarrillo (M – Medio)
- Verde claro (B - Bajo)
- Gris claro (MB – Muy Bajo)

Con este listado de clores coloreamos los valores cualitativos de cada uno de los activos de la empresa como podemos observar en la Tabla 7.

Tabla 7

Valoración de Riesgos en valores cualitativos para Activos

Activo	Valor	Impacto	Probabilidad
OLT Huawei (Optical Line Terminal)	MA	MA	A
Switch Cisco Borde	MA	A	M
Router MikroTik	MA	A	A
Switch POE (Power over Ethernt)	M	M	M
Servidor Core i7	MA	MA	A
Baterias gel	MA	MA	A
Inversor 3kva	A	A	M

ATS (Automatic Transfer Switch)	A	A	M
Generador 6500kva	MA	A	M
Onus (Optical Network Units)	MA	MA	A
Vehiculo	MA	M	MA
ONT (Optical Network Terminal)	MA	MA	MA
Cable de Fibra óptica	MA	MA	A
Patchcord	MA	M	B
NAP (Network Access Point)	MA	M	B
ODF (Optical Distribution Frame)	MA	A	M
Mangas	MA	M	B
Rack de Piso y pared	MA	A	B
Gabinete metálico de piso y poste	MA	M	M
Splitter óptico	MA	M	B
Barra Tensora	MA	M	B

Activos de nómina

De igual forma para la Tabla 8 coloreamos su valor, impacto y probabilidad con los colores mencionamos anteriormente de acuerdo con cada uno de sus cargos de los activos de nómina.

Tabla 8

Valoración de Riesgos en valores cualitativos para Activos de nómina

Nombre	Cargo	Valor	Impacto	Probabilidad
León Gudiño Susana del Rocío	Gerente General / Administración	MA	MA	M
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	MA	MA	A
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	A	A	A
Rodríguez Stalyn	Técnico	A	M	M
Vallejo Fabricio	Técnico	A	M	M
Romero Roberth	Técnico Externo	M	M	B
Jácome Roberto	Técnico Externo	M	M	B

El nivel de riesgo de los activos y de SITEC S.A. se clasifica en función del impacto y la probabilidad de las amenazas identificadas. Esta evaluación permite priorizar los riesgos críticos que requieren acciones inmediatas, implementar controles preventivos para riesgos altos y realizar monitoreos regulares en riesgos moderados, mientras que los riesgos bajos demandan una atención mínima. A continuación, se presentan las clasificaciones utilizadas para esta valoración según la metodología MAGERIT:

- **Crítico (21 – 25)**
- **Alto (16 – 20)**
- **Moderado (11 – 15)**
- **Bajo (6 – 10)**

- **Muy bajo (1 – 5)**

En la Tabla 9 tenemos el listado de los colores que van a hacer aplicados para cada nivel de riesgo. Estos colores son asignados desde la metodología de MAGERIT.

Tabla 9

Colores tomados de la metodología MAGERIT para el nivel de riesgo con valores cualitativos.

Color	Valor Cualitativo
Rojo	Critico
Naranja	Alto
Amarillo	Moderado
Verde claro	Bajo
Gris claro	Muy Bajo

Para realizar el cálculo del nivel de riesgo de cada uno de los activos de la Tabla 10 se procede a realizar la multiplicación entre el impacto y la probabilidad. Con el resultado que se obtiene procedemos a realizar la clasificación dependiendo la valoración que nos da la metodología de MAGERIT que va de 1 hasta 25. Para cada valor se tiene un color como se observa en la Tabla 9, aquellos activos que reciban una valoración critica, alto y moderado deberán ser objeto de atención inmediata.

Tabla 10

Clasificación del nivel de riego de cada uno de los activos

Nombre	Impacto	Probabilidad	Nivel de Riesgo	Clasificación
OLT Huawei (Optical Line Terminal)	5	4	20	Alto
Switch Cisco Borde	4	3	12	Moderado

Router MikroTik	4	4	16	Alto
Switch POE (Power over Ethernt)	3	3	9	Bajo
Servidor Core i7	5	4	20	Alto
Baterias gel	5	4	20	Alto
Inversor 3kva	4	3	12	Moderado
ATS (Automatic Transfer Switch)	4	3	12	Moderado
Generador 6500kva	4	3	12	Moderado
Onus (Optical Network Units)	5	4	20	Alto
Vehículo	3	5	15	Moderado
ONT (Optical Network Terminal)	5	5	25	Critico
Cable de Fibra óptica	5	4	20	Alto
Patchcord	3	2	6	Bajo
NAP (Network Access Point)	3	2	6	Bajo
ODF (Optical Distribution Frame)	4	3	12	Moderado
Mangas	3	2	6	Bajo
Rack de Piso y pared	4	2	8	Bajo
Gabinete metálico de piso y poste	3	3	9	Bajo
Splitter óptico	3	2	6	Bajo
Barra Tensora	3	2	6	Bajo

Activos de nómina

Se realiza lo mismo para el nivel de riego de los activos de nómina el cual va a hacer la multiplicación del impacto y la probabilidad. Como se muestra en la Tabla 11, se realiza con la valoración que nos da la metodología de MAGERIT que va de 1 hasta 25. Para cada valor

se tiene un color como se observa en la Tabla 9, aquellos activos que reciban una valoración critica, alto y moderado deberán ser objeto de atención inmediata.

Tabla 11

Clasificación del nivel de riego de cada activo de nómina

Nombre	Cargo	Impacto	Probabilidad	Nivel de riesgo	Clasificación
León Gudiño Susana del Rocío	Gerente General / Administración	5	3	15	Moderado
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	5	4	20	Alto
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	4	4	16	Alto
Rodríguez Stalyn	Técnico	3	3	9	Bajo
Fabricio Vallejo	Técnico	3	3	9	Bajo
Roberth Romero	Técnico Externo	3	2	6	Bajo
Roberto Jácome	Técnico Externo	3	2	6	Bajo

Clasificación de activos a través del nivel de riesgo que se toman en cuenta los colores rojos (Critico), Naranja (Alto) y amarillo (Moderado) teniendo en cuenta la metodología de MAGERIT donde se trabaja con estos controles para el análisis de riesgo. En la Tabla 12 tenemos ya clasificado todos los activos que necesitan ser atendidos de forma inmediata.

Tabla 12

Nivel de riego de cada uno de los activos

Nombre	Impacto	Probabilidad	Nivel de Riesgo	Clasificación
OLT Huawei (Optical Line Terminal)	5	4	20	Alto
Switch Cisco Borde	4	3	12	Moderado
Router MikroTik	4	4	16	Alto
Servidor Core i7	5	4	20	Alto
Baterias gel	5	4	20	Alto
Inversor 3kva	4	3	12	Moderado
ATS (Automatic Transfer Switch)	4	3	12	Moderado
Generador 6500kva	4	3	12	Moderado
Onus (Optical Network Units)	5	4	20	Alto
Vehículo	3	5	15	Moderado
ONT (Optical Network Terminal)	5	5	25	Critico
Cable de Fibra óptica	5	4	20	Alto
ODF (Optical Distribution Frame)	4	3	12	Moderado

Activos de nómina

De igual forma para los activos de nómina tenemos clasificado en colores naranja y amarillo teniendo en cuenta la metodología de MAGERIT donde se trabaja con estos controles

para el análisis de riesgo. En la Tabla 13 tenemos ya clasificado todos los activos que necesitan ser atendidos de forma inmediata.

Tabla 13

Nivel de riego de cada activo de nómina

Nombre	Cargo	Clasificación
León Gudiño Susana del Rocío	Gerente General / Administración	Moderado
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	Alto
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	Moderado

3.4.4 Identificación de riesgos y controles propuestos en activos y pasivos

Como se describe en el Anexo 2, durante una reunión con el Ing. Obando Villada Carlos Mario Fernando, se presentó los controles propuestos basados en una búsqueda en las herramientas Mitratec, AEIS SBC y OSware. Tras su revisión, se validaron y ajustaron los controles para asegurar su efectividad en relación con los riesgos identificados.

La identificación de riesgos en los activos de SITEC S.A. permite analizar las amenazas que podrían afectar la operación de la empresa. En esta sección se presentan los riesgos asociados a cada activo, junto con los controles propuestos para mitigarlos, asegurando la confidencialidad, integridad y disponibilidad de la información. A continuación, se muestran cada uno de los riesgos en las Tablas 14 y 15.

La tabla 14 presenta los riesgos asociados a los principales activos de la empresa y los controles propuestos para mitigar su impacto y probabilidad, asegurando la continuidad operativa y la seguridad de la información.

Tabla 14

Control propuesto para el nivel de riesgo de cada uno de los activos

Nombre	Riesgo	Control Propuesto
OLT Huawei (Optical Line Terminal)	Fallo del hardware, afectando la conectividad de los usuarios.	Monitoreo en tiempo real del estado y rendimiento.
Switch Cisco Borde	Fallas por sobrecarga	Análisis de tráfico para detección de anomalías
Router MikroTik	Ataques de Denegación de servicio distribuido (DDoS)	Monitoreo de tráfico para detección de patrones DDoS
Servidor Core i7	Infección por malware y pérdida de datos	Segmentación de red para limitar accesos no autorizados
Baterias gel	Descarga completa de batería	Alarmas de bajo nivel de carga
Inversor 3kva	Fallo en la conversión de energía	Gestión de energía eficiente y alertas automáticas
ATS (Automatic Transfer Switch)	Fallo en la conmutación automática	Monitoreo de continuidad de energía
Generador 6500kva	Falla por falta de mantenimiento	Capacitación del personal en operación y seguridad.
Onus (Optical Network Units)	Fallo en la unidad de red óptica	Supervisión de la conectividad y alertas de fallos

Vehiculo	Fallo en la infraestructura o daño	Monitoreo GPS en tiempo real
ONT (Optical Network Terminal)	Fallo en el software o desactualización	Actualizaciones automáticas de firmware y mantenimiento preventivo regular
Cable de Fibra óptica	Falla en la transmisión de datos o pérdida de conectividad	Análisis de tráfico para detectar posibles fallos
ODF (Optical Distribution Frame)	Falla en la conexión o mantenimiento incorrecto de las fibras.	Automatización de monitoreo para detectar fallos o desconexiones

Activos Personal

La tabla 15 presenta los riesgos asociados al personal clave de la empresa y los controles propuestos para minimizar errores humanos, asegurar un manejo adecuado de dispositivos y fortalecer la toma de decisiones estratégicas.

Tabla 15

Riesgos Identificados y Controles Propuestos para Activos Personales

Nombre Activo	**Riesgo**	**Control Propuesto**
León Gudiño Susana del Rocío	Pérdida de acceso, toma de decisiones erróneas o mal gestionadas	Capacitación en gestión de riesgos y toma de decisiones.

Obando Villada Carlos Mario	Malas decisiones basadas en información incompleta o errónea	Revisión continúa de información estratégica y monitoreo
León Gudiño Marcelo Wladimir	Fugas de información confidencial, errores en normativas.	Monitoreo de cambios en políticas y procedimientos regulatorios

3.5 Diseño de Políticas basadas en la norma ISO/IEC 27001:2013

En la implementación del sistema de gestión de seguridad de la información, el diseño de las políticas de seguridad es muy importante porque tiene como objetivo proteger los activos, garantizar la confidencialidad, integridad y disponibilidad de los datos y con esto mitigar los riegos identificados durante las vulnerabilidades. Se diseñarán las políticas de seguridad para la empresa con los resultados obtenidos del análisis de riesgo en base a los controles específicos de la ISO/IEC 27001:2013 de esta forma las políticas estarán alineadas con la norma, asegurando el cumplimiento internacional para la protección de la información.

Durante el análisis de riesgo realizado se identificaron diversas vulnerabilidades que representan riegos para los activos de la información de la empresa. Cada vulnerabilidad fue analizada a través de la metodología de MAGERIT.

Una vez que se tiene identificado las vulnerabilidades y el control propuesto de los activos tomando como referencia la Tabla 14, se procede a colocar las políticas de seguridad conforme a la norma ISO 27001:2013. La Tabla 16 tiene como finalidad de que los riesgos detectados pueden ser mitigados mediante la implementación de políticas alineados a los controles del Anexo A de la norma que se encuentran en el ANEXO 3 de la norma, así fortaleciendo el sistema de gestión de seguridad de la empresa.

Tabla 16

Políticas aplicadas a cada una de las vulnerabilidades

Vulnerabilidad	Control ISO 27001:2013
Fallo del hardware, afectando la conectividad de los usuarios.	Copia de Seguridad (A.12.3) Seguridad física y del entorno (A.11) Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17)
Fallas por sobrecarga	Seguridad física y del entorno (A.11) Registro y monitoreo (A12.4) Gestión de vulnerabilidades técnica (A12.6)
Ataques de Denegación de servicio distribuido (DDoS)	Control de accesos (A.9) Gestión de incidentes de seguridad de la información (A16) Seguridad de las comunicaciones (A.13)
Infección por malware y pérdida de datos	Control de accesos (A.9) Copias de seguridad (A.12.3) Protección contra un malware (A.12.2) Gestión de vulnerabilidad técnica (A.12.6)
Descarga completa de batería	Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17) Registro y monitoreo (A.12.4)

Fallo en la conversión de energía	Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17) Procedimientos y responsabilidades operacionales (A12.1)
Fallo en la conmutación automática	Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17) Consideraciones de auditoría de sistemas de información (A.12.7)
Falla por falta de mantenimiento	Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17) Seguridad física y del entorno (A.11) Durante el empleo (A.7.2)
Fallo en la unidad de red óptica	Seguridad de las Comunicaciones (A.13) Criptografía (A.10) Gestión de incidentes de seguridad de la información (A.16)
Fallo en la infraestructura o daño	Seguridad física y del entorno (A.11) Dispositivos móviles y teletrabajo (A.6.2)
Fallo en el software o desactualización	Gestión de vulnerabilidades técnica (A.12.6) Copia de seguridad (A.12.3) Criptografía (A.10)

Falla en la transmisión de datos o pérdida de conectividad	Seguridad física y del entorno (A.11) Registro y Monitoreo (A.12.4) Consideraciones de auditoría de sistemas de información (A.12.7)
Falla en la conexión o mantenimiento incorrecto de las fibras.	Seguridad física y del entorno (A.11) Aspectos de seguridad de la información para la gestión de la continuidad del negocio (A.17)

En la Tabla 17 se muestran los principales activos personal de la empresa con los controles aplicados asignados para reforzar la seguridad en función de sus responsabilidades y roles en la empresa. Con esto garantizando que cada área cuente con las medidas necesarias para proteger la integridad, confidencialidad y disponibilidad de la información.

Tabla 17

Políticas aplicadas a cada uno de los activos

Vulnerabilidades	**Política ISO 27001:2013**
Pérdida de acceso, toma de decisiones erróneas o mal gestionadas	Seguridad de los RRHH (A.7) Organización de la seguridad de la información (A.6)
Malas decisiones basadas en información incompleta o errónea	Control de Acceso (A.9) Organización de la seguridad de la información (A.6)
Fugas de información confidencial, errores en normativas.	Cumplimiento (A.18)

Una vez que tenemos los controles propuestos por la norma ISO 27001:2013 para cada una de las vulnerabilidades procedemos a crea las políticas para para cada una de estas vulnerabilidades. Estas políticas tienen el objetivo de detectar riesgos, garantizar la protección de los activos. En la Tabla 18 se detallan las políticas diseñadas para cada vulnerabilidad de los activos identificados en la empresa.

Tabla 18

Creación de políticas de las vulnerabilidades de la empresa

Vulnerabilidad	Política ISO 27001:2013
Fallo del hardware, afectando la conectividad de los usuarios.	Se debe de garantizar la disponibilidad de la información y servicios con un respaldo (copia de seguridad) y un entorno físico adecuado para los equipos de la red. Implementar un plan de recuperación ante fallas críticas de hardware.
Fallas por sobrecarga	Implementar mecanismos de monitoreo en tiempo real sobre uso de recursos de red y servidores con alertas de sobrecargas y evaluar de manera constante las vulnerabilidades del sistema para evitar saturaciones.
Ataques de Denegación de servicio distribuido (DDoS)	Establecer mecanismos de filtrado de tráfico no autorizado aplicando políticas de acceso restrictivas y segmentación de la red. Así se tendrá un protocolo de respuesta antes

	incidentes para actuar frente a los ataques de DDoS.
Infección por malware y pérdida de datos	Implementar un software de antivirus actualizado en cada uno de los dispositivos y mantener un esquema robusto de respaldos periódicos y realizar un escaneo continuo de vulnerabilidades para así anticipar las amenazas del malware.
Descarga completa de batería	Implementar un sistema de monitoreo de carga para los equipos alimentados por batería, asegurando fuentes de alimentación de respaldo y su respectivo mantenimiento.
Fallo en la conversión de energía	Establecer procedimientos operacionales para la verificación periódica de los equipos de conversión de energía y tener planes de contingencia en caso de fallos.
Fallo en la conmutación automática	Definir procedimientos de revisión y pruebas de sistemas para verificar su correcta operación.
Falla por falta de mantenimiento	Implementar un cronograma de mantenimiento preventivo para los activos y equipos de red.
Fallo en la unidad de red óptica	Implementar mecanismos de seguridad para el tráfico de datos a través de redes ópticas se debe utilizar cifrado de extremo a extremo.

Fallo en la infraestructura o daño	Implementar medidas de protección física en gabinetes cerrados y monitoreo de accesos. Los trabajadores deben acceder a sistemas críticos de forma segura mediante dispositivos móviles y políticas de continuidad de teletrabajo.
Fallo en el software o desactualización	Establecer actualizaciones del software, garantizando la aplicación de parches de seguridad y realizar respaldos antes de cada actualización con cifrado en módulos clave para proteger la integridad del sistema.
Falla en la transmisión de datos o pérdida de conectividad	Implementar sistemas de monitoreo continuo de tráfico en enlaces de red.
Falla en la conexión o mantenimiento incorrecto de las fibras.	Realizar un procedimiento técnico para la manipulación, instalación y mantenimiento de fibra óptica.
Pérdida de acceso, toma de decisiones erróneas o mal gestionadas	Establecer procedimientos para asignar y tomar accesos de manera controlada y documentada, capacitar al personal en la gestión de la información y en la toma de decisiones seguras.
Malas decisiones basadas en información incompleta o errónea	Realizar controles de acceso adecuados y validación de datos. Establecer sistemas de

	verificación de información para respaldar las decisiones de gerencia y operacionales.
Fugas de información confidencial, errores en normativas.	Establecer políticas de protección de datos confidenciales. Realizar notificaciones y respuestas en caso de fugas o incidentes que comprometan la privacidad de la información.

CAPÍTULO IV

Desarrollo del Plan de Seguridad

En el presente capítulo se presenta los resultados obtenidos de la evaluación de riesgos realizada en el Capítulo 3. Este análisis se enfocó en la aplicación de la metodología MAGERIT lo cual se identificó, evaluó y gestiono los riesgos asociados con la seguridad de los activos de la empresa. Se llevo a cabo una evaluación integral y sistemática facilitando la elaboración de estrategias de mitigación adaptadas a las necesidades de la empresa. El objetivo de este capítulo es proporcionar un contexto de los resultados de la evaluación, destacando los activos críticos, riesgos y vulnerabilidades identificadas.

4.1 Resumen de la Metodología Aplicada

La metodología de MAGERIT es aplicada para la gestión de riesgos de la información, teniendo fases necesarias para la evaluación completa. Esta metodología se divide en algunas etapas clave, que incluyen el diagnóstico de la situación actual, identificación de activos críticos, riesgos y vulnerabilidades, el análisis de la probabilidad y el impacto y se termina con el nivel de riesgo y controles propuestos. Con cada una de estas fases se asegura los riesgos a los que está expuesta la empresa.

La fase del diagnóstico de la situación actual implica la definición clara del alcance y los objetivos de evaluación, identificando los recursos de la empresa. Esta etapa es importante para asegurar que todas las partes de la organización sean consideradas y que la evaluación se realice de manera organizada. La fase de identificación de activos críticos, riesgos y vulnerabilidades se la realiza para tener los elementos importantes que necesitan protección y de las posibles fuentes de riesgo. El análisis de probabilidad y de impacto son pasos para determinar la gravedad de los riesgos identificados. La fase del nivel de riesgo integra evaluaciones de impacto para los riegos críticos, facilitando la priorización de los riegos.

Finalmente, los controles propuestos de cada activo evaluado se proceden a realizar un análisis en la cual se colocan controles para combatir estos riesgos de los activos de la empresa.

4.2 Resultados de la Evaluación de Riesgo

En evaluación de riesgo de la empresa se trató sobre el riego y vulnerabilidades de los activos. Se identifico y priorizo los riesgos que afectan la confidencial, integridad y disponibilidad de la información. A continuación, se describen los resultados obtenidos en este proceso de evaluación de la empresa.

4.2.1 Identificación de Activos Críticos

La identificación de activos de la empresa es principal para la evaluación de riesgo, ya que son activos críticos que necesitan protección para asegurar la operatividad y seguridad. Para la empresa SITEC S.A los activos críticos identificados son:

- OLT Huawei (Optical Line Terminal): Software propietario Huawei utilizado para gestionar la transmisión de datos entre la red de acceso de fibra óptica y red troncal.
- Switch Cisco Borde: Dispositivo utilizado para la conmutación de datos en la red.
- Router MikroTik: Se tiene tres de borde, uno de proveedor y dos de corporativos. Equipos de control de red LAN y acceso a la red WAN.
- Switch POE (Power over Ethernt): Dispositivo de trasmisión de datos que suministra energía eléctrica a los dispositivos conectados a través del mismo cable Ethernet como las cámaras de seguridad o puntos de accesos inalámbricos.
- Servidor Core i7: Servidor con Proxmox. DNS Cache en Debian: Servidor configurado para consultas DNS, mejorando el rendimiento y reducido el tiempo de respuesta en la red. Monitoreo Zabbix: Monitoreo de la infraestructura de la red. Radius en Debían: Servidor de autentificación y

autorización al acceso de la red. Telefonía Issabel basado en Linux: Gestiona las llamadas VoIP.

- Baterías gel: Respaldo de energía su propósito es tener encendida el nodo mientras no exista energía eléctrica y mientras se enciende el generador.
- Inversor 3kva: Cambiar la energía de las baterías 12v o 24v a 110v
- ATS (Automatic Transfer Switch): Mecanismo para prender automáticamente la energía por generador
- Generador 6500kva: Sirve para generar energía y mantener los nodos encendidos
- Onus (Optical Network Units): Dispositivo por donde los clientes acceden a internet
- Vehículo: Realizar trabajos en campo
- ONT (Optical Network Terminal): Software de propietario Huawei utilizado para conectar los usuarios a través de la red óptica
- Cable de Fibra óptica: Se utiliza para la transmisión de datos a largas distancias de la red.
- Patchcord: Cable de conexión utilizado para interconectar algunos dispositivos dentro de la red.
- NAP (Network Access Point): Dispositivo para conectar los usuarios a la red.
- ODF (Optical Distribution Frame): Dispositivo que facilita la gestión de las conexiones óptica y asegura que la señal se redirija
- Mangas: Elemento de protección para cables dentro de la infraestructura de la red
- Rack de Piso y pared: Estructuras utilizadas para montar y organizar los dispositivos de red como switches, Router y servidores

- Gabinete metálico de piso y poste: Es un armario de seguridad donde se almacenan equipos electrónicos como servidores o switches
- Splitter óptico: Dispositivo utilizado para dividir una señal de fibra óptica en varias señales.
- Barra Tensora: Estructura utilizada para soportar y tensar cables.

4.2.2 Riesgos y vulnerabilidades Identificadas

La identificación de riesgo y vulnerabilidades son importantes para el proceso de evaluación de riesgo. Los riesgos y vulnerabilidades incluyen ciberataques, desastres naturales y las intrusiones físicas. Los ciberataques como el malware, los ataques de denegación de servicios (DDoS), tienen como riesgo importante para la confidencialidad, integridad y disponibilidad de la información. Las instrucciones físicas que pueden comprometer la seguridad de los activos si no se implementa medidas de seguridad. Los riegos internos incluyen errores humanos, fallo de equipos y problemas por falta de mantenimiento. Los fallos de equipo como el mal funcionamiento de hardware o software. Las vulnerabilidades identificadas incluyen falta de políticas de seguridad, la ausencia de estas políticas puede llevar a una mala implementación de medidas de seguridad, así aumentando el riesgo de incidentes de seguridad.

4.2.3 Determinación del Riesgo

Para la determinación del riesgo se implica la evaluación de probabilidades e impacto de cada activo para calcular el nivel de riesgo asociada con cada riesgo identificado. Para esta evaluación se tomaron niveles de riesgo medio, alto y muy alto. Los riesgos con un nivel de riesgo muy alto requieren atención prioritaria y la implementación de medidas de mitigación.

4.3 Desarrollo de Estrategias de Mitigación

Las estrategias de mitigación se desarrollan para reducir riesgos identificados, estas estrategias se enfocan en amenazas y vulnerabilidades y se priorizan en función de su eficacia.

Para cada vulnerabilidad identificada, se proponen medidas específicas que pueden incluir la implementación de controles preventivos, defectivos o correctivos. Estos controles se alinean con las políticas de seguridad previamente diseñadas y con los controles establecidos por la norma ISO/IEC 27001:2013, garantizando que las medidas adoptadas estén en conformidad con los estándares internacionales de gestión de seguridad de la información.

4.4 Plan de Implementación de Medidas de Seguridad

El plan de implementación de medidas de seguridad se detalla en el cronograma con la asignación de recursos y responsabilidades para la implementación de las estrategias de mitigación. Con este plan se asegura que las medidas de seguridad se implementen de manera segura y efectiva, minimizando el riesgo de incidentes de seguridad.

- Cronograma: Establecer un cronograma detallado sobre la implementación de las medidas de seguridad en plazos específicos. Con este cronograma se va a asegurar que las actividades de implementación se realicen de manera organizada y dentro de los plazos establecidos.
- Asignación de Recursos: Tomar en cuenta los recursos necesarios para la implementación de las medidas de seguridad tomando en cuenta al personal y equipos. La asignación adecuada de recursos es importante para asegurar que todas las medidas de seguridad se implementen de manera efectiva.
- Planes de monitoreo continuo y revisión periódica: Realización continua de políticas de seguridad para proteger la empresa contra amenazas emergentes.

4.5 Plan de Seguridad para la Gestión de Riesgos

En este plan de seguridad se define la estructura los procedimientos necesarios para la gestión integral de riesgos de la empresa SITEC S.A. En este plan va a incluir la identificación de activos, evaluación de riegos y vulnerabilidades y la implementación de controles específicos para mitigar los riesgos detectados, conforme a la norma ISO/IEC 27001:2013. Con

las acciones descritas en este documento estarán diseñadas para garantizar la continuidad operativa, la protección de los datos y el cumplimiento de los objetivos.

4.6 Plan de Políticas de Seguridad

En este plan se seguridad de políticas de seguridad se presenta un conjunto de políticas alineadas a la norma ISO/IEC 27001 y el marco normativo aplicable en protección de datos y ciberseguridad. En el **ANEXO 3** se procede a explicar los procesos que se necesitan para cumplir cada una de las políticas establecidas en el plan de políticas.

SITEC S.A

PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS DE LA EMPRESA

VERSION 1.0

Plan de Seguridad para la Gestión de Riesgos Para la empresa SITEC S. A

Versión	**1.0**
Elaborado por:	**Sra. Jessica Fernanda Chiquito Caiza**
Firma:	Firmado electrónicamente por: JESSICA FERNANDA CHIQUITO CAIZA. Validar únicamente con FirmaEC
	MSc. Fabián Cuzme Rodríguez
Firma:	Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ. Validar únicamente con FirmaEC
Fecha de Elaboración:	**15/09/2025**
Revisado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC
Fecha de Revisión:	**23/10/2025**
Aprobado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC
Fecha de Aprobación:	**24/11/2025**
Aprobado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC

I. Introducción

El plan de Seguridad para la Gestión de Riesgos de la empresa SITEC S.A tiene como propósito garantizar la continuidad del negocio y protección de los activos críticos de la empresa frente a un entorno de amenazas. Este documento está basado en la metodología MAGERIT, identifica, analiza y gestiona los riesgos que afectan el ámbito físico como lógico. La seguridad de la información y el cumplimiento normativo son elementos clave que sustentan este plan, con esto busca proteger la infraestructura técnica asegurando la integridad, confidencialidad y disponibilidad de los datos de la empresa. Este plan incluye políticas y procedimientos estándares promoviendo la seguridad de la empresa.

Alcance del Plan: Este plan tiene la identificación de activos críticos, evaluación de riesgos, monitore, mejora continua y la implementación de políticas de seguridad alineadas con la norma ISO/IEC 27001:2013. Se enfocará en todos los activos de la empresa incluyendo hardware, software, datos e infraestructura física considerando las amenazas interno como externas.

Objetivo del Plan: El objetivo de este Plan de Gestión de Riesgos es establecer medidas para gestionar y mitigar los riesgos de seguridad de la información de la empresa SITEC S.A, siguiendo la metodología de MAGERIT. Este plan está diseñado para identificar y evaluar los riegos, implementar los controles y procedimientos adecuados con esto asegurar la continuidad de la empresa.

Importancia del Plan: Garantizar la disponibilidad, integridad y confidencialidad de los datos de la empresa que son fundamentales para el continuo de SITEC S.A. Un plan bien estructurado protege contra los incidentes de seguridad y el impacto financiero. La implementación de este plan da confianza a los clientes y socios, demostrando el compromiso de la empresa con la seguridad de la información.

Metodología utilizada MAGERIT: Se utiliza la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de información) para realizar el análisis de riesgo de la empresa y establecer controles de seguridad adecuados. Esta metodología proporciona un enfoque sistemático para identifica, evaluar y gestionar los riesgos de los activos de la empresa. Con esta metodología fue complementada con la implementación de los controles de seguridad que están establecidos por la norma ISO/IEC 27001:2013, lo que permitió desarrollar las políticas de seguridad para mitigar los riegos encontrados en la empresa. Se identifico las amenazas, vulnerabilidades y cálculo de impacto y probabilidad de los riesgos, lo que facilitó con sus resultados realizar la implementación de medidas de mitigación.

II. Glosario

Definiciones Clave:

- **Amenaza:** Evento que puede causar daño a los activos de la empresa SITEC. SA, siendo ataques cibernéticos o desastres naturales.
- **Activo:** Sistema. Recurso y componentes vitales para realizar el funcionamiento de la empresa incluyendo hardware, software, datos y la infraestructura física.
- **Riesgo**: Es la probabilidad de que una amenaza aproveche una vulnerabilidad para causar un impacto negativo de la empresa.
- **Control**: Medidas que se implementan para gestionar los riesgos estos controles pueden ser preventivos, detectivos y correctivos.
- **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una amenaza para causar daño.
- **Impacto:** La consecuencia o daño de que un evento puede causar a los activos de la empresa, afectando la confidencialidad, integridad y disponibilidad.
- **Probabilidad:** La posibilidad de que ocurra un evento o amenaza que pueden afectar los activos de la empresa.

- **Evaluación de riesgo:** Proceso de identificar, analizar y evaluar amenazas y vulnerabilidades que afectan a los activos de la empresa, determinando la probabilidad y el impacto de su ocurrencia para priorizar los riegos.
- **Exploit:** Técnica que se aprovecha de una vulnerabilidad en un sistema, aplicación o dispositivo para alterar su funcionamiento normal.
- **Mitigación:** Controles implementados para reducir la probabilidad de un riesgo sobre los activos de la empresa.
- **Control de Acceso:** Proceso para regular permisos y la autenticación de usuarios para poder acceder a sistemas, redes y datos de la empresa.
- **Ciberseguridad:** Conjunto de controles y practicas implementadas para proteger los sistemas de información.

Principios de seguridad de la información:

- Confidencialidad: Garantizar que la información sea solo accesible para personas autorizadas, protegiendo contra accesos no autorizados.
- Integridad: Asegurar que la información sea precisa, completa y no tenga ninguna alteración, protegiendo los datos de la empresa.
- Disponibilidad: Asegurar que la información y los recursos estén disponibles para los usuarios autorizados cuando lo necesiten.

III. Identificación de Activos de la Empresa

La identificación de los activos críticos es fundamental para el funcionamiento de la empresa, estos activos deben ser protegidos frente a amenazas y riesgos. En la Tabla 1 se detallan los activos críticos de la empresa SITEC S.A.

Tabla 1

Activos Críticos de la empresa SITEC S.A

Nombre Activo	Descripción
OLT Huawei (Optical Line Terminal)	Software propietario Huawei utilizado para gestionar la transmisión de datos entre la red de acceso de fibra óptica y red troncal.
Switch Cisco Borde	Dispositivo utilizado para la conmutación de datos en la red.
Router MikroTik	Se tiene tres de borde, uno de proveedor y dos de corporativos. Equipos de control de red LAN y acceso a la red WAN.
Switch POE (Power over Ethernt)	Dispositivo de trasmisión de datos que suministra energía eléctrica a los dispositivos conectados a través del mismo cable Ethernet como las cámaras de seguridad o puntos de accesos inalámbricos.
Servidor Core i7	Servidor con Proxmox - DNS Cache en Debian: Servidor configurado para consultas DNS, mejorando el rendimiento y reducido el tiempo de respuesta en la red. - Monitoreo Zabbix: Monitoreo de la infraestructura de la red. - Radius en Debían: Servidor de autentificación y autorización al acceso de la red.

- Telefonía Issabel basado en Linux: Gestiona las llamadas VoIP.

Baterias gel	Respaldo de energía su propósito es tener encendida el nodo mientras no exista energía eléctrica y mientras se enciende el generador.
Inversor 3kva	Cambiar la energía de las baterías 12v o 24v a 110v
ATS (Automatic Transfer Switch)	Mecanismo para prender automáticamente la energía por generador.
Generador 6500kva	Sirve para generar energía y mantener los nodos encendidos
Onus (Optical Network Units)	Dispositivo por donde los clientes acceden a internet.
Vehiculo	Realizar trabajos en campo
ONT (Optical Network Terminal)	Software de propietario Huawei utilizado para conectar los usuarios a través de la red óptica.
Cable de Fibra óptica	Se utiliza para la transmisión de datos a largas distancias de la red.
Patchcord	Cable de conexión utilizado para interconectar algunos dispositivos dentro de la red.
NAP (Network Access Point)	Dispositivo para conectar los usuarios a la red.
ODF (Optical Distribution Frame)	Dispositivo que facilita la gestión de las conexiones óptica y asegura que la señal se redirija correctamente.
Mangas	Elemento de protección para cables dentro de la infraestructura de la red.

Rack de Piso y pared	Estructuras utilizadas para montar y organizar los dispositivos de red como switches, routers y servidores.
Gabinete metálico de piso y poste	Es un armario de seguridad donde se almacenan equipos electrónicos como servidores o switches.
Splitter óptico	Dispositivo utilizado para dividir una señal de fibra óptica en varias señales.
Barra Tensora	Estructura utilizada para soportar y tensar cables.

Además, se tiene los activos de nómina como se describen en la Tabla 2 el nombre del personal, el cargo que desempeña en la empresa y en la sucursal que se encuentra trabajando.

Tabla 2

Activos de nómina de la empresa SITEC S.A

Nombre	**Cargo**	**Sucursal**
León Gudiño Susana del Rocío	Gerente General / Administración	Matriz
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	Matriz
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	Matriz
Rodríguez Stalyn	Técnico	Ibarra/Otavalo
Vallejo Fabricio	Técnico	Ibarra/Otavalo
Romero Roberth	Técnico Externo	Ibarra
Jácome Roberto	Técnico Externo	Otavalo

Categorización de los Datos

La categorización de los datos es fundamental para asegurar y proteger la información dependiendo su nivel de criticidad. Esta clasificación asegura que los controles aplicados sean proporcionales para la operatividad de la empresa. Se clasifican en datos críticos, importantes y de menor importancia.

Datos críticos estos datos son los de nivel muy alto lo que requieren atención de forma inmediata. Los datos importantes son los de nivel alto, su pérdida o interrupción afecten a la operabilidad de la empresa y se tiene por último los datos de menor importancia son los de nivel medio los que no necesitan atención de forma inmediata, pero si deben ser controlados ante amenazas significativas para la operación de la empresa.

IV. Evaluación de Riesgos

Identificación de Riesgos:

En esta evaluación primero se identifica el riesgo que afectan a cada uno de los activos en la Tabla 3 se detalla el nombre del activo con su riesgo y su control propuesto.

Tabla 3

Activos Críticos de la empresa SITEC S.A

Nombre	Riesgo	Control Propuesto
OLT Huawei (Optical Line Terminal)	Fallo del hardware, afectando la conectividad de los usuarios.	Monitoreo en tiempo real del estado y rendimiento.
Switch Cisco Borde	Fallas por sobrecarga	Análisis de tráfico para detección de anomalías
Router MikroTik	Ataques de Denegación de servicio distribuido (DDoS)	Monitoreo de tráfico para detección de patrones DDoS

Servidor Core i7	Infección por malware y pérdida de datos	Segmentación de red para limitar accesos no autorizados
Baterias gel	Descarga completa de batería	Alarmas de bajo nivel de carga
Inversor 3kva	Fallo en la conversión de energía	Gestión de energía eficiente y alertas automáticas
ATS (Automatic Transfer Switch)	Fallo en la conmutación automática	Monitoreo de continuidad de energía
Generador 6500kva	Falla por falta de mantenimiento	Capacitación del personal en operación y seguridad.
Onus (Optical Network Units)	Fallo en la unidad de red óptica	Supervisión de la conectividad y alertas de fallos
Vehiculo	Fallo en la infraestructura o daño	Monitoreo GPS en tiempo real
ONT (Optical Network Terminal)	Fallo en el software o desactualización	Actualizaciones automáticas de firmware y mantenimiento preventivo regular
Cable de Fibra óptica	Falla en la transmisión de datos o pérdida de conectividad	Análisis de tráfico para detectar posibles fallos

ODF (Optical Distribution Frame)	Falla en la conexión o mantenimiento incorrecto de las fibras.	Automatización de monitoreo para detectar fallos o desconexiones

Además, en la Tabla 4 tenemos los activos de nómina, riegos asociados con el personal de la empresa y los controles propuesto para minimizar los errores humanos.

Tabla 4

Activos Críticos de la empresa SITEC S.A

Nombre Activo	**Riesgo**	**Control Propuesto**
León Gudiño Susana del Rocío	Pérdida de acceso, toma de decisiones erróneas o mal gestionadas	Capacitación en gestión de riesgos y toma de decisiones.
Obando Villada Carlos Mario	Malas decisiones basadas en información incompleta o errónea	Revisión continúa de información estratégica y monitoreo
León Gudiño Marcelo Wladimir	Fugas de información confidencial, errores en normativas.	Monitoreo de cambios en políticas y procedimientos regulatorios

Análisis de Riesgo:

El nivel de riesgo de los activos y de SITEC S.A. se clasifica en función del impacto y la probabilidad de las amenazas identificadas. Esta evaluación permite priorizar los riesgos críticos que requieren acciones inmediatas, implementar controles preventivos para riesgos altos y realizar monitoreos regulares en riesgos moderados, mientras que los riesgos bajos

demandan una atención mínima. A continuación, se presentan las clasificaciones utilizadas para esta valoración según la metodología MAGERIT:

- **Crítico (21 – 25)**
- **Alto (16 – 20)**
- **Moderado (11 – 15)**
- **Bajo (6 – 10)**
- **Muy bajo (1 – 5)**

En la Tabla 5 tenemos el listado de los colores que van a hacer aplicados para cada nivel de riesgo. Estos colores son asignados desde la metodología de MAGERIT.

Tabla 5

Activos Críticos de la empresa SITEC S.A

Color	**Valor Cualitativo**
Rojo	Critico
Naranja	Alto
Amarillo	Moderado
Verde claro	Bajo
Gris claro	Muy Bajo

Para realizar el cálculo del nivel de riesgo de cada uno de los activos de la Tabla 5 se procede a realizar la multiplicación entre el impacto y la probabilidad. Con el resultado que se obtiene procedemos a realizar la clasificación dependiendo la valoración que nos da la metodología de MAGERIT que va de 1 hasta 25. Para cada valor se tiene un color como se observa en la Tabla 6, aquellos activos que reciban una valoración critica, alto y moderado deberán ser objeto de atención inmediata.

Tabla 6

Activos Críticos de la empresa SITEC S.A

Nombre	Impacto	Probabilidad	Nivel de Riesgo	Clasificación
OLT Huawei (Optical Line Terminal)	5	4	20	Alto
Switch Cisco Borde	4	3	12	Moderado
Router MikroTik	4	4	16	Alto
Switch POE (Power over Ethernt)	3	3	9	Bajo
Servidor Core i7	5	4	20	Alto
Baterias gel	5	4	20	Alto
Inversor 3kva	4	3	12	Moderado
ATS (Automatic Transfer Switch)	4	3	12	Moderado
Generador 6500kva	4	3	12	Moderado
Onus (Optical Network Units)	5	4	20	Alto
Vehículo	3	5	15	Moderado
ONT (Optical Network Terminal)	5	5	25	Critico
Cable de Fibra óptica	5	4	20	Alto
Patchcord	3	2	6	Bajo
NAP (Network Access Point)	3	2	6	Bajo
ODF (Optical Distribution Frame)	4	3	12	Moderado
Mangas	3	2	6	Bajo
Rack de Piso y pared	4	2	8	Bajo

Gabinete metálico de piso y poste	3	3	9	Bajo
Splitter óptico	3	2	6	Bajo
Barra Tensora	3	2	6	Bajo

Activos de nómina

Se realiza lo mismo para el nivel de riego de los activos de nómina el cual va a hacer la multiplicación del impacto y la probabilidad. Como se muestra en la Tabla 5, se realiza con la valoración que nos da la metodología de MAGERIT que va de 1 hasta 25. Para cada valor se tiene un color como se observa en la Tabla 7, aquellos activos que reciban una valoración critica, alto y moderado deberán ser objeto de atención inmediata.

Tabla 7

Activos Críticos de la empresa SITEC S.A

Nombre	**Cargo**	**Impacto**	**Probabilidad**	**Nivel de riesgo**	**Clasificación**
León Gudiño Susana del Rocío	Gerente General / Administración	5	3	15	Moderado
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	5	4	20	Alto
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	4	4	16	Alto
Rodríguez Stalyn	Técnico	3	3	9	Bajo
Fabricio Vallejo	Técnico	3	3	9	Bajo
Roberth Romero	Técnico Externo	3	2	6	Bajo
Roberto Jácome	Técnico Externo	3	2	6	Bajo

Clasificación de activos a través del nivel de riesgo que se toman en cuenta los colores rojos (Critico), Naranja (Alto) y amarillo (Moderado) teniendo en cuenta la metodología de MAGERIT donde se trabaja con estos controles para el análisis de riesgo. En la Tabla 8 tenemos ya clasificado todos los activos que necesitan ser atendidos de forma inmediata.

Tabla 8

Activos Críticos de la empresa SITEC S.A

Nombre	**Impacto**	**Probabilidad**	**Nivel de Riesgo**	**Clasificación**
OLT Huawei (Optical Line Terminal)	5	4	20	Alto
Switch Cisco Borde	4	3	12	Moderado
Router MikroTik	4	4	16	Alto
Servidor Core i7	5	4	20	Alto
Baterias gel	5	4	20	Alto
Inversor 3kva	4	3	12	Moderado
ATS (Automatic Transfer Switch)	4	3	12	Moderado
Generador 6500kva	4	3	12	Moderado
Onus (Optical Network Units)	5	4	20	Alto
Vehículo	3	5	15	Moderado
ONT (Optical Network Terminal)	5	5	25	Critico
Cable de Fibra óptica	5	4	20	Alto
ODF (Optical Distribution Frame)	4	3	12	Moderado

Activos de nómina

De igual forma para los activos de nómina tenemos clasificado en colores naranja y amarillo teniendo en cuenta la metodología de MAGERIT donde se trabaja con estos controles para el análisis de riesgo. En la Tabla 9 tenemos ya clasificado todos los activos que necesitan ser atendidos de forma inmediata.

Tabla 9

Activos Críticos de la empresa SITEC S.A

Nombre	Cargo	Clasificación
León Gudiño Susana del Rocío	Gerente General / Administración	Moderado
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	Alto
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	Moderado

V. Estrategias de Mitigación

La estrategia de mitigación se refiere a los controles que se implementan para reducir o eliminar los riesgos identificados en la empresa, estas estrategias garantizan a los activos que estén protegidos ante estos riegos.

1. **Estrategias de Mitigación de Seguridad Cibernética**

    - **Implementación de controles de accesos seguros**

    Descripción:

    Establecer controles de acceso para evitar el acceso no autorizado a sistemas, aplicaciones y datos críticos.

    Acciones específicas:

    Implementar controles de acceso basados en roles (RBAC).

    Monitoreo de accesos.

- **Uso de cifrado**

Descripción:

Proteger la confidencialidad de los datos tanto en tránsito y cuando se almacenan en servidores o bases de datos.

Acciones específicas:

Implementar cifrado de bases de datos, discos duros y sistemas de almacenamiento.

Implementar protocolos de comunicación segura TLS/SSL.

Implementar un sistema seguro de gestión de claves.

- **Actualización continua de hardware y software**

Descripción:

Para reducir vulnerabilidades mantener actualizados el hardware y software.

Acciones específicas:

Realizar auditorías para verificar que los sistemas se encuentren actualizados.

Implementar una política de actualización y mantenimiento continuo del hardware.

2. **Estrategia de Mitigación de Riesgos Físicos**

- **Protección física de activos**

  Descripción:

  Protección ante amenazas de activos de la empresa para que estén a salvo de daños, robos o acceso no autorizado.

  Acciones específicas:

  Implementar control de acceso mediante uso de códigos de acceso, lectores biométricos o tarjetas de identificación.

  Instalar cámaras de seguridad.

  Realizar mantenimiento constante a los activos para identificar daños o desgastes.

- **Seguridad de dispositivos móviles**

  Descripción:

  Seguridad para dispositivos como laptops y celulares que son vulnerables a robos, perdida o accesos no autorizado.

  Acciones específicas:

  Establecer una política interna que regule el uso de dispositivos móviles.

  Implementar cifrado en los dispositivos móviles.

  Realizar bloqueos remotos y borrado de datos.

3. **Estrategias de Mitigación de Riesgos de Errores Humanos**

- **Capacitaciones al personal**

  Descripción:

  Los errores humanos son resultados de falta de conocimiento o desinformación sobre gestión de datos, políticas de seguridad y operación de sistemas.

  Acciones específicas:

  Crear programas de capacitación para todo el personal.

  Implementar talleres y simulacros de incidentes de seguridad.

  Realizar evaluaciones constantes al personal para verificar el nivel de conocimiento.

- **Procedimientos operativos estandarizados**

  Descripción:

  Procedimientos fundamentales para garantizar que las actividades relacionadas con la seguridad sean correctas.

  Acciones específicas:

  Documentar procedimientos operativos estandarizados para el control de acceso, los datos sensibles y respuestas a incidentes de seguridad.

Establecer revisiones constantes para adaptarse a los cambios de la infraestructura, amenazas o nuevas políticas de seguridad.

4. **Estrategias de Mitigación para fallos de Infraestructura**

- **Planes de recuperación ante desastres**

  Descripción:

  Tener un plan de recuperación ante fallos de infraestructura, amenazas o vulnerabilidades en la empresa.

  Acciones específicas:

  Desarrollar un plan donde se describan los procedimientos a seguir en caso de un incidente o fallo de la infraestructura.

  Establecer un sistema de respaldo de datos de forma automática.

  Realizar pruebas sobre el plan de respaldo ante desastres, con eso verificar su efectividad.

  Establecer un equipo del personal que debe de ser entrenado para ejecutar el plan de recuperación rápida.

5. **Estrategia de Mitigación para desastres naturales**

- **Planes de continuidad del negocio**

  Descripción:

  Tener un plan para la continuidad del negocio para garantizar el funcionamiento de la empresa, pueda mantener la operabilidad y restaurar los servicios de manera rápida después de un desastre.

  Acciones específicas:

  Crear un plan donde se describan los procedimientos a seguir en caso de tener desastres naturales.

  Implementar copias de seguridad directamente en la nube.

Realizar simulacros sobre el plan para asegurar que las acciones de recuperación funcionen correctamente y sean efectivas.

- **Protección de instalaciones físicas**

  Descripción:

  Tener protección en las instalaciones físicas para minimizar el impacto de los desastres naturales que afectan a los activos de la empresa.

  Acciones específicas:

  Implementar barreras de protección contra inundaciones.

  Asegurar que estén funcionando correctamente los UPS y los generadores.

  Instalar sistema automáticos para incendios.

6. Estrategias de Mitigación de Riegos Regulatorios

- **Cumplimiento de normativas**

  Descripción:

  Cumplir con todas las leyes y regulaciones para garantizar la seguridad de operabilidad y evitar riesgos legales.

  Acciones específicas:

  Implementación de un Sistema de gestión de seguridad de la información con la norma ISO27001:2013.

  Cumplir con la legislación de la protección de los datos de la empresa.

  Establecer políticas para garantizar el manejo adecuado de la información.

- **Auditorias y revisiones**

  Descripción:

  En las auditorias se permite verificar que las políticas de seguridad estén aplicadas correctamente y que la empresa tengas los requisitos legales y regulatorios.

Acciones específicas:

Realizar auditorías internas para evaluar las políticas de seguridad y el cumplimiento de las normativas.

Realizar revisiones constantes de los contratos con proveedores y acuerdos de servicios.

Desarrollar informes después de cada auditoria.

7. **Estrategias de Mitigación de Riegos de Ciberataques**

- **Implementar firewall y sistemas de detección de intrusiones IDS/IPS**

Descripción:

El firewall actúa como una barrera que filtra el tráfico de red así bloqueando el acceso no autorizado. Y los IDS/IPS monitorean el tráfico de red proporcionando protección ante ataques.

Acciones específicas:

Configurar IDS/IPS que detecten patrones de ataques y actividades sospechosas en la red en tiempo real.

Definir reglas en los firewalls y IDS/IPS en la red interna para que detecten las vulnerabilidades o invasión de intrusos que afectan a la empresa.

Revisar que las reglas de seguridad estén actualizadas.

- **Segmentación de la red**

Descripción:

La segmentación de red es la que se divide la infraestructura de red en subredes pequeñas, para reducir la propagación de amenazas y daños a la red.

Acciones específicas:

Implementar políticas de seguridad para cada segmento de las subredes de la red.

Implementar VLANs para separar los flujos de tráfico, reduciendo la posibilidad de que un atacante ingrese a la red por completo.

Usar controles de acceso para filtrar el tráfico entre las subredes.

VI. Estrategias de Mitigación y Protección de Activos Críticos

1. Implementación de controles de acceso

Activos involucrados:

- Servidores
- Bases de datos
- Sistemas de red

Amenazas:

- Acceso no autorizado
- Explotación de vulnerabilidades

Medidas de Mitigación:

- Implementar autenticación Multifactor
- Control de acceso del personal
- Realizar auditorías de manera constante a los accesos de los sistemas.

2. Uso de cifrado

Activos involucrados:

- Bases de datos
- Servidores de almacenamiento

Amenazas:

- Intercepción de datos

- Acceso no autorizado

Medidas de Mitigación:

- Implementar cifrado de datos en todas las bases de datos
- Implementar un sistema seguro para gestionar y almacenar claves.

3. **Actualización de hardware y software**

Activos involucrados:

- Servidores
- Routers
- Switches

Amenazas:

- Fallos en la infraestructura
- Explotación de vulnerabilidades

Medidas de Mitigación:

- Establecer procedimientos de seguridad para todos los sistemas de la empresa.
- Realizar mantenimiento de los dispositivos de red.

4. **Protección física de activos**

Activos involucrados:

- Servidores
- Routers
- Switches
- Generadores
- UPS

Amenazas:

- Acceso no autorizado

- Desastres naturales
- Robo

Medidas de Mitigación:

- Implementar sistemas de acceso.
- Instalar cámaras de vigilancia en toda la empresa.
- Instalar sistemas de protección contra desastres naturales.

VII. Estrategias de Mitigación de Riegos

Sección de controles:

- **Control preventivo:**

  Implementación de refuerzos para proteger ante los desastres naturales, mantenimiento de hardware y software, y actualización de políticas.

- **Control detectivo:**

  Implementar sistemas de detección de intrusos para identificar actividades sospechosas de manera rápida.

- **Control correctivo:**

  Realizar planes de contingencia y recuperación de información ante desastres naturales.

Implementación de controles: Implementar cada control con un cronograma especifico con su respectiva asignación de responsabilidades.

Políticas y Procedimientos: Actualizaciones de las políticas de seguridad y documentar todas las prácticas de seguridad para verificar el seguimiento de todo el personal.

VIII. Programa de Formación y Concientización

Objetivo del programa

Concientizar al personal sobre el manejo de la seguridad de la información y como su comportamiento afecta la protección de los datos sensibles de la empresa.

Grupos de Interés

Este programa está dirigido a la organización de la empresa que tenga interacción con los sistemas de información incluyendo a la Gerencia Técnica y Gerencia General.

Métodos de Entrega

Se detalla las responsabilidades de cada grupo:

1. **Capacitación inicial**
    - Información al personal sobre las políticas de seguridad
    - Cada 6 meses reforzar el conocimiento sobre las amenazas y regulaciones de seguridad a todo el personal de la empresa.
2. **Módulos de formación**
    - Introducción a la seguridad de la información
    - Autenticación
    - Identificación de incidentes de seguridad
    - Seguridad en dispositivos móviles
    - Cumplimiento de normas
3. **Simulacros y pruebas**
    - Simulacros de incidentes de seguridad
    - Evaluación de los empleados para lograr identificar amenazas y que se debe de hacer en ese momento.

4. **Evaluación y seguimiento**
    - Evaluar el conocimiento adquirido durante la capacitación
    - Cada semestre revisar el nivel de cumplimiento de conocimiento del personal de la empresa con respecto a las políticas de seguridad.

IX. Monitoreo y Revisión

El monitoreo y la revisión son fundamentales para ver la efectividad de las políticas de seguridad implementadas en la empresa.

Método de monitoreo: Técnicas utilizadas para monitorear la seguridad de los controles de seguridad.

Frecuencia de las revisiones: Actualización y mejora del plan validando que las medidas de seguridad sean efectivas antes las amenazas identificas y nuevas.

XII. Mejora Continua

Actualización de políticas: Siempre realizar revisiones y actualizaciones de las políticas de seguridad.

Revisión tecnológica: Mantenerse siempre informado de las nuevas tecnologías y herramientas para mejor la seguridad de la información de la empresa.

XIII. Plan de Acción

Acciones inmediatas:

1. **Formación del equipo de seguridad:** Formación de un equipo el cual supervisara la implementación y mejora del plan de seguridad de la empresa.
2. **Asignación de recursos humanos:** Recursos para ejecutar todas las fases del plan con capacitaciones, soporte financiero adecuados y herramientas tecnológicas.

3. **Desarrollo de las políticas y procedimientos:** Este manual desarrollado es su primera versión de las políticas de seguridad a partir de este se basa para seguir actualizando la información de manera continua asegurando que refleje las mejores prácticas.
4. **Capacitación inicial:** Realizar capacitaciones con enfoqué a las nuevas políticas de seguridad se debe de garantizar que todo el personal de la empresa comprenda las amenazas de seguridad.
5. **Inicio de la implementación de las medidas de seguridad:** Implementar las actualizaciones de hardware y software para que los activos estén protegidos ante amenazas.

Corto Plazo (0 – 6 meses):

1. **Implementación de medidas de seguridad:** realizar actualización de hardware y software en servidores, sistemas y dispositivos de la red.
2. **Revisión de accesos críticos:** verificar los niveles de acceso de los usuarios en sistemas principales de la empresa.
3. **Copias de seguridad:** Actualizar sistemas de copias de seguridad.

Mediano Plazo (6-12 meses):

1. **Fortalecimiento de ciberseguridad:** Actualizar las políticas que ya están diseñadas e implementar controles de firewall avanzadas.
2. **Simulacros de recuperación de información:** Realizar simulacros para poner a prueba la efectividad del plan al momento re recuperar la información ante desastres.
3. **Monitoreo de seguridad:** Tener sistemas de monitoreó en tiempo real para prevenir incidentes de seguridad.
4. **Auditorias:** Realizar auditorías para verificar la efectividad de las medidas implementadas y modificarlas en caso de tener nuevas amenazas.

Largo Plazo (12-24 meses):

1. **Recisiones periódicas del plan de seguridad:** Actualizaciones de políticas y procedimientos basándose en las auditorías internas que se van a realizar.
2. **Mejora continua:** Implementar mejoras de las auditorías internas y simulacros de la empresa con esto se tendrá evoluciones conforme se va avanzando en la tecnología digital.

XIV. Cumplimiento Legal y Normativo

El cumplimiento legal y normativo es fundamental para l agestión de la información ya que garantiza que las políticas se seguridad este creadas conforme a las leyes.

Ley Orgánica de Protección de datos Personales

Esta ley regula como las empresas deben manejar y proteger los datos personales de los clientes y trabajadores. Las medidas implementadas aseguran que los datos sean manejados bajo controles de confidencialidad. Se tiene la implementación de controles de acceso y monitoreo constante para evitar tener accesos no autorizados.

Normativa de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

El ARCOTEL es el encargado de regular y controlar las telecomunicaciones, sus normativas están orientadas a la presta de servicios de telecomunicaciones. De esta normativa tienes el siguiente cumplimiento, implementación de medidas para garantizar la presta de servicios de telecomunicaciones con la minimización de los riesgos de la empresa.

Código orgánico Integral Penal (COIP)

El código orgánico integral penal del ecuador regula los delitos y sanciones penales de las actividades ilegales. Esta normativa tiene penas para los que cometen fraude cibernético, robo de datos y acceso no autorizado. Y el cumplimiento con este código tenemos la implementación de controles para prevenir accesos no autorizados y ciberataques.

Ley Orgánica de Telecomunicaciones

La ley orgánica de telecomunicaciones regula las actividades sobre seguridad y protección de la infraestructura y tiene medidas de seguridad de la re y protección del usuario. Del cumplimiento de esta ley tenemos la implementación de medidas que garantizan la disponibilidad de servicios y asegurando la operabilidad de la empresa este alineada con los estándares técnicos y normativas establecidas por las autoridades.

Proceso de Implementación de la Norma ISO/IEC27001:2013

La norma ISO/IEC 27001:1013 es un estándar internacional en el cual define los requisitos para implementar un Sistema de Gestión de Seguridad de la Información, lo que se avanzado en la implementación es la identificación de áreas que permitan cumplir con los requisitos de la norma, se creó las políticas y procedimientos asegurando el cumplimiento de la norma. Ya que se tengan implementados los controles se iniciará una auditoria con el fin de obtener una certificación.

SITEC S.A

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA EMPRESA

VERSION 1.0

Versión	**1.0**
Elaborado por:	**Sra. Jessica Fernanda Chiquito Caiza**
Firma:	Firmado electrónicamente por: JESSICA FERNANDA CHIQUITO CAIZA. Validar únicamente con FirmaEC
	MSc. Fabián Cuzme Rodríguez
Firma:	Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ. Validar únicamente con FirmaEC
Fecha de Elaboración:	**20/09/2025**
Revisado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC
Fecha de Revisión:	**23/10/2025**
Aprobado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC
Fecha de Aprobación:	**24/11/2025**
Aprobado por:	**Ing. Fernando Obando**
Firma:	Firmado electrónicamente por: CARLOS MARIO FERNANDO OBANDO VILLADA. Validar únicamente con FirmaEC

Manual de Politicas de Seguridad

1. **Objetivo del Manual**

   El siguiente manual tiene como objetivo establecer un conjunto de políticas de seguridad para la protección de los activos de la empresa SITEC S.A. Estas políticas están diseñadas para mitigar riesgos, proteger la confidencialidad, integridad y disponibilidad de la información de la empresa.

2. **Alcance**

   Este manual aplica a los empleados de la empresa SITEC S.A. a todos los que tengan acceso de los sistemas, datos, infraestructura y servicios de la empresa. Se cubren aspectos relacionados con la seguridad física y lógica, control de acceso y manejos de información.

3. **Levantamiento de Políticas de Seguridad**

Proceso para el Levantamiento de Políticas de Seguridad:

1. **Formas del Equipo de Trabajo:** Establecer un equipo que será responsable de definir y revisar las políticas de seguridad. Se incluirá personal de tecnología de la información, seguridad, gestión de riesgos, operaciones y representantes de alta dirección.
2. **Identificación de Requisitos**: Identificar los requisitos legales, normativos y corporativos que deben cumplirse.
3. **Análisis de Riesgo:** Realizar un análisis de riesgo para identificar las amenazas y vulnerabilidades, que son necesarias para las políticas de seguridad.
4. **Desarrollo de Políticas:** Redactar las políticas basadas en los requisitos identificados y tomar en cuenta los resultados del análisis riesgo. Las políticas cubren áreas del control de acceso, la protección de datos, la seguridad física, la gestión de incidentes y continuidad del negocio.

5. **Revisión y Aprobación:** Las políticas creadas deben someterse a una revisión detallada por parte del equipo de trabajo y obtener la aprobación.
6. **Implementación y difusión:** Implementar las políticas de seguridad y asegurar su difusión a todo el personal de la empresa.
7. **Monitoreo y actualización**: Establecer un proceso de monitoreo continuo para asegurar que las políticas de seguridad este actualizadas.

4. Políticas de Seguridad

4.1 Política de Gestión de Accesos

Objetivo: Controlar el acceso del personal a la empresa para asegurar que solo el personal autorizado tenga acceso a los sistemas y a la información.

Alcance: Aplicar control de acceso a todos los sistemas de información de la empresa.

Políticas:

- **a.** Definir niveles de acceso con su respectivo permiso para el personal en base de sus responsabilidades.
- **b.** Implementar mecanismos de autentificación, como autenticación multifactor (MFA), para reducir la probabilidad de accesos no autorizados en las plataformas de los equipos Huawei y VPN.
- **c.** Activar servicios de Logs a sistemas críticos que corresponden a bases de datos y a los dispositivos de accesos a la red.
- **d.** Accesos por VPN seguras que corresponden a las actualizaciones de las NIST SP 800-77 R1

e. Realizar revisiones constantes de los accesos para asegurar que sean apropiados y estén alineados con las funciones actuales de cada empleado, tomando en cuenta con los cambios en la estructura organizativa.

4.2 Política de Protección de Datos

Objetivo: Resguardar la datos sensibles, datos almacenados y datos transmitidos por la empresa.

Alcance: asegurar datos financieros, datos operativos y datos de clientes que se encuentren almacenados en la base de datos.

Políticas:

a. Establecer medidas de protección para la clasificación de datos sensibles asegurando la información para que se maneje conforme a los principios de confidencialidad, integridad y disponibilidad.

b. Implementar medidas de encriptación para proteger los datos en tránsito y en reposo, asegurando que la información confidencial sea inaccesible para usuarios no autorizados, se consideran los siguientes algoritmos según las recomendaciones del NIST SP 800-111 R1:

Encriptación Simétrica:

- AES (Advanced Encryption Standard): Estándares recomendados para la protección de datos en repodo y en tránsito.

Encriptación Asimétrica:

- RSA (Rivest-Shamir-Adleman): Longitudes de clave de al menos 2048 bits para seguridad básica o 3072 bits para mayor robustez.

Algoritmo de Hash:

- SHA-2 (Secure Hash Algorithm) y SHA-512 (Secure Hash Algorithm: algoritmos para garantizar la integridad de los datos.
- SHA-3(Secure Hash Algorithm): Recomendado para aplicaciones que requieren mayor resistencia criptográfica.

Intercambios de claves:

- Diffie-Hellman (DH) y Elliptic Curve Diffie-Hellman (ECDH): Métodos robustos para establecer claves compartidas.

Firma digital:

- RSA (Rivest-Shamir-Adleman): Garantizar la autenticidad de los datos.
- ECDSA: Firma digital basada en curva elípticas
- EdDSA: (Edwards-Curve Digital Signature Algorithm): Algoritmo para escenarios que requieran velocidad y seguridad.

c. Asegurar que los datos se almacenen y manejen conforme a las normativas de protección de datos, mediante la implementación de estándares internacionales y algoritmos criptográficos recomendados por NIST.

d. Implementar DLP (Prevención de Pérdidas de Datos) con la finalidad de proteger los datos críticos de la empresa evitando que salgan de la red corporativa de forma no autorizada, ya sea por error, malicia o negligencia

4.3 Política de seguridad física

Objetivo: Garantizar protección física de los activos mediante algunos controles para prevenir perdidas, robo o daños.

Alcance: Aplicar a todos los puntos de acceso de la empresa.

Políticas:

- **a.** Implementar controles físicos para restringir el acceso a las instalaciones criticas tales como los servidores, equipos de red y otros dispositivos que son fundamentales para la empresa.
- **b.** Asegurar la protección física de los equipos y dispositivos tomando medidas como cámaras de vigilancia, sistemas de alarma y acceso autorizado.
- **c.** Establecer procedimientos para la protección de equipos físicos, con el fin de evitar su perdida, robo o acceso no autorizado.
- **d.** Establecer el proceso de registro e identificación de equipos nuevos.
- **e.** Implementar controles de salida de equipos y el tiempo establecido para su devolución y realizar un plan de mantenimiento de equipos.
- **f.** Implementar inventario de Equipos.

4.4 Política de Gestión de Incidentes

Objetivo: Definir procesos de identificación, respuesta y soluciones de incidentes que permitan defender los activos de la empresa.

Alcance: Aplicar a todos los involucrados de la seguridad de la información ante incidentes de ataques, violaciones de datos y fallos en el hardware y software.

Políticas:

- **a.** Definir un proceso para la identificación, reporte y respuesta de accidentes de seguridad para actuar se forma rápida y mitigar los daños.
- **b.** Establecer un equipo de respuesta a incidentes con actividades y responsabilidades, para actuar de manera organizada y minimizar el impacto de los incidentes en la empresa.
- **c.** Implementar un sistema de registro y análisis de incidentes, con esto evaluar los incidentes ocurridos y tener un análisis, con esto prevenir incidentes futuros.

d. Establecer mecanismo de gestión de incidentes que involucren la participación de proveedores externos.

4.5 Política de Continuidad del negocio

Objetivo: Asegurar que los sistemas de la empresa puedan seguir funcionando ante amenazas o desastres.

Alcance: Aplicar la política a todos los sistemas como servidores, bases de datos, redes, móviles y aplicaciones esenciales.

Políticas:

a. Desarrollar un plan de continuidad del negocio con esto se asegura la operatividad de los servicios de la empresa ante fallos de infraestructura o situaciones inesperadas.

b. Implementar plan de continuidad que verifique la efectividad y asegure que los procedimientos sean funcionales en situaciones emergentes.

c. Establecer procedimientos de recuperación antes desastres, tener respaldos de datos y equipos disponibles para ser implementados de forma rápida ante una emergencia.

5. Cronograma de ejecución de los Procesos de las Políticas

Tenemos tres tipos de tiempos estimados para la realización de los controles de cada una de las políticas. Estos controles se van a clasificar dependiendo de su medida de atención que serán corto plazo (0 0- 6 meses), mediano Plazo (6- 12 meses) y lago plazo (12 – 24 meses).

Corto plazo (0 – 6 meses)

En la Tabla 19 tenemos los controles que son prioridad alta para ser atendidas. Tenemos el control a seguir, el tiempo establecido para realizar este control y el responsable de la empresa que va a realizar este control.

Tabla 19

Cronograma de controles de políticas a corto plazo.

Controles	**Tiempo estimado**	**Responsable**
Definir niveles de acceso y permisos por rol.	1 mes	Presidente / Gerencia Técnica
Implementar autenticación MFA	1-2 meses	Presidente / Gerencia Técnica
Activar logs en los sistemas críticos	2 meses	Técnico
Habilitar acceso VPN seguro	2 meses	Técnico
Clasificar datos sensibles	1 mes	Presidente / Gerencia Técnica
Implementar encriptación	2 meses	Presidente / Gerencia Técnica
Configuración DLP (Prevención de perdida de datos)	2 meses	Técnico
Identificar áreas críticas físicas	1 mes	Técnico
Instalar cámaras de seguridad	1 mes	Técnico

Restringir acceso físico a servidores y racks	2 meses	Técnico
Inventario de equipos	1 mes	Técnico
Crear registros de salida de equipos	1 mes	Presidente / Gerencia Técnica
Establecer equipos de respuesta a incidentes	1 mes	Presidente / Gerencia Técnica
Identificar sistemas y datos críticos del negocio	1 mes	Técnico
Crear respaldos automáticos	2 mes	Presidente / Gerencia Técnica
Crear un plan de recuperación ante desastres (DRP)	2 meses	Presidente / Gerencia Técnica

Mediano Plazo (6 -12 meses)

En la Tabla 20 tenemos los controles de fortalecimiento estables y avanzados. Tenemos el control a seguir, el tiempo establecido para realizar este control y el responsable de la empresa que va a realizar este control.

Tabla 20

Cronograma de controles de políticas a mediano plazo.

Control	Tiempo estimado	Responsable
Revisión periódica de acceso y ajuste a sistemas de la empresa	6 -12 meses	Presidente / Gerencia Técnica

Configurar intercambio de claves con ECDH (Elliptic-curve Diffie-Hellman)	7 meses	Presidente / Gerencia Técnica
Implementar DLP (Prevención de pérdida de datos)	8 meses	Presidente / Gerencia Técnica
Registro de equipos y verificarlos	6 meses	Técnico
Probar el plan de recuperación ante desastres (DRP)	6 meses	Todos los empleados.
Realizar simulacros y pruebas de restauración	8 meses	Todos los empleados.
Evaluación de incidentes reportados	8 meses	Técnico

Largo Plazo (12 – 24 meses)

En la Tabla 21 tenemos los controles que son mejora continua, la madurez del sistema SGSI. Tenemos el control a seguir, el tiempo establecido para realizar este control y el responsable de la empresa que va a realizar este control.

Tabla 21

Cronograma de controles de políticas a largo plazo.

Control	**Tiempo estimado**	**Responsable**
Automatizar sistema de inventario	15 meses	Presidente / Gerencia Técnica

Automatizar control de salida de equipos	15 meses	Presidente / Gerencia Técnica
Actualización del plan DRP (Plan de recuperación ante desastres)	19 meses	Presidente / Gerencia Técnica
Actualizar políticas según auditorias y riesgos.	15 meses	Presidente / Gerencia Técnica
Simulacros anuales de continuidad del negocio	12 meses	Todos los empleados

5.1 Análisis de la política implementada de Gestión de Accesos Literal C.

Los logs en general son registros automáticos que generan los sistemas con el fin de dejar constancia de todas las actividades que ocurre en el equipo, servidor o en la red. Estos registros permiten monitorear eventos, detectar errores y fortalecer la seguridad de la información. En el ANEXO 4 se presenta la guía de aplicación de la política de gestión de Accesos, política que dice activar servicios de Logs a sistemas críticos que corresponden a bases de datos y a los dispositivos de accesos a la red. Para ello primero se accedió al programa Winbox, que permite la conexión y administración del dispositivo MikroTik. Una vez realizada la conexión se procedió a la activación de cuatro tipos de logs: critial, error, info y warning. El log critical permite identificar situaciones críticas como sistemas de archivo en modo de solo lectura; el log error se utiliza para visualizar fallo del sistema, problemas de configuración, servicios que no funcionen correctamente y errores de red; el log info registra los inicios y cierres sesión de usuarios, conexiones y desconexiones de PPoE y mensajes del sistema y el log warning corresponde a advertencias, permitiendo observar eventos como cambios en interfaces, retrasos o respuestas lentas, intentos fallidos y problemas temporales de red. Una

vez que tenemos aplicados estos logs se realizaron las pruebas correspondientes para de cada uno de los logs y evidenciar su correcto funcionamiento.

Con respecto de la base de datos el sistema cuenta por defecto con logs habilitados por lo que se seleccionaron tres logs principales con el objetivo de cumplir funciones similares del MicroTik. Se activo el log auth.log que permite observar accesos por consola y logins, siendo fundamental para la seguridad y el control de accesos; el log syslog que registra eventos del sistema, servicios y errores en general y el log pve-firewall.log el cual permite monitorear la seguridad del firewall de Proxmox incluyendo paquetes bloqueados, reglas aplicadas, tráfico, análisis de paquetes y seguridad. Se realizaron las pruebas correspondientes para verificar el funcionamiento, confirmándose la correcta aplicación y operación de estos.

6. Conclusiones y Recomendaciones

6.1 Conclusiones

A través de una recolección de información se logró identificar los activos críticos de la empresa, con esto realizar una evaluación de riegos mediante la metodología MAGERIT permitiendo identificar amenazas y vulnerabilidades de la infraestructura tecnológica de la empresa SITEC S.A.

Durante el análisis de la infraestructura tecnológica de la empresa SITEC. S.A se identificó que carecía de procesos documentados y mecanismos de monitoreo. Con ello se procede a definir e implementar controles técnicos y organizativos, que mitigan los riesgos y garantizan una respuesta más rápida y eficaz ante incidentes futuros.

Con el análisis de riesgo se mostró los riesgos relacionados con accesos no autorizados, fallos de red, fallos de infraestructura y manejo inadecuado de equipos. Estos riesgos fueron clasificados en 5 niveles (Muy Bajo, Bajo, Moderado, Alto, Crítico) de los cuales los niveles Moderado, Alto y Critico son los que requieren atención inmediata.

Para diseñar las políticas de seguridad para cada uno de los riesgos se basó en el estándar de la norma ISO/IEC 27001 la cual está orientada a proteger la confidencialidad, integridad y disponibilidad de la información. Las políticas que se desarrollaron fueron de gestión de accesos, protección de datos, seguridad física, gestión de incidentes y continuidad del negocio. Las políticas de seguridad son una base fundamental para el desarrollo de un SGSI (Sistema de Gestión de Seguridad de la Información) ya que están alineados con estándares internacionales.

Con la aplicación de este SGSI (Sistema de Gestión de Seguridad de la Información) donde consta de controles de riesgos, políticas de seguridad y estrategias, permitan a la empresa SITEC S.A a mejorar su ciberseguridad, reduciendo riesgos graves. En el ANEXO 4 se muestra la aplicación de una política con sus respectivas pruebas.

La investigación realizada demuestra que la seguridad de la información no depende solo de la parte tecnológica, sino también de procesos, roles, personal y responsabilidades bien definidas en todos los niveles de la empresa.

6.2 Recomendaciones

Realizar auditorías internas en la empresa por lo menos una vez al año para realizar una evaluación de los controles implementados, políticas de seguridad y garantizar la mejora continua de los procesos.

Proteger la gestión de acceso de la empresa SITEC S.A mediante la implementación de revisiones semestrales, que permita verificar de forma sistemática el personal activo y sus responsabilidades. Con esto garantizando el acceso innecesario o no autorizado por el personal.

Implementar herramientas avanzadas de monitoreo en tiempo real como DLP (Prevención de perdida de datos), que permita identificar, alertar y responder de forma rápida antes comportamientos anómalos con esto prevenir fugas de datos.

Capacitar al personal técnico y administrativo de la empresa continuamente sobre el manejo seguro de la información. Respuestas a incidentes y el uso adecuado de los sistemas críticos de la empresa.

Actualizar las políticas de seguridad cada 6 meses y de forma inmediata ante cambios importantes en la infraestructura de red, regulaciones, riesgos o amenazas en la empresa. Toda actualización debe ser documentada y validad para asegurar su correcta implementación y cumplimiento organizacional.

Mantener un inventario de la información crítica disponibilidad sobre el estado actual de la infraestructura de la red o física, ya que dicha información servirá para mejorar el tiempo de resolución de fallos y ayudar a nuevos administradores con esta información.

Bibliografía

Affairs. (2023). *Informe de los Objetivos de Desarrollo Sostenible 2023: Edición especial*. United Nations. https://doi.org/10.18356/9789210024938

Amutio Gómez, M. A. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

ARCOTEL. (2018, diciembre 5). Requisitos: ACCESO A INTERNET - Agencia de Regulación y Control de las Telecomunicaciones. *Agencia de Regulación y Control de las Telecomunicaciones - Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios.* https://www.arcotel.gob.ec/requisitos-acceso-a-internet2/

ASAMBLEA NACIONAL DEL ECUADOR. (2008). *ASAMBLEA NACIONAL DEL ECUADOR*. Imprenta del Gobierno.

Barrezueta, H. D. P. (2021). *DIRECTOR DEL REGISTRO OFICIAL*.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2020). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

DiMaggio, J. (2022). *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press.

Farinango Farinango, M. F. (2023). *Desarrollo de un plan de contingencia de servicios TI para la dirección de tecnologías de la información del Gobierno Autónomo*

Descentralizado Municipal de San Miguel de Ibarra, aplicando el marco de trabajo ITIL V3 [bachelorThesis]. https://repositorio.utn.edu.ec/handle/123456789/14762

Greene, B. R., & Smith, P. (2020). *Cisco ISP Essentials*. Cisco Press.

Gutiérrez, N. (2022, febrero 17). *30 Estadísticas sobre Seguridad Informática | Prey Blog*. https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Guzmán Iles, S. S. (2023). *Diseño de un Sistema de Gestión de la Seguridad de la Información para el Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte basado en la Norma ISO/IEC 27001* [bachelorThesis]. https://repositorio.utn.edu.ec/handle/123456789/14069

Humphreys, E. (2007). *Implementación del estándar del sistema de gestión de seguridad de la información ISO/IEC 27001*. https://www.google.com.ec/books/edition/Implementing_the_ISO_IEC_27001_Informati/wa8ZAQAAIAAJ?hl=es-419&gbpv=0&bsq=%22Implementing%20the%20ISO/IEC%2027001%20Information%20Security%20Management%20System%20Standard%22%20de%20Edward%20Humphreys%20en%20Amazon

INNOTEC, F. S.-. (2023, diciembre 29). *Inicio*. PILAR. https://pilar.ccn-cert.cni.es/

ISO 27001 Seguridad de la Información | Normas ISO. (s. f.). Recuperado 16 de noviembre de 2024, de https://www.normas-iso.com/iso-27001/

Kosseff, J. (2022). *Cybersecurity Law*. John Wiley & Sons.

Ocasio, K. (2023, mayo 29). *43 Small Business Cybersecurity Statistics*. Small Business Trends. https://smallbiztrends.com/small-business-cybersecurity/

Perugachi Espinosa, C. A. (2018). *Modelo de seguridad de gestión de la información basado en la norma ISO 27001, para el data-center de la facultad de Ingeniería en Ciencias*

Aplicadas, en la Universidad Técnica del Norte [bachelorThesis]. https://repositorio.utn.edu.ec/handle/123456789/7933

Salomon, D. (2020). *Data Privacy and Security*. Springer Science & Business Media.

Samaniego Mena, E., & Ponce Ordóñez, J. (2021). *Libro Fundamentos de seguridad informática*.

Steinberg, J. (2019). *Cybersecurity For Dummies*. John Wiley & Sons.

Taplin, R. (2019). *Managing Cyber Risk in the Financial Sector: Lessons from Asia, Europe and the USA*. Routledge.

ANEXOS

ANEXO 1

1. **TEMA:** REUNIÓN TÉCNICA PARA IDENTIFICAR ACTIVOS Y PASIVOS CON SU RESPECTIVA VALORACIÓN EN SITEC S.A
2. **LUGAR DE LA REUNIÓN:** Oficina General Técnica – SITEC S.A, matriz.
3. **PARTICIPANTES:**

   Presidente/Gerente técnico: Ing. Obando Villada Carlos Mario Fernando.

   Tesista de Ingeniería en Telecomunicaciones: Sra. Chiquito Caiza Jessica Fernanda.

4. **OBJETIVO DE LA REUNIÓN:**

   Identificar los activos y pasivos que existen en la empresa SITEC S.A, para asignarles valores en cuanto a su importancia, impacto y probabilidad de amenaza en base a los criterios establecidos por la metodología MAGERIT versión 3, como parte del desarrollo del análisis de riegos del Capítulo III.

5. **DESCRIPCIÓN DE LA REUNIÓN:**

   En esta reunión, se llevó a cabo la identificación de los activos y pasivos que componen el sistema de información de SITEC SA. Se incluyeron tanto los recursos tecnológicos (hardware y software), como los recursos humanos y pasivos físicos (infraestructura de soporte). Con la guía del Ing. Obando Carlos, se verificó la existencia, funcionalidad y criticidad de cada uno de estos componentes, evaluando su impacto en las operaciones de la empresa. Además, se realizarán valoraciones cualitativas respecto al impacto que podría generar una posible (hardware y software), como los recursos humanos y pasivos físicos (infraestructura de soporte).

6. RESULTADOS OBTENIDOS:

A partir de esta reunión, se identificaron los siguientes grupos de activos:

Nombre Activo	Descripción
OLT Huawei (Optical Line Terminal)	Software propietario Huawei utilizado para gestionar la transmisión de datos entre la red de acceso de fibra óptica y red troncal.
Switch Cisco Borde	Dispositivo utilizado para la conmutación de datos en la red.
Router MikroTik	Se tiene tres de borde, uno de proveedor y dos de corporativos. Equipos de control de red LAN y acceso a la red WAN.
Switch POE (Power over Ethernt)	Dispositivo de trasmisión de datos que suministra energía eléctrica a los dispositivos conectados a través del mismo cable Ethernet como las cámaras de seguridad o puntos de accesos inalámbricos.
Servidor Core i7	Servidor con Proxmox - DNS Cache en Debian: Servidor configurado para consultas DNS, mejorando el rendimiento y reducido el tiempo de respuesta en la red. - Monitoreo Zabbix: Monitoreo de la infraestructura de la red. - Radius en Debían: Servidor de autentificación y autorización al acceso de la red.

	- Telefonía Issabel basado en Linux: Gestiona las llamadas VoIP.
Baterias gel	Respaldo de energía su propósito es tener encendida el nodo mientras no exista energía eléctrica y mientras se enciende el generador.
Inversor 3kva	Cambiar la energía de las baterías 12v o 24v a 110v
ATS (Automatic Transfer Switch)	Mecanismo para prender automáticamente la energía por generador.
Generador 6500kva	Sirve para generar energía y mantener los nodos encendidos
Onus (Optical Network Units)	Dispositivo por donde los clientes acceden a internet.
Vehiculo	Realizar trabajos en campo
ONT (Optical Network Terminal)	Software de propietario Huawei utilizado para conectar los usuarios a través de la red óptica.
Cable de Fibra óptica	Se utiliza para la transmisión de datos a largas distancias de la red.
Patchcord	Cable de conexión utilizado para interconectar algunos dispositivos dentro de la red.
NAP (Network Access Point)	Dispositivo para conectar los usuarios a la red.
ODF (Optical Distribution Frame)	Dispositivo que facilita la gestión de las conexiones óptica y asegura que la señal se redirija correctamente.

Mangas	Elemento de protección para cables dentro de la infraestructura de la red.
Rack de Piso y pared	Estructuras utilizadas para montar y organizar los dispositivos de red como switches, routers y servidores.
Gabinete metálico de piso y poste	Es un armario de seguridad donde se almacenan equipos electrónicos como servidores o switches.
Splitter óptico	Dispositivo utilizado para dividir una señal de fibra óptica en varias señales.
Barra Tensora	Estructura utilizada para soportar y tensar cables.

Activo de nómina

Nombre	**Cargo**	**Sucursal**
León Gudiño Susana del Rocío	Gerente General / Administración	Matriz
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	Matriz
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	Matriz
Rodríguez Stalyn	Técnico	Ibarra/Otavalo
Vallejo Fabricio	Técnico	Ibarra/Otavalo
Romero Roberth	Técnico Externo	Ibarra
Jácome Roberto	Técnico Externo	Otavalo

Después de identificar los activos se evalúa cada uno a una escala de valoración de 1 a 5. Valoración que se toma de la metodología MAGERIT.

- ✓ **Valor del activo:** importancia de la empresa.
- ✓ **Impacto:** consecuencias de incidentes sobre el activo.
- ✓ **Probabilidad:** frecuencia estimada de ocurrencia de una amenaza.

Activos

Activo	Valor	Impacto	Probabilidad
OLT Huawei (Optical Line Terminal)	5	5	4
Switch Cisco Borde	5	4	3
Router MikroTik	5	4	4
Switch POE (Power over Ethernt)	3	3	3
Servidor Core i7	5	5	4
Baterias gel	5	5	4
Inversor 3kva	4	4	3
ATS (Automatic Transfer Switch)	4	4	3
Generador 6500kva	5	4	3
Onus (Optical Network Units)	5	5	4
Vehiculo	5	3	5
ONT (Optical Network Terminal)	5	5	5
Cable de Fibra óptica	5	5	4

Patchcord	5	3	2
NAP (Network Access Point)	5	3	2
ODF (Optical Distribution Frame)	5	4	3
Mangas	5	3	2
Rack de Piso y pared	5	4	2
Gabinete metálico de piso y poste	5	3	3
Splitter óptico	5	3	2
Barra Tensora	5	3	2

Activo Personal

Nombre	**Cargo**	**Valor**	**Impacto**	**Probabilidad**
León Gudiño Susana del Rocío	Gerente General / Administración	5	5	3
Obando Villada Carlos Mario Fernando	Presidente / Gerencia Técnica	5	5	4
León Gudiño Marcelo Wladimir	Secretario, Encargado de regulación	4	4	4
Rodríguez Stalyn	Técnico	4	3	3
Fabricio Vallejo	Técnico	4	3	3
Romero Roberth	Técnico Externo	3	3	2
Jácome Roberto	Técnico Externo	3	3	2

Se da la valoración a los activos y con estos valores son utilizados para calcular el nivel de riesgo con la fórmula Riesgo = Impacto * Probabilidad. Y con el resultado del nivel de riesgo se realiza una clasificación en los siguientes niveles:

- **Crítico (21 – 25)**
- **Alto (16 – 20)**
- **Moderado (11 – 15)**
- **Bajo (6 – 10)**
- **Muy bajo (1 – 5)**

Con esta clasificación permite priorizar las acciones de control y mitigación con los principios de gestión de riego de MAGERIT.

7. CONCLUSIÓN DE LA REUNIÓN

En esta reunión se identificaron los activos y pasivos presentes en la empresa, evaluando para cada uno de los activos su valor, impacto y probabilidad. Con estos valores, se calculó el nivel de riesgo asociado a cada activo.

Firmado electrónicamente por:
CARLOS MARIO FERNANDO OBANDO VILLADA
Validar únicamente con FirmaEC

Ing. Obando Villada Carlos Mario Fernando

Firmado electrónicamente por:
JESSICA FERNANDA CHIQUITO CAIZA
Validar únicamente con FirmaEC

Sra. Chiquito Caiza Jessica Fernanda

ANEXO 2

1. TEMA: PRESENTACIÓN Y ANÁLISIS DE LOS CONTROLES PROPUESTOS PARA LOS RIESGOS IDENTIFICADOS EN LOS ACTIVOS DE LA EMPRESA

2. **LUGAR DE LA REUNIÓN:** Oficina General Técnica – SITEC S.A, matriz.

3. PARTICIPANTES:

Presidente/Gerente técnico: Ing. Obando Villada Carlos Mario Fernando.

Tesista de Ingeniería en Telecomunicaciones: Srta. Chiquito Caiza Jessica Fernanda.

4. OBJETIVO DE LA REUNIÓN:

Presentar los controles propuestos para mitigar los riesgos identificados en los activos de la empresa, basados en una búsqueda de los controles más adecuados desde de los programas Mitratec, AEIS SBC y OSware y seleccionar cuál de los controles propuestos es el más adecuado según el nivel de riesgo asociado a cada activo.

5. DESCRIPCIÓN DE LA REUNIÓN:

La reunión se realizó la presentación del análisis de riesgos para los activos de la empresa. Se identifican varios riesgos asociados a los activos, y para cada uno se propuso tres controles específicos. Estos controles fueron obtenidos mediante una búsqueda en las herramientas Mitratec, AEIS SBC y OSware, que proporcionan medidas especializadas para la gestión de riesgos en infraestructura tecnológica.

Tras la presentación de los controles, el Ing. Obando Villada Carlos Mario Fernando dedicó tiempo a leer y analizar cada uno de los controles propuestos. Durante este proceso, se discutieron los posibles impactos y la aplicabilidad de los controles en relación con los riesgos identificados. El Ing. Obando evaluó cuáles controles serán los más apropiados para cada activo en función de su importancia y criticidad. El control que este coloreado de color verde es el que se elige el control propuesto para cada uno de los riesgos.

6. RESULTADOS OBTENIDOS:

Selección del control propuesto para el riesgo de los activos, se lo identifica la aprobación con color verde. A continuación, se presentan cada uno de los activos:

- **Activos en Hardware**

1. OLT Huawei (Optical Line Terminal)

   Riesgo: Fallo del hardware, afectando la conectividad de los usuarios.

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Implementación de redundancia de equipos críticos	Monitoreo en tiempo real del estado y rendimiento.	Actualizaciones automáticas de firmware y software.

2. Switch Cisco Borde

   Riesgo: Fallas por sobrecarga

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Configuración de QoS Calidad de Servicio	Análisis de tráfico para detección de anomalías.	Gestión centralizada de configuraciones

3. Router MikroTik

   Riesgo: Ataques de Denegación de servicio distribuido (DDoS)

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 Propuesto (OSware)**

Implementación de firewall con reglas específicas	Monitoreo de tráfico para detección de patrones DDoS	Protección contra ataques de denegación de servicio

4. Servidor Core i7

   Riesgo: Infección por malware y pérdida de datos

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Instalación de software antivirus y antimalware	Encriptación de discos y respaldos de datos	Segmentación de red para limitar accesos no autorizados

5. Generador 6500kva

   Riesgo: Falla por falta de mantenimiento

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Programa de mantenimiento preventivo regular	Monitoreo de niveles de combustible y estado general	Capacitación del personal en operación y seguridad.

6. Baterías gel

   Riesgo: Descarga completa de batería

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**

Monitoreo de niveles de carga y descarga	Programación de ciclos de mantenimiento de batería.	Alarmas de bajo nivel de carga

7. Inversor 3kva

   Riesgo: Fallo en la conversión de energía

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Gestión de energía eficiente y alertas automáticas	Monitoreo continuo de la carga	Auditoría de fallos del sistema eléctrico

8. ATS (Automatic Transfer Switch)

   Riesgo: Fallo en la conversión de energía

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Configuración de transferencias automáticas	Monitoreo de operaciones	Monitoreo de continuidad de energía

9. Generador 6500kva

   Riesgo: Fallo por falta de mantenimiento

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**

Monitoreo del generador en tiempo real	Monitoreo de la carga y pruebas de funcionamiento	Planificación de mantenimientos regulares

10. Onus (Optical Network Units)

Riesgo: Fallo en la unidad de red óptica

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Implementación de redundancia de red	Gestión centralizada de unidades ópticas	Supervisión de la conectividad y alertas de fallos

11. Vehículo

Riesgo: Fallo en la infraestructura o daño

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**
Monitoreo GPS en tiempo real	Seguridad en la transmisión de datos móviles	Seguimiento de acceso y monitoreo de seguridad

12. ONT (Optical Network Terminal)

Riesgo: Fallo en el software o desactualización

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control Propuesto 3 (OSware)**

Redundancia de ONTs	Monitoreo en tiempo real	Actualizaciones automáticas de firmware y mantenimiento preventivo regular

13. Cable de Fibra Óptica

Riesgo: Falla en la transmisión de datos o pérdida de conectividad

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Monitoreo constante de la calidad de la fibra y pruebas regulares.	Análisis de tráfico para detectar posibles fallos	Monitoreo de red y alertas de posibles interrupciones.

14. ODF

Riesgo: Falla en la conexión o mantenimiento incorrecto de las fibras

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Revisión y mantenimiento regular de las conexiones.	Control de acceso a las configuraciones y mantenimiento de ODF	Automatización de monitoreo para detectar fallos o desconexiones

- **Activo Personal**

1. León Gudiño Susana del Rocío – Gerente General

   Riesgo: Pérdida de acceso, toma de decisiones erróneas o mal gestionadas

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Autenticación multifactor en sistemas críticos	Control de acceso a sistemas críticos	Capacitación en gestión de riesgos y toma de decisiones.

2. Obando Villada Carlos Mario Fernando - Presidente / Gerencia Técnica

   Riego: Malas decisiones basadas en información incompleta o errónea

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Revisión continua de información estratégica y monitoreo	Capacitación en seguridad de la información.	Revisión periódica de los informes y análisis de riesgo.

3. León Gudiño Marcelo Wladimir – secretario / Encargado de Regulación

   Riesgo: Fugas de información confidencial, errores en normativas

Control propuesto 1 (Mitratec)	**Control propuesto 2 (AEIS SBC)**	**Control 3 (OSware)**
Control de acceso a documentos confidenciales	Monitoreo de cambios en políticas y procedimientos regulatorios	Revisión periódica de cumplimiento de normativas

7.CONCLUSIÓN DE LA REUNIÓN:

En esta reunión se permitió validar los controles propuestos para los riegos de los activos, basados en herramientas especializados como Mitratec que ayuda en la gestión de riesgos, AEIS SBC ayuda al análisis de tráfico y seguridad de red, y OSware herramienta de monitoreo y gestión de infraestructura. Se analizo los controles propuestos y se seleccionó uno por cada activo.

Ing. Obando Villada Carlos Mario Fernando

Sra. Chiquito Caiza Jessica Fernanda

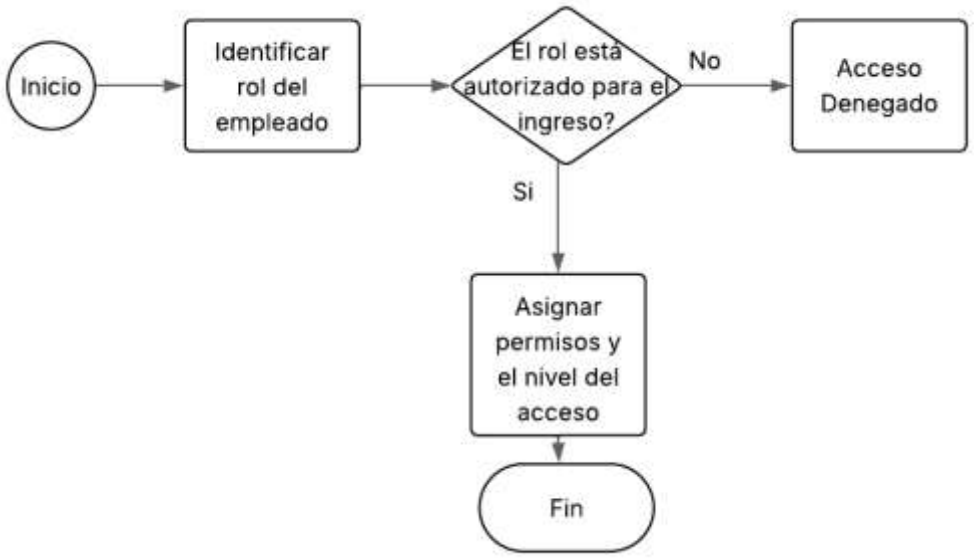
ANEXO 3

PROCESOS DE CADA UNA DE LAS POLÍTICAS DE SEGURIDAD

1. Política de Gestión de Accesos

- Definir niveles de acceso con su respectivo permiso para el personal en base de sus responsabilidades.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

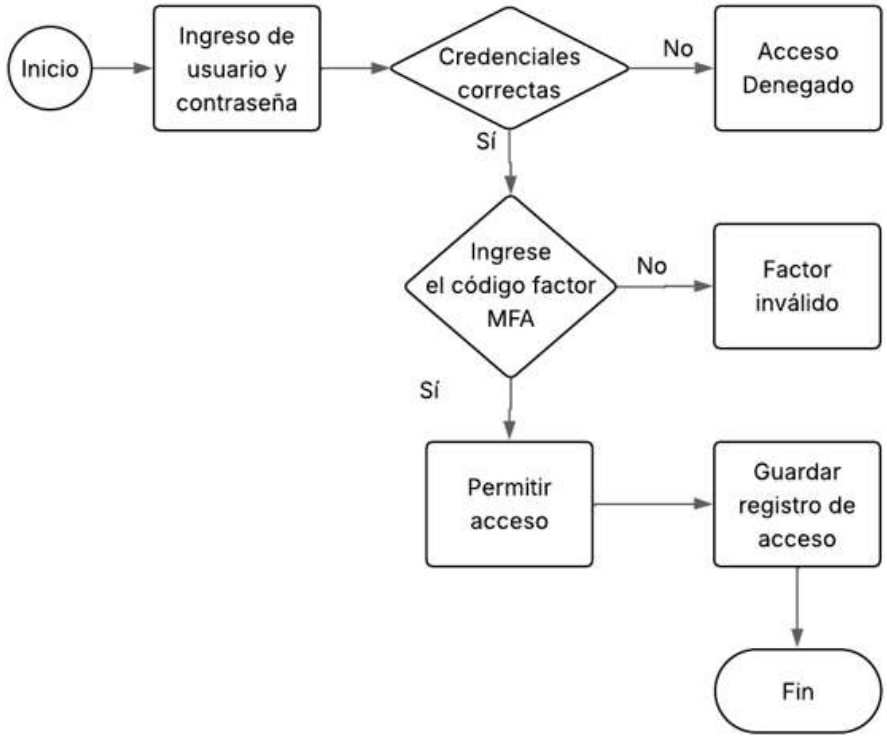
Identificar rol del empleado: Verificar el rol en el organigrama oficial de la empresa.

El rol está autorizado para el ingreso: Decisión al saber si el rol del empleado existe en la empresa pasa a darle permisos y a darle in nivel de acceso al empleado caso contrario tiene un acceso denegado a la empresa.

Fin: Fin del proceso

f. Implementar mecanismos de autentificación, como autenticación multifactor (MFA), para reducir la probabilidad de accesos no autorizados en las plataformas de los equipos Huawei y VPN.

Diagrama de flujo de la política:



Descripción de cada paso:

I**nicio:** Comienza el proceso de implementación de la política de seguridad de la información.

Ingreso de usuario y contraseña: Ingreso de credenciales del empleado

Credenciales correctas: Si el usuario y la contraseña son correctas se continua al siguiente paso caso contrario tiene un acceso invalido.

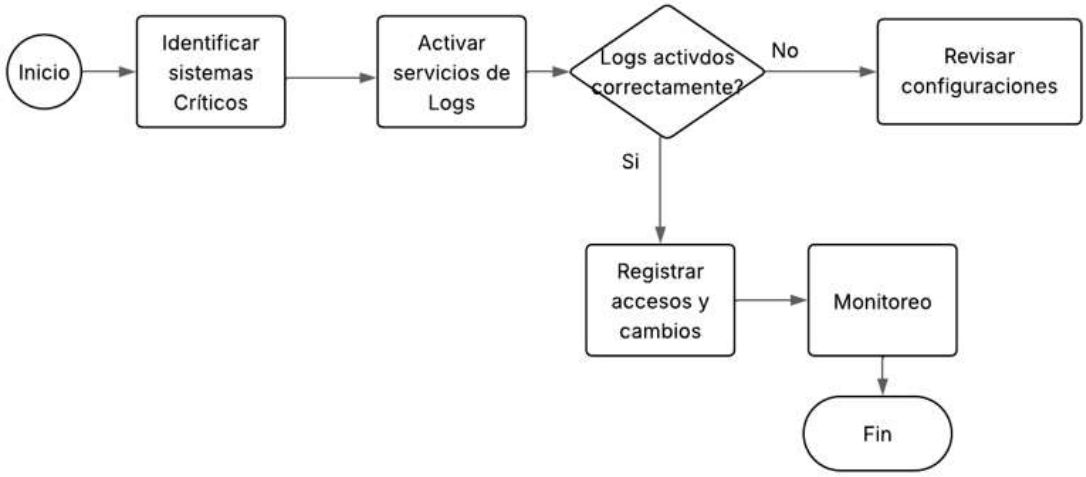
Ingrese el código factor MFA: Una vez que se tiene las credenciales correctas se procede a enviar un código de autenticación. Si el código es correcto se tiene el acceso caso contrario se tiene un factor inválido.

Guardar registro de acceso: Se procede a guardar el registro del acceso correcto o erróneo.

Fin: Fin del proceso.

g. Activar servicios de Logs a sistemas críticos que corresponden a bases de datos y a los dispositivos de accesos a la red.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

Identificar sistemas Críticos: Identificar sistemas y aplicaciones donde se deben habilitar Los Logs.

Activar servicios de Logs: Habilitar registros de acceso en los sistemas seleccionados.

Logs activados correctamente: ¿Servicios de Logs funcionando correctamente? No, revisar configuraciones y volverlos activar. Si, continuar al siguiente proceso.

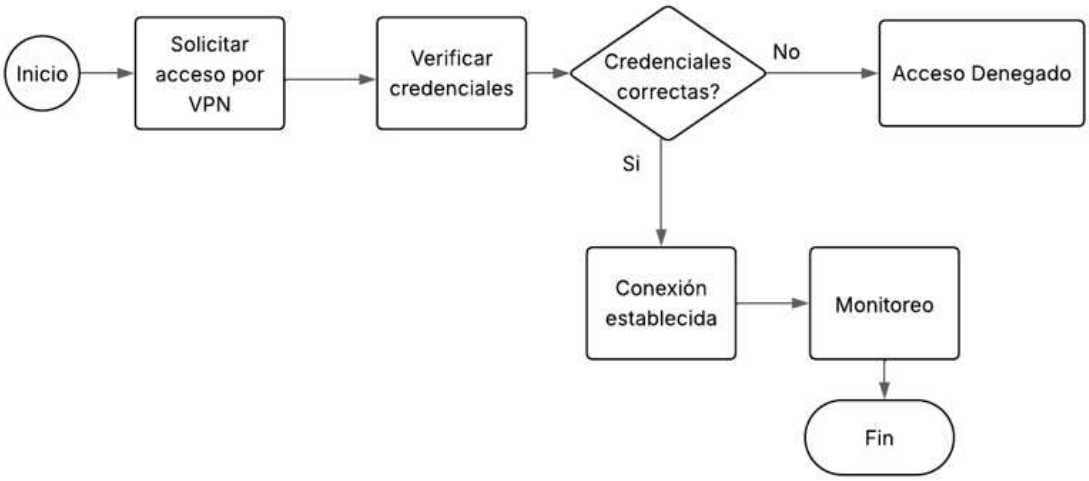
Registrar accesos y cambios: Guardar información sobre accesos, modificaciones y errores.

Monitoreo: Revisar Logs constantemente pata detectar accesos no autorizados.

Fin: Fin del proceso.

h. Accesos por VPN seguras que corresponden a las actualizaciones de las NIST SP 800-77 R1

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

Solicitar acceso por VPN: El empelado solicita conexión VPN a la red de la empresa.

Verificar credenciales: Autenticar usuario con credenciales y su rol en la empresa.

Credenciales correctas: No, acceso denegado. Si, continuar con el proceso.

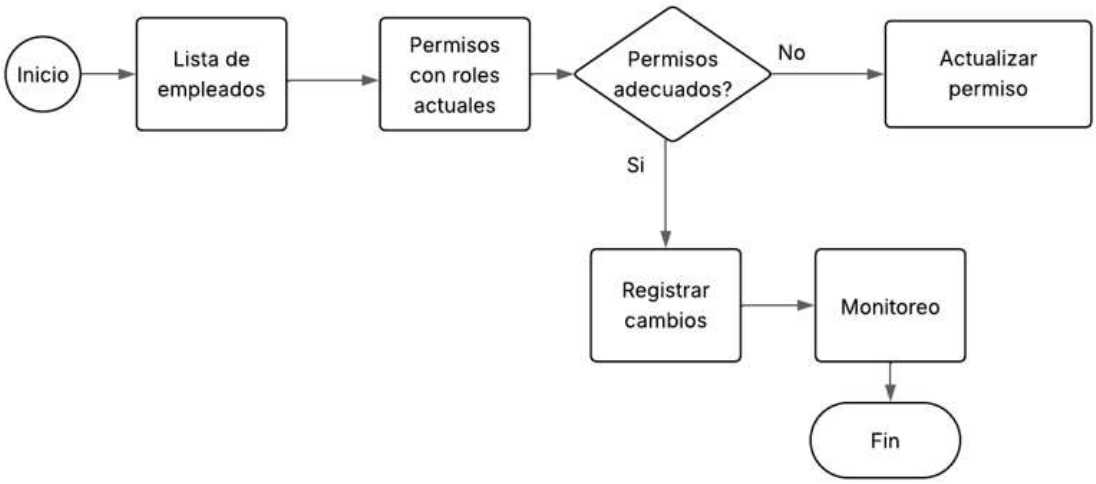
Conexión establecida: Se permite el acceso a la red mediante VPN segura**.**

Monitoreo: Revisar continuamente los registros por VPN para detectar accesos no autorizados.

Fin: Fin del proceso.

i. Realizar revisiones constantes de los accesos para asegurar que sean apropiados y estén alineados con las funciones actuales de cada empleado, tomando en cuenta con los cambios en la estructura organizativa.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

Lista de empleados: Recopilar un listado actual de empleados y permisos asignados en los sistemas

Permisos controles actuales: Verificar que los permisos asignados coincidan con las funciones actuales del empleado.

Permisos adecuados: No, actualizar permisos para ajustar con el rol actual del empleado. Si, continuar con el proceso.

Registrar cambios: Documentar ajustes de permisos

Monitoreo: Monitorear de manera constante el rol del empleado.

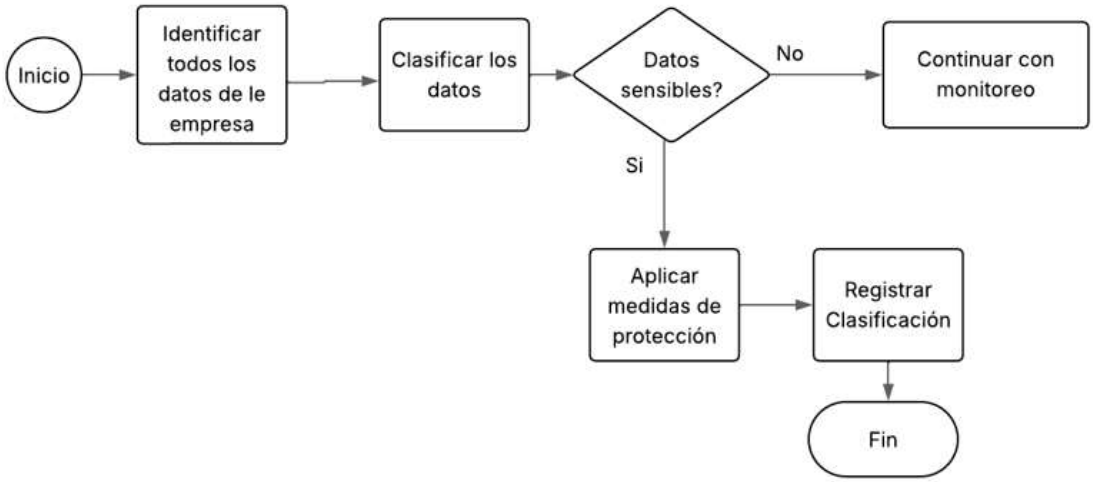
Fin: Fin del proceso.

2. Política de Protección de Datos

Políticas:

e. Establecer medidas de protección para la clasificación de datos sensibles asegurando la información para que se maneje conforme a los principios de confidencialidad, integridad y disponibilidad.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad de la información.

Identificar todos los datos de la empresa: Revisar servidores, bases de datos y sistemas de información.

Clasificar los datos: Asignar categorías publica, interna, confidencialidad y secreta.

Datos sensibles: No, continuar con el monitoreo. Sí, continuar con el proceso.

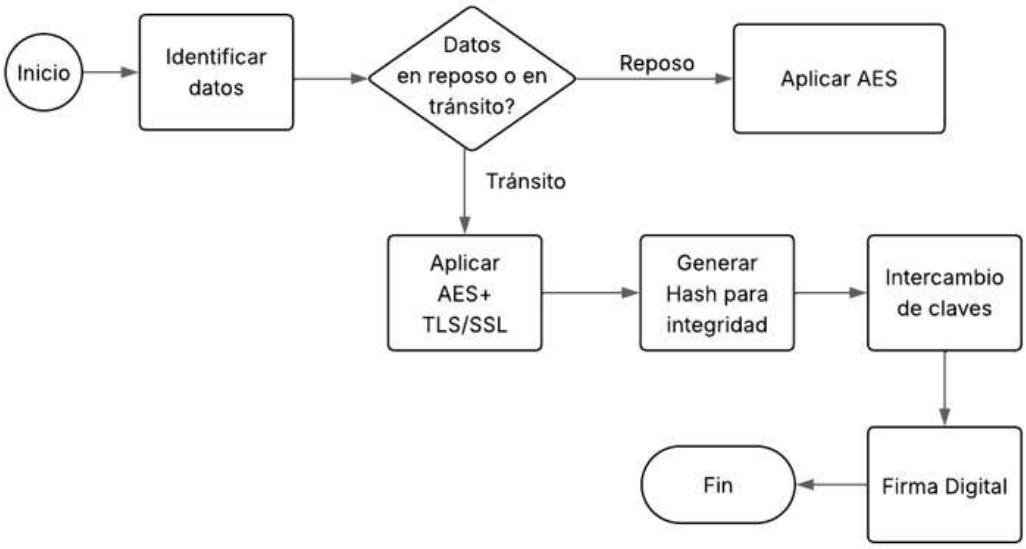
Aplicar medidas de protección: Encriptación AES para los datos en reposo, TLS/SSL para datos en tránsito, controles de acceso y Backup**.**

Registrar clasificación: Documentar la clasificación y los controles aplicados

Fin: Fin del proceso.

f. Implementar medidas de encriptación para proteger los datos en tránsito y en reposo, asegurando que la información confidencial sea inaccesible para usuarios no autorizados, se consideran los siguientes algoritmos según las recomendaciones del NIST SP 800-111 R1

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificar datos: Clasificar los datos según su sensibilidad.

Datos en reposo o en tránsito: Para los datos en reposo se aplica AES así se protege el almacenamiento. Para los datos en tránsito aplicar AES+TLS/SSL para proteger la comunicación.

Generar Hash para integridad: control SHA-2, SHA-52 o SHA-3 según la recomendación de NIST

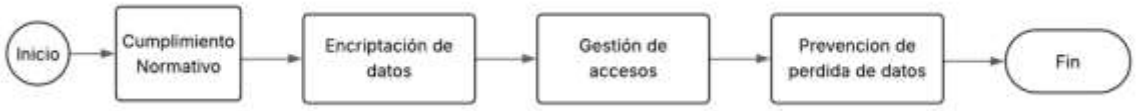
Intercambio de claves: Aplicar Diffie-hellman (DH) ECDH para crear claves seguras entre sistemas.

Firma Digital: Aplicar RSA, ECDSA o EdDSA para garantizar autenticidad

Fin: Fin del proceso.

g. Asegurar que los datos se almacenen y manejen conforme a las normativas de protección de datos, mediante la implementación de estándares internacionales y algoritmos criptográficos recomendados por NIST.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Cumplimiento Normativo: aplicar leyes y regulaciones como la ley orgánica de protección de datos personales.

Encriptación de datos: Datos en reposo, datos en tránsito, control de integridad, intercambio de claves y firma digital.

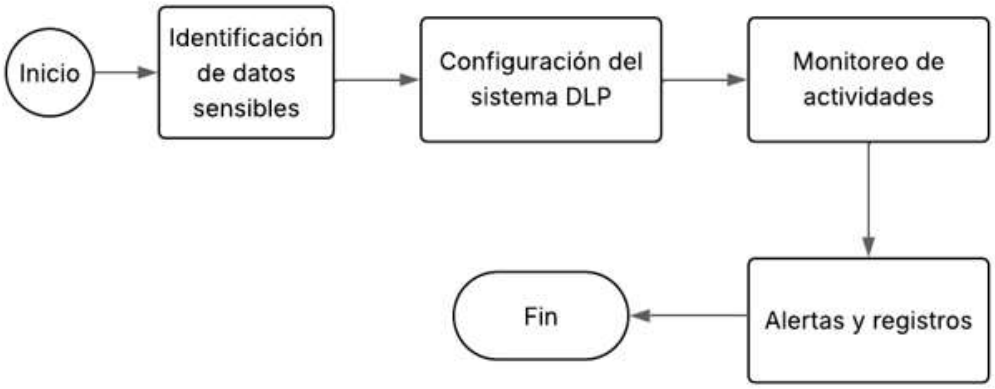
Gestión de accesos: Autenticación Multifactor y registro de actividades en Logs

Prevención de perdida de datos: Alertas automáticas ante anomalías y monitoreo y bloqueo de envíos no autorizados.

Fin: Fin del Proceso.

h. Implementar DLP con la finalidad de proteger los datos críticos de la empresa evitando que salgan de la red corporativa de forma no autorizada, ya sea por error, malicia o negligencia

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificación de datos sensibles: Clasificar los datos críticos en confidencialidad, interna, publica.

Configuración del sistema DLP: Bloquear la transferencia de datos sensibles a dispositivos no autorizados.

Monitoreo de actividades: Supervisa e flujo de datos para detectar intentos de fuga o acceso indebido.

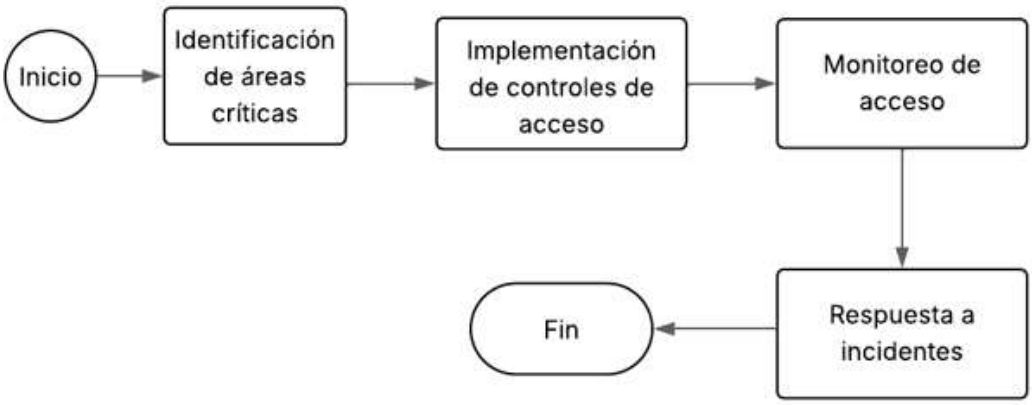
Alertas y registros: Alertas automáticas de cualquier evento.

Fin: Fin del proceso**.**

3. Política de Seguridad Física

i. Implementar controles físicos para restringir el acceso a las instalaciones criticas tales como los servidores, equipos de red y otros dispositivos que son importantes para la empresa.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificación de áreas críticas: realizar una revisión de todas las instalaciones y equipos que requieren acceso restringido.

Implementación de controles de acceso: colocar cerraduras, tarjetas de acceso, biometría o códigos de seguridad.

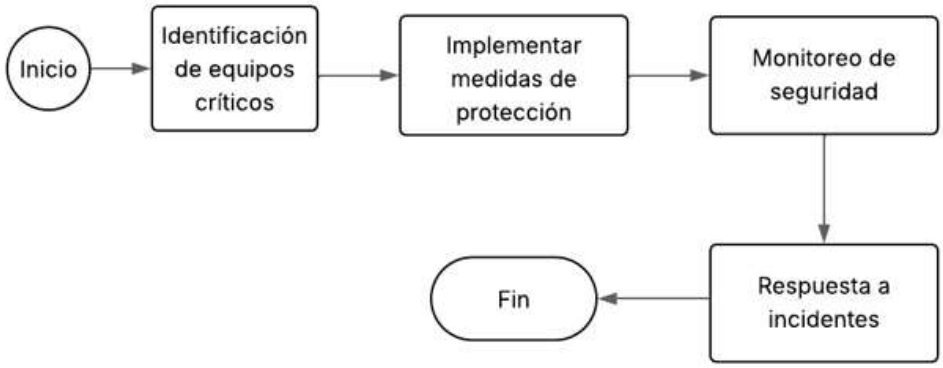
Monitoreo de acceso: instalar cámaras de seguridad y sistemas de alarma.

Respuesta a incidentes: establecer protocolos para reportar intentos de acceso no autorizado**.**

Fin: Fin del proceso.

j. Asegurar la protección física de los equipos y dispositivos tomando medidas como cámaras de vigilancia, sistemas de alarma y acceso autorizado.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificación de equipos críticos: revisar toso los equipos y dispositivos que requieren protección física

Implementar medidas de protección: instalar cámaras de seguridad en áreas críticas. Configurar sistemas de alarmas. Restringir el acceso a personal autorizado.

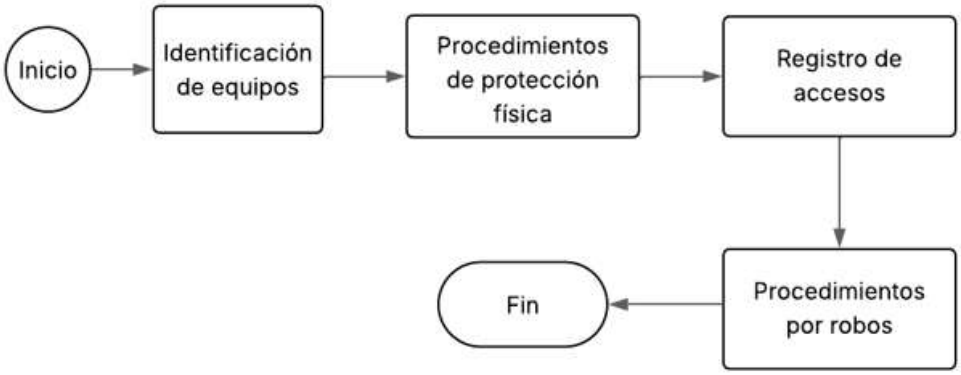
Monitoreo de seguridad: revisar cámaras y alarmas de forma continua.

Respuestas a incidentes: establecer procedimientos para alertas, intervenciones y reportes en caso de incidentes de físicos.

Fin: Fin del proceso.

k. Establecer procedimientos para la protección de equipos físicos, con el fin de evitar su perdida, robo o acceso no autorizado.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificación de equipo: revisar todos los equipos físicos críticos con su ubicación y a estos asignarles un responsable de cada equipo o área.

Procedimiento de protección física: instalar cámaras de vigilancia, etiquetar cada equipo, implementar un inventario periódico de todos los dispositivos.

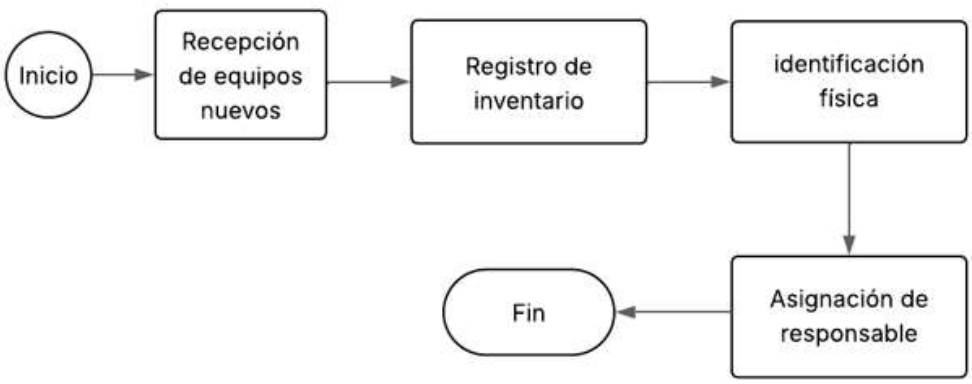
Registro de accesos: registrar quien accede a cada equipo con su hora, fecha y lugar.

Procedimiento por robos: establecer procedimientos para reportar robos, perdidas, Access no autorizados.

Fin: Fin del proceso.

l. Establecer el proceso de registro e identificación de equipos nuevos.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Recepción de equipos nuevos: verificar el funcionamiento de los equipos nuevos.

Registro de inventario: ingresar los quipos en el sistema de inventario con el número de factura, número de serie, modelo, fecha de ingreso, responsable asignado.

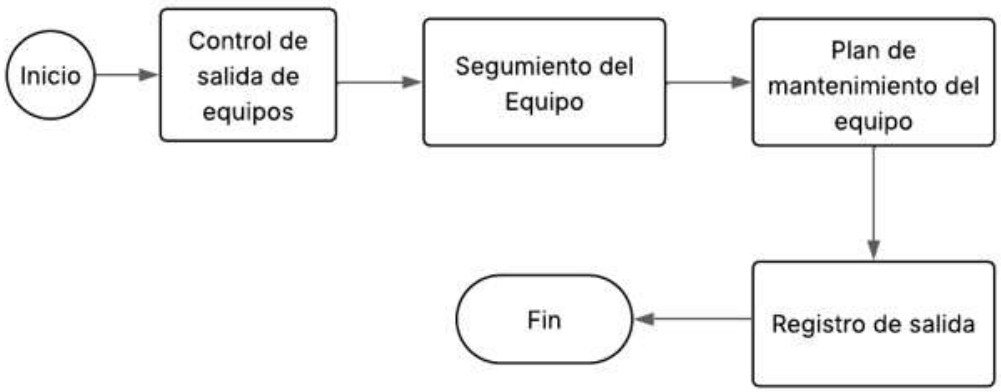
Identificación física: etiquetar físicamente casa equipos con el código, identificación del propietario o área.

Asignación de responsable: designar a un empleado o área responsable del equipo.

Fin: Fin del proceso.

m. Implementar controles de salida de equipos y el tiempo establecido para su devolución y realizar un plan de mantenimiento de equipos.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Control de salida de equipos: registrar cada salida de equipos en un sistema de control. Verificar que el equipo tenga un responsable autorizado. Establecer un protocolo de firma o autorización para retirar el equipo.

Seguimiento del equipo: registrar la fecha, hora y el motivo de la salida. Supervisar que el equipo se devuelva en la fecha establecida y este en perfectas condiciones.

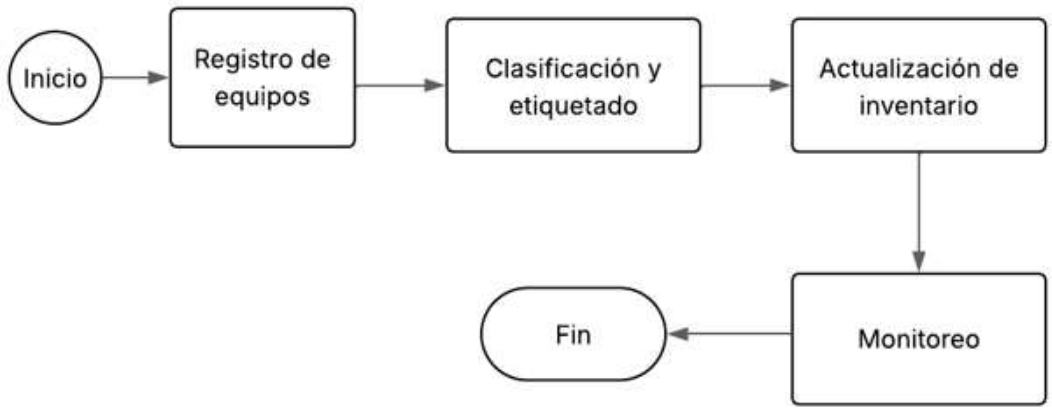
Plan de mantenimiento del equipo: establecer mantenimiento como limpieza, actualización de software y revisión física.

Registro de salida: verificar los registros de salida y mantenimientos estén completos y actualizados.

Fin: Fin del proceso.

n. Implementar inventario de Equipos.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Registro de equipos: identificar el equipo al momento de ingresar a la empresa, registrar la información del número de factura, número de serie, modelo, fecha de ingreso y un responsable.

Clasificación y etiquetado: asignar códigos únicos, clasificar según su criticidad o su tiempo de uso.

Actualización de inventario: registrar cualquier cambio ya sean traslados, mantenimientos, daños, robos.

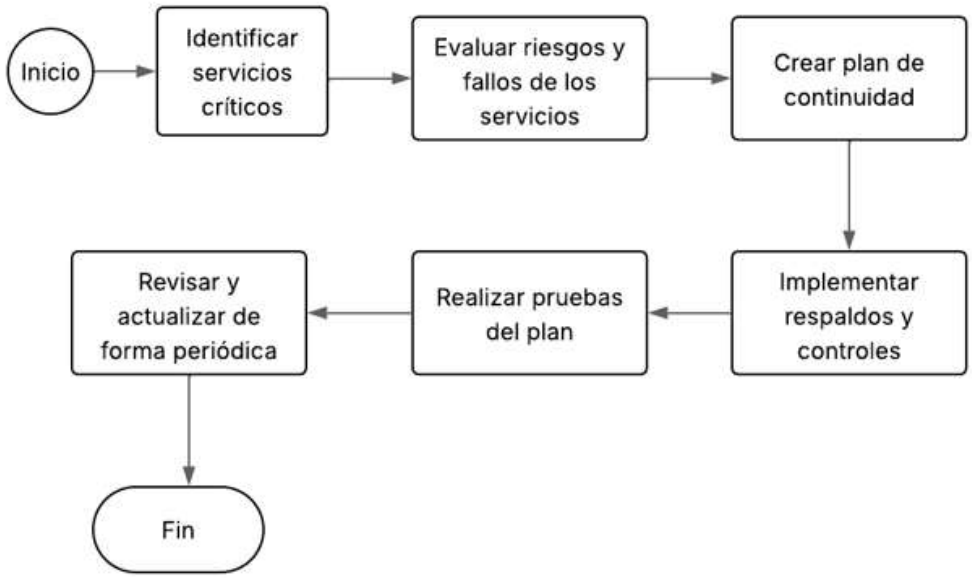
Monitoreo: revisar el inventario constantemente para poder reportar cualquier anomalía que exista.

Fin: Fin del proceso.

4. Políticas de Continuidad del Negocio

o. Desarrollar un plan de continuidad del negocio con esto se asegura la operatividad de los servicios de la empresa ante fallos de infraestructura o situaciones inesperadas.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Identificar servicios críticos: Determinar servicios fundamentales para la operación de la empresa.

Evaluar riegos y fallos de los servicios: Analizar las amenazas que afectan a los servicios críticos de la empresa.

Crear un plan de continuidad: Redactar un plan donde conste quienes son los responsables, que se debe de hacer ante una falla y que procedimientos se deben de realizar.

Implementar respaldos y controles: Realizar copias de seguridad

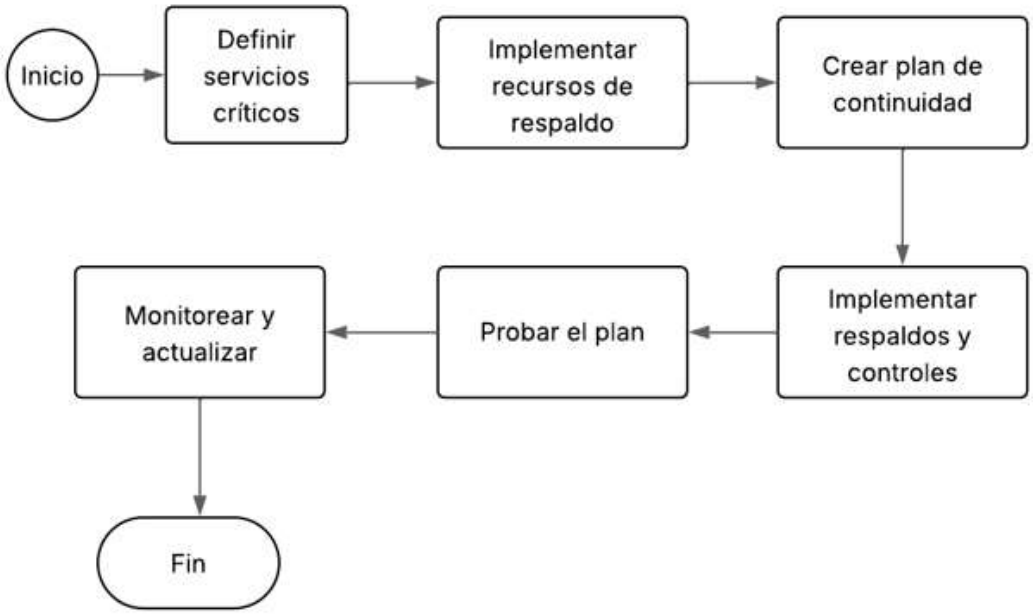
Realizar pruebas del plan: Se debe realizar simulacros para poner en prueba el plan realizado.

Revisar y actualizar de forma periódica: Revisar y actualizar cambios como la infraestructura, personal de la empresa, nuevas amenazas.

Fin: Fin del proceso.

p. Implementar plan de continuidad que verifique la efectividad y asegure que los procedimientos sean funcionales en situaciones emergentes.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Definir servicios críticos: Identificar servicios fundamentales para la operación de la empresa.

Implementar recursos de respaldo: Configurar respaldos, enlaces alternos, generador, ATS, VPN.

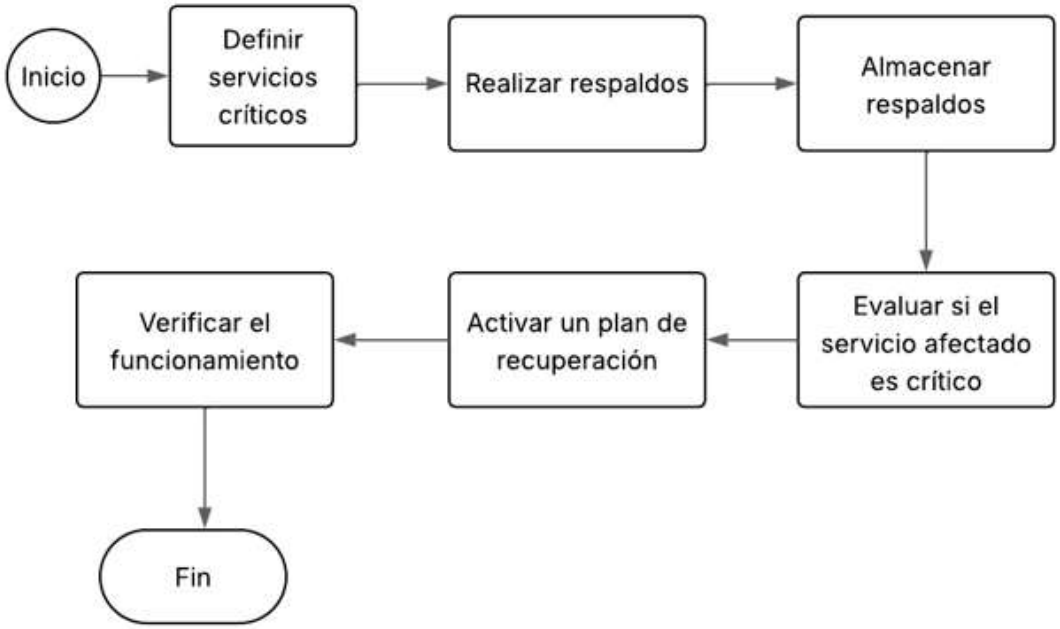
Probar el plan: Realizar simulacros para poner en prueba el plan realizado.

Monitorear y Actualizar: Realizar periódicamente el plan para mantenerlo vigente.

Fin: Fin del proceso.

q. Establecer procedimientos de recuperación antes desastres, tener respaldos de datos y equipos disponibles para ser implementados de forma rápida ante una emergencia.

Diagrama de flujo de la política:



Descripción de cada paso:

Inicio: Comienza el proceso de implementación de la política de seguridad

Definir servicios críticos: Identificar servicios críticos de la empresa.

Realizar respaldos: Generar copias de seguridad automática.

Almacenar respaldos: Los respaldos se deben guardar en un lugar seguro.

Evaluar si el servicio afectado es crítico: Revisar si el sistema afectado es vital para la operación.

Activar un plan de recuperación: Colocar un personal responsable para que sea el responsable de ejecutar los procedimientos para la recuperación.

Verificar el funcionamiento: Realizar pruebas de operatividad del sistema recuperado para asegurar que funcione correctamente y sin errores.

Fin: Fin del proceso.

ANEXO 4

Guía de aplicación de la política

Política de gestión de acceso:

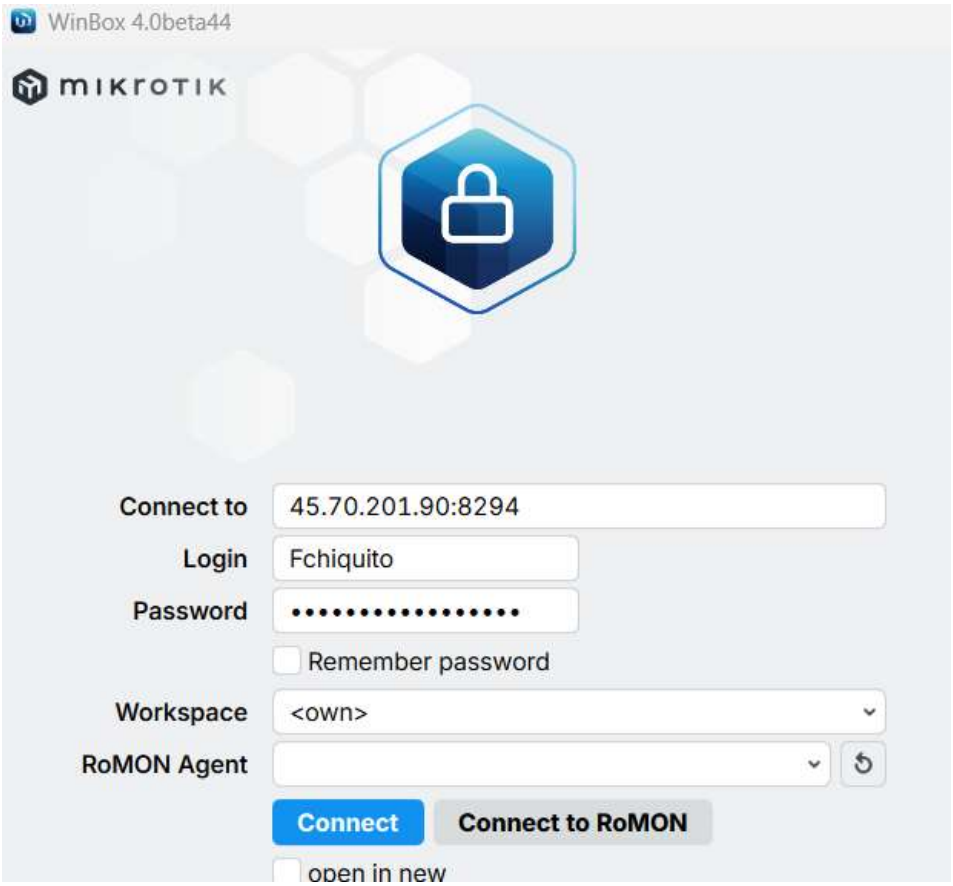
“Activar servicios de Logs a sistemas críticos que corresponden a la base de datos y a los dispositivos de acceso a la red”.

1. Activación de logs MikroTik

1.1 En primer lugar, se procede a ingresar al Core de la red con el objetivo de activar los logs correspondientes a los accesos a la red como se muestra en la Figura 1. El acceso se realiza mediante el programa de WinBox, herramienta utilizada para la administración del dispositivo MikroTik. Para ello se ingresa la dirección IP del equipo, el nombre de usuario y la contraseña correspondiente y posteriormente se selecciona en conectar para establecer la conexión.

Figura 1

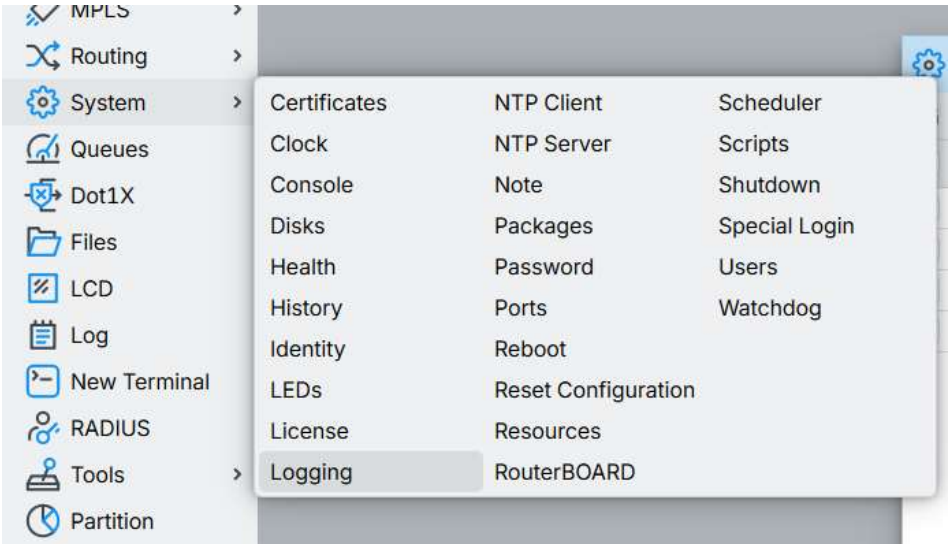
Acceso MikroTik



1.2 Para realizar la activación de los Logs, se procede a ingresar al menú System y seguidamente a la opción de Logging, donde se configura el registro de eventos del sistema como se muestra en la Figura 2.

Figura 2

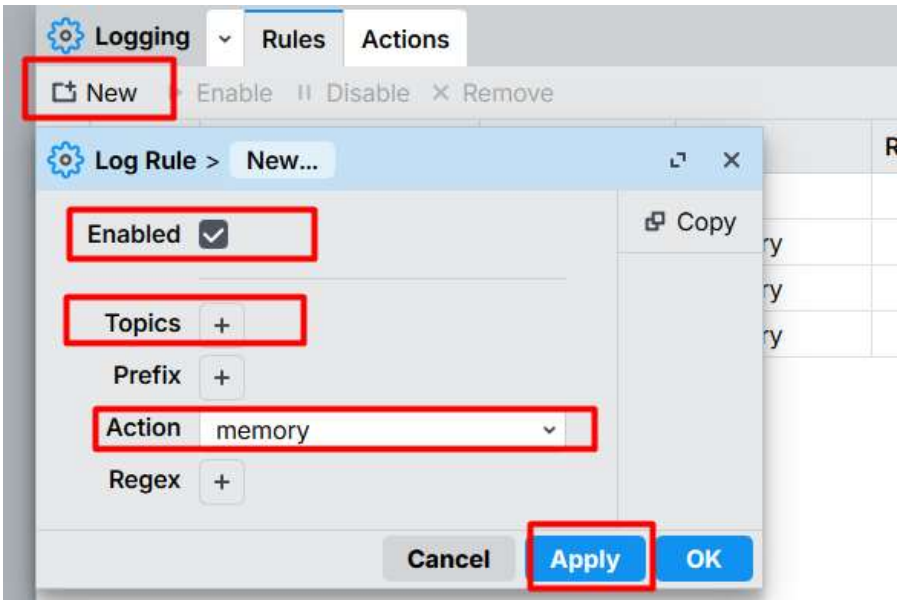
Menú de creación de logs.



1.3 Una vez dentro del apartado correspondiente, se selecciona la opción New y se procede a crear el log de acuerdo con las necesidades y requerimientos establecidos. Posteriormente creado el log se procede aplicar el log. Como se muestra los requerimientos de la creación de log en la Figura 3

Figura 3

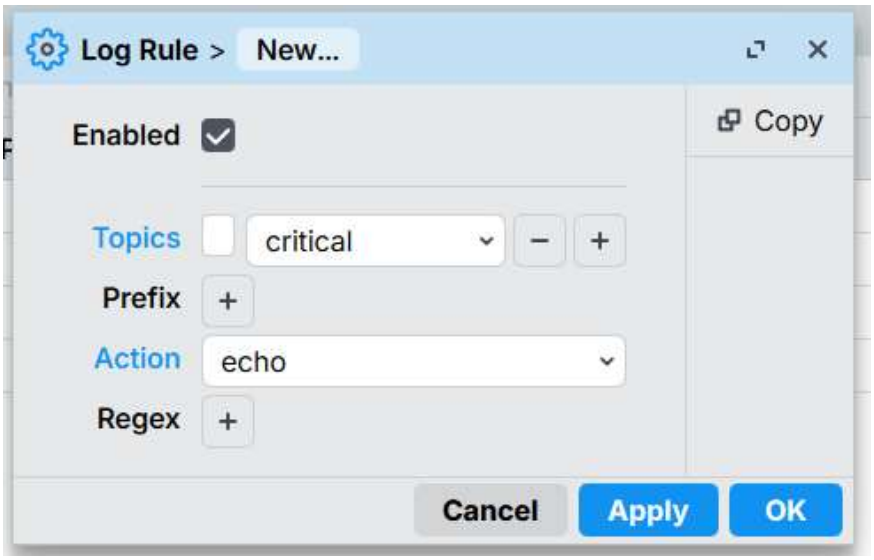
Requerimientos de la creación de logs.



1.4 La Regal de Log se utiliza para definir que eventos serán registrados y que acción realizará el Router con dichos eventos. En la Figura 4 se muestra la configuración de log, en el campo Enabled se indica que la regla se encuentra activada. En Topics se define el tipo de evento que se desea registrar; en este caso se selecciona critical, el cual permite identificar situaciones críticas como sistemas de archivo en modo solo lectura, fallas de memoria y errores de memoria. En el campo Prefix permite agregar un texto adicional antes del mensaje del log lo cual no se configura ningún prefijo, En Action se establece la acción que realizará el Router con el log generado, se selecciona la opción echo la cual permite mostrar el mensaje únicamente en el terminal. Esta acción resulta útil para la realización de pruebas y diagnósticos en tiempo real.

Figura 4

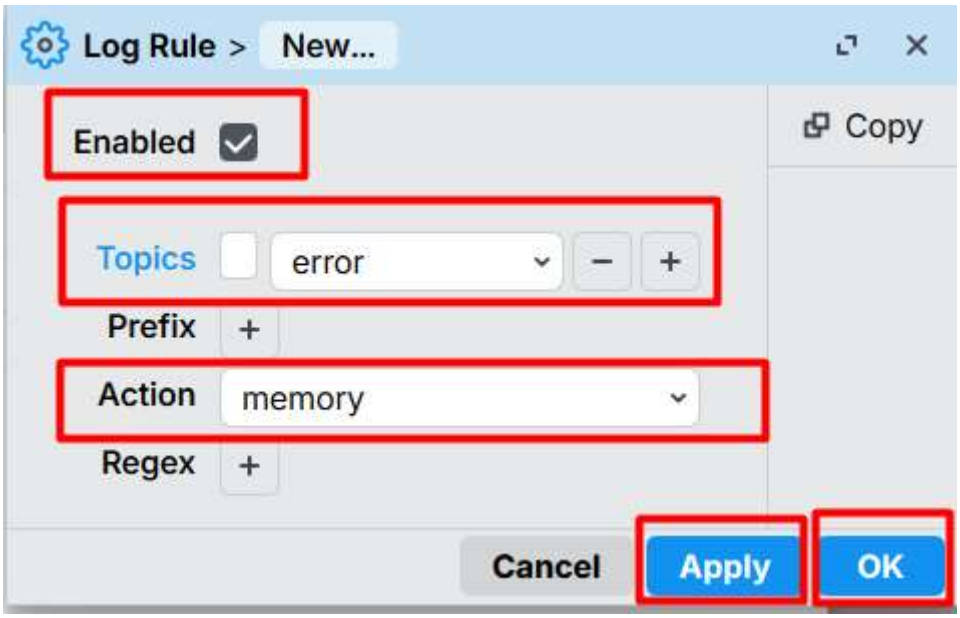
Creación de log Action.



1.5 La Regal de Log permite definir que eventos serán registrados y que acción realizará el Router con dichos eventos. En la Figura 5 tenemos las configuraciones para la creación del log, en el campo Enabled se indica que la regla se encuentra activada, en el campo de Topics se establece el tipo de evento que se desea registrar en este caso escogemos error, el cual permite identificar fallos del sistema, problemas de configuración, servicios que no funcionan correctamente y errores de red. En el campo Prefix permite agregar un texto previo al mensaje del log, esta configuración no se añade y tenemos el campo Action en donde se define la acción que ejecutara el Router sobre los eventos registrados, seleccionamos en memory que toda la información será guardara en la memoria RAM del Router, esta acción es útil para la visualización de errores recientes y la realización de diagnósticos rápidos.

Figura 5

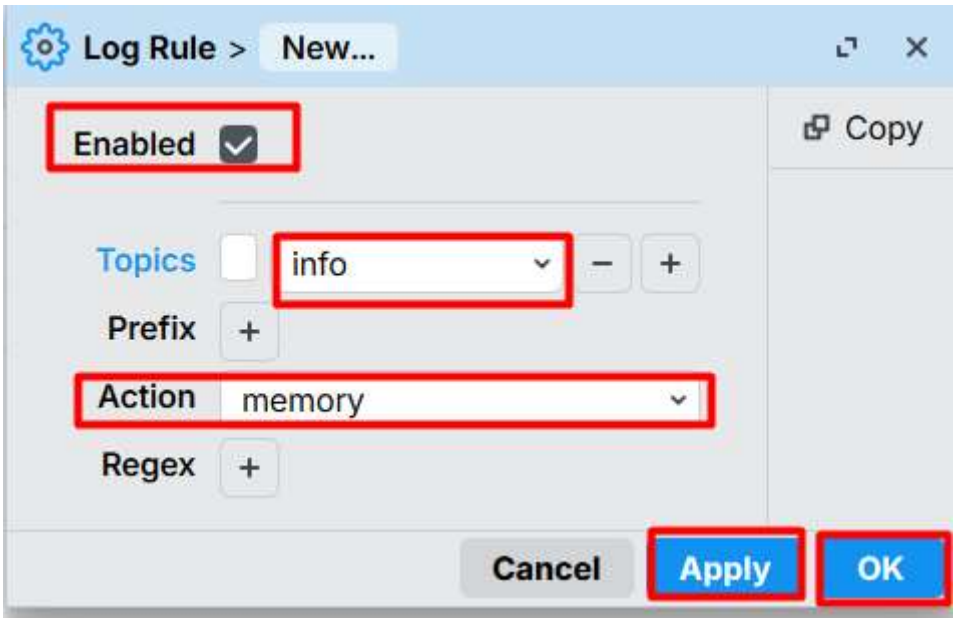
Creación de log error.



1.6 En la Figura 6 se tiene la configuración del log, en el campo Enabled se indica que la regla se encuentra activada. En el campo de Topics se define el tipo de vento que se desea registrar en este caso se selecciona info lo que permite visualizar los inicios y cierres de sesión, las conexiones y desconexiones de PPoE y mensajes normales del sistema. En el campo Prefix permite agregar un texto adicional antes del mensaje del log lo cual no se establece ningún prefijo. Y tenemos el ultimo campo Action se define la acción que realizará el Router con los eventos registrados, seleccionando la opción memory que permite almacenar en la memoria RAM del Router los mensajes informativos del sistema para su posterior revisión.

Figura 6

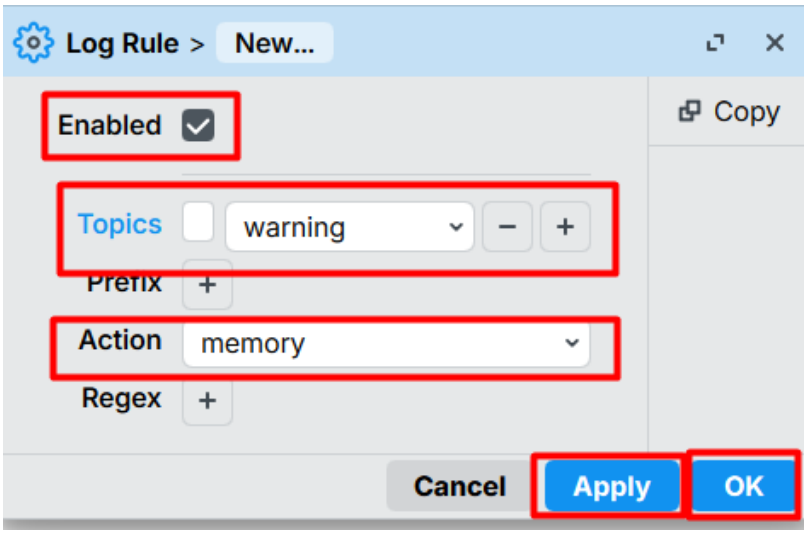
Creación de log info.



1.7 En el campo Enabled se indica que la regla se encuentra activada, en el campo Topics se establece el tipo de evento que se registra en este caso se selecciona warning (advertencia), lo cual permite identificar eventos como cambios en interfaces, retrasos o respuesta lentas, intentos fallidos, problemas temporales de red. En el campo Prefix permite agregar un texto previo al mensaje log, lo cual no se va a agregar esta configuración, ahora tenemos el campo Action se define la acción que ejecutará el Router sobre los eventos registrados, seleccionándose la opción memory que permite guardar en la memoria RAM del Router todos los mensajes de advertencia generados por el sistema para posterior análisis.

Figura 7

Creación de log warning



2. Activación de log base de datos

2.1 Para acceder ala base de datos es necesario contar con la conexión VPN. En la Figura 8 se encuentra como realizar la configuración, Para ello se ingresa a la configuración del computador se seleciona la opción Red e Internet y posteriormente se procede agregar una coneción VPN lo cual permitirá establecer un acceso seguro a la red donde se encuentra alojada la base de datos.

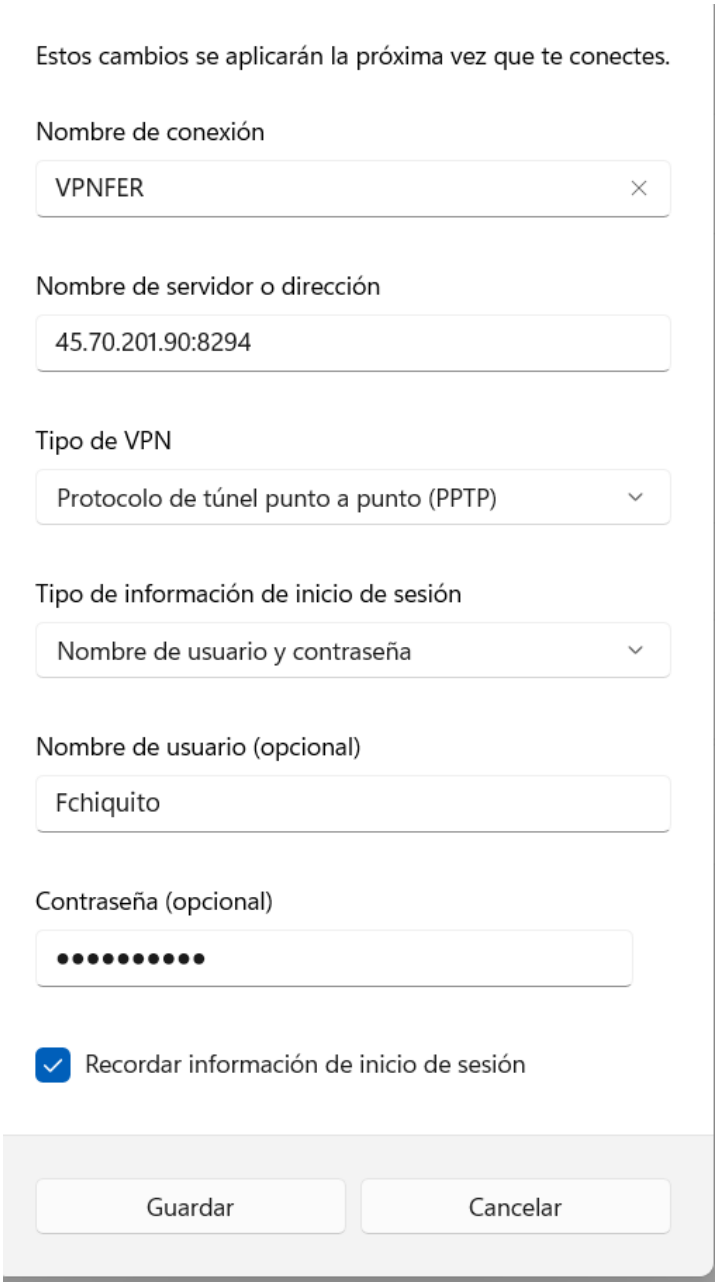
Figura 8

Configuración del computador para la VPN

2.2 Posteriormente se procede a completar los campos requeridos para la configuración de la VPN, tales como el nombre asignado a la conexión, la dirección del servidor, el tipo de VPN y finalmente el usuario y la contraseña. Este proceso se ilustra en la Figura 9

Figura 9

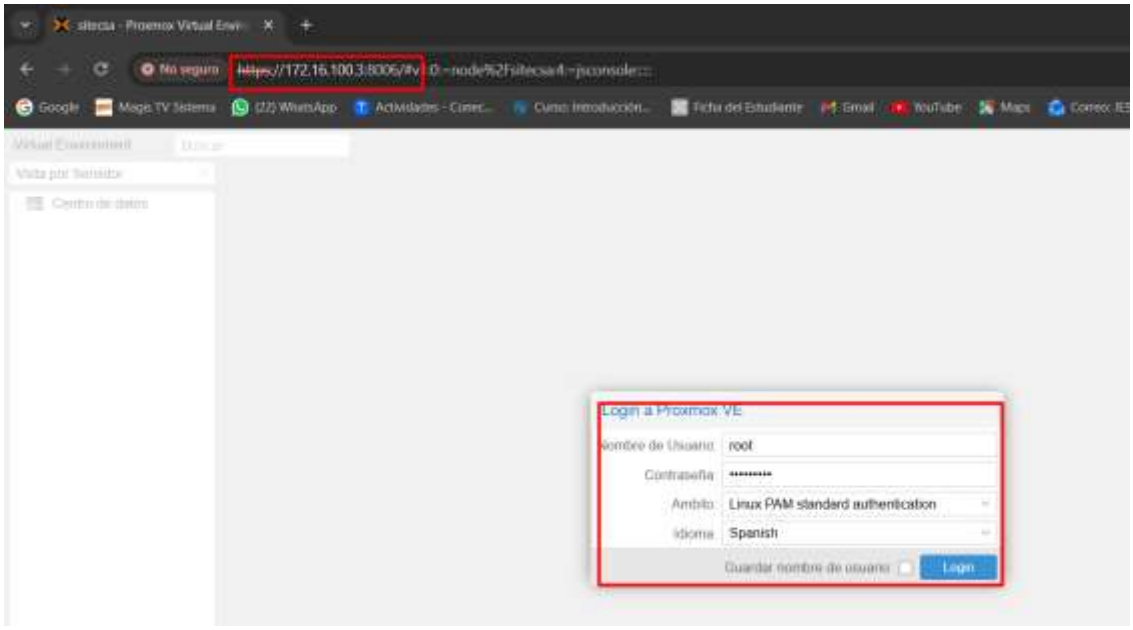
Requisitos para crear la VPN



2.3 Desde un navegador web se accede al servidor ingresando la dirección IP, una vez que se accedió al servidor se debe de llenar los requisitos como el nombre de usuario y la contraseña este procedimiento se muestra en la Figura 10.

Figura 10

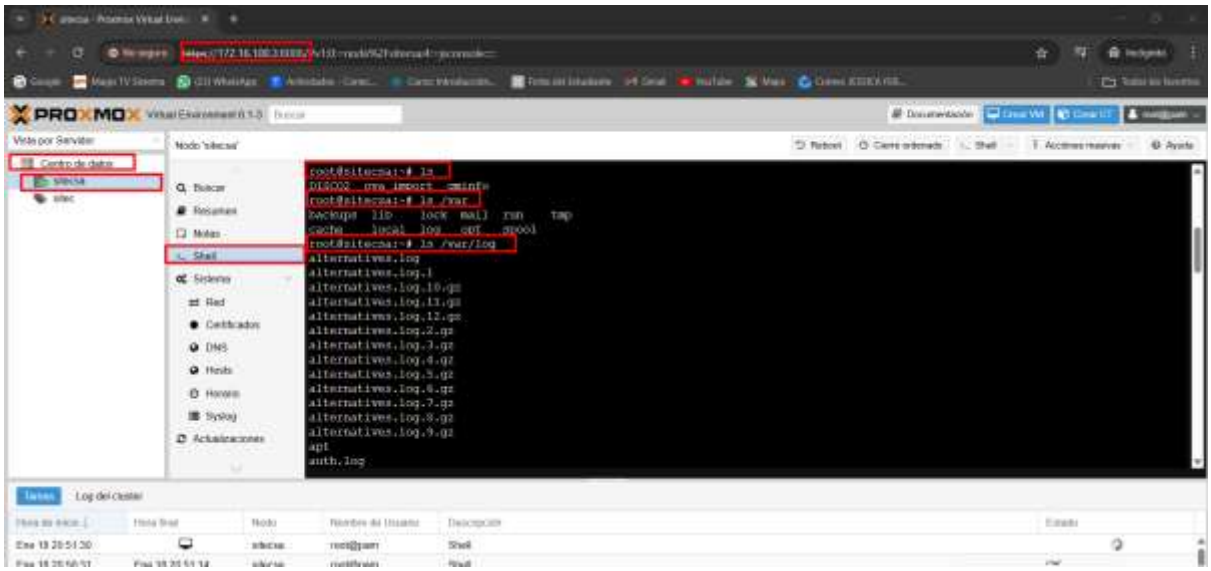
Ingreso al servidor desde el navegador



2.4 Una vez que se ha ingresado al servidor, se accede a la terminal con el objetivo de visualizar los registros del sistema. Para ello se ejecuta el comando ls /var/log el cual permite listar los archivos de logs disponibles. Este peocedimiento se observa en la Figura 11

Figura 11

Logs activados de la base de datos



3. Resultados:

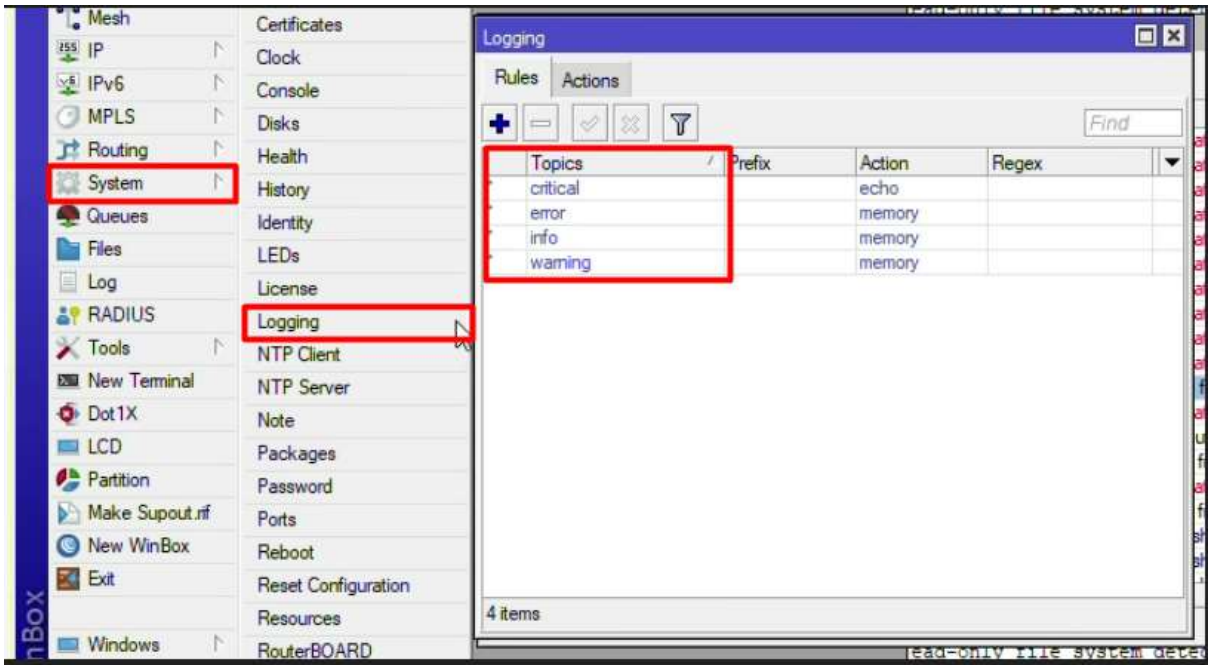
Una vez realizada la activación de los logs, se procede a realizar las pruebas correspondientes con el fin de verificar el correcto funcionamiento de la aplicación y el registro de eventos del sistema.

Resultados Activación de logs MikroTik

3.1 De esta manera, se evidencio que los cuatro logs configurados se encuentran funcionando correctamente. Esta configuración se ilustra en la Figura 12.

Figura 12

Logs activados en MikroTik

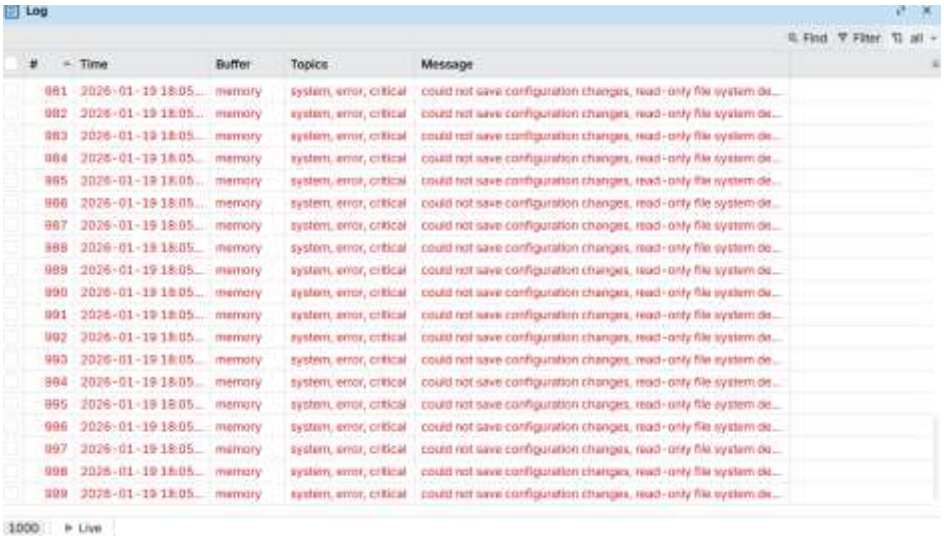


3.2 En la Figura 13 se presenta el resultado de la activación del log critical, el cual opera de manera automática y envía los mensajes generados directamente al terminal. Los registros mostrados confirman la correcta ejecución de la regla, se evidencio eventos clasificados como System, error y critical. Estos mensajes indican que el sistema de archivos del equipo se encuentra en modo de solo lectura, que la memoria interna no admite escrituras y e dispositivo no puede guardar cambios en su configuración.

El correcto registro y visualización de estos eventos permite identificar fallas críticas del sistema y facilita el diagnostico de problemas relacionamos con el almacenamiento y estabilidad del equipo cumpliendo así con la política de gestión de accesos y seguridad de la información.

Figura 13

Resultado log critical



3.3 En la figura 14 se muestra el terminal utilizado para visualizar el resultado del log error. Para comprobar el funcionamiento de esta regla, se accede al terminal y se ejecuta el comando print, el cual permite mostrar los registros generados y verificar el correcto funcionamiento del log configurado.

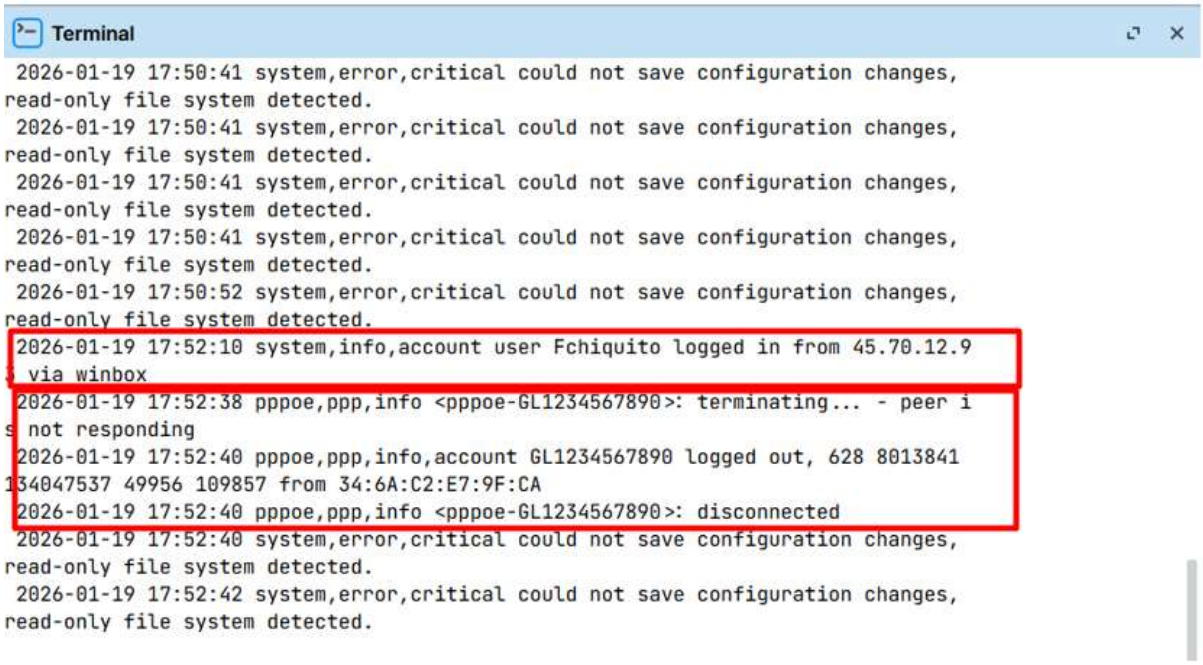
Figura 14

Resultado log error

3.4 En la Figura 15 se observan los errores registrados por el sistema, donde detecta que el sistema de archivos se encuentre en modo solo lectura. Asimismo se evidencia el acceso de usuario identificado como Fchiquito, asi como el ingreso y salida correcta de un cliente lo que confirma el adecuado registro de los eventos configurados.

Figura 15

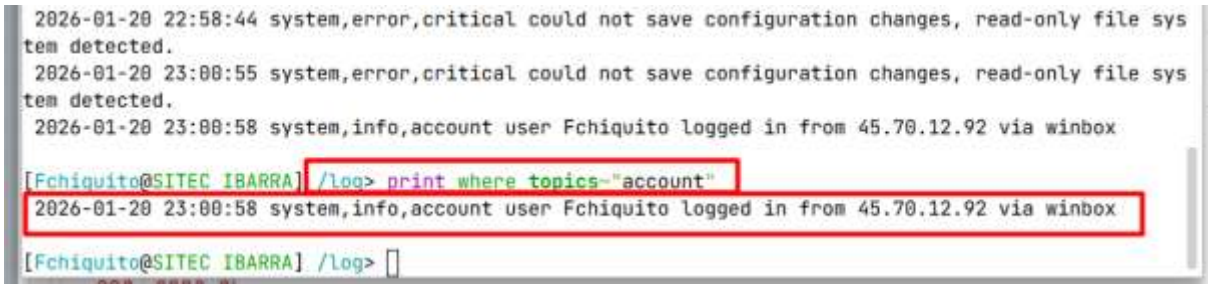
Resultado log error



3.5 Para visualizar el log info que es para visualizar únicamente los accesos de usuarios, se ejecuta en el terminal el comando /log print where topics~”account”, el cual permite mostrar los registros correspondientes a los usuarios que se conectan al dispositivo MikroTik. Este procedimiento se observa en la Figura 16.

Figura 16

Resultado log info



3.6 Para visualizar únicamente los registros correspondientes a los clientes PPPoE, se ejecuta el terminal el comando /log print where topics~”pppoe”. Mediante este comando se puede observar correctamente el ingreso y posterior desconexión de un cliente, tal como se muestra en la Figura 17.

Figura 17

Resultado log info

```
[Fchiquito@SITEC IBARRA] /log> print where topics~"pppoe"

 2026-01-19 17:52:38 pppoe,ppp,info <pppoe-GL1234567890>: terminating... - peer i
s not responding
 2026-01-19 17:52:40 pppoe,ppp,info,account GL1234567890 logged out, 628 8013841
134047537 49956 109857 from 34:6A:C2:E7:9F:CA
 2026-01-19 17:52:40 pppoe,ppp,info <pppoe-GL1234567890>: disconnected
 2026-01-19 17:52:40 system,error,critical could not save configuration changes,
read-only file system detected.
```

3.7 Para visualizar las waring (advertencias), se ingresa en el terminal el comando /log print follow where topics~”waring”, al ejecutar este comando el sistema muestra de forma inmediata los eventos que ocurren en tiempo real. En este caso no se registran advertencias lo que indica que el sistema se encuentra estable y no presenta fallos en las interfaces ni problemas de funcionamiento.

Figura 17

Resultado log waring

```
[Fchiquito@SITEC IBARRA] /log> print follow where topics~"warning"
- Ctrl-C to quit. Space prints separator. New entries will appear at bottom.
```

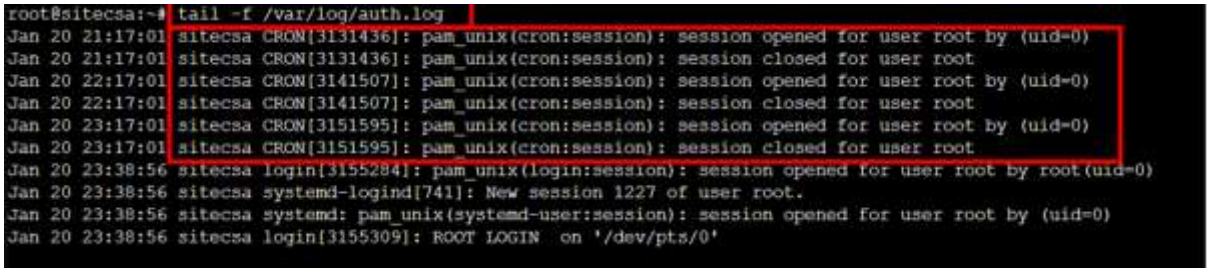
Resultados Activación de log base de datos

3.8 Para visualizar en tiempo real los logs de autenticación y permisos. Se ejecuta el comando tail -f /var/log/auth.log. Mediante este comando se puede observar los accesos realizados por

consola, conexión SSH y procesos de inicio de sesión (logins). Este log es fundamental para el control de la seguridad y la gestión de accesos al sistema. Como se muestra en la Figura 18.

Figura 18

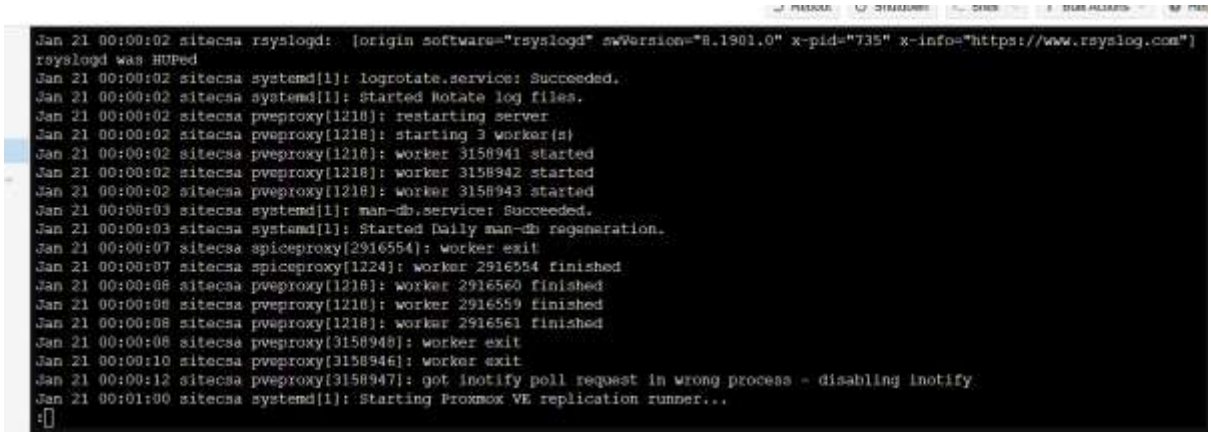
Resultado log auth.log



3.9 Mediante el uso del comando less/var/log/syslog se pueden visualizar los eventos del sistema, el estado de los servicios y los errores generales registrados. Este log es utilizado para el monitoreo y registro del funcionamiento general del sistema, tal como se muestra en la Figura 19.

Figura 19

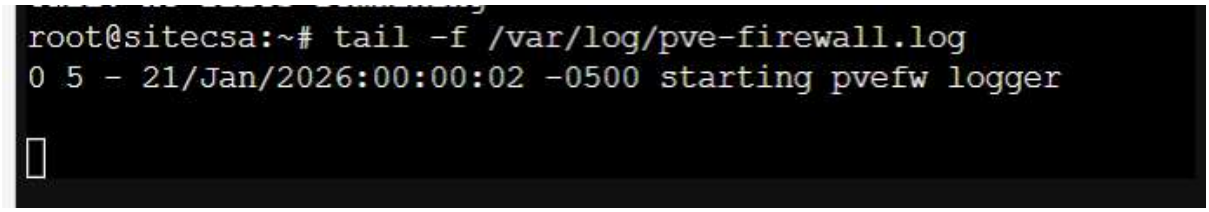
Resultado log syslog



3.10 Mediante este log se puede analizar la seguridad del firewall de Proxmox permitiendo observar información relacionada con paquetes bloqueados, reglas aplicadas, tráfico de red, análisis de paquetes y eventos de seguridad, tal como muestra la Figura 20.

Figura 20

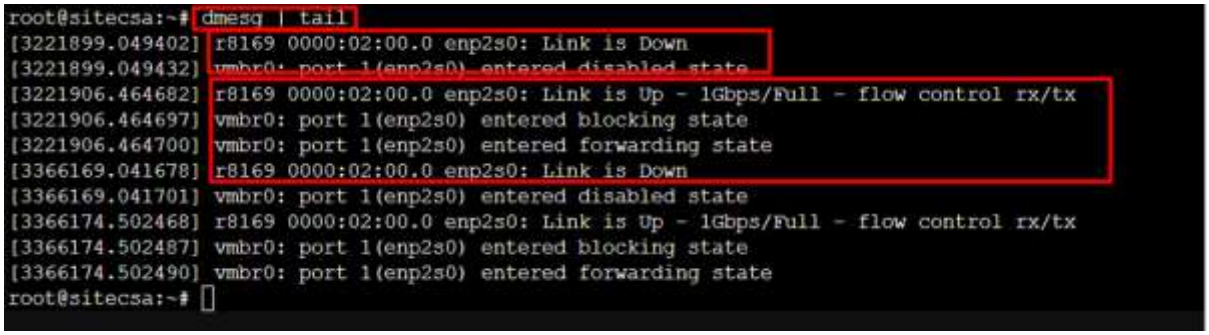
Resultado log pve-firewall.log



3.11 Mediante el análisis del archivo de kern.log se puede identificar eventos relacionados con errores de disco, interfaces de red, hardware y fallos físicos. En este log se observa que el controlador r8169 correspondiente a la interfaz enp2s0 perdió el enlace físico, lo que indica una interrupción temporal de la conexión de red. Posteriormente el mensaje Enp2s0: link is up – 1Gbps/Full -flow control rx/tx evidencia que la conexión fue restablecida correctamente, indicando una velocidad de 1 Gbps un dúplex completo y su flujo esta activo. Asimismo, se registra que el Bridge vmbr0 fue deshabilitado temporalmente, lo que se impidió él envió de tráfico durante la pérdida del enlace, sin embargo, el estado de bridge se normaliza una vez que la conexión es restablecida, estos eventos se muestran en la Figura 21.

Figura 21

Resultado log kern.log



4. Conclusión de la Guía

Se evidencia la correcta activación de diversos tipos de log en el dispositivo de red y en el servidor de base de datos, lo que permite fortalecer la seguridad. La implementación de los servicios de logs demostró ser un proceso practico y eficiente, la correcta aplicación depende

principalmente de comprender el propósito de cada log y la función que se desea asignar. Las configuraciones del MikroTik logs críticos, error, informativos y de advertencia lo que permitió registrar eventos facilitando el monitoreo del estado del sistema. El servidor Proxmox se comprobó el adecuado funcionamiento de los logs habilitados tales como auth.log, syslog, pve-firewall.log y kern.log los cuales proporcionan información sobre accesos, eventos del sistema, seguridad del firewall y posibles fallos en la red.

ACTA DE ENTREGA DE DOCUMENTACIÓN

Fecha: 26/01/2026

Lugar: Ibarra

Estimado Ing. Carlos Mario Fernando Obando Villada

Reciba un cordial saludo.

Por medio de la presente, yo Jessica Fernanda Chiquito Caiza, hago constar que en esta fecha ha elaborado y entregado a la empresa SITEC S.A la siguiente documentación:

- Plan de Seguridad para la Gestión de Riesgos de la Empresa.
- Manual de políticas de Seguridad de la Empresa.

Los documentos antes mencionados fueron elaborados por mi persona como parte del desarrollo de mi trabajo de titulación "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27001 PARA LA EMPRESA SITEC S.A" Dicha documentación es entregada al Ing. Carlos Mario Fernando Obando Villada, Gerente Técnico de la empresa, para su conocimiento y aplicación conforme a los fines técnicos.

Para constancia de lo expuesto, se firma el Acta de entrega de Documentación.

Firmado electrónicamente por:
JESSICA FERNANDA CHIQUITO CAIZA
Validar únicamente con FirmaEC

Jessica Fernanda Chiquito Caiza

Firmado electrónicamente por:
CARLOS MARIO FERNANDO OBANDO VILLADA
Validar únicamente con FirmaEC

Ing. Carlos Mario Fernando Obando Villada

SITEC
Navega sin límites

ACTA DE RECEPCIÓN DE DOCUMENTACIÓN

Fecha: 26/01/2026

Lugar: Ibarra

Estimada Sra. Jessica Fernanda Chiquito Caiza

Reciba un cordial saludo.

Por medio de la presente, la empresa SITEC S.A, deja constancia de que en esta fecha ha recibido formalmente de parte de la Sra. Jessica Fernanda Chiquito Caiza hago la siguiente documentación:

- Plan de Seguridad para la Gestión de Riesgos de la Empresa.
- Manual de políticas de Seguridad de la Empresa.

Los documentos antes mencionados fueron elaborados por Jessica Fernanda Chiquito Caiza como parte del desarrollo de su trabajo de titulación "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27001 PARA LA EMPRESA SITEC S.A" Dicha documentación es recibida por el Ing. Carlos Mario Fernando Obando Villada, Gerente Técnico de la empresa, para su conocimiento y aplicación en la empresa.

Para constancia de lo expuesto, se firma el Acta de Recepción de Documentación.

Ing. Carlos Mario Fernando Obando Villada Mgtr.