UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Diseño de un modelo de ciberseguridad basado en el marco ISO 27110:2021/NIST, caso de estudio Fortidex

AUTOR

Pincay Mero, José Andrés

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Espinal Santana, Albert Giovanny

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
ALBERT GIOVANNY ESPINAL SANTANA

Ing. Albert Espinal Santana, Ph.D.
TUTOR

Firmado electrónicamente por:
EDISSON POMPILIO QUINTUNA PADILLA

Ing. Edisson Quintuña Padilla, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lic. Daniel Quirumbay Yagual, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Pincay Mero José Andrés, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
ALBERT GIOVANNY
ESPINAL SANTANA

Albert Giovanny Espinal Santana

Santa Elena, 13 de diciembre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
DECLARACIÓN DE RESPONSABILIDAD

Yo, **Pincay Mero José Andrés**

DECLARO QUE:

El trabajo de Titulación, Diseño de un modelo de ciberseguridad basado en el marco ISO 27110:2021/NIST, caso de estudio Fortidex previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 13 de diciembre de 2024

EL AUTOR

Firmado electrónicamente por:
JOSE ANDRES PINCAY MERO

José Andrés Pincay Mero

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Diseño de un modelo de ciberseguridad basado en el marco ISO 27110:2021/NIST, caso de estudio Fortidex, presentado por el estudiante, Pincay Mero José Andrés fue enviado al Sistema Antiplagio Compilatio, presentando un porcentaje de similitud correspondiente al 4%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

UPSE Tesis Jose Pïncay

4%
Textos sospechosos

3% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos
9% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: UPSE Tesis Jose Pincay.docx
ID del documento: 2de3d782648538d47c81da3abc2c43cdb9adbad7
Tamaño del documento original: 2,61 MB
Autores: []

Depositante: ALBERT GIOVANNY ESPINAL SANTANA
Fecha de depósito: 13/12/2024
Tipo de carga: interface
fecha de fin de análisis: 13/12/2024

Número de palabras: 24.117
Número de caracteres: 165.624

Ubicación de las similitudes en el documento:

TUTOR

Firmado electrónicamente por:
ALBERT GIOVANNY ESPINAL SANTANA

Albert Giovanny Espinal Santana

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Pincay Mero José Andrés**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo Propuestas metodológicas y tecnológicas avanzadas con fines de difusión pública, además apruebo la reproducción de este trabajo de propuestas metodológicas y tecnológicas avanzadas dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 13 de diciembre de 2024

EL AUTOR

Firmado electrónicamente por:
JOSE ANDRES PINCAY MERO

José Andrés Pincay Mero

AGRADECIMIENTO

Agradezco primero a Dios por darme vida, a mi esposa e hijos, a mis padres, a mi hermano y amigos que me brindaron su comprensión y ánimo durante todo este proceso.

Agradezco a la Universidad Península de Santa Elena por brindarme la oportunidad de realizar mis estudios de maestría en esta gran institución. Agradezco a mi tutor PhD. Albert Espinal, sus consejos fueron una gran fuente de conocimiento y ayuda. A todos, mi más profundo agradecimiento.

José Andrés, Pincay Mero

DEDICATORIA

Dedico este trabajo a toda mi familia, siempre me ha brindado todo su apoyo y motivación durante toda mi formación académica. A mis padres que en todo momento me brindaron su ayuda incondicional en todo lo necesario.

Con mayor orgullo, dedico este trabajo a mi esposa y mis hijos, son mi motor y motivo para cumplir cualquier objetivo que me proponga, todos mis triunfos son gracias y para ustedes.

José Andrés Pincay Mero

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El trabajo de investigación tiene como objetivo diseñar un marco de ciberseguridad integral basado en las mejores prácticas internacionales establecidas por la Organización Internacional de Normalización (ISO) 27110:2021y el Instituto Nacional de Estándares y Tecnología (NIST).

Se diseñará un marco de ciberseguridad personalizado que se adapte a las necesidades de la organización, proporcionando una guía estructurada y efectiva para la gestión de ciberseguridad en sus activos de información críticos, mejorando su capacidad para prevenir, detectar, responder y recuperarse de amenazas cibernéticas, el mismo será diseñado en un ambiente controlado y de pruebas de la empresa Fortidex.

Directrices claras y buenas prácticas de las normas NIST e ISO 27110:2021 permitan implementar medidas de ciberseguridad efectivas sobre los activos críticos de información. La integración de ambas normas permite hacer frente a amenazas cibernéticas lo que asegura que la organización esté preparada para responder ante cualquier incidente de manera efectiva.

Palabras claves: Marco Ciberseguridad, NIST, ISO

ABSTRACT

The research work aims to design a comprehensive cybersecurity framework based on international best practices established by the International Organization for Standardization (ISO) 27110:2021 and the National Institute of Standards and Technology (NIST).

A customized cybersecurity framework will be designed to suit the needs of the organization, providing structured and effective guidance for cybersecurity management across its critical information assets, improving its ability to prevent, detect, respond and recover from cyber threats, It will be designed in a controlled and testing environment of the Fortidex company.

Clear guidelines and good practices from NIST and ISO 27110:2021 standards allow for the implementation of effective cybersecurity measures on critical information assets. The integration of both standards allows us to face cyber threats, which ensures that the organization is prepared to respond to any incident effectively.

Keywords: Cybersecurity Frameworks, NIST, ISO

INTRODUCCIÓN

Actualmente, la mayoría de las empresas del Ecuador, sin importar su tamaño, requieren estar protegidas y preparadas para responder oportunamente a cualquier incidente de ciberseguridad que pueda afectar la continuidad de las operaciones, ante esta problemática, se han elaborado diversas normas que ayuden a cumplir con este objetivo, procurando servir de referente para aquellas empresas que desean proteger la continuidad de sus operaciones críticas de negocio ante incidentes de ciberseguridad, a través de la reducción continua de sus riesgos de ciberseguridad.

Los ataques cibernéticos tienes varios objetivos, desde el robo de información, interrupción de servicios críticos, daños financieros significativos, perjudicar la confianza pública y comprometer la integridad de los activos críticos de información. Ante esta problemática, nace la necesidad de desarrollar e implementar marcos de ciberseguridad robustos y efectivos que permitan a la organización estar protegida contra las amenazas emergentes. Un marco de ciberseguridad bien diseñado proporciona una estructura y un conjunto de directrices que facilitan la identificación, evaluación y mitigación de riesgos cibernéticos, garantizando así la resiliencia y la seguridad de los sistemas de información.

Por tal motivo, es necesario un plan para asegurar la información y los activos, independientemente del tamaño de la organización, dado que cualquier vulnerabilidad en la seguridad que ponga en riesgo los activos críticos e información de la organización puede ocasionar pérdidas considerables en los activos, la funcionalidad de la empresa y las responsabilidades legales que eventualmente pueden conducir a una pérdida completa de la organización (Ramirez Vargas & Pereda Otero, 2021).

El diseño que se propone está basado en dos normativas reconocidas a nivel internacional: National Institute of Standards and Technology (NIST) Cybersecurity Framework, con su ciclo PDCA (Ruiz, Valqui, & Davila, 2021), ayuda a gestionar y reducir los riesgos relacionados con la ciberseguridad. Su estructura es flexible y escalable, se puede adaptar a diversas necesidades organizativas, proporcionando un enfoque basado en funciones esenciales como Identificación, Protección, Detección, Respuesta y Recuperación.

Por otro lado, la ISO/IEC 27110:2021, como parte de la serie ISO/IEC 27000, se encarga de ofrecer directrices, estableciendo un marco de ciberseguridad integral y flexible (Bastidas Pérez, 2021), proporciona una guía específica para la gestión de la ciberseguridad en organizaciones. Se enfoca en el diseño y la implementación de controles de seguridad para la protección de la información. La norma ofrece un marco estructurado que facilita la integración de prácticas de seguridad en los procesos organizativos existentes.

Ambos marcos tienen la capacidad de ser aplicados a cualquier organización, no importa el tamaño, la naturaleza o el tipo, pues poseen los conceptos necesarios para organizar un marco de ciberseguridad que responda de forma correcta y coherente a las necesidades del contexto.

Planteamiento de la investigación

Las organizaciones a nivel de Ecuador y de manera mundial a menudo se enfrentan a dificultades al intentar adoptar marcos de ciberseguridad ya que no existe un modelo estandarizado que integre las mejores prácticas internacionales a su entorno o giro de negocio para la protección de activos críticos de información. La fragmentación de enfoques y desconocimiento puede dar lugar a implementaciones ineficiente o inconsistente, dejando a la organización vulnerable a ciberataques. Se necesita un modelo de ciberseguridad que tenga un enfoque unificado y adaptable a las diferentes estructuras organizativas.

Formulación del problema de investigación

¿Existen definidos procesos, planes de acción o políticas relacionadas con normas o regulaciones sobre ciberseguridad que se ejecuten sobres los activos críticos de la organización?

¿Existe conocimiento sobre el potencial dañino que conllevan los riesgos cibernéticos?

¿Conoce de alguna norma o regulación la cual pueda ser implementada en la organización para protección de sus activos críticos?

Objetivo General:

Diseñar un marco de ciberseguridad aplicando normas NIST e ISO 27110:2021 para minimizar el riesgo cibernético en activos de información críticos de la organización.

Objetivos Específicos:

1. Contextualizar los fundamentos teóricos sobre buenas prácticas de seguridad de la información basado en las normas ISO 27110:2021 y NIST.
2. Identificar activos críticos de información de la organización.
3. Establecer mecanismos de evaluación y mejora continua del diseño propuesto.

Planteamiento hipotético

El desconocimiento de las organizaciones sobre las regulaciones o normas de Ciberseguridad expone sus activos críticos de información a riesgos cibernéticos.

Justificación

La ciberseguridad no es exclusiva de las grandes empresas, en Ecuador el 38% de las pequeñas y medianas empresas afirman haber experimentado problemas de ciberseguridad, si una organización maneja un gran volumen de datos, o datos que son considerados confidenciales, además de ser vulnerable a los ataques, está expuesta a ataques dirigidos a la fuga o secuestro de datos, y necesita protegerse con mayor rigurosidad.

En el año 2021 EcuCERT (Centro de respuesta a incidentes informáticos del Ecuador) tuvo alrededor de 8178 notificaciones por incidentes de malware, ataques de fuerza bruta, escaneo de puerto entre otras. (Ecucert, 2021)

Kaspersky en su website nos muestra mediante estadísticas que Ecuador está en el puesto #53 entre los países con mayores ataques de ciberseguridad, en un día se han llegado a contabilizar hasta 23990 ciberataques. (Kaspersky, 2024)

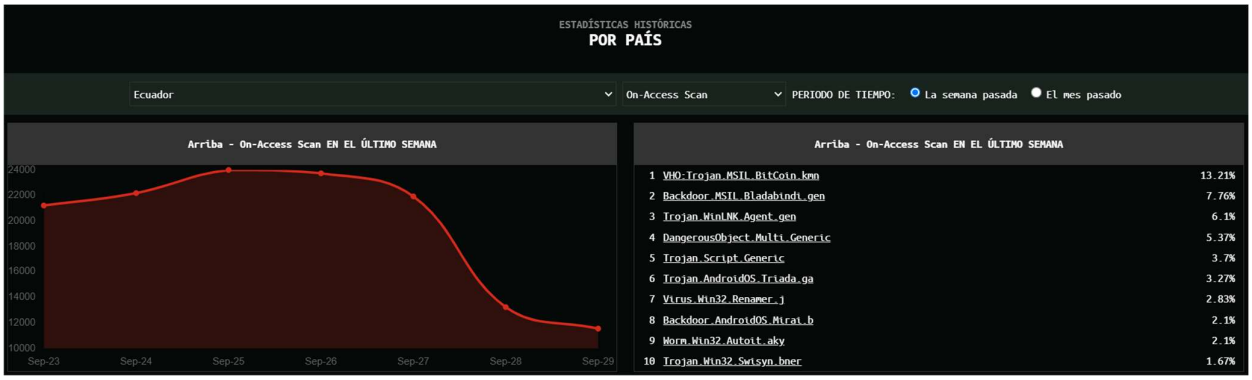

Figura 1 Top Ten Ataques Cibernéticos

Fuente - Kaspersky

La justificación para el diseño de este marco radica en su capacidad de ofrecer una solución integral, flexible, alineada a las mejores prácticas internacionales para protección de activos críticos de información.

Este marco proporcionará las herramientas necesarias para adaptarse y responder a las futuras amenazas emergentes, garantiza una protección robusta y sostenible a los activos digitales.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Revisión de literatura

(Sánchez, 2023) en su tesis Marco mínimo de ciberseguridad para PYMEs en el contexto de la Industria 4.0, nos menciona que la ciberseguridad se encarga de proteger los activos de una organización de los ataques de los cibercriminales, dada la naturaleza de los activos, pueden tener vulnerabilidades, las cuales puede ser explotadas por medio de un ataque, los profesionales de ciberseguridad tienen que poner controles (mecanismos de mitigación, salvaguardas, contramedidas), estos controles a su vez pueden contener otras vulnerabilidades que deben ser mitigadas.

(Nacimba Nacimba, 2024) en su tesis Diseño de Políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui, nos menciona sobre la importancia de la exploración y comprensión de las amenazas emergentes en ciberseguridad, esta radica en la necesidad de anticiparse y estar preparados para los nuevos desafíos y riesgos que surgen constantemente en el entorno digital. Al comprender y explorar estas amenazas emergentes, se pueden desarrollar estrategias y medidas de prevención y respuesta más efectivas.

(Guayara Murillo & Moyano Murcia, 2022) en su tesis Propuesta de orientación en ciberseguridad para la formación de los estudiantes de media técnica especializada del Colegio OEA I.E.D basado en el marco NIST SP800-181, nos indica que, con la digitalización de todos los sectores económicos y la interconexión entre ellos, aumentan las amenazas día a día que ponen en riesgo la seguridad de la información. Por eso se ha hecho imprescindible para las organizaciones tener medidas técnicas, de gestión de riesgos, de recuperación de desastres, políticas y capacitación del personal, entre otras. Uno de los principales inconvenientes que radica es que el mercado no se encuentra estandarizado y existen varias soluciones y alternativas para sobrellevar lo antes mencionado, lo que las empresas buscan se basa en tendencias y otros elementos de valor que no aplican para todos los casos.

(Utreras Guerra, 2024) en su tesis Análisis e implantación de una solución de seguridad perimetral aplicando el marco de trabajo de ciberseguridad del NIST, hace un enfoque en la utilización de NIST Cybersecurity Framework, la misma sirve como guía hacia las mejores prácticas de ciberseguridad, mediante la utilización o generación de

recursos tecnológicos o documentales, dan como resultado perfiles de gestión y gobernabilidad de riesgos. NIST mediante su metodología aplicada, genera perfiles de uso recursivo, hace un enfoque a la mejora continua y a la correcta comunicación de todos los involucrados.

(Suárez & Ruíz, 2022) en su tesis Guía para el abordaje de la Norma ISO 27110:2021 Creación de Marcos de Ciberseguridad nos menciona que la norma ISO/IEC 27110:2021 utiliza un conjunto mínimo de conceptos en la definición de marcos de ciberseguridad, aliviando la carga a los creadores de marcos, con el objetivo de que estos sean flexibles con otras normas e implementaciones ya realizadas de la organización, así como interoperabilidad y compatibilidad con otros marcos. Entre otros principios y objetivos de la norma, está la capacidad de ser aplicada a cualquier organización, sin importa el tamaño, la naturaleza o el tipo, pues posee los conceptos necesarios para organizar un marco de ciberseguridad que responda de forma correcta y coherente a las necesidades de la organización.

(Herrera Flórez & Tellez Monsalve, 2021) en su artículo Diseño de un framework de ciberseguridad, seguridad y privacidad de la información para un proveedor de servicios de telecomunicaciones en un ambiente multirregión, propone una metodología para la identificación y selección de uno o varios Framework de Ciberseguridad, Seguridad y Privacidad para un proveedor de servicios de Telecomunicaciones a lo largo de toda la región enfocado en clientes B2B. Menciona que entre los beneficios de diseñar, definir e implementar el framework que apoye la gestión de la seguridad alineado a su visión y estrategia de negocio, se encuentran:

- Proporcionar un entorno de confianza centrado en el negocio
- Proteger a los clientes, la marca y la reputación
- Satisfacer los requerimientos normativos, legales y regulatorios con respecto a la protección de información personal
- Medir la efectividad de los controles de ciberseguridad, seguridad y privacidad implementados
- Proporcionar una visión global del estado de la seguridad a nivel de las diferentes operaciones hacia el equipo ejecutivo desde la perspectiva del negocio por medio de tableros de control

(Criollo Neira, Flores Urgilés, Flores Urgilés, Santacruz Espinoza, & Ron Egas, 2023) en su artículo Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano nos menciona que la creciente dependencia de la tecnología de la información y las comunicaciones ha hecho que la ciberseguridad se convierta en un componente crítico para los estados, organizaciones y ciudadanos en el mundo. También detalla da a conocer que desde el año 2019 los delitos informáticos en el Ecuador fueron 10279, mientras que en el 2020 han disminuido a 5048, de acuerdo con la Fiscalía General del Estado, los delitos más frecuentes son la intercepción ilegal de los datos, suplantación de identidad, falsificación, acceso no autorizado, contacto con finalidad sexual, apropiación fraudulenta, ataque a la integridad de los sistemas informáticos.

(Rodríguez Márquez, 2021) en su artículo científico Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano, nos menciona que el marco para la ciberseguridad NIST, cuya primera versión se lanzó en 2014, se actualizó en 2018 y se basó en el marco CIS, COBIT y la ISO/IEC 27001. Se caracteriza por considerar la ciberseguridad como un ciclo de proceso evolutivo que permite obtener una mejora continua en las organizaciones alrededor del tema de ciberseguridad.

(Fuentes Penna, Gómez Cárdenas, & González Ibarra, 2024) en su artículo científico La Ciberseguridad en México y los derechos humanos en la era digital, menciona que la ciberseguridad ha demostrado ser una inversión necesaria para los organismos públicos y las empresas. La tecnología ha proporcionado al gobierno nuevas formas de atender e interactuar con los ciudadanos, siendo indispensable crear un marco legal y soluciones de ciberseguridad adecuadas para garantizar que los organismos y los ciudadanos puedan cumplir sus misiones sabiendo que su información está protegida.

1.2. Desarrollo teórico y conceptual

Marco Ciberseguridad NIST

El ciber ataque es uno de los delitos informáticos que más ha crecido desde el 2005, el robo de información y la afectación a instituciones públicas y privadas son las principales consecuencias de los ataques cibernéticos (Chang, 2020), Ecuador como muchos otros países en América Latina, ha visto un crecimiento significativo en el uso

de tecnologías digitales en los últimos años. La digitalización de varios servicios gubernamentales, comercio electrónico y el aumento en el uso de redes sociales han impulsado la necesidad de fortalecer la ciberseguridad en el país. Este avance tecnológico también ha traído consigo una mayor exposición a amenazas cibernéticas. Ecuador aún no cuenta con una estrategia de ciberseguridad, sin embargo, se han logrado mejoras significativas para hacer frente a estas amenazas, una de ellas fue la creación del EcuCERT (Centro de respuesta a incidentes informáticos del Ecuador) en el año 2014. Su principal objetivo es masificar el uso seguro de internet, las tecnologías de la información y los sistemas de telecomunicaciones de todo el Ecuador (Ecucert, 2021), y su vez que satisfaga la confianza de la comunidad o región que las utiliza. (Arcotel & EcuCert, 2014).

La mayoría de empresas del ámbito local ecuatoriano han experimentado una demora en la adopción de tecnología y medidas de seguridad para gestionar eficazmente los riesgos a los que se enfrentan, debido a la transformación digital han tenido que evolucionar en el ámbito tecnológico innovando sus comunicaciones, infraestructura y sistemas de información, las cuales se adaptan al ciberespacio, fomentando la eficacia y rapidez de sus activos, aumentando los niveles de producción y minimizando sus costos (Peralta & Aguilar, 2021), por lo que no pueden darse el lujo de ignorar este problema y deben tomar medidas proactivas para proteger sus sistemas y activos digitales, con el objetivo de reducir el peligro de ser víctimas de ataques informáticos, es crucial que se implementen recomendaciones de ciberseguridad específicas y escalonadas. Las organizaciones en Ecuador, tanto públicas como privadas, están expuestas a estos riesgos, que pueden causar daños financieros y comprometer la privacidad de los datos.

El diseño de un marco de ciberseguridad efectivo es crucial para la protección de la información y los sistemas en un entorno digital, abordando conceptos fundamentales y normativas que forman la base para el desarrollo de un marco de ciberseguridad, es importante que estas recomendaciones sean adecuadas para las necesidades y capacidades de cada organización, con el fin de mejorar significativamente su capacidad para detectar, prevenir y responder a posibles amenazas, nuestro diseño utilizar las normas de ciberseguridad Framework Cybersecurity NIST y la norma ISO/IEC 27110:2021.

El instituto National Institute of Standards and Tecnology (NIST) generó un marco de ciberseguridad el cual se basa en la mitigación y demás políticas anti-riesgo para la organización (Veridas, 2022). Esta guía diseñada para ayudar a las organizaciones tiene el objetivo de gestionar los riesgos de ciberseguridad. Fue desarrollado en respuesta a la Orden Ejecutiva 13636 del Presidente Barack Obama Framework for Improving Critical Infrastructure Cybersecurity, fue emitida en 2013, con la necesidad de crear un marco para mejorar la ciberseguridad de la infraestructura crítica en Estados Unidos. (OAS, 2019), a través de la colaboración entre el sector público y privado, esta publicación fue denominada CSF 1.0, esta versión representó un avance significativo en la gestión de la ciberseguridad, proporcionando una estructura sólida y flexible para enfrentar los riesgos cibernéticos. Su desarrollo, basado en la colaboración y la retroalimentación, estableció un estándar valioso para la protección de la infraestructura crítica.

Su propósito era proveer una guía voluntaria y flexible para que las organizaciones gestionen y reduzcan los riesgos de ciberseguridad, especialmente en infraestructuras críticas. (Technology, Framework for Improving Critical Infrastructure Cybersecurity, 2014)

Componentes principales:

Core (Núcleo): Representan las áreas clave que deben ser gestionadas para protegerse contra los riesgos cibernéticos. Está estructurado en torno a cinco funciones principales, que proporcionan una visión general de la gestión de ciberseguridad:

- Identificar: Comprender el entorno organizacional para gestionar el riesgo cibernético. Incluye la identificación de activos, el contexto, y los riesgos.
- Proteger: Implementar medidas para proteger los activos y datos. Incluye controles de acceso, formación de usuarios, y medidas de protección de datos.
- Detectar: Desarrollar capacidades para identificar eventos de ciberseguridad. Incluye la monitorización continua y la detección de anomalías.

- Responder: Gestionar y mitigar los incidentes de ciberseguridad. Incluye la comunicación, análisis y mitigación de impactos.
- Recuperar: Restaurar las operaciones y mejorar las prácticas después de un incidente. Incluye la mejora continua y la restauración de servicios.

Implementation Tiers (Niveles de Implementación): Los niveles de implementación definen el grado de las prácticas sobre gestión de riesgos de ciberseguridad de la organización, muestran las características definidas en el marco de ciberseguridad (OAS, 2019), representan los niveles de madurez de la ciberseguridad de una organización, describen cómo las organizaciones gestionan los riesgos cibernéticos y la integración de sus prácticas de seguridad en la estructura organizacional general. Son una parte integral del marco y proporcionan una forma de evaluar y mejorar la postura de ciberseguridad:

- Parcial: En este nivel, las prácticas de ciberseguridad son ad hoc y no están formalizadas. Las respuestas a los incidentes de ciberseguridad son reactivos y generalmente se basan en la experiencia individual en lugar de procesos estandarizados. Los procesos de ciberseguridad no están documentados ni estandarizados. No existe una coordinación formal entre las distintas partes de la organización en cuanto a ciberseguridad.
- Riesgo Informado: En este nivel, las prácticas de ciberseguridad están gestionadas y documentadas, pero no están completamente integradas en toda la organización. Existen algunas políticas y procedimientos documentados, aunque no se aplican uniformemente en toda la organización.
- Repetible: En este nivel, la organización ha desarrollado y estandarizado procesos y prácticas de ciberseguridad. Las prácticas están documentadas, se aplican de manera consistente y se revisan regularmente. Los procesos de ciberseguridad están bien definidos, documentados y son aplicados consistentemente en toda la organización. Se proporciona formación continua al personal, y hay un enfoque sistemático para mejorar la seguridad cibernética.
- Adaptado: En este nivel, las prácticas de ciberseguridad están completamente integradas en la organización y adaptadas continuamente

a las amenazas y cambios en el entorno. La organización tiene un enfoque proactivo para la gestión de riesgos. La organización realiza mejoras continuas en las prácticas de ciberseguridad basadas en los resultados de las evaluaciones y la retroalimentación. La ciberseguridad es parte integral de la cultura organizacional, con una fuerte alineación entre las políticas de ciberseguridad y los objetivos empresariales.

Profiles (Perfiles): Permiten a las organizaciones alinear sus actividades de ciberseguridad con sus necesidades y objetivos. Permiten a las organizaciones comparar su estado actual con sus objetivos deseados, identificar brechas y planificar mejoras en su postura de ciberseguridad.

- Perfil Actual: Representa el estado actual de las prácticas y controles de ciberseguridad de la organización.
- Perfil Objetivo: Representa el estado deseado o futuro de las prácticas y controles de ciberseguridad de una organización. Define los objetivos que la organización quiere alcanzar y las capacidades que desea desarrollar o mejorar.

Figura 2 Componentes NIST

Fuente NIST

En abril de 2018, se lanzó la versión 1.1 del NIST Cybersecurity Framework, esta versión incorpora varias mejoras y ajustes basados en la retroalimentación de las partes interesadas y en la evolución del panorama de ciberseguridad.

Hizo actualizaciones y dio énfasis en los siguientes puntos:

- Gestión de Riesgos de Terceros
- Evaluación Continua
- Adaptación a Nuevas Amenazas
- Alineación con Otros Estándares

La versión 1.1 representa una evolución significativa del marco original, incorpora mejoras importantes como integración y aplicación práctica. (Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 2018).

Figura 3 Evolución NIST

Fuente NIST

En 2023, NIST anunció el desarrollo de la versión 2.0 del Cybersecurity Framework, comenzando con la publicación de un borrador. (Technology, The NIST Cybersecurity Framework (CSF) 2.0, 2024)

Entre sus objetivos más relevantes encontramos:

- Nueva función Gobernar
- Enfoque en la cadena de suministro
- Mayor énfasis en la cultura de seguridad

Figura 4 NIST 2.0

Fuente NIST

Las actualizaciones y revisiones del marco aseguran que siga siendo relevante y efectivo, proporcionando un enfoque de mejora continua para la gestión de riesgos de ciberseguridad.

NIST inicialmente fue creada como una herramienta para evaluar la ciberseguridad en las Infraestructuras Criticas de EEUU, su enfoque y punto de vista, ha demostrado que es adaptable a diferentes áreas, sectores y países, tiene la facilidad de poder adaptarlo en los procesos de auditoria, tiene la función de adaptarse y poder generar un nuevo programa de ciberseguridad o como herramienta guía para analizar brechas de programas o marcos de ciberseguridad existentes y poder mejorarlos. (OAS, 2019)

ISO 27110:2021

La ISO/IEC TS 27110:2021 proporciona un marco teórico sólido y flexible para el desarrollo de estrategias de ciberseguridad personalizadas. Su enfoque se basa en una serie de principios y conceptos clave que guían la implementación de un sistema de gestión de la ciberseguridad eficaz, la norma está elaborada para implementarse en cualquier industria empresarial. Se complementa con otras normas de la familia ISO 27000, como la ISO/IEC 27001, que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La ISO 27110 proporciona una guía más específica para el desarrollo de marcos de ciberseguridad, mientras que la ISO 27001 ofrece un enfoque más amplio para la gestión de la seguridad de la información, esta norma ofrece una descripción general de los sistemas de gestión de seguridad de la información, así como los términos que se deben interpretar y usar. (Duque & Orozco-Alzate, 2017)

ISO/IEC 27000, que abarca un conjunto de normas para la gestión de la seguridad de la información, esta serie incluye la ISO/IEC 27001 (requisitos para un sistema de gestión de seguridad de la información) y la ISO/IEC 27002 (prácticas de control de seguridad), entre otras.

A partir de 2008, la serie ISO/IEC 27000 comenzó a expandirse con nuevas normas para abordar diferentes aspectos de la seguridad de la información y la ciberseguridad. Así nacen la norma ISO/IEC 27005 que proporciona directrices para la gestión de riesgos de seguridad de la información e identificar vulnerabilidades y a tomar medidas proactivas para proteger los activos de información. ISO 27005 tiene un proceso paso a paso que incluye implantar el entorno, evaluar los peligros de estabilidad de la información, gestionar los peligros de estabilidad de la información, admitir los peligros de estabilidad de la información, comunicar los peligros de estabilidad de la información, monitorear y verificar los peligros y la estabilidad de la información. (Martos Paredes & Villazon Sosa, 2024)

También se crean las normas ISO/IEC 27017 y ISO/IEC 27018 se enfocaron en la seguridad de la información en la nube y la protección de la información personal en servicios en la nube, respectivamente, promoviendo la implementación de controles de seguridad de la información específicos para la nube; dicho de otra manera, constituye

un código de buenas prácticas dirigido a clientes y proveedores de servicios en la nube. (Ruiz Imbat, 2021)

En el año 2010 nace la ISO 27003 que proporciona directrices sobre cómo establecer, implementar, mantener y mejorar un SGSI, e ISO 27004 que ofrece directrices sobre cómo medir y evaluar la eficacia de un SGSI, incluyendo la definición de indicadores clave de rendimiento (KPI) y otros métodos para monitorizar y evaluar el rendimiento del sistema, asegurando que se cumplen los objetivos de seguridad de la información.

Para el 2012 se publica la norma ISO 27032:2012 que proporciona directrices para la ciberseguridad, abordando la seguridad en el contexto de las redes y el uso de Internet, atiende la seguridad en el ciberespacio o asuntos de ciberseguridad los cuales se concentran en reducir las brechas entre los diferentes dominios de ciberseguridad en el ciberespacio (González Reyes, 2021). Al seguir sus directrices, las organizaciones pueden proteger mejor sus activos de información, gestionar riesgos y fomentar un entorno de ciberespacio seguro, es un marco de intercambio de información y coordinación, y aunque se emergen con ella controles de seguridad en la red, es preciso mencionar que tal como se define el ciberespacio, destacado como un entorno complejo, lo hace altamente variable en riesgos y amenazas.

En el año 2018 se crea la norma ISO 27103 proporciona una guía integral para la implementación de un enfoque coordinado de ciberseguridad basado en la familia de normas ISO/IEC 27000. Al seguir estas directrices, las organizaciones pueden fortalecer su postura de ciberseguridad, gestionar los riesgos de manera eficaz y asegurar la protección continua de sus activos de información.

Posteriormente, en el 2020, nace la ISO/IEC 27100:2020 es una norma internacional que proporciona los conceptos y principios fundamentales de la ciberseguridad. Esta norma proporciona una guía clara sobre los conceptos y principios fundamentales de la ciberseguridad. Proporciona definiciones claras de términos claves en ciberseguridad. Herramienta invaluable para cualquier organización que busca fortalecer su postura de seguridad cibernética.

Proporciona una base sólida y estandarizada para la comprensión y aplicación de la ciberseguridad. Al seguir los conceptos y principios definidos en esta norma, las

organizaciones pueden mejorar su postura de ciberseguridad, facilitar la comunicación y colaboración efectiva, y establecer una base sólida para la implementación de otras normas y prácticas de ciberseguridad (Cistoldi, y otros, 2023)

En el año 2021 se publica la ISO/IEC 27110:2021 es una norma internacional que proporciona una estructura y directrices para la implementación de un programa de gestión de ciberseguridad (CSMP, por sus siglas en inglés). Esta norma fue desarrollada para ayudar a las organizaciones a establecer, implementar, mantener y mejorar continuamente un programa de ciberseguridad que sea efectivo y alineado con las mejores prácticas internacionales.

Proporciona un marco integral y estructurado para gestionar la ciberseguridad de manera efectiva, ayudando a las organizaciones a protegerse contra las amenazas cibernéticas y a mejorar continuamente su postura de seguridad, proporcionando un conjunto de directrices para desarrollar un marco de ciberseguridad personalizado y efectivo.

El objetivo de la norma es garantizar que se utilice un conjunto mínimo de conceptos para definir marcos de ciberseguridad, alivianando carga a los creadores, haciendo del marco resultante una herramienta interoperable con otras organizaciones, así como flexible y compatible con otras actividades y herramientas ya implementadas, garantizando la continuidad de los esfuerzos invertidos en dicho ámbito. (Bastidas Pérez, 2021)

Entre las características de esta normativa tenemos:

- Definir términos y conceptos relacionados con la ciberseguridad para facilitar la comunicación y la colaboración entre organizaciones.
- Ofrecer un marco de referencia para el desarrollo de nuevos marcos de ciberseguridad, facilita su diseño e implementación.
- Permitir que las organizaciones adapten el marco a sus necesidades específicas.
- Ayudar a las organizaciones a prepararse para responder a incidentes de seguridad y recuperarse rápidamente.

La norma se basa en cinco funciones fundamentales que son: identificar, proteger, detectar, responder y recuperar.

- Identificar: Reconocer y entender los riesgos asociados.
- Proteger: Implementar controles y medidas preventivas para mitigar los riesgos identificados.
- Detectar: Identificar rápidamente incidentes de seguridad.
- Responder: Actuar ante un incidente para minimizar su impacto.
- Recuperar: Restaurar las operaciones y servicios después de un incidente.

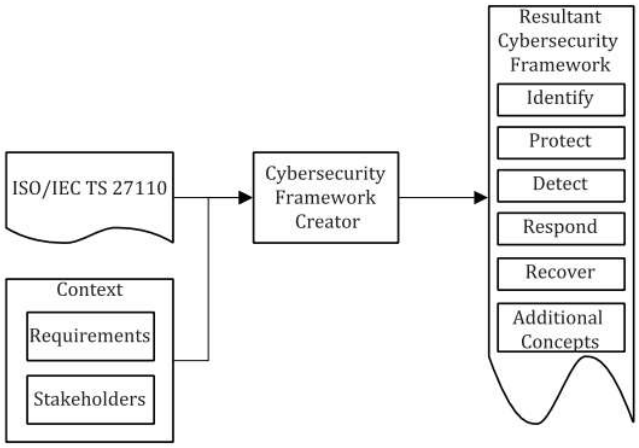

Figura 5 Funciones ISO 27110:2021

Fuente Norma ISO 27110:2021

Activos Críticos Informáticos

Un activo crítico informático es cualquier recurso o información que resulta esencial para el funcionamiento de una organización. Estos activos son tan vitales que su pérdida, daño o compromiso podrían tener un impacto significativo en las operaciones, la reputación y la continuidad del negocio.

Los activos críticos contienen información valiosa que permite a la organización tomar decisiones estratégicas, desarrollar nuevos productos o servicios y mantener una ventaja competitiva, muchas organizaciones dependen en gran medida de sus sistemas informáticos para llevar a cabo sus operaciones diarias. La pérdida o corrupción de estos sistemas puede paralizar la actividad. Muchas industrias están sujetas a regulaciones les

exigen la protección de ciertos tipos de datos. El incumplimiento de estas normas puede resultar en sanciones económicas y legales.

Los activos de información crítica son la columna vertebral de la seguridad y la resiliencia organizacional. Al comprender su diversidad y relevancia, las empresas pueden diseñar estrategias sólidas para proteger estos activos vitales y garantizar la continuidad de sus operaciones en un mundo digitalmente interconectado. La gestión consciente y proactiva de estos activos es esencial para la prosperidad a largo plazo de cualquier organización en la era de la información.

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

En base a lo mencionado, la investigación plantea el diseño de un modelo de ciberseguridad basada en el marco de ciberseguridad NIST e ISO 27110:2021 en la empresa Fortidex.

Fortidex es una empresa que se dedica a la elaboración de harina y solubles de pescado y otros animales acuáticos para alimento de animales, no aptos para el consumo humano. Geográficamente se encuentra ubicada al norte de la ciudad de Guayaquil, podemos ubicarla con las siguientes coordenadas -2.17451288840828, -79.90788900589261.

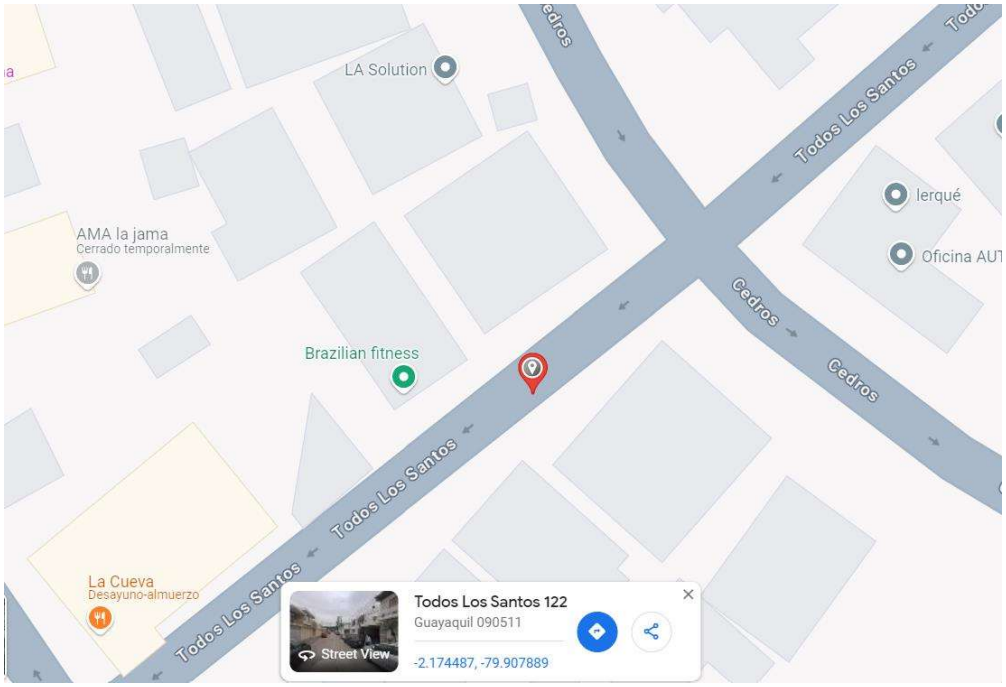

Figura 6 Ubicación Fortidex Matriz

Fuente Google

Consta con 3 plantas ubicadas:

• Data de Posorja coordenadas -2.7016333663915453, -80.29469258138512

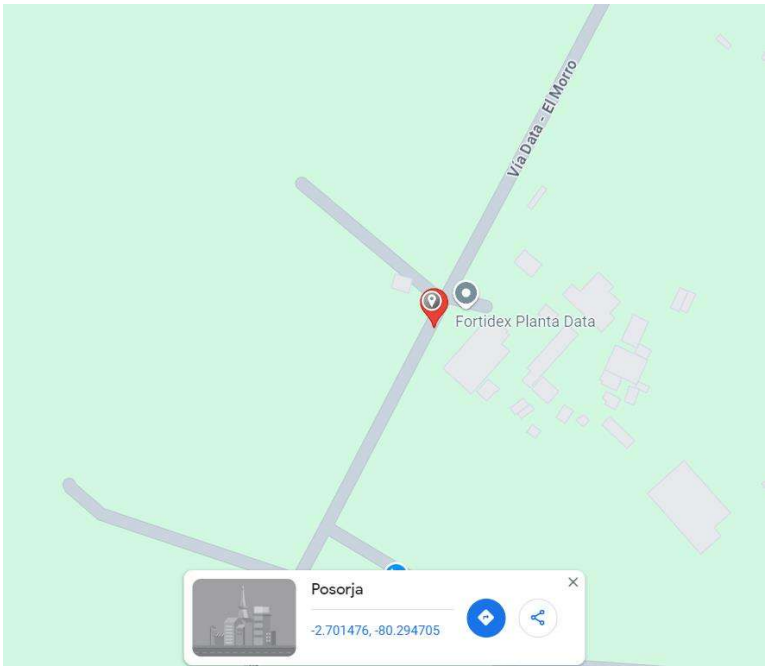

Figura 7 Ubicación Fortidex Data

Fuente Google

• Posorja coordenadas -2.702998407241791, -80.24428012001158.

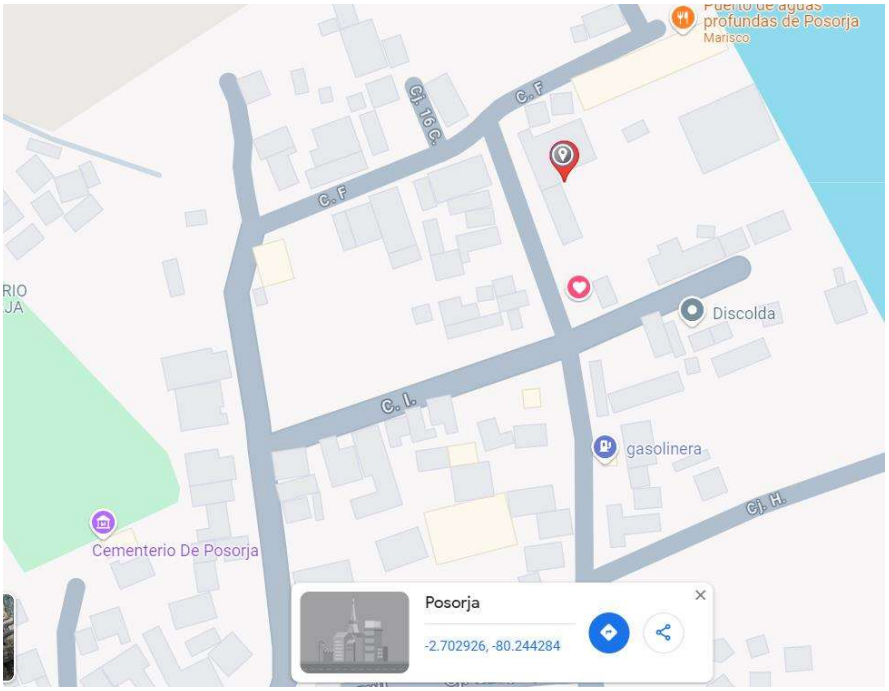

Figura 8 Ubicación Fortidex Posorja

Fuente Google

• Parroquia Virgen de Fatima coordenadas -2.234532901505065, 79.6999183200132.

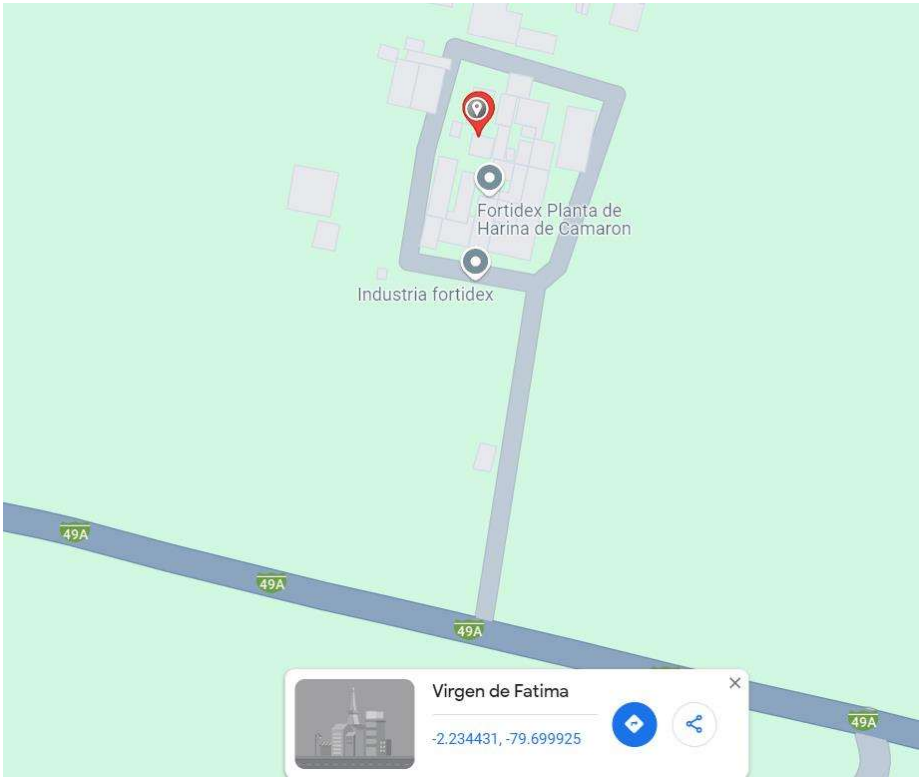

Figura 9 Ubicación Fortidex Taura

Fuente Google

El diseño del modelo de ciberseguridad que se propone en esta investigación está siendo ejecutado en un ambiente de pruebas controlado. Este entorno ha sido creado para simular condiciones reales de operación y evaluar la eficacia del modelo propuesto ante diversas amenazas y vulnerabilidades.

2.2. Diseño y alcance de la investigación

En esta investigación, se adopta un enfoque no experimental, el diseño del marco de ciberseguridad propuesto fundamentado bajo las normas NIST e ISO 27110:2021, con el objetivo de ayudar a reducir el riesgo cibernético en activos de información críticos de la organización, está enfocado en la observación y análisis de situaciones reales sin

manipulación de variables, lo que permite una evaluación más contextualizada del diseño propuesto.

El alcance de la investigación será descriptivo, permitirá documentar de manera sistemática los elementos del marco de ciberseguridad propuesto. Se describirán las políticas, procedimientos y controles de seguridad recomendados, así como su impacto en la reducción de riesgos cibernéticos en activos de información críticos, este enfoque permitirá documentar de manera sistemática y detallada los componentes clave del marco propuesto y su relevancia en la mitigación de riesgos cibernéticos en activos de información críticos.

2.3. Tipo y métodos de investigación

La presente investigación se clasifica como mixto, combinando enfoques cuantitativos y cualitativos para abordar el diseño de un marco de ciberseguridad que aplique las normas NIST e ISO 27110:2021. El uso de un enfoque de investigación mixto permitirá obtener una visión integral del diseño del marco de ciberseguridad, combinando datos cuantitativos que midan su efectividad con información cualitativa que brinde contexto y profundidad a los hallazgos. Esta metodología enriquecerá la comprensión sobre el diseño del marco de ciberseguridad basado en las normas NIST e ISO 27110:2021.

Emplearemos el método deductivo en esta investigación, con lo cual estructuraremos el diseño del marco de ciberseguridad a partir de teorías y principios establecidos en las normas NIST e ISO 27110:2021. Identificaremos las directrices y principios fundamentales que se encuentran en las normas ISO 27110:2021 y NIST.

El objetivo de este método es la de proporcionar una base sólida para el diseño del marco de ciberseguridad, Esto asegurará que el marco propuesto no solo sea relevante, sino que también se respalde por evidencia empírica y valide su efectividad en la mitigación de riesgos cibernéticos.

2.4. Población y muestra

La población objetivo del presente trabajo de investigación, se tomará en cuenta a los trabajadores de la empresa Fortidex, esta población suma alrededor de 300 empleados.

En la presente investigación se ha determinado que la muestra seleccionada será personal de TI y jefes de las diferentes áreas de la empresa Fortidex que suman 30 empleados, debido a que sus procesos forman parte del diseño del marco de ciberseguridad que permitirá la seguridad y confidencialidad de su información en el entorno virtual, nuestra muestra será

La muestra es de tipo no probabilística debido a que se ha relacionado con el objetivo de la investigación y no se ha procedido a evaluar un proceso de selección aleatoria.

2.5. Técnicas e instrumentos de recolección de datos

Para la recolección de información utilizaremos técnicas cuantitativas y cualitativas, se elaborará encuestas y entrevistas de acuerdo con las variables que previamente definimos en esta investigación.

Las preguntas empleadas serán las siguientes:

Entrevista a Personal de TI

Preguntas - Entrevista
¿Qué prácticas de ciberseguridad utiliza la organización para proteger los activos críticos de información?
¿Existen definidos procesos, planes de acción o políticas relacionadas con normas o regulaciones sobre ciberseguridad?
¿Existe software que se utiliza actualmente para la protección de los sistemas y datos?
¿Cómo se evalúa la efectividad de las prácticas de ciberseguridad en la organización para la protección de activos críticos de información?

Tabla 1 Entrevista Personal IT

Encuestas Personal Administrativo

Preguntas - Encuesta	**Opciones de Respuesta**	
¿Tiene conocimiento sobre el potencial dañino que conllevan los riesgos cibernéticos sobre los activos críticos de información?	Si	No
¿Se le ha proporciona capacitación específica sobre buenas prácticas de ciberseguridad?	Si	No
¿Conoce de alguna herramienta que asegure su información digital?	Si	No
¿Ejecuta o practica a diario buenas prácticas referente a ciberseguridad?	Si	No

Tabla 2 Encuesta Personal Administrativo

A. 2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

Debido a nuestro tipo de recolección de datos que es mixta, tabularemos y realizaremos todo el análisis de la data mediante Excel.

Validaremos estos datos con un consultor externo especializado en el ámbito del diseño de marcos de ciberseguridad.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

3.1 Resultados de Encuestas y Entrevistas

Pregunta N°1- Encuesta - Personal Administrativo	SI	NO
¿Tiene conocimiento sobre el potencial dañino que conllevan los riesgos cibernéticos sobre los activos críticos de información?	14	16

Tabla 3 Resultados Encuesta Pregunta 1

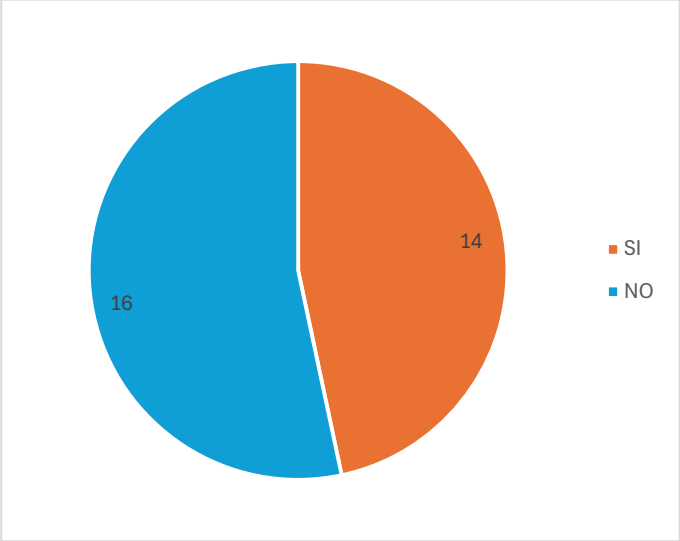

Figura 10 Resultados Encuesta Pregunta 1

Pregunta N°2- Encuesta - Personal Administrativo	SI	NO
¿Se le ha proporcionado capacitación específica sobre buenas prácticas de ciberseguridad?	5	25

Tabla 4 Resultados Encuesta Pregunta 2

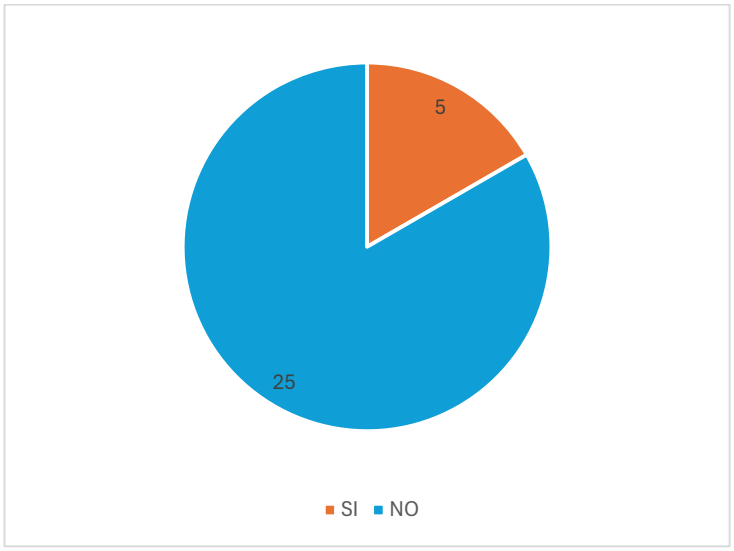

Figura 11 Resultados Encuesta Pregunta 2

Pregunta N°3- Encuesta - Personal Administrativo	SI	NO
¿Conoce de alguna herramienta que asegure su información digital?	8	22

Tabla 5 Resultados Encuesta Pregunta 3

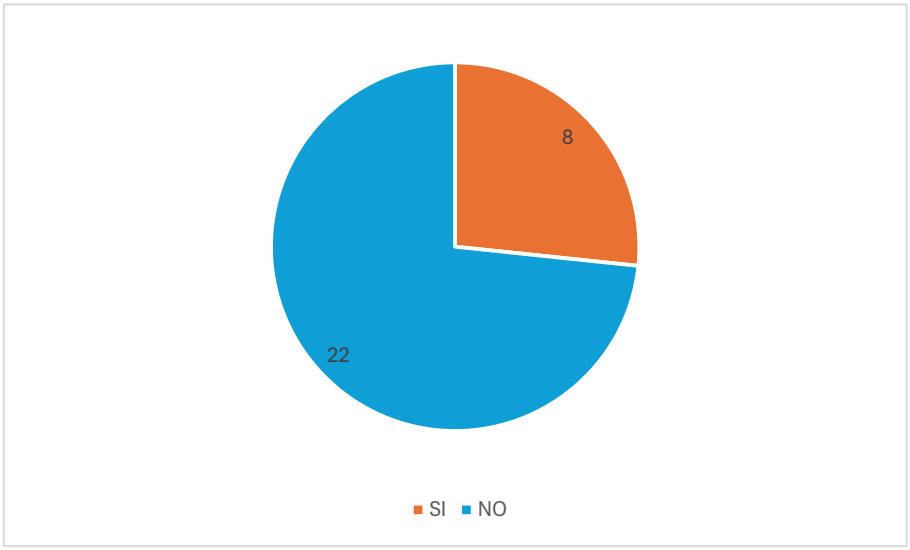

Figura 12 Resultados Encuesta Pregunta 3

Pregunta N°4- Encuesta - Personal Administrativo	SI	NO
¿Ejecuta o practica a diario buenas prácticas referente a ciberseguridad?	5	25

Tabla 6 Resultados Encuesta Pregunta 4

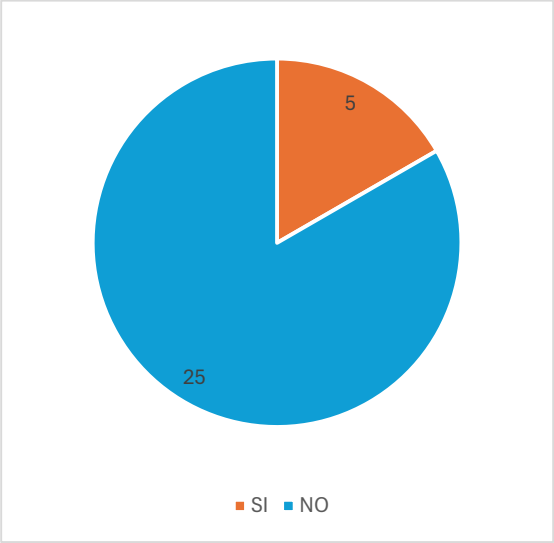

Figura 13 Resultados Encuesta Pregunta 4

1. **¿Qué prácticas de ciberseguridad utiliza la organización para proteger los activos críticos de información?**

Entrevista 1 - Personal TI

Es una de las principales preocupaciones de la organización, para garantizar la seguridad de los activos críticos de información de la organización, tenemos una serie de prácticas de ciberseguridad robustas y actualizadas, entre las cuales tenemos:

- Determinar activos críticos de la organización y cuáles son los sistemas y aplicaciones que la contienen.
- Evaluar los sistemas y aplicaciones en busca de debilidades que puedan ser explotadas por atacantes externos, y poder identificar amenazas y su potencial impacto en la organización.

- Autenticación multifactor para acceder a sistemas y aplicaciones de la organización.
- Encriptación de datos
- Realizar copias de seguridad regulares, estableciendo escenarios de recuperación.

Entrevista 2 - Personal TI

Existen varias prácticas de ciberseguridad que la organización utiliza para proteger sus activos críticos de información entre las cuales tenemos:

- Autenticación Multifactor
- Cifrado de datos
- Firewall y routers de borde
- Antivirus y antimalware en sus activos críticos de información
- Copias de seguridad regulares

2. **¿Existen definidos procesos, planes de acción o políticas relacionadas con normas o regulaciones sobre ciberseguridad?**

Entrevista 1 - Personal TI

Actualmente en la organización sí existen definidas políticas sobre los activos críticos de información, pero las mismas no están relacionadas con normas o regulaciones sobre ciberseguridad.

Entrevista 2 - Personal TI

Estos procesos son fundamentales para que la organización garantice la protección de los activos críticos de información y se cumplan con los requisitos legales y normativos gubernamentales del país, pero la organización actualmente no se encuentra alineada con este tipo de regulaciones.

3. **¿Existe software que se utiliza actualmente para la protección de los sistemas y datos?**

Entrevista 1 - Personal TI

Existe una amplia gama de software diseñado para la protección de activos críticos de información en el mercado, pero actualmente la organización tiene implementado lo siguiente:

- Antivirus y Antimalware, sus bases se actualizan a diario, tienen funciones adicionales de IDS e IPS

Entrevista 2 - Personal TI

Si actualmente la organización cuenta con software actualizado para la protección contra virus y malware en los activos críticos de información, adicionalmente se lo monitorea a diario en búsqueda de novedades

4. **¿Cómo se evalúa la efectividad de las prácticas de ciberseguridad en la organización para la protección de activos críticos de información?**

Entrevista 1 - Personal TI

Evaluar la efectividad de las prácticas de ciberseguridad es un proceso continuo, actualmente en la organización estas no se evalúan, pero a futuro se está pensando en implementar:

- Auditorías informáticas,
- Simulacros y escenarios de recuperación
- Evaluar cumplimiento de normativas, monitoreo continuo y pruebas de penetración.

Entrevista 2 - Personal TI

Actualmente en la organización no se evalúa las prácticas de ciberseguridad, es una mejora que ha futuro se requiere implementar por el giro del negocio y número de empleados que tiene la organización con el fin de tener una visión clara de la efectividad de estas prácticas y tomar las medidas necesarias para mejorarla.

3.2 Categorías y Subcategorías utilizados en el diseño del marco de ciberseguridad

A continuación, se incluyen todas las categorías y subcategorías que se utilizaron para el diseño del marco de ciberseguridad de cada una de las fases:

3.2.1 Fase Identificar

NIST		
Categoría: Gestión de Activos - ID.AM		**Objetivo**
Subcategorías	01	Identificar e inventariar activos críticos de información de la organización
	02	Inventariar software que ejecuta activo critico de información de la organización
	03	Identificación de la comunicación de red en la organización y como fluyen los datos en la red interna y externa
	04	Identificar los servicios suministrados por los proveedores a los activos críticos de información
	05	Priorizar el activo critico de información en función de su criticidad e impacto en la organización
	08	Gestionar activo critico de información durante su ciclo de vida
Categoría: Mejora - ID.IM		**Objetivo**
Subcategorías	01	Identificación de las mejoras con la ayuda de evaluaciones
	02	Ejecución de pruebas y ejercicios de seguridad, se debe incluir proveedores
	03	Ejecución de procesos, procedimientos y actividades con el fin de identificar las mejoras
	04	Se mejoran los planes de respuesta a incidentes de ciberseguridad que afectan a los procesos de la organización
Categoría: Evaluación de riesgos - ID.RA		**Objetivo**
Subcategorías	01	Su meta es identificar las vulnerabilidades de los activos críticos de información de la organización
	02	Se debe compartir información sobre ciber amenazas en foros y otras fuentes de intercambio
	04	Su meta es identificar los impactos y validar la probabilidad de que a la amenaza se explote su vulnerabilidad
	05	Su meta es comprender el riesgo al que el activo está expuesto, mediante amenazas y vulnerabilidades

Tabla 7 NIST Fase Identificar

ISO 27110:2013	
Norma - Categoría - Subcategoría	**Objetivo**
ISO/IEC 27002:2013, 8.1.1, 8.1.2 ISO/IEC 27019:2017, 9.2.1	Realizar inventario de los activos y sistemas físicos de la organización.
ISO/IEC 27002:2013, 8.1.1, 8.1.2	Realizar inventario del software que se ejecuta sobre los activos de la organización.
ISO/IEC 27002:2013, 13.2.1	Monitorear la comunicación de la organización
ISO/IEC 27002:2013, 11.2.6, 8.2.1	Catalogar los activos críticos de información externos
ISO/IEC 27002:2013, 11.2.6, 8.2.1	Priorizar el activo critico de información en función de su criticidad e impacto en la organización

Tabla 8 ISO 27110:2021 Fase Identificar

3.2.1.1 Gestión de Activos

Los activos críticos de información permiten a la organización lograr los propósitos comerciales con el core de la organización, su protección es esencial para la continuidad de la organización, se los identifican y gestionan de manera consistente según su importancia relativa para los objetivos de la organización.

Inventario de Activos - Hardware: Un inventario de activos es un registro completo del hardware, por ejemplo, servidores físicos y virtuales, equipos de cómputo, portátiles, equipos de terceros como equipos de telecomunicaciones o cualquier otro dispositivo que este categorizado como un activo critico de información en la organización.

El inventario debe ser actualizado con frecuencia. Se debe actualizar el inventario de activos de información crítico al menos una vez al año, se deben identificar activos nuevos si el caso lo amerita.

Para el diseño del marco de ciberseguridad de este trabajo se recomienda:

- Establecer políticas y procedimientos para la gestión de activos críticos de información.

- Documentación del inventario de activos, incluida la frecuencia con la que se actualiza para mantener los datos actualizados, la frecuencia con la que se revisa y el responsable de esta tarea, y el método del inventario si es automatizado, manual o combinación de ambos.
- Mapeo y descubrimiento de nuevos activos críticos de información si amerita el caso.
- Definir procesos, roles, responsabilidades relacionado con el inventario de activos críticos de información.

Inventario de Activos - Software: Se debe llevar un registro completo del software, aplicaciones, software y repositorios de la organización. El sistema de registro de inventario actual se actualiza con la frecuencia necesaria para que la organización gestione con éxito los procesos posteriores basándose en un inventario de activos preciso.

El registro normalmente incluirá el tipo de dispositivo que ejecuta el software, la versión del software y la fecha de finalización del soporte para ayudar a la organización a administrar las actualizaciones, parches y reemplazos del software. Por lo general, incluirá el propietario o grupo responsable, la ubicación/región y el nivel de criticidad o sensibilidad.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Documentación del inventario de software, incluida la frecuencia con la que se actualiza el inventario para mantener los datos actuales y el método del inventario (por ejemplo, automatizado, manual).
- Definir procesos de revisión de plataformas y aplicaciones.
- Definir procesos, roles, responsabilidades y evidencia relacionados con software del activo crítico de información.

Gestión Ciclo Vida Activo: El ciclo de vida de un activo critico de información es una secuencia de etapas por las que pasan los activos de la organización durante el período de vida útil. (IBM, 2022) Gestionar formalmente los activos desde la adquisición hasta su final de vida, ayuda a proporcionar su sensibilidad, criticidad y valor comercial.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Definir políticas y procedimientos sobre gestión de vida de activos críticos de información, estas deben incluir fecha de compra del activo y fin de vida de cada activo.
- Procesos, roles, responsabilidades relacionadas con ciclo de vida de activos.
- Definir políticas, estándares y procesos para eliminación segura de información electrónica, que pueden incluir destrucciones físicas, destrucciones lógicas, estas deben incluir certificados de destrucción emitidas por un ente local autorizado.
- Definir políticas para la gestión de sistemas no soportados, final de vida útil, que incluyan certificados de destrucción.

Priorización de Activos: Clasificar y priorizar activos críticos de información según su sensibilidad y criticidad, en función de la información que contiene el activo y su función en procesos comerciales críticos.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Utilizar métodos de cifrado y controles de acceso con el fin de asegurar la protección contra accesos no autorizados hacia activos críticos de información de la organización.
- Establecer políticas y procedimientos sobre cómo manejo, almacenamiento y transmisión de información sensible.
- Determinar el nivel de sensibilidad de la información y asignar una clasificación apropiada, como confidencial, restringida y secreta.

Seguridad de Red: Asegurar que la información transmitida a través de la red ya sea de manera interna o externa, esté adecuadamente protegida contra interceptaciones y accesos no autorizados. Se debe proporcionar información relacionada con el inventario de activos de la organización que demuestre que el inventario incluye mapas de red, conexiones con recursos externos y móviles, se debe incluir tanto conexiones internas o externa. Se debe proporcionar información sobre los controles establecidos para garantizar la autenticación y autorización adecuadas para acceder a los activos de la

organización, como dispositivos VPN, enrutadores, recursos de red externos y tecnologías inalámbricas.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Definir responsables para la gestión de datos, incluidas funciones y responsabilidades.
- Mapas de red, diagramas de red y conexiones de terceros.
- Definir políticas de acceso remoto a los activos críticos de la organización.
- Definir políticas de acceso a proveedores externos que proveen algún tipo de servicio a los activos críticos de la organización.

Activos críticos de información gestionado por terceros: Los activos de hardware, softwares mantenidos por o ubicados en proveedores o terceros se incluyen en el inventario y el ciclo de vida de gestión de activos de la organización. El inventario debe enumerar todos los proveedores de servicios conocidos, incluir clasificaciones y designar un contacto empresarial para cada proveedor de servicios.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Establecer y mantener un inventario de proveedores de servicios.
- Revisar y actualizar el inventario de manera anual o cuando se produzcan cambios empresariales importantes.
- Documentar información del punto de contacto de sistemas externos.

3.2.1.2 Evaluación de Riesgos

La evaluación de riesgos es un proceso continuo que se adapta a los cambios en la organización y su entorno, ayuda a identificar y reconocer las amenazas y vulnerabilidades que pueden afectar a los activos de información. Esto incluye tanto riesgos internos como externos.

Identificación de Vulnerabilidades en activos críticos de información: Proporciona información sobre cómo la organización, identifica, evalúa y documenta riesgos y vulnerabilidades potenciales sobre sus activos críticos de información. Ayuda a establecer la base para la evaluación y gestión de riesgos, permitiendo a la organización priorizar sus esfuerzos de ciberseguridad.

Se promueve el uso de inteligencia para la identificación de amenazas, mejorar la detección de incidentes cibernéticos, al integrar esta información en los procesos de detección, la organización puede mejorar significativamente su capacidad para prevenir y responder a incidentes de ciberseguridad.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Evaluar y documentar las amenazas que podrían afectar a los activos, como ciberataques, desastres naturales, errores humanos, etc.
- Documentar y ejecutar pruebas de penetración en activos críticos de información.
- Unirse a comunidades y organizaciones que comparten información sobre amenazas cibernéticas.

Evaluación del riesgo en activos críticos de información: La evaluación de riesgos es fundamental para tomar decisiones sobre ciberseguridad. Al identificar los riesgos más significativos, la organización puede priorizar sus esfuerzos de protección y asignar recursos de manera más eficiente, lo que permiten tomar decisiones basadas en datos sobre cómo asignar recursos de seguridad, permite a la organización a comprender mejor su exposición a las amenazas.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Realizar evaluaciones de impacto empresarial, estimando la probabilidad de una amenaza en particular explote una vulnerabilidad específica sobre algún activo.
- Realizar evaluaciones de riesgos y controles sobre los activos críticos de información, asignando valores numéricos o categorías a las amenazas, vulnerabilidades, probabilidades e impactos para obtener una medida cuantitativa del riesgo.

3.2.1.3 Mejora Continua

Se centra en el proceso de mejorar continuamente capacidades de identificación de riesgos en activos de la organización. Es esencial para mantener la efectividad de ciberseguridad y adaptarse a un entorno en constante cambio.

Identificación de riesgos y activos: Es clave para asegurar que los procesos de gestión de riesgos se mantengan actualizados en el tiempo, se enfoca en establecer y mantener un proceso sistemático para la identificación y gestión de activos a lo largo del tiempo, incorporando mejoras basadas en la experiencia y la retroalimentación.

3.2.2 Fase Proteger

NIST		
Categoría: Gestión de identidades, autenticación y control de acceso - PR.AA		**Objetivo**
Subcategorías	01	Gestionar las identidades y credenciales de los usuarios, que acceden a los activos críticos de información
	02	Cuentas de usuario comprobadas y vinculadas
	03	Los usuarios, servicios y hardware están autenticados
	04	Cuentas de usuarios de la organización deben protegerse
	05	Buenas practicas referente al acceso y autorización al activo critico de información
	06	Se debe supervisar el acceso físico de los activos
Categoría: Concienciación y capacitación - PR.AT		**Objetivo**

Subcategorías	01	Capacitar al personal de las diferentes áreas de la organización en temas referente a ciberseguridad
	02	Capacitar al personal del área de TI de la organización en temas referente a ciberseguridad
Categoría: Seguridad de la plataforma - PR.PS		**Objetivo**
Subcategorías	01	Buenas practicas referente a la configuración del activo critico de información
	02	Eliminación de software categorizado como riesgoso para el activo critico de información
	03	Eliminación de hardware categorizado como riesgoso para el activo critico de información
	04	Generación, almacenamiento de registros de los activos críticos de información
	05	Se prohíbe la instalación de software no autorizado
Categoría: Resiliencia de la infraestructura tecnológica PR-IR		**Objetivo**
Subcategorías	01	Protección de la red y el entorno del activo critico de información
	02	Los activos críticos de información deben estar protegidos contra amenazas
	03	Capacidad de resiliencia del entorno ante situaciones anormales y complejas

	04	Se debe garantizar la disponibilidad del activo critico de información

Tabla 9 NIST Fase Proteger

ISO 27110:2013	
Norma - Categoría - Subcategoría	**Objetivo**
ISO/IEC 27002:2013, 12.3.1	Las copias de seguridad se realizan, mantienen y prueban.
ISO/IEC 27002:2013, 11.1.4, 11.2.1, 11.2.2, 11.2.3 ISO/IEC 27019:2017, 9.1.1, 9.1.2, 9.2.3, 9.1.7, 9.1.8, 9.1.9	El entorno operativo físico cumple con las políticas y regulaciones para los activos de la organización.
ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 16.1.6	La comunicación de la eficacia de las tecnologías de protección es compartido con las partes apropiadas
ISO/IEC 27002:2013, 7.2.2	Todos los usuarios están informados y formados.
ISO/IEC 27002:2013, 7.2.1, 7.2.2, 6.1.1, 8.2.1	Funciones y responsabilidades de todo el personal de la organización. Se debe incluir información de los proveedores externos

Tabla 10 ISO 27110:2021 Fase Proteger

3.2.2.1 Gestión de Acceso

Esta función es esencial para controlar quién puede acceder a los activos críticos de información y a qué recursos específicos pueden acceder, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

Control de Acceso a Activos: Implementación de mecanismos de autenticación y autorización con el fin de controlar el acceso a los activos críticos de información.

Al implementar este control de manera efectiva, se reduce significativamente el acceso no autorizado, la pérdida de datos y ataques cibernéticos.

El acceso debe autorizarse únicamente a personas cuya identidad este establecida, y sus actividades se deben limitar al mínimo requerido. Los cambios en los privilegios

de acceso de los activos críticos deben monitorearse continuamente y cualquier cambio en esos privilegios de acceso debe generar una alerta y notificar al equipo adecuado, con el fin de investigar, documentar y resolver cualquier problema.

Se debe garantizar que todos los usuarios estén identificados y autenticados al acceder a los activos críticos de información. Se debe solo permitir el acceso autorizado a usuarios para realizar las tareas asignadas de acuerdo con sus funciones en la organización. Se debe proporcionar información sobre el ciclo de vida del acceso otorgado implementado para garantizar una seguridad estricta sobre la creación, uso y terminación de credenciales de acceso, revisiones de propiedad de cuentas, visibilidad para uso autorizado y protección contra el uso interno malicioso.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Incluir mecanismos de autenticación complejos, como contraseñas fuertes, autenticación de múltiples factores y certificados digitales.
- Definir responsabilidades que determinen qué usuarios tienen acceso a qué activos.
- Definir política, estándares y procedimientos de identificación y autenticación de usuarios.
- Definir políticas de acceso basadas en el principio de menor privilegio.

Identificación de Accesos a los Activos: Revisiones periódicas de los accesos de usuarios hacia los activos críticos de información, asegurando que se alineen con las políticas de seguridad y las necesidades actuales de la organización. La revisión regular de accesos ayuda a identificar y corregir accesos no autorizados. Facilita una gestión más eficiente de las identidades y los accesos dentro de la organización, alineando los permisos con las necesidades operativas.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Definir, implementar y evaluar procesos, procedimientos y medidas técnicas y / o contractuales para mantener la seguridad adecuada de los

dispositivos finales de terceros con acceso a los activos críticos de información de la organización.

- Definir política, estándar y procedimientos de control de acceso a los activos críticos de información
- Definir política, estándar y procedimientos de seguridad de conectividad remota.
- Documentación de autorización sobre conexión de terceros
- Identificar, implementar y evaluar procesos, procedimientos y medidas técnicas para verificar que el acceso a los activos de información críticos es autorizado.
- Documentación de roles y responsabilidades para dependencias externas.
- Implementar controles físicos preventivos y de detección adecuados para protección de los activos e infraestructura contra personas malintencionadas o no autorizadas.

Capacitación en ciberseguridad: La organización debe tener un programa de capacitación en ciberseguridad diseñado para aumentar la conciencia situacional de los empleados sobre las amenazas cibernéticas y el conocimiento de los controles de ciberseguridad. La capacitación debe apoyar temas de conciencia situacional y competencias para la protección de datos, manejo de datos personales, obligaciones de cumplimiento, trabajo con terceros, detección de riesgos cibernéticos y cómo reportar cualquier actividad o incidente inusual. A medida que se implementa nueva tecnología, la organización debe ser responsable de capacitar a todo el personal sobre el nuevo sistema y cualquier tecnología y riesgo de ciberseguridad que lo acompañe. Se debe validar la eficacia de la formación en ciberseguridad y actualizarla periódicamente.

La organización debe establecer estándares y certificaciones mínimas para el personal y exigir educación especializada en materia de ciberseguridad. La capacitación debe ser actualizada y relevante. A medida que las amenazas cambian, se debe adoptar capacitación para abordar el cambiante panorama de amenazas.

La capacitación en ciberseguridad debe estar alineada con el nivel de riesgo de ciberseguridad que existe dentro de una unidad de negocios. Se debe desarrollar un programa de capacitación en ciberseguridad que incluya metas y objetivos de aprendizaje

que alineen la ciberseguridad con los roles y responsabilidades de los empleados. Usuarios privilegiados, como administradores de redes, sistemas o bases de datos, a los cuales se les otorgan privilegios de acceso elevados, deben tener capacitaciones adicionales que se centre en la gestión de la seguridad del activo y el uso de su privilegio. Las funciones, a quienes se les otorgan permisos y privilegios de acceso elevados, también deben recibir capacitación adicional en concientización sobre seguridad cibernética para sus roles y el uso sensato de su acceso privilegiado.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Informes, cronograma, materiales y registros de capacitación en ciberseguridad.
- Definir políticas, estándares y procedimientos de capacitación en ciberseguridad de terceros.
- Definir políticas y procedimiento al personal sobre como informar incidentes o actividad cibernéticos inusual
- Definir planes de formación y desarrollo
- Elaboración de informes sobre la comunicación de información de respuesta a incidentes, incluidos roles y responsabilidades, a las partes interesadas.

3.2.2.2 Protección de Plataformas

Engloba un conjunto de controles diseñados para asegurar que el hardware, software y servicios que conforman las plataformas tecnológicas de la organización estén gestionados de manera segura, protegiendo así la confidencialidad, integridad y disponibilidad de los datos y sistemas.

Protección de activos: Este elemento es fundamental para garantizar que los activos críticos de información de la organización estén protegidos contra accesos no autorizados, implica establecer un estado de referencia conocido y seguro para los activos, y asegurar que se mantenga ese estado a lo largo del tiempo. La organización debe desarrollar estándares básicos de configuración de seguridad para sus activos basados en el riesgo y de acuerdo con las pautas de configuración aplicables.

La organización también debe asegurar de configurar de forma segura los componentes de la red, sistemas operativos, aplicaciones, bases de datos, etc., para así

garantizar que solo se permitan acceso a los puertos, protocolos y servicios aprobados y deshabilitar todos los servicios, puertos y protocolos innecesarios, se debe aplicar el concepto de funcionalidad mínima, que establece que los sistemas de información están configurados para proporcionar sólo capacidades esenciales y prohibir o restringir el uso de funciones no esenciales, como puertos, protocolos y/o servicios que no son integrales para la operación.

También se deben establecer estándares, métodos y prácticas de gestión de cifrado de acuerdo con los estándares internacionales definidos, los algoritmos de cifrado deben ser reconocidos a nivel internacional. Los datos en reposo, los datos en uso y los datos en tránsito de los activos de información críticos deben emplear métodos de cifrado para proteger la confidencialidad e integridad de los datos.

Se deberían realizar copias de la información, del software y de las imágenes del activo, se deberían probar de manera regular de acuerdo con una política de respaldo acordada.

Los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal; en situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante cifrado. Se debería contar con respaldos adecuadas para garantizar que toda la información se puede recuperar después de un desastre o ante una falla.

Los activos críticos de información físicamente se deben de ubicar en un lugar determinado con temperatura y humedad adecuada, estar protegido contra cortes de luz y otras interrupciones provocadas por fallas en los servicios básicos.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Documentación sobre cómo se lleva el control antivirus y antimalware
- Definir políticas o procedimientos para el monitoreo de la integridad de los activos críticos de información.
- Definir métodos y prácticas sobre la gestión de cifrado.
- Definir e implementar procesos para remediar las vulnerabilidades de seguridad de los activos críticos de información, automatizando la corrección cuando sea posible.

- Establecer una política de respaldo de sobre los activos críticos de información
- Implementar suministro de energías de redundancia en caso de que el suministro de energía eléctrico principal falle, a fin de tener encendidos y operativos los activos de información críticos.

3.2.3 Fase Detectar

NIST		
Categoría: Monitoreo continuo - DE.CM		**Objetivos**
Subcategorías	01	Con el fin de detectar amenazas potenciales, se debe monitorear la red
	02	Con el fin de detectar amenazas potenciales, se debe monitorear el entorno físico
	03	Con el fin de detectar amenazas potenciales, se debe monitorear las actividades del personal
	06	Con el fin de detectar amenazas potenciales, se debe monitorear a los proveedores
	09	Con el fin de detectar amenazas potenciales, se debe monitorear hardware y software del activo critico de información
Categoría: Análisis de acontecimientos adversos - DE.AE		**Objetivos**
Subcategorías	02	Se analizan escenarios a fin de comprender el entorno del activo critico de información
	03	Se correlaciona la información procedente de diversas fuentes

	04	Análisis del impacto
	06	Información sobre los escenarios al personal de la organización
	07	Las amenazas cibernéticas de los activos críticos de información son analizadas
	08	Los incidentes se generan, cuando los acontecimientos cumplen con la definición de criterio de incidente

Tabla 11 NIST Fase Detectar

ISO 27110:2013	
Norma - Categoría - Subcategoría	**Objetivo**
ISO/IEC 27033	Se debe establecer una línea base con respecto a las operaciones de la red
ISO/IEC 27002:2013, 16.1.1, 16.1.4 ISO/IEC 27035	Los eventos detectados se analizan para comprender los objetivos y métodos de los ataques
ISO/IEC 27002:2013, 12.4.1, 14.2.7, 15.2.1	Monitoreo de la red, el entorno físico, el personal y el proveedor de servicios para detectar posibles eventos.
ISO/IEC 27002:2013, 12.4.1, 14.2.7, 15.2.1	Se realiza monitoreo de personal, conexiones, dispositivos y software no autorizados.
ISO/IEC 27002:2013, 6.1.1 ISO/IEC 27019:2017, 8.1.1	Las funciones y responsabilidades de detección están bien definidas para garantizar la rendición de cuentas
ISO/IEC 27002:2013, 16.1.6 ISO/IEC 27035	Los procesos de detección se mejoran continuamente

Tabla 12 ISO 27110:2021 Fase Detectar

3.2.3.1 Seguridad Proactiva

Los activos críticos de información deben monitorearse con el fin de encontrar anomalías y otros eventos adversos.

Monitoreo de eventos: Los sistemas de detección o prevención de intrusiones, software antivirus se pueden utilizar para ayudar a identificar actividades inusuales analizando el tráfico alertando para tomar medidas o decisiones. Los incidentes que pueden estar relacionados con amenazas internas pueden incluir intentos fallidos de inicio de sesión, transferencias de grandes cantidades de datos, codificación alterada en archivos confidenciales entre otros. Un ciberataque disruptivo hace que una actividad se interrumpa o no se pueda llevar a cabo de forma normal de manera indefinida (CyberZaintza, 2021). Ciberataques disruptivos como los ataques de denegación de servicio (DoS)/denegación de servicio distribuido (DDoS) se basa en una recopilación y un análisis coordinados de alertas y datos de rendimiento, que a menudo incluyen proveedores externos, proveedores de servicios de Internet, es por esto que debemos diseñar e implementar enfoques de mitigación de acuerdo a la exposición/riesgo de la organización.

Se debe incluir un sistema integral para el monitoreo del acceso no autorizado a los componentes y software de los activos críticos de información, con el fin de detectar y prevenir cambios en el hardware o software y pueden alertar al administrador cuando se ejecutan ciertos intentos de cambios.

La organización debe tener un sistema para monitorear activos y conexiones que no están autorizados o no cumplen con la política de seguridad. Herramientas de escaneo de vulnerabilidades pueden monitorear y detectar activos sin parches, denegar conexiones y administrar alertas.

La organización debe poseer sistema de detección para el entorno físico, por ejemplo, áreas restringidas, repositorios de datos confidenciales, áreas de bóvedas, cajeros automáticos, etc., proporcionado información sobre controles al acceso físico no autorizado a componentes y ubicaciones del sistema de alto riesgo donde reposan los activos críticos de información.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Desplegar mecanismos o herramientas para alertar o notificar al administrador sobre posibles ataques y activar el plan de respuesta a incidentes.
- Elaborar procedimientos y soluciones para mitigación sobre los ciberataques disruptivos.
- Establecer políticas y procedimiento para monitorear la presencia de usuarios, dispositivos, conexiones y software no autorizados.
- Desplegar herramientas relacionadas con la prevención, monitoreo para remediar el acceso no autorizado desde/hacia dispositivos, conexiones y transferencias de datos de los activos críticos de información.
- Se debe de monitorear todas las actividades sobre los activos críticos de información ejecutado por proveedores externos esto debe incluir la administración y mantenimientos remotos.

3.2.3.2 Monitoreo continuo de seguridad

Conjunto de controles diseñados para identificar, analizar y responder eventos de seguridad, tales como un incidente o una amenaza.

Análisis de eventos: Describe la evaluación y análisis de eventos de seguridad de los activos críticos de información, el cual nos permitirá medir su impacto, relevancia y posibles consecuencias para la organización.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Utilizar la gestión de eventos e información de seguridad u otras herramientas para monitorear continuamente los eventos de registro en busca de actividades maliciosas y sospechosas conocidas.
- Creación y distribución de informes sobre eventos de seguridad en los activos críticos de información, asegurando que la información relevante llegue a las partes interesadas de manera oportuna y efectiva.

Mejora continua: Se deberían establecer las responsabilidades y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información de los activos críticos de información. Se debería utilizar la información

obtenida de la evaluación de los incidentes de seguridad de la información de los activos críticos de información para identificar los incidentes recurrentes o de alto impacto

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Identificar y monitorear eventos relacionados con la seguridad dentro de las aplicaciones y los activos críticos de información.
- Supervisar los registros de auditoría de seguridad de los activos críticos de información para detectar actividad fuera de los patrones típicos o esperados. Establecer y seguir un proceso definido para revisar y tomar las acciones apropiadas y oportunas frente a las anomalías detectadas.
- Establecer y monitorear métricas de incidentes de seguridad de la información de los activos críticos de información
- Utilizar tecnología de correlación de eventos de activos críticos de información para recopilar información capturada por múltiples fuentes

3.2.4 Fase Responder

NIST		
Categoría: Gestión de Incidentes - RS.MA		**Objetivos**
Subcategorías	01	En conjunta coordinación se ejecuta el plan de respuesta a incidentes una vez que se da la alarma de un incidente
	02	Chequear y validar los informes de los incidentes
	03	Clasificación de incidentes
	04	Escalamiento del incidente según sea necesario
	05	Se inicia la recuperación ante los incidentes
Categoría: Análisis de Incidentes - RS.AN		**Objetivos**
Subcategorías	03	Analizar porque se dio el incidente y cuáles fueron las consecuencias para que ocurriera

	06	Listar las actividades para preservar la integridad y registros durante la investigación
	07	Preservar los registros de datos y metadatos del incidente, manteniendo su integridad y procedencia
	08	Se estima la magnitud del incidente
Categoría: Notificación y comunicación de la respuesta al incidente - RS.CO		**Objetivos**
Subcategorías	02	Notificar el incidente a las partes internas y externas de la organización
	03	Compartir la información del incidente con las partes internas y externas de la organización
Categoría: Mitigación de Incidentes - RS.MI		**Objetivos**
Subcategorías	01	Contención de los incidentes
	02	Erradicación de los incidente

Tabla 13 NIST Fase Responder

ISO 27110:2013	
Norma - Categoría - Subcategoría	**Objetivo**
ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.1, 16.1.1 ISO/IEC 27035 ISO/IEC 27019:2017, 6.1.6, 8.1.1	El personal conoce sus funciones y el orden de las operaciones cuando ocurre una incidencia
ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.3, 16.1.2 ISO/IEC 27035	Se deben informar los eventos con criterio establecido
ISO/IEC 27002:2013, 12.4.1, 12.4.3, 16.1.5 ISO/IEC 27039	Las notificaciones enviadas por el sistema de detección deben ser investigadas
ISO/IEC 27002:2013, 16.1.4	Clasificación de los incidentes, basado en el plan de respuesta

Tabla 14 ISO 27110:2021 Fase Responder

3.2.4.1 Gestión de Incidentes

Se centra en identificar, evaluar y gestionar los riesgos relacionados con los sistemas de información y activos de una organización.

Ejecución coordinada del plan de respuesta a incidentes: Ayuda a la organización a comprender su perfil de riesgo y tomar decisiones informadas sobre la seguridad y la gestión de activos, establece que una vez que se declara un incidente de seguridad, el plan de respuesta a incidentes debe ser ejecutado en coordinación con todas las partes interesadas, tanto internas como externas a la organización.

Se debe involucrar a proveedores de servicios, socios comerciales, agencias gubernamentales o cualquier otra entidad externa que pueda ser relevante para la gestión del incidente del activo crítico, se debe seguir los procedimientos y protocolos establecidos en el plan de respuesta a incidentes de manera eficiente y eficaz se debe aplicar criterios técnicos para estimar la gravedad del incidente, previamente se deben revisar los informes de incidentes para confirmar que están relacionados con ciberseguridad y requieren actividades de respuesta a incidentes sobre los activos críticos de información. La clasificación y la priorización del incidente puede ayudar a identificar el impacto y el alcance de un incidente.

Clasificación y evaluación del incidente: La clasificación de los incidentes ayuda a los equipos de respuesta a tomar decisiones estratégicas sobre cómo abordar cada situación. El plan de respuesta a incidentes debe incluir pasos apropiados para evaluar la causa raíz del incidente, y si incluye orientación adecuada para realizar análisis y determinar las acciones y los pasos operativos que minimizarían el impacto del incidente en los activos críticos de información, se debe priorizar los incidentes en función de su alcance, impacto probable y naturaleza crítica. Se debe seleccionar estrategias de respuesta a incidentes equilibrando la necesidad de recuperarse rápidamente de un incidente.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Asegurar de que todas las actividades de respuesta a incidentes se registren correctamente para el posterior análisis

- Establecer, implementar y evaluar procesos, procedimientos y medidas técnicas para clasificar los eventos relacionados con la seguridad del activo critico de información.
- Procedimientos de priorización y escalamiento de eventos/incidentes.
- Para respaldar el proceso que se ha ejecutado, elaborar informes de incidentes de seguridad

3.2.4.2 Análisis de Riesgos

Se centra en la importancia de realizar análisis detallados para entender y evaluar los riesgos que enfrenta la organización, especialmente en relación con sus sistemas de información y activos

Análisis Exhaustivo: Al realizar un análisis exhaustivo, la organización puede proteger mejor sus activos críticos de información, cumplir con las regulaciones y mejorar su postura de seguridad en general, ayudara a la determinación de la secuencia de eventos que ocurrieron durante el incidente y qué activos y recursos estuvieron involucrados en cada evento.

Se deben realizar investigaciones forenses de ciberseguridad a los equipos comprometidos o afectados. Se debe proporcionar información sobre la función forense y los procesos relacionados con las investigaciones e ingeniería de controles de protección y detección.

En caso de que la organización no cuente con un departamento forense pueden subcontratar este análisis forense a terceros siempre y cuando sean capacitados y calificados. Se debe preservar y salvaguardar la integridad de todos los datos y metadatos del incidente según los procedimientos de preservación de evidencia, los datos forenses relacionados se capturan, aseguran y conservan para respaldar la integridad, la procedencia y el valor probatorio.

Se debe de revisar otros activos críticos potenciales del incidente para buscar indicadores de compromiso y evidencia de persistencia.

Estos incidentes podrían afectar la reputación de la organización, el área financiera, las relaciones con los clientes. La organización debe determinar si el incidente constituye un hecho material para la empresa y sus partes interesadas, estas

determinaciones deben tomarse con los niveles más altos de la organización y con el asesoramiento legal y el representante de Seguridad de la Información.

Informar sobre el incidente: El plan de respuesta a incidentes de la organización debe especificar qué incidentes se deben informar, cuándo se deben informar y a quién según el nivel de gravedad del incidente. Las partes notificadas de incidentes incluyen a la Gerencia, Jefatura de Seguridad de la información, asesor legal, entre otros. También se debe incluir presentación de informes sobre el incidente.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Implementar herramientas y técnicas especializadas, para examinar la evidencia, identificar patrones, anomalías y posibles indicadores de compromiso.
- Generar informes detallados que describan los hallazgos, los métodos utilizados y las conclusiones.
- Establecer políticas, estándares y procedimientos de seguridad forense sobre activos.
- Desarrollar guías forenses sobre el incidente suscitado.
- Identificación de las causas raíz y el impacto cuando los ataques cibernéticos sobre el activo tienen resultados con pérdidas materiales.

Contención y erradicación de incidentes: Establece que la organización debe tener las capacidades y procedimientos necesarios para limitar la propagación de un incidente de seguridad y minimizar su impacto. Describir los procesos establecidos para implementar planes de mitigación de vulnerabilidades, así como validar su cumplimiento y efectividad. Proporcionar información sobre cómo se revisan y acuerdan los planes de mitigación con las partes interesadas de la organización.

Se debe contar con estrategias y procedimientos de mitigación y erradicación para una contención oportuna de las vulnerabilidades del activo, se debe hacer enfoque en las acciones continuas que se deben tomar para mitigar los efectos de un incidente de seguridad sobre un activo, incluso después de que la amenaza inicial haya sido contenida.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Establecer procesos y planes de mitigación de vulnerabilidades, involucrando a proveedores y experiencia externos según sea necesario.
- Implementar medidas para detener la actividad maliciosa y prevenir daños adicionales sobre otros activos críticos.
- Restaurar activos afectados a un estado operativo seguro

3.2.5 Fase Recuperar

NIST		
Categoría: Ejecución del Plan de Recuperación de Incidentes - RC.RP		**Objetivos**
Subcategorías	01	La fase de recuperación del plan de respuesta a incidentes debe ser ejecutado
	02	Se ejecutan las acciones de recuperación
	03	Las copias de seguridad se les debe verificar la integridad antes de ser usadas
	04	Se establecen normas operativas, luego de haber ocurrido el incidente, teniendo en cuenta funciones criticas
	05	Se verifican los activos restaurados en conjunto con sus servicios, se confirma la operatividad del mismo
	06	Se culminan actividades ejecutadas sobre el incidente, se debe documentar todo lo relacionado referente a este incidente
Categoría: Comunicación de la recuperación del incidente - RC.RO		**Objetivos**
Subcategorías	03	Se comunican a las partes internas y externas sobre los procesos de recuperación y su progreso

	04	Se hace de manera publica la comunicación sobre el incidente y su recuperación.

Tabla 15 NIST Fase Recuperar

ISO 27110:2013	
Norma - Categoría - Subcategoría	**Objetivo**
ISO/IEC 27002:2013, 16.1.5 ISO/IEC 27031	Ejecución del plan de recuperación
ISO/IEC 27001:2013, 7.4	Las actividades de recuperación se comunican a las partes interesadas internas y externas

Tabla 16 ISO 27110:2021 Fase Recuperar

3.2.5.1 Recuperación

Se enfoca en las actividades que la organización debe realizar para tener una recuperación exitosa después de un incidente de ciberseguridad.

Plan de Recuperación: Plan claro y detallado que describe los pasos a seguir para recuperar el activo critico de información después de un incidente o desastre.

Se debe describir cómo se utiliza el plan de respuesta de la organización como guía informada para desarrollar y gestionar planes de tareas y actividades de respuesta específicos, seleccionando acciones de recuperación en función de los criterios definidos en el plan de respuesta a incidentes y los recursos disponibles.

Un plan de respaldo y recuperación describe cómo se respaldan y restauran los activos críticos en caso de pérdida o corrupción de sus datos. La organización debe tener procesos para validar las capacidades de recuperación, garantizando que las herramientas, las tecnologías y los procesos de recuperación sean efectivos en la reanudación de las operaciones críticas. La restauración de los activos críticos de información debe realizarse dentro de un tiempo de recuperación definido.

Se debe preparar un informe posterior a la acción que documente el incidente en sí, las acciones de respuesta y recuperación tomadas, posterior se debe declarar el fin de la recuperación del incidente una vez que se cumplan con todos los criterios.

Comunicar el estado recuperación sobre el incidente: Informar al personal interno, sobre el estado de la recuperación y cuales han sido las medidas tomadas. Se debe compartir de forma segura esta información, incluir el progreso de la restauración. Actualizar periódicamente a la alta gerencia sobre el estado de recuperación y el progreso de la restauración. Seguir las reglas y protocolos definidos en los contratos para el intercambio de información de incidentes entre la organización y sus proveedores.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos de gestión de la continuidad del negocio y resiliencia operativa. Revise y actualice las políticas y procedimientos al menos una vez al año.
- Verificar los activos críticos de información en conjunto con su propietario luego de su restauración para detectar indicadores de compromiso, corrupción de archivos y otros problemas de integridad antes de su uso.
- Documentar agendas y actas de las reuniones de comités relacionados
- Establecer plan de comunicación externa hacia los proveedores.

3.2.6 Fase Gobernanza

NIST		
Categoría: Contexto organizativo - GV.OC		**Objetivos**
Subcategorías	03	Se gestiona y revisan los requisitos legales, contractuales, normativos de la organización en lo que compete a materia de ciberseguridad.
	04	Se determinan los servicios críticos de la organización y se identifican las áreas que dependen de estos servicios

	05	Se comunican los servicios críticos identificados y las áreas que dependen de estos servicios para continuar su operatividad
Categoría: Funciones – Responsabilidades - Autoridades - GV.RR		**Objetivos**
Subcategorías	01	Fomentar una cultura sobre los riesgos de la ciberseguridad
	02	Establecer y comunicar funciones y responsabilidades relacionadas con la gestión de riesgo cibernético
	03	Asignar recursos adecuados de acuerdo con la gestión de riesgos cibernéticos
	04	Recursos Humanos debe incluir buenas practicas referente a ciberseguridad

Tabla 17 NIST Fase Gobernanza

3.2.6.1 Contexto Organizativo

Se refiere a la comprensión profunda que la organización tiene de sí misma, establece la base sobre la cual se construyen todas las demás medidas de seguridad.

Alineación de la ciberseguridad con los objetivos de la organización: Describir las estrategias, arquitecturas y programas de ciberseguridad que establecen prioridades para la misión, los objetivos y las actividades de la organización. Documentar la información sobre la publicación de regulaciones y obligaciones contractuales de ciberseguridad, nuevas o mejoradas.

Para el diseño del marco de ciberseguridad de este trabajo se propone:

- Definir la misión de la organización
- Definir matriz de asignación de responsabilidades y roles

- Identificar y documentar las partes interesadas internas y externas relevantes y sus expectativas relacionadas con la ciberseguridad de los activos críticos de información.
- Definir y documentar a partir de un análisis de impacto empresarial los activos críticos de información que son vitales para lograr los objetivos de la misión y el impacto potencial de una pérdida de dichas operaciones.
- Definir política y estándares de ciberseguridad ambientado a los activos críticos de información.
- Definir y documentar las dependencias externas que son puntos potenciales de falla para los activos críticos de información de la organización, y compartir esa información con el personal apropiado
- Los responsables de la supervisión de tecnología y ciberseguridad de la organización deben garantizar el cumplimiento de las normas y políticas de la organización.

A continuación, se da a conocer el diseño de ciberseguridad basado en las normas NIS/ISO 27110:2021 en el ambiente de pruebas de este trabajo:

La organización Fortidex es una empresa ecuatoriana su función principal es industrialización y comercialización de harina de pescado, camarón y aceite, con un estricto cumplimiento de las regulaciones nacionales e internacionales, satisfaciendo los más exigentes requisitos de los clientes, con personal capacitado y comprometidos con el medio ambiente y apoyo a la comunidad, así como la constante mejora de los procesos. (FORTIDEX, s.f.).

El departamento TI de la organización será el responsable de tratar y transmitir a la organización a las partes internas y externas interesadas de la organización cualquier eventualidad o incidente relacionado con la seguridad de la información de los activos críticos de información. Las partes interesadas internas constan la Alta Dirección o Gerencia, Usuarios internos que constan empleados de las distintas áreas y personal operativo de planta si el caso lo amerita. Las partes externas constan los proveedores, clientes.

Todos los proveedores que presten servicios a los activos críticos de información se adaptaran a los niveles de seguridad previamente planteados con el fin de mantener la

confidencialidad, integridad y disponibilidad de los datos del activo. Se les debe exigir que implementen medidas de protección de datos adecuadas, En la parte contractual se deben incluir cláusulas de confidencialidad y tratamiento de información a la cual acceden por el servicio que se presta a la organización. El proveedor también presentar su plan de continuidad que debe incluir contingencia, recuperación y tiempo de recuperación. Para el caso de los proveedores que presten servicios de conexión a internet y datos deben contar con un proceso continuo de monitoreo del servicio.

En fases previas presentadas en este trabajo hemos definido:

- Política de Identificación y Clasificación de Activo
- Política de Identificación, Control y Clasificación de Software
- Política de Desactivación y Eliminación de Activos Críticos Obsoletos
- Política Autenticación y Control de Acceso
- Política Priorización y Clasificación de Activos
- Política Seguridad de Red y Activos Críticos de Información
- Política Activos Críticos de Información Gestionados por Terceros
- Política Pruebas de Penetración e identificación de vulnerabilidades en Activos Críticos de Información
- Política Evaluaciones de Impacto y Riesgo Empresarial
- Política Mejora Continua
- Política Capacitación Continua en Ciberseguridad
- Política Integridad sobre el activo critico de información
- Política Respuesta a Incidentes
- Política Análisis de Eventos de Seguridad
- Política Investigación Forense
- Política Recuperación ante Desastres Cibernéticos

Todas las políticas previamente mencionadas ayudaran a garantizar la protección de los activos críticos de información y reducir los riesgos asociados con las amenazas cibernéticas. Como parte de la mejora continua estas políticas deben ser revisadas y actualizadas regularmente para poder adaptarse al cambio constante de nuevas amenazas y poder satisfacer a las normativas que se encuentran en constante evolución.

ID	Gestión de Activos
0001	Política de Identificación y Clasificación de Activo
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Identificar y clasificar adecuadamente el activo critico de información de la organización según su importancia y riesgo.
Normas	• Crear un inventario detallado, clasificando al activo critico de información en función de su impacto potencial en la organización • Activo estará clasificado según su impacto en la organización: **Alto:** Activos en los cuales existir casos de pérdida ocasionaría un impacto negativo en lo referente a lo legal, económico, la operación o continuidad de la organización. Ejemplo: Activos Información Confidencial o Misión Crítica, servidores, equipos de nómina, equipos donde se registran la producción. **Medio:** Activos en los cuales existir casos de pérdida, ocasionaría un impacto negativo moderado referente a lo económico, legal, existiría demora en las actividades, procesos y sus operaciones. Ejemplo: Equipos ubicados en el área de bodega, si algo llegara a pasar las transacciones de bodega como ejemplo despacho de materiales demoraría el proceso de reparación de algún otro departamento. **Bajo:** Activos en los cuales en caso de sufrir pérdida representaría impacto poco significativo para la organización.

	Ejemplo: Equipo de Mantenimiento, no afectaría o modificaría algún proceso interno de la organización. • El mapeo e identificación de nuevos activos críticos de información se lo realizara de manera automatizada con la ayuda de un software, el cual permita descubrir, mapear y gestionar activos de información. Adicional se debe incluir la fecha de compra del activo, el método y la criticidad del activo. • El departamento que es custodio del activo velará por la buena gestión, protección, debe garantizar la disponibilidad, confidencialidad e integridad de estos activos. • Activos gestionados por un tercero externo de la organización, debe existir administración compartida entre personal de TI y el proveedor. • La función del responsable del activo es velar por la gestión diaria del activo crítico de información.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 18 Política de Identificación y Clasificación de Activo

A continuación, se comparte Inventario de hardware de información crítica de la organización, en las cuales se incluye ubicación, fecha de toma del inventario, método de recolección de los datos y la criticidad de este:

Inventario Hardware Equipos de Cómputo

N°	Ítem	Marca	Modelo	Serie	Procesador	Almacenamiento	Memoria Ram	Sistema Operativo	Ubicación	Responsable Activo	Localidad	Responsable Inventario	Custodio del Activo	Fecha Inventario	Método	Criticidad
1	PC Escritorio	Dell	3681 SSF	CIM3OXZN	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Alta
2	PC Escritorio	Dell	3681 SSF	ZJU6XIGX	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
3	PC Escritorio	Dell	3681 SSF	5RQ7QLSC	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
4	PC Escritorio	Dell	3681 SSF	UHOBJ3DQ	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
5	PC Escritorio	Dell	3681 SSF	PSP2ZBJB	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
6	PC Escritorio	Dell	3681 SSF	5DXY88GK	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio

7	PC Escritorio	HP	Prodesk 400 G4	UHGGJYKF	i5-10400	256GB SSD	8GB DDR4	Windows 11 Pro	Administración	Mantenimiento	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
8	PC Escritorio	Lenovo	M70q Gen 4	R7TDDGJE	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Administración	Bodega	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
9	PC Escritorio	HP	Prodesk 400 G2.5	MTEPBEYR	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Bodega	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
10	PC Escritorio	HP	Prodesk 400 G2.5	8CSHX2OX	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Seg. Industrial	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Bajo
11	PC Escritorio	HP	Prodesk 400 G2.5	Z78EP3B5	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	RRHH	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
12	PC Escritorio	HP	Prodesk 400 G2.5	QYRZPTUM	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Produccion	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Alta
13	PC Escritorio	HP	Prodesk 400 G2.5	RNS6GCC5	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Produccion	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Alta

14	Portátil	Lenovo	IdeaPad Slim	AHJSUZRV	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Administración	Contabilidad	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
15	Portátil	Lenovo	IdeaPad Slim	PV3CKLED	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Administración	Produccion	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
16	Portátil	Lenovo	IdeaPad Slim	JTRBJDZR	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Gerencia	Gerencia	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Medio
17	PC Escritorio	Dell	3681 SSF	O4DMTO8W	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Alta
18	PC Escritorio	Dell	3681 SSF	HUATDBGB	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio
19	PC Escritorio	HP	Prodesk 400 G4	KHWWUTAU	i5-10400	256GB SSD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
20	PC Escritorio	HP	Prodesk 400 G4	XWGHN6VK	i5-10400	256GB SSD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
21	PC Escritorio	HP	Prodesk 400 G4	FRPJWZLC	i5-10400	256GB SSD	8GB DDR3	Windows 10 Pro	Laboratorio	Calidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
22	PC Escritorio	Dell	3681 SSF	SCB9HAXP	i5-10400	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Contabilidad	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo

23	PC Escritorio	Dell	3681 SSF	K8X8KY8Y	i5-10400	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Produccion	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Alta
24	PC Escritorio	Dell	3681 SSF	JCMLMD8M	i5-10400	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Produccion	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio
25	PC Escritorio	Dell	3681 SSF	UI4SD3WB	i5-10400	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Bodega	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
26	PC Escritorio	HP	Prodesk 400 G2.5	KYEUZZBY	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Bodega	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
27	PC Escritorio	HP	Prodesk 400 G2.5	BIPNBH3A	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Mantenimiento	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio
28	PC Escritorio	HP	Prodesk 400 G2.5	4ZWDEBCN	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Mantenimiento	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio
29	Portátil	Lenovo	IdeaPad Slim	DK4IYCNV	i7 11370H	1 TB SSD	16 GB DDR4	Windows 11 Pro	Administración	Seg. Industrial	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Bajo
30	Portátil	Lenovo	IdeaPad Slim	DK4IYCNV	i7 11370H	1 TB SSD	16 GB DDR4	Windows 11 Pro	Administración	RRHH	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio
31	Portátil	Lenovo	IdeaPad Slim	QWMXD43R	i7 11370H	1 TB SSD	16 GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	22/8/2024	Manual	Medio

32	PC Escritorio	Lenovo	M70q Gen 4	GKUP7GUH	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Laboratorio	Calidad	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Alta
33	PC Escritorio	Lenovo	M70q Gen 4	HTLT2GZH	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Laboratorio	Calidad	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
34	PC Escritorio	Dell	3681 SSF	CQZZFMBM	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Administración	Contabilidad	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Bajo
35	PC Escritorio	Dell	3681 SSF	DNILLJBQ	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Administración	Produccion	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Alta
36	PC Escritorio	Dell	3681 SSF	2NQ7SZMB	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Administración	Produccion	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
37	PC Escritorio	Dell	3681 SSF	G4BAKBE4	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Administración	Bodega	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
38	PC Escritorio	Dell	3681 SSF	TNSBICYT	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Administración	Bodega	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Bajo
39	PC Escritorio	HP	Prodesk 400 G2.5	BNS7HGLK	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Mantenimiento	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Bajo
40	PC Escritorio	HP	Prodesk 400 G2.5	9K84MVNQ	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Mantenimiento	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Bajo

41	PC Escritorio	HP	Prodesk 400 G2.5	N4ZKVRPU	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	Seg. Industrial	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Alta
42	PC Escritorio	HP	Prodesk 400 G2.5	8KP8N3NP	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Administración	RRHH	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
43	Portátil	Lenovo	IdeaPad Slim	8MRVUPHV	i7 11370H	1 TB SSD	16 GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
44	Portátil	Lenovo	IdeaPad Slim	MEGTTOBO	i7 11370H	1 TB SSD	16 GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	25/8/2024	Manual	Medio
45	PC Escritorio	HP	Prodesk 400 G2.5	A2TWBNC3	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Oficina Contabilidad	Contabilidad	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Alta
46	PC Escritorio	HP	Prodesk 400 G2.5	RCCCCTX2	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Oficina Contabilidad	Contabilidad	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
47	Portátil	Lenovo	M70q Gen 4	UCSY8EJG	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Oficina Sistemas	Sistemas	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
48	Portátil	Lenovo	M70q Gen 4	QU7AP2RD	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Oficina Sistemas	Sistemas	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio

49	PC Escritorio	HP	Prodesk 400 G2.5	LSCBWZFE	i5-4590S	1TB HHD	8GB DDR3	Windows 10 Home	Oficina RRHH	RRHH	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Alta
50	PC Escritorio	Dell	3681 SSF	ZR42LX73	i5-10400	1TB HHD	8GB DDR3	Windows 10 Pro	Oficina Bodega	Bodega	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
51	Portátil	Lenovo	IdeaPad Slim	FPFBKP7L	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Oficina Logística	Logística	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
52	Portátil	Lenovo	IdeaPad Slim	SXYFXNUI	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Oficina Compras	Compras	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
53	Portátil	Lenovo	IdeaPad Slim	4YGCSFNS	i7 11370H	1 TB SSD	16 GB DDR4	Windows 10 Pro	Gerencia Financiera	Gerencia Financiera	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Alta
54	Portátil	Lenovo	M70q Gen 4	YRSJG6AP	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
55	Portátil	Lenovo	M70q Gen 4	RZZPKFXR	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Medio
56	Portátil	Lenovo	M70q Gen 4	RYRBG2OY	I5-13400T	256GB SSD	16GB DDR4	Windows 11 Pro	Gerencia	Gerencia	Matriz	Departamento de Sistemas	Departamento de Sistemas	30/8/2024	Manual	Alta

Tabla 19 Inventario Hardware Equipos de Cómputo

Inventario Hardware Equipo Telecomunicaciones

N°	Ítem	Marca	Modelo	Serie	Ubicación	Responsable	Localidad	Responsable Inventario	Custodio del Activo	Fecha Inventario	Método	Criticidad
1	Switch Principal	Cisco	Catalyst 2960	CK3L7LP001554	Rack Principal Matriz	Departamento de Sistemas	Matriz	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
2	Router	Cisco	ISR900	PSZ23101A9R345	Rack Principal Administración	Departamento de Sistemas / Proveedor Internet	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
3	Router	Cisco	ISR900	PSZ23101A9R897	Rack Principal Planta Posorja	Departamento de Sistemas / Proveedor Internet	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
4	Router	Cisco	ISR900	PSZ23101A9R145	Rack Principal Planta Taura	Departamento de Sistemas / Proveedor Internet	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
5	Router	Cisco	ISR900	PSZ23101A9R344	Rack Principal Matriz	Departamento de Sistemas / Proveedor Internet	Matriz	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
6	Switch Secundario	HP	OfficeConnect 1920S	RZG22GC000771	Rack Principal Matriz	Departamento de Sistemas	Matriz	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio
7	Access Point	Unifi	Unifi AP		Rack Principal Matriz	Departamento de Sistemas	Matriz	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Bajo

8	Access Point	Unifi	Unifi AP		Rack Administración	Departamento de Sistemas	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Bajo
9	Access Point	Unifi	Unifi AP		Rack Gerencia	Departamento de Sistemas	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Bajo
10	Access Point	Unifi	Unifi AP		Rack Administración	Departamento de Sistemas	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Bajo
11	Switch Principal	HP	OfficeConnect 1920S	CN15TUAP4Q5	Rack Principal Administración	Departamento de Sistemas	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
12	Switch Principal	HP	OfficeConnect 1920S	CN22WP8010	Rack Administración	Departamento de Sistemas	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
13	Switch Principal	HP	OfficeConnect 1920S	CN27KPR0131	Rack Gerencia	Departamento de Sistemas	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Alta
14	Switch Secundario	HP	OfficeConnect 1920S	CN55AAJ4Z5	Rack Oficina Calidad	Departamento de Sistemas	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio
15	Switch Secundario	HP	OfficeConnect 1920S	CN35K3K0AA	Rack Oficina RRHH	Departamento de Sistemas	Planta Data Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio

16	Switch Secundario	HP	OfficeConnect 1920S	TW1BK3Q160	Rack Oficina Produccion	Departamento de Sistemas	Planta Posorja	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio
17	Switch Secundario	HP	OfficeConnect 1920S	TW71K3Q12A	Rack Administración	Departamento de Sistemas	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio
18	Switch Secundario	HP	OfficeConnect 1920S	CN12KPD010	Rack Oficina Calidad	Departamento de Sistemas	Planta Taura	Departamento de Sistemas	Departamento de Sistemas	2/9/2024	Manual	Medio

Tabla 20 Inventario Hardware Equipo Telecomunicaciones

Inventario Servidores

N°	Ítem	Marca	Modelo	Serie	Procesador	Almacenamiento	Ram	Sistema Operativo	Ubicación	Responsable	Localidad	Responsable Inventario	Custodio del Activo	Fecha Inventario	Método	Criticidad
1	Servidor	HP	Prodesk 400 G2.5 Sff	S6TKNC7U	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	2 TB	32 GB	Windows Server 2019	Rack Principal Matriz	Departamento de Sistemas Proveedor Administrador Servidor	Matriz	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Alta
1	Servidor	HP	Prodesk 400 G2.5 Sff	S6TKNTBX	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	2 TB	32 GB	Windows Server 2019	Rack Principal Matriz	Departamento de Sistemas Proveedor Administrador Servidor	Matriz	Departamento de Sistemas	Departamento de Sistemas	31/8/2024	Manual	Alta

Tabla 21 Inventario Servidores

ID	Gestión de Activos
0002	Política de Identificación, Control y Clasificación de Software
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Inventariar el software, servicios y sistemas gestionados por la organización
Normas	• Gestionar, controlar y auditar las aplicaciones y software de la organización, garantizando el cumplimiento legal, la seguridad, la optimización de los recursos y la eficiencia operativa. • Administrar de manera eficiente las licencias, se debe asegurar de que no exista software innecesario o sin uso dentro de la organización. • Determinar que el software utilizado en la organización debe estar debidamente licenciados cumpliendo con las leyes de propiedad intelectual. • Se prohíbe la instalación de software no licenciado u obsoleto, instalar este tipo de software podría incurrir en explotar vulnerabilidades sobre los activos críticos de información de la organización. • Debe existir un proceso de compra formal para la adquisición de nuevo software, para proceder con esta compra se debe incluir la necesidad para adquirirlo, la justificación de adquirirlo y la aprobación del departamento de TI y los altos mandos de la organización. • Llevar registros detallados de todas las compras de software, incluyendo facturas, contratos de licencias y

	términos de uso. • Solo los administradores de TI o personal autorizado podrán instalar software en los dispositivos de la organización. • Realizar auditorías de software, asegurando que el software instalado coincide con el inventariado registrado, se debe asegurar que el licenciamiento sea válido. • El equipo de TI debe garantizar que el software instalado en los equipos de la organización se encuentre al día con las actualizaciones y parches de seguridad, a fin de identificar vulnerabilidades conocidas del software instalado. • Identificar y eliminar software obsoleto que se encuentre instalado en los activos críticos de información. • El equipo de TI de la organización será el responsable de mantener actualizado el inventario de software, además de garantizar el cumplimiento de todas las políticas y procedimientos previamente planteadas.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 22 Política de Identificación, Control y Clasificación de Software

A continuación, se detalla el inventario de software que se ejecutan sobre los activos críticos de información.

N	Nombre	Versión	Categoría	Responsable	Localidad	Responsable Inventario	Fecha Inventario	Método	Criticidad
1	Windos Server 2019	Standard	Sistema Operativo	Departamento de Sistemas / Proveedor Administrador Servidor	Matriz	Departamento de Sistemas	31/8/2024	Manual	Alta
2	Windows 10 Pro	Professional	Sistema Operativo	Departamento de Sistemas	Matriz/Planta Taura Planta Data/Planta Posorja	Departamento de Sistemas	31/8/2024	Manual	Alta
3	Windows 11 Pro	Professional	Sistema Operativo	Departamento de Sistemas	Matriz/Planta Taura Planta Data/Planta Posorja	Departamento de Sistemas	31/8/2024	Manual	Alta
4	Windows 10 Home	Home	Sistema Operativo	Departamento de Sistemas	Matriz/Planta Taura Planta Data/Planta Posorja	Departamento de Sistemas	31/8/2024	Manual	Alta
5	Office 2019	Professional Plus	Software Utilitario	Departamento de Sistemas	Matriz/Planta Taura Planta Data/Planta Posorja	Departamento de Sistemas	31/8/2024	Manual	Baja

6	ERP	2.556	ERP	Departamento de Sistemas / Proveedor Desarrollo ERP	Matriz	Departamento de Sistemas	31/8/2024	Manual	Alta
7	Zoom	5	Videoconferencia	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
8	DWG TrueView	2,3	Diseño	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
9	Mozilla Firefox	119	Navegador	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
10	JAVA	8	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
11	Google Chrome	132	Navegador	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
12	Firma digital EC	1	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
13	Adobe Acrobat Reader	17	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja

14	Whatsapp	9	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
15	ESET	Endpoint Security	Antivirus	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Alta
16	Epson Scan	2	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
17	Anydesk	8	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja
18	Winrar	7	Utilitario	Departamento de Sistemas	Matriz	Departamento de Sistemas	31/8/2024	Manual	Baja

Tabla 23 Inventario Software

ID	Gestión de Activos
0003	Política de Desactivación y Eliminación de Activos Críticos Obsoletos
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Gestionar hardware, software, servicios y datos durante todo su ciclo de vida
Normas	• Asegurar que los activos críticos de información obsoletos sean desactivados y eliminados de manera segura al final de su ciclo de vida, • Deben ser retirados de manera controlada, asegurando que la información crítica que contienen sea completamente eliminada. • Los dispositivos y equipos que contengan información crítica deben ser destruidos física y digitalmente, asegurando que no haya riesgo de filtración de información. • La eliminación de datos sensibles debe seguir un proceso seguro, utilizando herramientas y métodos de borrado que aseguren que la información no pueda ser recuperada. • El acta de eliminación del activo critico de información debe ir adjunta con las firmas de los responsables, departamento de TI, si fuera el caso de que el activo se envía a destrucción con una empresa externa a esta se debe agregar sello, firma y certificado de la empresa responsable de la destrucción del activo critico de información.

	• Se debe llevar un registro de la eliminación de los activos para fines de auditoría, tanto el responsable del activo como el propietario del activo serán los responsables y darán seguimiento referente al ciclo de vida del activo critico de información
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 24 Política de Desactivación y Eliminación de Activos Críticos Obsoletos

A continuación, se detalla formato que se debe de llenar y compartir a los involucrados cuando se tenga que dar de baja al activo critico de información:

Código	Descripción	Serie	Cantidad	Estado	Fecha de Compra	Fecha de baja de Activo	Responsable
1	CPU Laboratorio	XXXXXXX	1	Obsoleto	15/5/2012	15/5/2024	Dep. Calidad

Tabla 25 Formato Baja de Activo

ID	Gestión de Activos
0004	Política Autenticación y Control de Acceso
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Garantizar que solo los usuarios autorizados puedan acceder a los activos críticos de información de la organización de manera segura
Normas	• Implementar autenticación multifactor para el acceso a los dispositivos críticos de información, se recomienda que este tipo de autenticación sea basado en contraseñas, PIN o biometría como huellas dactilares o reconocimiento facial. • Se debe exigir que las contraseñas sean complejas y únicas utilizando combinaciones de caracteres alfanuméricos. • Se establecerá roles y permisos de acceso basados en funciones laborales, así garantizaremos que los usuarios solo puedan acceder a los dispositivos o recursos que sean necesarios para su trabajo diario. • Los activos críticos de información se les debe cifrar el disco por completo, para proteger los datos incluso si el dispositivo es robado o comprometido físicamente. • Establecer cifrado de punto a punto, asegurando que solo los destinarios autorizados puedan leer esta data cifrada, este tipo de cifrado es fundamental cuando los activos se comunican entre diferentes sistemas y es necesario que los datos permanezcan protegidos. • La longitud de las contraseñas debe ser de al menos 12 caracteres.

	• Registrar y monitorear accesos a los activos críticos, asegurando que se revisen regularmente los registros de acceso para detectar actividades sospechosas. • Las cuentas de usuario deben serán revisadas periódicamente garantizando que no haya usuarios con privilegios innecesarios o cuentas inactivas. • Una vez creada la cuenta para un nuevo empleado de la organización, este debe ser notificado con sus credenciales y debe recibir capacitación sobre las políticas de seguridad internas y normas relacionadas con el acceso a los activos críticos de información. • Al momento de desactivar una cuenta de algún empleado cesante de la organización, de inmediato se debe validar si esa cuenta tenía acceso a recursos críticos o confidenciales, se debe garantizar que esos accesos sean revocados de manera inmediato. • Los registros de intentos de acceso a los activos críticos de información deben ser registrados, se deben incluir detalles relevantes como la hora, la IP de origen de conexión, el recurso al que se intentó acceder. • Todos los activos críticos de información de la organización deben tener un software antivirus instalado, debe actualizarse de manera periódica, debe contar con una alta capacidad de detección y eliminación de amenazas. • El antivirus debe ejecutar escaneos regulares para identificar cualquier anomalía. • El personal de TI será el encargado de monitorear el software antivirus en busca de anomalías como posibles infecciones en los equipos críticos de información.

	• Se deben presentar informes mensuales sobre el comportamiento del antivirus ejecutado sobre los activos críticos de información. • El cifrado de datos debe ser implementado con un algoritmo de cifrado robusto, para el desarrollo de este trabajo se utilizará AES-256.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 26 Política Autenticación y Control de Acceso

ID	Gestión de Activos
0004	Política Priorización y Clasificación de Activos
Dirigido a	Departamento de TI
Objetivo	Priorizar activos, deben ser clasificados según su criticidad, recursos e impacto en la organización
Normas	• Se clasificará el activo según la información que maneje, este según el acceso o nivel de sensibilidad la hemos catalogada de la siguiente manera: **Confidencial Nivel 1**, Accesible solo para personas autorizadas, tiene un alto nivel de sensibilidad. **Restringida Nivel 2**, Accesible solo para un grupo selecto de personas autorizadas dentro de la organización. **Secreta Nivel 3**, Acceso muy restringido, solo la alta Gerencia de la organización tiene acceso a esta información.

Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 27 Política Priorización y Clasificación de Activos

ID	Gestión de Activos
0005	Política Seguridad de Red y Activos Críticos de Información
Dirigido a	Departamento de TI Proveedores Externos
Objetivo	Detallar la comunicación de red autorizada en la organización y los flujos de datos de red internos y externos
Normas	• Se deben establecer procedimientos para la protección de la infraestructura de red de la organización frente a amenazas, garantizando la integridad, confidencialidad y disponibilidad de los activos críticos de información. • Definir quién puede acceder a qué recursos de la red y con qué privilegios. • Se debe implementar redes privadas virtuales (VPN) seguras solo para el uso y utilización de trabajadores remotos que necesitan acceder a los activos críticos de información, así garantizaremos que los datos transmitidos a través de la red pública viajen de manera cifrada.

	• Los proveedores, contratistas u alguna otra parte externa que necesite interactuar con los sistemas activos críticos de información de la organización, lo deben de hacer de manera controlada y segura mediante la utilización de la VPN. • La VPN por defecto estará deshabilitada para todos los usuarios internos o personal externo, mediante una solicitud y coordinación previa con el departamento de TI, se habilitará la VPN en el tiempo y horario previamente establecido. • Se implementará un firewall de red para filtrar y bloquear tráfico malicioso y segmentación de la red a fin de separar la red interna en donde se encuentran los activos críticos de información de la red pública. • El proveedor de servicio de internet se le solicitar que implemente el servicio de monitoreo del enlace, a fin de poder auditar el tráfico de la red e identificar posibles intrusiones. • El departamento de TI será el responsable de garantizar que la infraestructura de red esté segura y que los datos que circulan por los activos críticos de información estén protegidos de accesos no autorizados. • Se deben entregar y actualizar de manera semestral diagramas de red de todas las localidades de la organización, con el direccionamiento especifico, con lo cual tendremos una guía a nivel visual de la infraestructura y los controles de red implementados, lo que facilitará la comprensión de cómo se distribuyen los recursos y como está catalogado los niveles de protección en la red. • Revisar información de foros y fuentes sobre amenazas, con el fin compartir guías de información sobre amenazas cibernéticas emergentes con el fin de prevenir y mitigar ataques cibernéticos.

	• Colaborar con estos foros permite a la organización compartir detalles de incidentes de seguridad ya ocurridos para prevenir la repetición de estos incidentes. • Los proveedores, contratistas o un tercero que requiera acceso a los activos de información deben firmar acuerdos de confidencialidad y cumplir con las políticas de seguridad internas de la organización. • El acceso de terceros debe ser limitado a los activos críticos de información, solo con los privilegios y permisos necesarios para la realización de sus actividades. El incumplimiento de esta medida en la organización puede dar lugar a medidas disciplinarias, como la revocación de acceso, sanciones económicas, y en casos graves la terminación del contrato o la finalización de la relación comercial con terceros. • El acceso de proveedores o terceros será monitoreado de manera continua, en caso de existir termino de contrato con el proveedor se revocarán todos los accesos al concluir este con el proveedor. • Los activos críticos de información deben estar fijados a superficies seguras, con el fin de evitar robos o malas manipulaciones. Deben estar ubicados en salas aisladas con acceso restringido. • El uso de dispositivos externos como memorias USB, discos duros externos en activos críticos de información debe ser restringido, con el fin de evitar transferencia no autorizada de información sensible o critica. • Se debe de implementar sistemas de control de acceso, como tarjetas de proximidad, lectores biométricos con el fin de garantizar que solo personas autorizadas puedan acceder a áreas restringidas donde reposan los activos críticos de información. • Establecer control y gestión del suministro eléctrico con el fin de garantizar la continuidad de la operación de la organización,

	• Implementar sistemas de energía de respaldo, como generadores eléctricos o sistemas de alimentación ininterrumpida con el fin de asegurar que los activos críticos de información continúen operando en caso de una interrupción del suministro eléctrico. • Incorporar detectores de humo y sistemas de detección de calor en áreas donde reposen los activos críticos de información. • Los sistemas eléctricos, generadores deben ubicarse en áreas seguras y protegidas contra el acceso no autorizado. • Implementar sistemas de monitoreo energético de las instalaciones con el fin de que pueden alertar sobre fluctuaciones en el suministro eléctrico, fallos de componentes o condiciones anómalas en tiempo real. • Se debe prevenir y responder a intentos de intrusión en la red de la organización, una intrusión en la red es muy grave y los mismos pueden incluir ataques de denegación de servicio (DoS), ataques de malware, exploits de vulnerabilidades, en activos críticos de información.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 28 Política Seguridad de Red y Activos Críticos de Información

A continuación, se detalla diagrama de red de la organización tanto de su oficina principal como de las plantas:

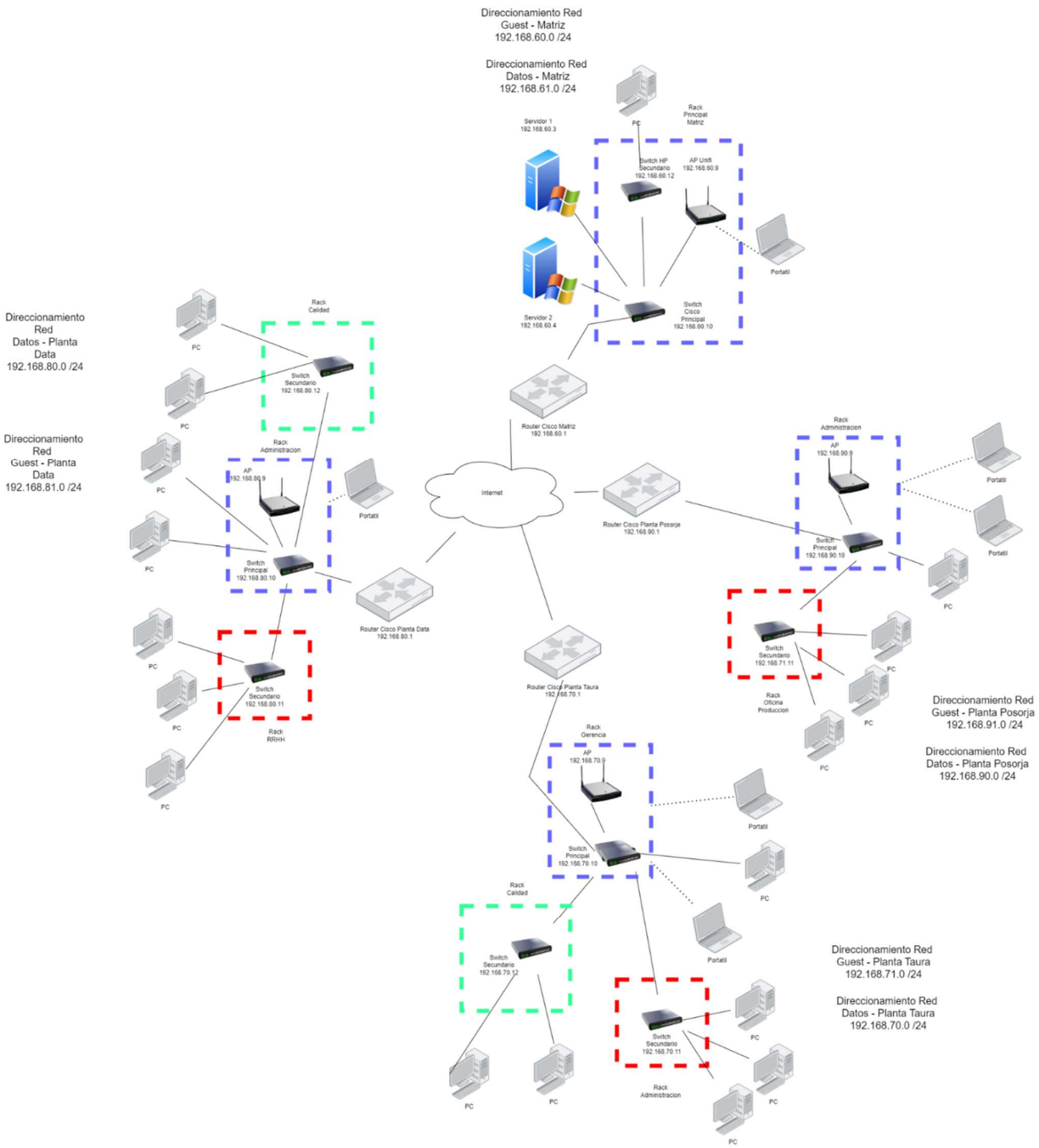

Figura 14 Diagrama de Red

A continuación, se detalla direccionamiento de red de la organización tanto de su oficina principal como de las plantas:

Direccionamiento de Red		
Matriz	Red Datos Corporativa	192.168.60.0 /24
	Red Guest	192.168.61.0 /24
Planta Data	Red Datos Corporativa	192.168.80.0 /24
	Red Guest	192.168.81.0 /24
Planta Posorja	Red Datos Corporativa	192.168.90.0 /24
	Red Guest	192.168.91.0 /24
Planta Taura	Red Datos Corporativa	192.168.70.0 /24
	Red Guest	192.168.71.0 /24

Tabla 29 Direcionamiento de red

ID	Gestión de Activos
0006	Política Activos Críticos de Información Gestionados por Terceros
Dirigido a	Departamento de TI Proveedores Externos
Objetivo	Detallar la comunicación de red autorizada en la organización y sus los flujos de datos de red internos y externos
Normas	• Se debe gestionar, controlar y asegurar la protección de los activos cuando estos son gestionados o procesados por proveedores o contratistas. • Se debe exigir al proveedor que se entregue un inventario actualizado cada 6 meses, en el inventario debe detallarse el número de serie, marca modelo del activo critico de información y fecha de actualización de firmware o parche de seguridad.

	• En caso de que el activo se encuentre obsoleto y ya no reciba actualizaciones por parte del fabricante, será notificado de inmediato con el proveedor del servicio a fin de migrar este activo por otro de similares características que reciban actualizaciones periódicamente. • Se debe incluir un formato en el cual se incluya información de contacto del proveedor con el fin de poderse comunicar de manera eficiente con él, abordar problemas, gestionar solicitudes o tomar decisiones relacionadas con los activos críticos de información que provee.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 30 Política Activos Críticos de Información Gestionados por Terceros

A continuación, se adjunta formato de contacto de los proveedores

Activo	Ubicación	Proveedor	Contacto Principal	Teléfono Principal	Contacto Secundario	Teléfono Secundario
Router	Planta Data Posorja	Telecomunicaciones	Proveedor A Principal	04 39 22 000	Proveedor A Secundario	
Router	Planta Posorja	Telecomunicaciones	Proveedor A Principal	04 39 22 000	Proveedor A Secundario	
Router	Planta Taura	Telecomunicaciones	Proveedor A Principal	04 39 22 000	Proveedor A Secundario	

Router	Matriz	Telecomunicaciones	Proveedor A Principal	04 39 22 000	Proveedor A Secundario	
Servidor	Rack Principal Matriz	Servidores	Proveedor B Principal	3530130	Proveedor B Secundario	
Servidor	Rack Principal Matriz	Servidores	Proveedor B Principal	3530130	Proveedor B Secundario	

Tabla 31 Tabla contactos

ID	Evaluación de riesgos
0007	Política Pruebas de Penetración e identificación de vulnerabilidades en Activos Críticos de Información
Dirigido a	Departamento de TI Proveedores Externos
Objetivo	Identificar, validar y registrar las vulnerabilidades de los activos críticos de información de la organización
Normas	• Se deben de realizar y ejecutar de manera anual pruebas de penetración a los activos críticos de información con el fin de evaluar la seguridad de estos, ayudara a identificar vulnerabilidades o tengan debilidades en sus configuraciones. • Se recomienda que esta prueba sea ejecutada por una empresa externa especializada, tendremos una evaluación profesional e imparcial que ayudara a mejorar la postura de seguridad de los activos críticos de información de la organización y cumplir con los estándares regulatorios.

	• Se deben firmar acuerdos de confidencialidad para evitar fuga de información. Esta prueba de penetración debe ser coordinada por el departamento de TI de la organización. • El alcance de estas pruebas de penetración será identificar vulnerabilidades en los activos críticos de información. • No debe existir exclusión, todos los activos críticos de información deben ser evaluados. • Ejecutada la prueba de penetración la empresa externa entregará un informe general con los hallazgos detallando las vulnerabilidades encontradas y como fueron explotados. En el informe también se deben incluir recomendaciones y consejos para remediar las vulnerabilidades encontradas. De este informe debe entregarse a la alta Gerencia una copia. • Se debe evaluar y documentar de manera anual, todo tipo de amenazas que podrían afectar a los activos críticos de información permitirá identificar su impacto y ayudara a la correcta toma de decisiones para proteger los activos críticos. • A continuación, identificación de amenazas: Amenazas Naturales: Terremotos, inundaciones, tormentas, incendios forestales, huracanes. Presentan el impacto, pérdida o daño de activos críticos de información, interrupción de servicios prestados por los activos críticos de información, pérdida de datos críticos almacenados en los activos.

	Amenazas Humanas: Ataques cibernéticos su impacto podría verse reflejado comprometiendo datos sensibles de loa activos críticos de información. Actos malintencionados internos su impacto podría verse reflejado en la alteración de datos de los activos críticos de información. Actos humanos su impacto podría verse reflejado en la eliminación accidental de información de algún activo critico de información. Amenazas Externas: Acceso no autorizado su impacto podría verse reflejado en el robo o perdida de información de los activos críticos de información Amenazas Falla Técnica: Falla en el software o hardware del activo critico de información podría verse reflejada la interrupción de la operación e inaccesibilidad al activo. • Implementar remediación de vulnerabilidades en los activos críticos de información. • Identificar, evaluar, corregir y verificar las vulnerabilidades en los activos críticos de información que podrían ser explotadas por atacantes y comprometer la seguridad, confidencialidad, integridad o disponibilidad del activo. Esto debe aplicarse a todos los activos críticos de información. • Ejecutar de manera periódica, con la ayuda de herramientas, escaneo de vulnerabilidades. • Según su severidad las vulnerabilidades las categorizaremos alta, media y baja. • Ejecutar el escaneo de vulnerabilidades con una empresa externa, ya que estos aportan una visión

	imparcial y objetiva sobre la seguridad de los activos críticos de información, además de contar con herramientas de última generación que están continuamente actualizadas para detectar nuevas amenazas y vulnerabilidades. • Es obligación del proveedor que realizo el escaneo que notifique de manera inmediata cualquier vulnerabilidad de alta severidad que pueda afectar los activos críticos de información. • El proveedor debe emitir informes detallados sobre las vulnerabilidades detectadas, las acciones correctivas que se deben implementar y el seguimiento de la remediación. • El departamento de TI se encargará de realizar esta actividad en conjunto con el proveedor cada 6 meses.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 32 Política Pruebas de Penetración e identificación de vulnerabilidades en Activos Críticos de Información

Se elabora una matriz tomando de referencia, la probabilidad de ocurrencia e impacto.

Amenaza	Ocurrencia	Impacto
Naturales	Media	Alto
Humanas	Alta	Alto
Externas	Alta	Medio
Falla Técnica	Media	Alto

Tabla 33 Matriz Probabilidad Amenazas

ID	Evaluación de riesgos
0008	Política Evaluaciones de Impacto y Riesgo Empresarial
Dirigido a	Departamento de TI
Objetivo	Identificar y registrar el impacto potencial y la probabilidad en que la amenazas exploten esa vulnerabilidad
Normas	• Se deben identificar, analizar y priorizar los efectos de las interrupciones o fallos en las operaciones de los activos críticos de información pueden tener sobre los procesos y las funciones de la organización, a través de este • Mediante evaluaciones, se pueden tomar decisiones informadas sobre qué medidas de mitigación implementar para reducir el impacto de posibles crisis o incidentes sobre los activos críticos de información, estas evaluaciones abarcaran todos los activos críticos de información. Las evaluaciones se estructuran de la siguiente manera: 1. Se debe trabajar con cada responsable del activo critico de información para identificar los procesos de la organización más críticos, luego se debe establecer una clasificación según la criticidad del proceso del activo critico de información. 2. Se debe evaluar el impacto que tendrá la interrupción de algún proceso del activo critico de información, también se debe

	indicar si esta interrupción traerá consigo consecuencias financieras, pérdida de ingresos entre otros. 3. Se debe establecer el tiempo máximo de recuperación aceptable para restaurar el proceso del activo critico de información de la organización. 4. Se deben designar Responsabilidades General y Departamentales La función del responsable General es la de coordinar y supervisar la realización de la evaluación, el departamento de TI será designado como el responsable General. Los responsables departamentales colaborarán en la recopilación de datos e identificación de procesos de los activos críticos de información, todos los jefes departamentales de la organización se les asignara esta responsabilidad. 5. Las evaluaciones serán revisadas de forma anual. • Se deben realizar evaluaciones de riesgos anuales o después de incidentes importantes. • En las evaluaciones se toma en cuenta todos los aplicativos que se ejecutan sobre los activos críticos de información, también se evalúan los equipos pertenecientes a terceros o proveedores externos. • Se debe designar un director de Seguridad de la Información que será el responsable de supervisar todas las actividades relacionadas con la ciberseguridad de la organización incluyendo la

	evaluación de riesgos, el mismo debe ser designado por el Departamento de TI. • Se debe ejecutar evaluaciones de riesgos orientada a los activos críticos de información, con el propósito de analizar todos los riesgos a los que se enfrenta los activos críticos de información. • En los informes se debe anexar información acerca del incidente con el fin de tener información detallada sobre los eventos de seguridad que afectaron la organización. Se detalla un ejemplo en la tabla 36.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 34 Política Evaluaciones de Impacto y Riesgo Empresarial

A continuación, se muestra un formato de las evaluaciones de impacto empresarial que se utilizaran en la organización:

Análisis de Impacto					
Actividad o Proceso	**Departamento**	**Dependencia /Servicios TI**	**Nivel criticidad**	**Tiempo de recuperación esperado**	**¿la capacidad de sistemas cubre los requisitos del proceso?**
Gestión nóminas	Administración	ERP Corporativo	Alto	1 hora	SÍ

Gestión stock	Almacén	Herramienta de inventario de activos	Medio	3 horas	No. La capacidad actual de sistemas no permite cubrir los requisitos

Tabla 35 Formato de Evaluación

Información Incidente	
N Incidente	1111
Fecha Apertura	1/1/2024
Hora Apertura	10:01
Clasificación Incidente	Virus, Corte de Energía, Malware
Prioridad	Grave, Medio, Bajo
Estado	Abierto, Cerrado, En curso
Impacto	Alto, Medio, Bajo
Acciones Ejecutadas	
Fecha Cierre	2/2/2024
Hora Cierre	14:00
Responsable	J.P.

Tabla 36 Información de Incidente

Para el análisis de riesgos de este proyecto hemos utilizado el formato proporcionado por INCIBE (Instituto Nacional de Ciberseguridad de España), Instituto que trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia del mercado digital. (INCIBE, 2024).

1. Determinar el riesgo para los activos críticos de información de la organización, determinando 9 como más alto y 1 como más bajo.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Debajo se recogen tablas orientativas para realizar las valoraciones de impacto según escalas de tres valores. En función del nivel de detalle que se desee conseguir, puede aumentarse el número de intervalos de la escala.

Asimismo, se incluye una tabla para la definición del riesgo aceptable, que debe ser definido previamente a la realización del análisis de riesgos de acuerdo a la estrategia corporativa.

Esta información es facilitada por INCIBE de forma absolutamente gratuita y debe considerarse como una primera aproximación. INCIBE no se responsabiliza del uso que pueda hacerse de la misma.

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

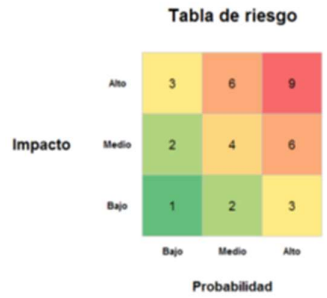

Figura 15 Tabla de Riesgo

Fuente INCIBE

2. Identificar los activos críticos de información de la organización.

	Identificador	Activo	Aplicación
Modelo A	A1	ordenador(es)	SI
	A2	móvil(es) principalmente para telefonía	
	A3	conexión a Internet e incluso wifi	
Modelo B	B1	ordenadores y conexión a Internet (con wifi)	SI
	B2	dispositivos móviles para telefonía y datos	
	B3	soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento *cloud*	
	B4	una página web sencilla alojada y gestionada por un proveedor externo	
Modelo C	C1	ordenadores e incluso algún servidor (web, correo electrónico,...)	SI
	C2	conexión a Internet con wifi	SI
	C3	dispositivos móviles con datos y apps para su trabajo	
	C4	herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	SI
	C5	página web / tienda online y redes sociales que gestionan desde la empresa	
	C6	herramientas para empresas en la nube	
	C7	e-administración para su relación con las AAPP	

Figura 16 Activos Críticos de Información

Fuente INCIBE

3. Identificar las amenazas que aplican a cada uno de los activos críticos de información.

Esta información es facilitada por INCIBE de forma absolutamente gratuita. INCIBE no se responsabiliza del uso que pueda hacerse de la misma.

Amenazas
Fuego
Daños por agua
Desastres naturales

Amenazas
Fuga de información
Introducción de falsa información
Alteración de la información
Corrupción de la información
Destrucción de información
Interceptación de información (escucha)

Amenazas
Corte del suministro eléctrico
Condiciones inadecuadas de temperatura o humedad
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Desastres industriales

Amenazas
Degradación de los soportes de almacenamiento de la información
Difusión de software dañino
Errores de mantenimiento / actualización de programas (software)
Errores de mantenimiento / actualización de equipos (hardware)
Caída del sistema por sobrecarga
Pérdida de equipos
Indisponibilidad del personal
Abuso de privilegios de acceso
Acceso no autorizado

Amenazas
Errores de los usuarios
Errores del administrador
Errores de configuración

Amenazas
Denegación de servicio
Robo
Indisponibilidad del personal
Extorsión
Ingeniería social

Figura 17 Amenazas

Fuente INCIBE

4. Establecer la probabilidad y el impacto de que dicha amenaza se materialice.

Mostrar Activos	ANÁLISIS DE RIESGOS				
	Activo	Amenaza	Probabilidad	Impacto	Riesgo
	ordenador(es)	Fuego	Alto (3)	Alto (3)	9
	ordenador(es)	Desastres naturales	Alto (3)	Alto (3)	9
	ordenador(es)	Fuga de información	Bajo (1)	Medio (2)	2
	ordenador(es)	Introducción de falsa información	Medio (2)	Medio (2)	4
	ordenador(es)	Alteración de la información	Medio (2)	Alto (3)	6
	ordenador(es)	Corrupción de la información	Alto (3)	Alto (3)	9
	ordenador(es)	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
	ordenador(es)	Fallo de servicios de comunicaciones	Medio (2)	Alto (3)	6
	ordenador(es)	Interrupción de otros servicios y suministros esenciales	Medio (2)	Medio (2)	4
	ordenador(es)	Desastres industriales	Alto (3)	Alto (3)	9
	ordenador(es)	Acceso no autorizado	Medio (2)	Alto (3)	6
	ordenadores y conexión a Internet (con	Fuego	Alto (3)	Alto (3)	9
	ordenadores y conexión a Internet (con	Desastres naturales	Alto (3)	Medio (2)	6
	ordenadores y conexión a Internet (con	Fuga de información	Medio (2)	Medio (2)	4
	ordenadores y conexión a Internet (con	Introducción de falsa información	Medio (2)	Medio (2)	4
	ordenadores y conexión a Internet (con	Alteración de la información	Medio (2)	Medio (2)	4
	ordenadores y conexión a Internet (con	Corrupción de la información	Alto (3)	Alto (3)	9
	ordenadores y conexión a Internet (con	Corte del suministro eléctrico	Alto (3)	Alto (3)	9
	ordenadores y conexión a Internet (con	Fallo de servicios de comunicaciones	Medio (2)	Alto (3)	6
	ordenadores y conexión a Internet (con wifi)	Interrupción de otros servicios y suministros esenciales	Medio (2)	Medio (2)	4
	ordenadores y conexión a Internet (con	Desastres industriales	Alto (3)	Alto (3)	9
	ordenadores y conexión a Internet (con	Acceso no autorizado	Medio (2)	Alto (3)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Fuego	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Desastres naturales	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Fuga de información	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Introducción de falsa información	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Alteración de la información	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web, correo electrónico,...)	Corrupción de la información	Alto (3)	Medio (2)	6
	ordenadores e incluso algún servidor (web,				

Figura 18 Riesgo del Activo

ID	Mejora
0009	Política Mejora Continua
Dirigido a	Departamento de TI
Objetivo	Identificación de mejorar continuamente las capacidades de identificación de riesgos y activos en la organización
Normas	• Identificar la ejecución de procesos, procedimientos y actividades operativas, establece que los controles de tecnología, ciberseguridad deben probarse periódicamente para validar el diseño y la eficacia operativa de los controles sobre los activos críticos de información. • Las mejoras deben identificarse a partir de pruebas y ejercicios de seguridad. • Establecer que se deben ejecutar auditorías y evaluaciones de aseguramiento/garantías de acuerdo con planes basados en riesgos, a su vez se debe verificar el cumplimiento de todas las normas, regulaciones, requisitos legales/contractuales y estatutarios que sean relevantes y aplicables a la auditoría. • Evaluar los procesos, procedimientos y medidas técnicas para la realización periódica de pruebas de penetración por terceros independientes hacia los activos críticos de información. • Documentar los procedimientos para la seguridad de las aplicaciones a fin de proporcionar una guía

	para la planificación, entrega y soporte adecuados de las capacidades de seguridad de las aplicaciones de la organización. Estos deben ser deben ser revisados y actualizados, anualmente
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 37 Política Mejora Continua

ID	Concienciación y capacitación
0010	Política Capacitación Continua en Ciberseguridad
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Garantizar que todos los miembros de la organización, desde los empleados hasta la alta dirección, comprendan las amenazas cibernéticas y cómo actuar para proteger los activos de críticos de información, con el fin de promover cultura de ciberseguridad en la organización
Normas	• Realizar pruebas prácticas y talleres interactivos al personal administrativo de la organización, en las que se simulen ataques cibernéticos, con el fin de que se puedan experimentar la situación y aprender a reconocer las amenazas en tiempo real, conocimiento necesario para identificar, prevenir y responder a amenazas de ciberseguridad.

	• En las capacitaciones se debe indicar que cualquier anomalía o sospecha de amenaza debe ser informado al departamento de TI. • Estas capacitaciones deben ser acompañados de evaluaciones para medir la comprensión de los temas tratados y asegurar la efectividad de la capacitación. • Las prácticas y talleres deben ser ejecutados continuamente de manera semestral. El departamento de TI será el encargado de desarrollar y actualizar el contenido de las presentaciones • Se debe llevar un registro de las capacitaciones realizadas las cuales se incluya firma del personal que recibe esta capacitación. • El personal de TI debe tener un plan de formación y desarrollo en temas de ciberseguridad en los cuales se adquiera conocimientos fundamentales y avanzados en ciberseguridad mediante entrenamiento presencial como talleres prácticos o escenarios simulados en los cuales se enfrenten a ataques cibernéticos y poner en prueba el conocimiento adquirido. • La frecuencia de formación debe ser de manera anual.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 38 Política Capacitación Continua en Ciberseguridad

ID	Integridad
0011	Política Integridad sobre el activo critico de información
Dirigido a	Departamento de TI
Objetivo	Supervisar de manera continua el activo critico de información con el fin de que no sean alterados o se vean comprometidos
Normas	• Toda modificación en los activos críticos de información debe ser registrada, controlada y auditada. • Se debe implementar herramientas de Monitoreo de Integridad de Activos, estas herramientas verifican y registran cambios en los activos, como por ejemplo cambio de dirección IP o modificación de su almacenamiento. • Se debe mantener registros o logs de todas las acciones realizadas en los activos críticos de información. Esto incluye la creación, modificación, eliminación de datos o configuraciones, así como el registro de acceso. • Los registros deben ser revisados regularmente y almacenados de forma segura. • El sistema de monitoreo debe estar configurado o parametrizado para que genere alertas automáticas cuando se detecten cambios no autorizados o sospechosos en los activos críticos de información.

	• Las alertas deben ser procesadas y priorizadas para asegurar que se tomen acciones rápidamente ante posibles compromisos de integridad. • Los respaldos de los activos críticos de información deben ejecutarse de forma regular en un lugar seguro y accesible. • Todos los activos críticos de información deben tener respaldos. • Los respaldos deber ser completos e incrementales con el fin de optimizar los recursos de almacenamiento y minimizar el tiempo de recuperación. • La frecuencia de respaldos **completos** debe ser ejecutado cada semana, y los respaldos incrementales deben ser diarios realizando una copia de los cambios realizados desde el último respaldo completo. • Los respaldos serán almacenados de manera interna, en dispositivos de almacenamiento conectados a la red interna de la organización administrados por el departamento de sistemas. • Todos los respaldos deben estar cifrados. • El tiempo de almacenamiento de los respaldos será de máximo 12 meses para los completos y 6 de los incrementales. • El departamento de TI de la organización será el responsable de la planificación, implementación y monitoreo de los procesos de respaldo de los activos críticos de información.

Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 39 Política Integridad sobre el activo critico de información

ID	Incidentes
0012	Política Respuesta a Incidentes
Dirigido a	Departamento de TI Jefaturas de la organización
Objetivo	Definir el proceso de respuesta ante incidentes de seguridad que afecten a los activos críticos de información de la organización
Normas	• Previamente se debe de identificar al activo y se haber evaluado el riesgo según sus amenazas. • Identificar las áreas de riesgo junto con la ubicación y clasificación de los activos. • Crear Equipo de Respuesta a Incidentes, el área de TI de la organización debe designar las personas o candidatos idóneos y asignar responsabilidades. El equipo responsable será estructurado de la siguiente manera: 1. Líder del equipo que será responsable de la coordinación en general 2. Especialistas en seguridad informática. 3. Especialistas en infraestructura tecnológica.

	4. Departamento jurídico, ejecutara acciones legales si el caso lo amerita. • Los activos con Riesgo >= 4 se considera que es riesgo considerable y debe proceder su tratamiento • Los activos con Riesgo <= 4 el riesgo se considera poco reseñable. • El plan está estructurado en 5 fases: Preparación, Detección y análisis, Contención y eliminación, Recuperación y Mejora continua ✓ Preparación: La detección de intrusiones en red con el fin de identificar, prevenir y responder a intentos de intrusión en la red de la organización, una intrusión en la red es muy grave y los mismos pueden incluir ataques de denegación de servicio (DoS), ataques de malware, exploits de vulnerabilidades, en activos críticos de información. Tal como se mencionó en fases previas del modelo propuesto, debe de implementarse un firewall el cual debe tener funciones de IDS el cual va a detectar y alertar sobre actividades sospechosas en la red, e IPS el cual a más de detectar va a prevenir activamente ataques, bloqueando el tráfico malicioso. Establecer protocolos de comunicación interna y externa para incidentes. Como se mencionó en fases previas del modelo propuesto, debe existir entrenamiento y capacitación con frecuencia regular para el equipo de respuesta. ✓ Detección y Análisis: Es aquí en esta etapa donde se detectan los incidentes. Debe existir una identificación temprana de incidentes o anomalías

	sobre los activos críticos de información, a través de un monitoreo continuo y constante a los activos críticos de información mediante la ayuda de sistemas de detección de intrusos, firewalls, y herramientas de monitoreo de redes. Una vez identificado el incidente o anomalía, se debe verificar su legitimidad, con la ayuda del equipo de respuesta a incidentes deberán analizar datos del incidente y compararlo con otros incidentes que previamente se ejecutaron y validar si se encuentra alguna relación. ✓ Contención: Todas las incidencias identificadas deben ser contenidas para minimizar su alcance y efectos sobre los activos críticos de información. Si algún activo critico de información llega a ser comprometido deben tomarse medidas para evitar que el ataque no cause mayores daños. Se deben aislar los activos críticos de información afectados con el fin de evitar la propagación del incidente. Se debe llevar un registro continuo de los hechos y determinar la causa raíz de la amenaza, se deben desplegar parches de seguridad o configuraciones necesarias sobre el activo critico de información. Una vez contenidas todas las amenazas, deben ser eliminadas de los activos críticos de información, debe llevarse una limpieza meticulosa, y así disminuir la probabilidad de que se vuelva a repetir el incidente. ✓ Recuperación: Con la amenaza erradica, el equipo de respuesta debe enfocarse en la recuperación del activo critico de información, entre las actividades mas importantes esta la recuperación y

	restauración de información dañada o comprometida, con la ayuda de las copias de seguridad que previamente se abordó en fases anteriores de este proyecto. Se debe monitorear el activo crítico de información restaurado con el fin de asegurarse de que el incidente no se repita. ✓ Mejora continua: Una vez que el incidente este resuelto de manera exitosa y no se tengan mayores novedades, todo el proceso de resolución debe queda documentado. Se deben actualizar informes e implementar cambios correctivos necesarios ante futuras amenazas, a los informes se les debe anexar la cronología del incidente, cuáles fueron las medidas tomadas y lecciones aprendidas • Debe evaluarse el impacto del incidente sobre los activos críticos de información como tiempo de inactividad, impactos financieros. • Actualizar los controles de seguridad tomando en cuenta las vulnerabilidades que fueron explotadas durante el incidente.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 40 Política Respuesta a Incidentes

ID	Monitoreo Continuo

0013	Política Análisis de Eventos de Seguridad
Dirigido a	Departamento de TI
Objetivo	Recopilar y analizar eventos de activos críticos de información, con el fin de identificar actividades sospechosas o comportamientos anormales sobre los activos críticos de información
Normas	• Catalogar como evento de seguridad a cualquier acción o incidente. Esto debe ser aplicado a todos los activos críticos de información. • Se debe de implementar un SIEM, que es un sistema que tiene control sobre los eventos de los activos críticos de la información con el fin de poder detectar patrones anómalos. • Los eventos deben ser monitoreados de manera constante entre los más importantes tenemos intentos fallidos de inicio de sesión, cambios de configuración en activos críticos de información, modificación o eliminación de archivos sensibles, conexiones a los activos desde ubicaciones geográficas inusuales. • Se debe categorizar los eventos según su gravedad y urgencia, los hemos categorizados de la siguiente manera: Crítico: Representan una amenaza inmediata a la seguridad de la organización de los activos críticos de información – en esta categoría constan intrusión en activos, ejecución de virus o código malicioso

	Alto: Requieren una intervención inmediata – en esta categoría constan fallo en programa que se ejecutan sobre activos críticos de información Medio: Indican una posible vulnerabilidad, pero no tienen impacto inmediato – en esta categoría constan conexiones a los activos desde ubicaciones geográficas inusuales Bajo: Rutinarios o menores que no requieren acción inmediata – en esta categoriza constan acceso con éxito al activo. • Todos los eventos investigados deben ser documentados, incluyendo las acciones tomadas, las lecciones aprendidas y las recomendaciones para mejorar la prevención en el futuro. • Los resultados del análisis de eventos deben ser documentados en informes que deben ser entregados de manera periódica. • Correlacionar eventos con el fin de tener una detección proactiva, reducción de falsos positivos, y tener una respuesta rápida y eficaz.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 41 Política Análisis de Eventos de Seguridad

ID	Incidentes
0014	Política Investigación Forense

Dirigido a	Departamento de TI Proveedores Externos
Objetivo	Garantizar que las investigaciones sobre incidentes de seguridad cibernética suscitado en la organización se realicen de manera efectiva, asegurando que todos los datos relevantes de la investigación forense se preserven adecuadamente
Normas	• La investigación forense debe ser ejecutada por una empresa, la misma debe tener expertos altamente capacitados, contar con herramientas avanzadas y poder manejar casos complejos de manera objetiva e imparcial. • El departamento de TI se encargará de gestionar la investigación forense con la empresa externa. • Contractualmente se deben definir cláusulas de acuerdo de confidencialidad ya que la mayoría de los activos críticos almacenan información sensible. • Se debe definir el alcance de la investigación forense indicando los activos críticos que serán investigados de los cuales se tendrá que recolectar la información o evidencia digital. • Se debe exigir al proveedor cadena de custodio. • Por parte del proveedor debe existir un análisis detallado, relacionar los datos obtenidos de diversas fuentes con el fin de construir un panorama completo del incidente.

	• Identificar la causa raíz de cómo ocurrió el incidente, qué vulnerabilidades exploto y cómo se lograron comprometer los activos. • El proveedor debe entregar un informe detallando los hallazgos, detalles sobre la evidencia, conclusiones y recomendaciones. El informe puede ser utilizado para procedimientos legales si el caso lo amerita.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 42 Política Investigación Forense

ID	Recuperación
0015	Política Recuperación ante Desastres Cibernéticos
Dirigido a	Departamento de TI
Objetivo	Asegurar que la organización pueda restaurar sus activos críticos de información después de un ciberataque
Normas	• Minimizar el impacto de incidentes graves, como ataques de ransomware sobre activo critico de información, fallo masivo en los activos críticos de información, problemas en activos críticos de

	información de terceros que prestan servicios a la organización. • Identificar y priorizar la restauración de sistemas y aplicaciones que sean fundamentales para las operaciones comerciales. • Designar roles y responsabilidades, los mismo serán designados por el departamento TI de la organización • Realizar copias de seguridad de todos los activos críticos de información y de las configuraciones de los dispositivos de telecomunicaciones catalogados como activos críticos. • Se debe asegurar que las copias de seguridad estén actualizadas, cifradas y almacenadas en ubicaciones seguras tanto en sitio como fuera de sitio. • Las copias de seguridad en sitio serán almacenas en discos duros externos de gran capacidad de almacenamiento. • Las copias de seguridad fuera de sitio serán almacenadas en la nube, • Se debe contratar un repositorio en la nube que garantice que la información repose de manera cifrada y con alta disponibilidad y gran capacidad de almacenamiento. • Los respaldos tanto internos como no internos deben hacerse de manera regular diariamente. • Crear alternativas que aseguren la disponibilidad de los activos críticos de información ante cualquier interrupción.

	• Luego de ocurrido el evento, determinar el grado de gravedad del desastre. • Luego de ocurrido el evento y de haber determinado el grado de gravedad del desastre, se debe ejecutar el procedimiento de recuperación adecuado. • Luego de ejecutar el procedimiento de recuperación se debe verificar y validar el correcto funcionamiento del activo critico de información, posterior a esto debe hacerse un monitoreo continuo, realizar una evaluación del desempeño y ajustar el plan según sea necesario. • El plan debe ser revisado y actualizado regularmente para asegurar que se mantenga vigente frente a nuevas amenazas.
Desarrollada por	Departamento TI
Revisada por	Departamento TI
Rige a partir de	1/1/2025

Tabla 43 Política Recuperación ante Desastres Cibernéticos

Rol	**Responsabilidad**
Líder Plan Recuperación	Coordinar Respuesta y Restauración
Líder Infraestructura TI	Encargado de la restauración de la infraestructura TI
Responsable Seguridad Activo Critico Información	Encargado de garantizar la integridad y confidencialidad de los datos del activo critico durante la recuperación.
Responsable Comunicación	Encargado de gestionar las comunicaciones internas y externas

Tabla 44 Responsabilidades

Escenario de incidente	Estrategias de recuperación	Procedimiento de recuperación
Desastre Natural: Terremoto, Inundaciones	Cambio a un equipo nuevo	Restaurar ultima copia de seguridad sobre el equipo nuevo
Corte suministro energético	Conexión a un suministro de energía externos	Conexión del dispositivo acometidas eléctrica de backup o UPS
		Conexión del equipo a banco de batería externa de UPS
Condiciones Inadecuadas de temperatura o humedad	Revisar Ventilación del área	Abrir puertas y ventanas para ventilación del área
		Conversar con departamento de Mantenimiento y revisar equipos de ventilación
	Mover activo a otra área	Traslado del activo a área ventilada libre de humedad, hasta que el área de mantenimiento rectifique los daños
Fallo servicio de comunicación	Revisar Conexiones del Activo	Cambio en las conexiones de red del activo
		Notificar al proveedor externo y valide factibilidad de la comunicación
	Revisar Hardware del Equipo	Cambio de tarjeta de red del activo
Robo de equipo	Cambio a un equipo nuevo	Restaurar ultima copia de seguridad sobre el equipo nuevo
		Equipo de TI debe de dar de baja al activo e inactivar cuentas del usuario o acceso del activo robado
Corrupción de la información	Ejecución de software antivirus	Eliminar cualquier amenaza que pueda comprometer el activo

	Exclusión del activo	En caso de encontrar alguna amenaza, se debe excluir el equipo de la red
Difusión de software dañino	Ejecución de software antivirus	Eliminar cualquier amenaza que pueda comprometer el activo
	Exclusión del activo	En caso de encontrar alguna amenaza, se debe excluir el equipo de la red
	Identificación de malware	Eliminar archivos infectados
		Restaurar ultima copia de seguridad sobre el activo
Errores de mantenimiento / actualización de programas (software)	Identificar el error en la actualización o mantenimiento	Documentación del error
		Restaurar ultima copia de seguridad sobre el activo
Errores de mantenimiento / actualización de equipos (hardware)	Identificar el error en la actualización o mantenimiento	documentación del error
		Utilizar equipo de contingencia
		Restaurar ultima copia de seguridad sobre el activo
		Chequear activo con problemas de hardware
Denegación de servicio	ejecución de software antivirus	Eliminar cualquier amenaza que pueda comprometer el activo
	exclusión del activo	En caso de encontrar alguna amenaza, se debe excluir el equipo de la red

Tabla 45 Procedimiento Recuperación

CONCLUSIONES

El diseño de un modelo de ciberseguridad basado en el marco ISO 27110:2021/NIST permitirá a la organización Fortidex ofrecer una solución práctica y efectiva para la protección de los activos críticos de información, en un entorno cada vez más interconectado y vulnerable al riesgo cibernético, las políticas planteadas en este trabajo fueron compartidas con personal administrativo de la organización, se elaboró una pequeña encuesta tomando una muestra de 9 personas del área administrativa, los resultados de la misma se encuentran en los anexos del presente trabajo, el 100% del personal entrevistado está de acuerdo en recibir capacitación sobre ciberseguridad con el fin de experimentar la situación y aprender a reconocer amenazas cibernéticas, saber que directrices seguir y cómo actuar ante un ataque cibernético.

Para el diseño de marco de ciberseguridad propuesto, se han adoptado directrices claras y buenas prácticas de las normas NIST e ISO 27110:2021, las cuales permitan implementar medidas de ciberseguridad efectivas sobre los activos críticos de información. La integración de ambas normas permite hacer frente a amenazas cibernéticas lo que asegura que la organización esté preparada para responder ante cualquier incidente de manera efectiva, hemos elaborado políticas que abarcan cada una de las fases del modelo NIST e ISO 27110:2021, luego de compartir las políticas y ejecutar la encuesta, el 100% considero las Normas NIST e ISO 27110:2021 permitirán a la organización estar preparada para responder ante cualquier incidente de manera efectiva.

El desconocimiento sobre normas o regulaciones de ciberseguridad representa un desafío significativo para la organización, al no tener conocimiento sobre directrices claras para la protección de sus activos críticos de información las expone a los crecientes riesgos cibernéticos de hoy en día, esto podemos verlo reflejado en los resultados del personal encuestado, ya que solo el 46% tiene conocimiento sobre el potencial dañino que conllevan los riesgos cibernéticos sobre los activos críticos de información.

En la organización existe desconocimiento sobre normas o regulaciones de ciberseguridad la cual pueda ser implementada en la organización para la protección de los activos críticos de información, esto podemos denotarlo ya que alrededor del 80% del personal encuestado no ha recibido capacitación sobre buenas prácticas de ciberseguridad. Luego de haber presentado las políticas podemos denotar este desconocimiento en una de las preguntas planteadas sobre software licenciado el 78% considera que se debe adquirir software licenciado, mientras que el 22% restante considera que no es necesario adquirir este tipo de licenciamiento y que debe buscarse alternativas como software opensource para reducir los costos que implicar adquirir software licenciado. En otra pregunta de la encuesta se les consulto sobre las claves o contraseñas utilizadas para acceder a los activos críticos de información, el 67% utiliza y sigue las recomendaciones de las normas de contraseñas mencionadas en la Política de Autenticación y Control de Acceso, mientras que el 33% restante utiliza claves débiles debido a que son fáciles de recordar y menos complejas.

En la organización se ha identificado e inventariado los activos críticos de información, se los ha clasificado según su nivel de criticidad y asignado un responsable luego de presentar la Política de Identificación y Clasificación de Activo, la mayoría no estuvo de acuerdo con la responsabilidad del activo y velar por la buena gestión del mismo, el 78% del personal entrevistado está de acuerdo con la política, mientras que el 22% restante no está de acuerdo ya que indica que no se responsabiliza y es deber de la organización velar por la buena gestión del activo. Siguiendo con la Política de Identificación y Clasificación de Activo, el 78% del personal encuestado considera que el factor humano es pieza fundamental para la ciberseguridad de la organización, mientras que el 22% considera que no, la tecnología latente y el auge de la inteligencia artificial será el nuevo pilar de la ciberseguridad.

Para un diseño de marco de ciberseguridad la evaluación y mejora continua son esenciales ya que, en un entorno digital, nuevas amenazas y vulnerabilidades emergen de manera continua, por lo que es necesario que se implemente mecanismos para evaluar el desempeño y realizar ajustes periódicos, entre las más importantes auditorias, revisión y actualización de políticas e indicadores de cumplimiento.

Luego de presentar las políticas al personal encuestado como mejora continua se propone que se audite a los proveedores que gestionan activos críticos de información de la organización, el 100% estuvo de acuerdo en que se deban monitorear y auditar, ya que la información que reposa los activos es muy confidencial.

Evaluar y mejorar continuamente conlleva a gastos, el 100% de los encuestados está de acuerdo en que se deba destinar presupuesto para soluciones de ciberseguridad con el fin de garantizar la integridad del activo crítico de la información, en misma cantidad de porcentaje está de acuerdo en que la conexión remota que se utiliza para acceder a los activos de la compañía este siempre monitoreado para identificar posibles intrusiones y evitar cualquier robo o fuga de información.

RECOMENDACIONES

Para garantizar la efectividad del diseño de marco de ciberseguridad propuesto mediante las normas NIST e ISO 27110:2021, es crucial que la organización adopte recomendaciones claves, entre las más importantes la creación de una cultura organizacional de ciberseguridad, formación continua sobre aspectos de ciberseguridad y evaluaciones de cumplimiento.

Tomar como pilar base el diseño propuesto orientado a activos críticos de información de la organización, a fin de poder diseñar marcos de ciberseguridad orientado a otros recursos de tecnologías de la información de la organización entre los más importantes Infraestructura de Servidores, Infraestructura de Red y Gobernanza TI.

Se debe mantener el inventario de activos críticos de información actualizado, se recomienda realizar actualizaciones al menos 1 vez al año. Un inventario actualizado le permite conocer en todo momento en dónde se encuentra activo y cuál es el nivel de protección que requiere.

Para mejoras y evaluación del diseño de ciberseguridad orientada a activos críticos de información se propone que se elaboren informes de desempeño y se ejecuten auditorías de seguridad periódicas, se deben presentar estos resultados en reuniones estratégicas con la alta dirección de la organización.

Al ser un marco de ciberseguridad personalizado que se adapta a las necesidades de la organización, a futuro se podrían agregar a este diseño buenas prácticas de seguridad de otras normas con el objetivo de robustecer políticas y procedimientos y poder adaptarlos a la tecnología que cada día evoluciona y propone nuevos desafíos.

REFERENCIAS

Arcotel, & EcuCert. (2014). *Ecucert*. Obtenido de https://www.ecucert.gob.ec/centro-derespuesta-a-incidentes-informaticos-del-ecuador/#

Bastidas Pérez, S. M. (2021). Análisis de riesgo en la seguridad de los datos médicos mediante la utilización de la norma ISO/IEC 27110: 2021.

Cauja Altamirano, M. J. (2024). Metodología de un Sistema DLP (data loss prevention) para la entidad financiera "Cooperativa de Ahorro y Crédito Santa Anita Ltda." basada en la norma ISO/IEC 27002:2022. *Universidad Tecnica del Norte*, 28.

Cepeda, H. F., Vargas, A. D., & Botello, F. M. (2021). ANÁLISIS DE RIESGO DEL DOMINIO 8 GESTIÓN DE ACTIVO DE LA ISO 27001-2013 A LA UNIVERSIDAD COOPERATIVA DE COLOMBIA ÁREA GESTIÓN TECNOLÓGICA SEDE ARAUCA. *UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE ARAUCA*.

Chang, J. E. (2020). Análisis de ataques cibernéticos hacia el Ecuador. *Revista Científica Aristas*, 18-27.

Cistoldi, P., Parra de Gallo, H., Luz Clara, B., Aráoz Fleming, J., Dorado, J., Greco, F., & Ambrústolo, M. (2023). Seguridad de la Información y Ciberseguridad en Laboratorios de Informática Forense. Necesidades de las fiscalías. *UCASAL*, 13.

CORBETTA, P. (2007). METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN CUALITATIVAS. MADRID: MC GRAW HILL.

Criollo Neira, E. G., Flores Urgilés, C. H., Flores Urgilés, C. M., Santacruz Espinoza, J. J., & Ron Egas, M. B. (2023). Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano. *Pro Sciences: Revista De Producción, Ciencias E Investigación*.

CyberZaintza. (2021). *Ciberglosario*. Obtenido de https://www.ciberseguridad.eus/ciberglosario/ataque-disruptivo

de la Cuesta Benjumea, C. (Jul-Sep de 2015). LA CALIDAD DE LA INVESTIGACIÓN CUALITATIVA: DE EVALUARLA A LOGRARLA. *Florianópolis, 24*(3), 883-890. doi:http://dx.doi.org/10.1590/0104-070720150001150015

Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista lbérica de Sistemas y Tecnologías de Información*, 3.

Ecucert. (12 de 2021). *Seguridad de Redes de Telecomunicaciones*. Obtenido de https://www.ecucert.gob.ec/wp-content/uploads/2022/01/infografia-mensual-122021.pdf

FORTIDEX. (s.f.). *Nuestra Empresa*. Obtenido de https://fortidex.com/nuestra-empresa.html

Fuentes Penna, A., Gómez Cárdenas, R., & González Ibarra, J. (2024). La Ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos*.

Gómez Suarez, Á. J. (2019). Diseño de un programa de ciberseguridad de una empresa basado en el marco de trabajo NIST. *Universidad de Jaén*, 11.

González Reyes. (2021). *Diseño del plan director de ciberseguridad para las aplicaciones expuestas en internet por el banco agrario de Colombia basado en la norma ISO/IEC 27032: 2012.* Bogotá: UNIVERSIDAD PILOTO DE COLOMBIA.

Guayara Murillo, E. A., & Moyano Murcia, E. F. (2022). *Propuesta de orientación en ciberseguridad para la formación de los estudiantes de media técnica especializada del colegio OEA IED basado en el marco NIST SP800-181.* Bogotá: Universidad Católica de Colombia.

Herrera Flórez, A. N., & Tellez Monsalve, J. C. (2021). Diseño de un framework de ciberseguridad, seguridad y privacidad de la información para un proveedor de servicios de telecomunicaciones en un ambiente multiregion. *Departamento de ingeniería de Sistemas y Computación*.

Huilcapi, Castro, & Jácome. (2017). Motivación: las teorías y su relación en el ámbito empresarial. *Dominio de las Ciencias, 3*(2), 311-333. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.2.311-333

IBM. (30 de 03 de 2022). *¿Qué es la gestión del ciclo de vida de los activos?* Obtenido de https://www.ibm.com/mx-es/topics/asset-lifecycle-management#:~:text=El%20ciclo%20de%20vida%20de,sus%20activos%20utilizando%20varios%20m%C3%A9todos.

INCIBE. (2024). *¿Que es INCIBE?* Obtenido de https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe

INEC. (2010). *Instituto Nacional de Estadistica y Censos.* Obtenido de INEC: https://www.ecuadorencifras.gob.ec/wp-content/descargas/Manu-lateral/Resultados-provinciales/santa_elena.pdf

IsecT, L. (2024). *ISO/IEC TS 27100:2020 — Information technology — Cybersecurity — Overview and concepts (first edition)*. Obtenido de https://www.iso27001security.com/html/27100.html

ISO/IEC. (2018). *ISO/IEC TR 27103*. Obtenido de https://cdn.standards.iteh.ai/samples/72437/a0eb663a742f4b879ec5ec65784067bf/ISO-IEC-TR-27103-2018.pdf

Johanna Carolina González Reyes, J. R. (2021). Diseño del plan director de Ciberseguridad para las aplicaciones expuestas en internet por el Banco Agrario de Colombia basado en la norma ISO/IEC 27032:2012. *Universidad Piloto de Colombia*, 27.

Kaspersky. (30 de Septiembre de 2024). *CIBERAMENAZAS LIVE-MAP*. Obtenido de https://cybermap.kaspersky.com/es/stats#country=35&type=OAS&period=w

Martos Paredes , J. H., & Villazon Sosa, J. A. (2024). *IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA OCTAVE-S.* Perú: Universidad Señor de Sipán.

Moscoso, F. M. (2017). Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos. *Universidad de Cuenca*, 18.

Nacimba Nacimba, M. X. (2024). *Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior.* Quito: Universidad Tecnológica Israel.

OAS. (2019). *MARCO NIST*. Obtenido de Un abordaje integral de la Ciberseguridad: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Peralta, M. L., & Aguilar, D. N. (2021). La ciberseguridad y su concepción en las Pymes de Cuenca, Ecuador. *Universidadde Cuenca*, 103.

Ramirez Vargas, J. A., & Pereda Otero, L. R. (2021). *Propuesta de implementación de un modelo de ciberseguridad para la defensa contra ataques cibernéticos en la Oficina de Estadística e Informática del Instituto Nacional de Salud del Niño basado en el marco NIST v1. 1.* Ambato.

Rodríguez Márquez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. *Revista UIS Ingenierías*.

Ruiz Imbat, G. (2021). *Sistema de gestión de seguridad de la información de servicios en la nube para la empresa "Masiva" de la ciudad de Quito, con base en la norma ISO/IEC 27017.* Ibarra: UNIVERSIDAD TÉCNICA DEL NORTE.

Ruiz, J. E., Valqui, C. V., & Davila, E. J. (2021). Modelo de seguridad de la información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque . *UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO* , 27.

Sampieri. (2010). *Metodología de la Investigación.* México: McGRAW-HILL.

Sánchez, R. D. (2023). *Marco Mínimo de Ciberseguridad Para PYMEs En El Contexto de La Industria 4.0.* Queretaro: CIATEQ, A. C. Centro de Tecnología Avanzada.

Santiago Chávez, N. I., Romero Fernández, A. J., & Álvarez Gómez, G. A. (julio-septiembre de 2017). Actualidad y proyecciones de desarrollo del turismo internacional en Ecuador. *UNIANDES EPISTEME: Revista de Ciencia, Tecnología e Innovación, 4*(3).

Suárez, A. R., & Ruíz, F. A. (2022). Guía para el abordaje de la Norma ISO 27110:2021 creación de Marcos de Ciberseguridad. *Universidad Católica de Colombia*, 10.

Talavera Álvarez, V. R. (2015). Diseño de un sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. *Pontificia Universidad Católica del Perú*, 14.

Technology, N. I. (12 de Febrero de 2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Obtenido de https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Technology, N. I. (16 de Abril de 2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Technology, N. I. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.*

Technology, N. I. (26 de Febrero de 2024). *The NIST Cybersecurity Framework (CSF) 2.0*. Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Utreras Guerra, J. A. (2024). *Análisis e implantación de una solución de seguridad perimetral aplicando el marco de trabajo de ciberseguridad del NIST.* Quito: Escuela Politécnica Nacional.

Veridas. (11 de 2022). *¿Qué es el NIST?* . Obtenido de https://veridas.com/es/que-es-el-nist/

ANEXOS

A continuación, se presenta resultados de encuesta realizada a personal administrativo sobre las políticas implementadas en el diseño que se propone en este trabajo.

Pregunta N°1- Encuesta - Personal Administrativo	SI	NO
¿Está de acuerdo con recibir de manera periódica capacitación y talleres sobre ciberseguridad con el fin de experimentar la situación y aprender a reconocer amenazas cibernéticas?	9	0

Tabla 46 Pregunta N°1- Encuesta - Resultados Políticas

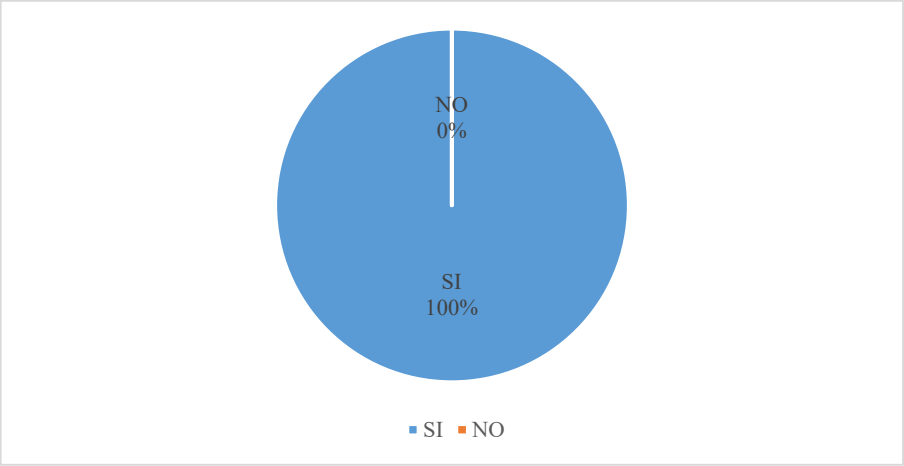

Figura 19 Pregunta N°1- Encuesta - Resultados Políticas

Pregunta N°2- Encuesta - Personal Administrativo	SI	NO
¿Está de acuerdo en que se deban monitorear y auditar a proveedores que gestionan activos críticos de información de la organización?	9	0

Tabla 47 N°2- Encuesta - Resultados Políticas

Figura 20 N°2- Encuesta - Resultados Políticas

Pregunta N°3- Encuesta - Personal Administrativo	SI	NO
¿Está de acuerdo que el software utilizado sobre los activos críticos de información de la organización deba ser licenciado y cumplir con las leyes de propiedad intelectual?	7	2

Tabla 48 N°3- Encuesta - Resultados Políticas

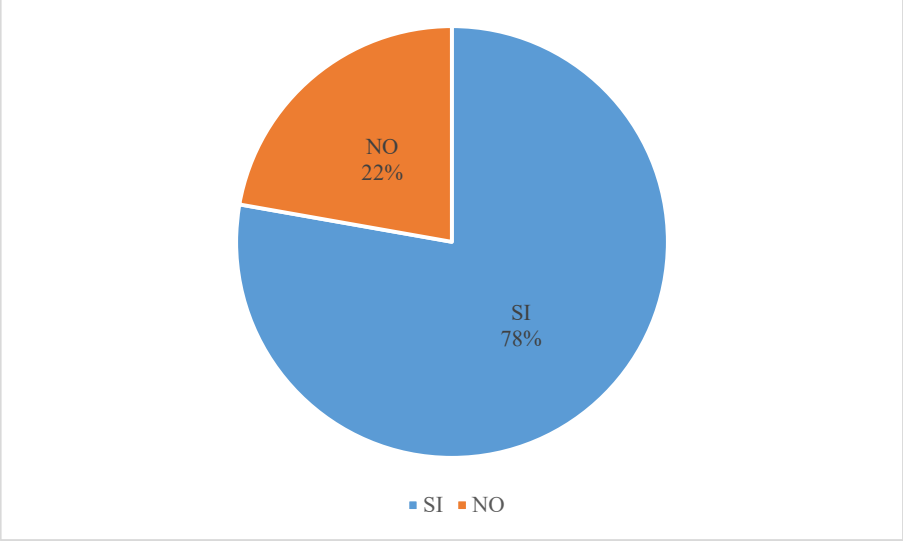

Figura 21 N°3- Encuesta - Resultados Políticas

Pregunta N°4- Encuesta - Personal Administrativo	SI	NO
¿Considera que las claves o contraseñas que usted utiliza para acceder a los activos críticos de información se adaptan a las normas de contraseñas mencionadas en la Política de Autenticación y Control de Acceso?	6	3

Tabla 49 N°4- Encuesta - Resultados Políticas

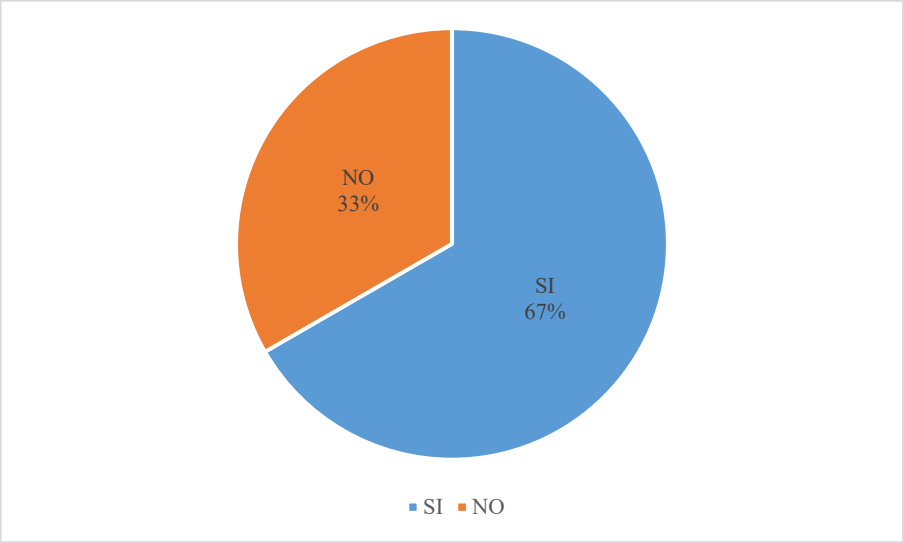

Figura 22 N°4- Encuesta - Resultados Políticas

Pregunta N°5- Encuesta - Personal Administrativo	SI	NO
¿Considera usted que la organización debe destinar presupuesto para soluciones de ciberseguridad con el fin de garantizar la integridad del activo crítico de la información ?	9	0

Tabla 50 N°5- Encuesta - Resultados Políticas

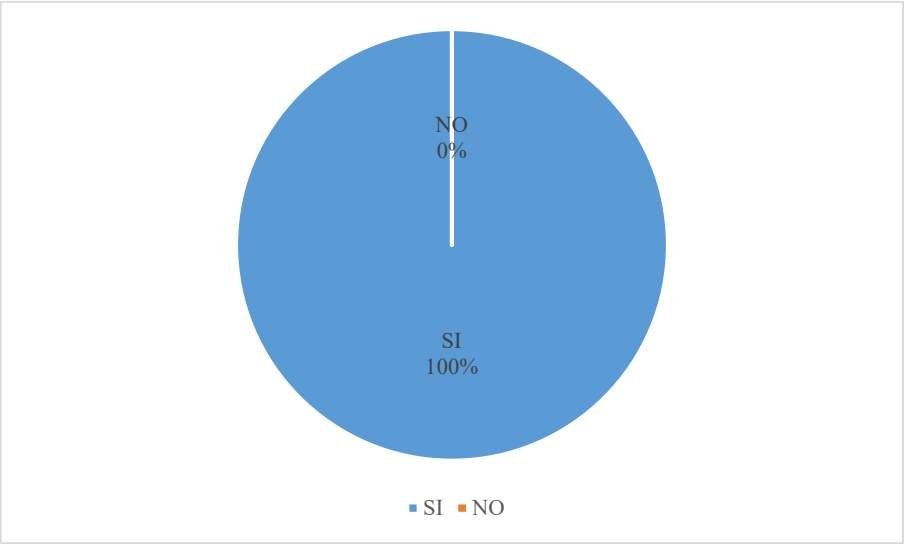

Figura 23 N°5- Encuesta - Resultados Políticas

Pregunta N°6- Encuesta - Personal Administrativo	SI	NO
¿Está de acuerdo que la conexión remota que usted utiliza para acceder a los activos de la organización este cifrada y este siendo monitoreada con el fin de auditar el tráfico de red e identificar posibles intrusiones?	9	0

Tabla 51 N°6- Encuesta - Resultados Políticas

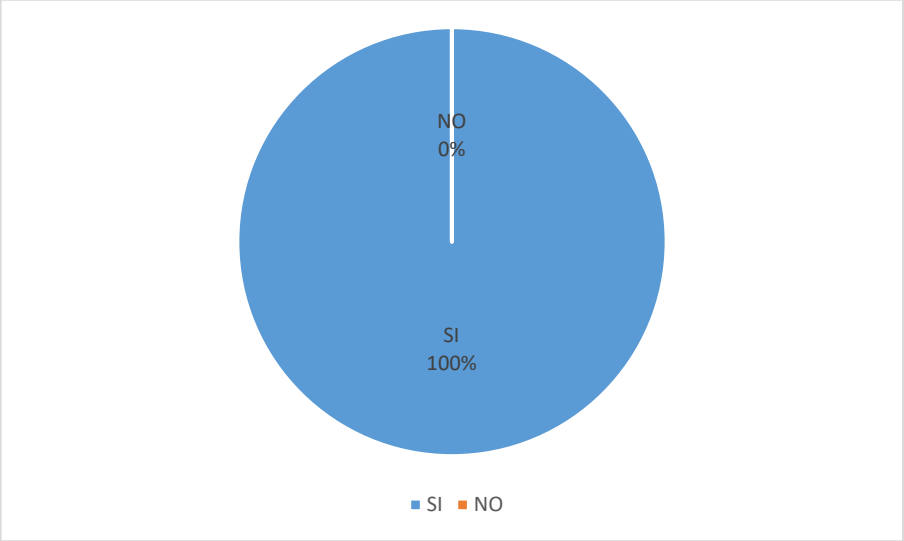

Figura 24 N°6- Encuesta - Resultados Políticas

Pregunta N°7- Encuesta - Personal Administrativo	SI	NO
¿Está de acuerdo con la norma de la Política de Identificación y Clasificación de Activo la cual indica que usted es el responsable del activo y que debe velar por la buena gestión del mismo?	7	2

Tabla 52 N°7- Encuesta - Resultados Políticas

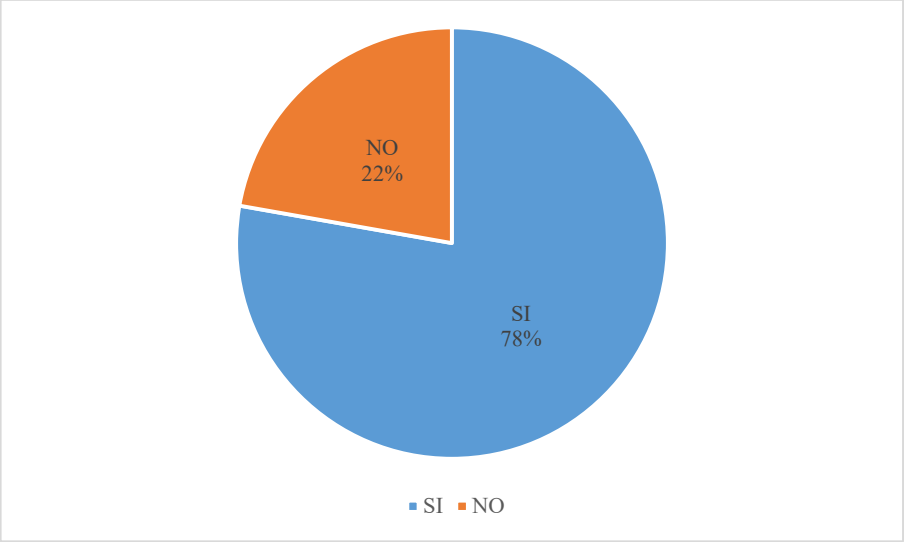

Figura 25 N°7- Encuesta - Resultados Políticas

Pregunta N°8- Encuesta - Personal Administrativo	SI	NO
¿Considera usted que las Normas NIST e ISO 27110:2021 utilizadas para la creación de las políticas, permitirá a la organización estar preparada para responder ante cualquier incidente de manera efectiva?	9	0

Tabla 53 N°8- Encuesta - Resultados Políticas

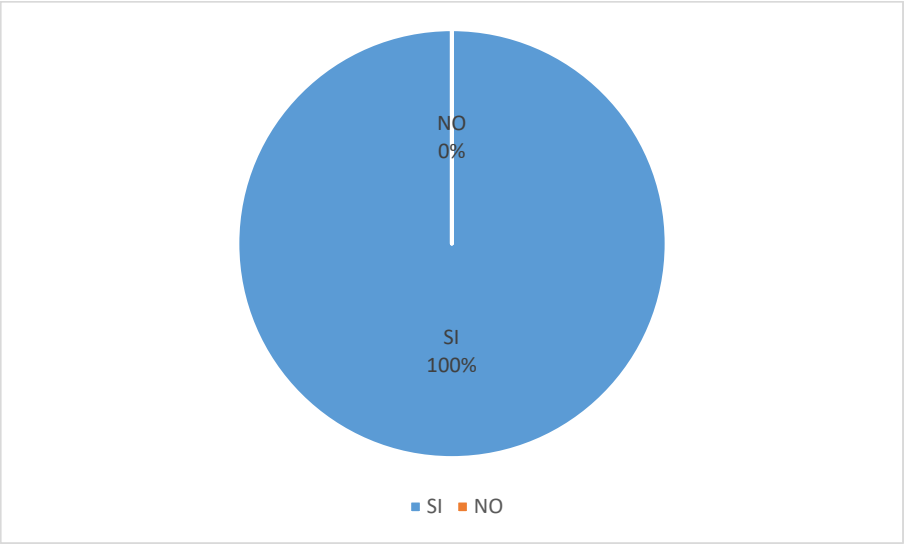

Figura 26 N°8- Encuesta - Resultados Políticas

Pregunta N°9- Encuesta - Personal Administrativo	SI	NO
¿Luego de leer todas las Políticas planteadas, sabe que directrices seguir y cómo actuar ante un ataque cibernético?	9	0

Tabla 54 N°9- Encuesta - Resultados Políticas

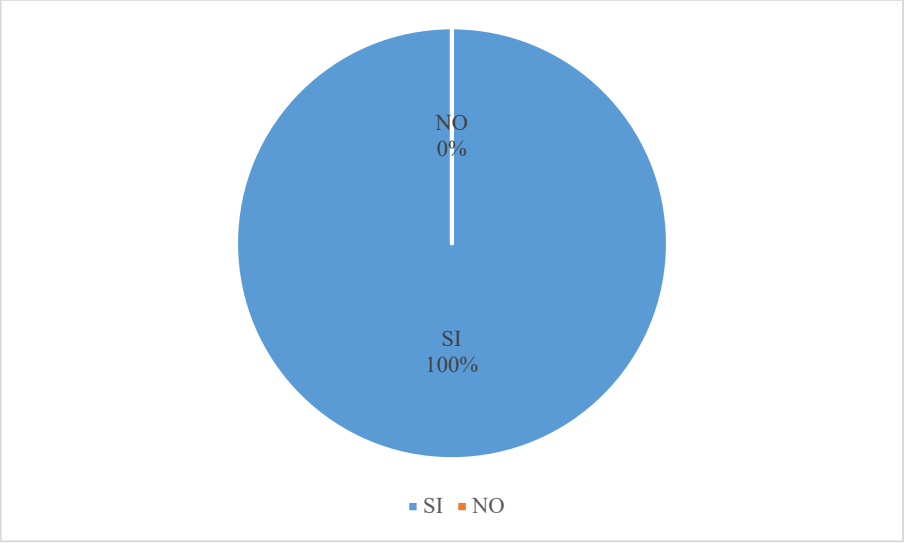

Figura 27 N°9- Encuesta - Resultados Políticas

Pregunta N°10- Encuesta - Personal Administrativo	SI	NO
¿Luego de leer las Políticas considera que el personal humano es fundamental para la ciberseguridad de la organización?	7	2

Tabla 55 N°10- Encuesta - Resultados Políticas

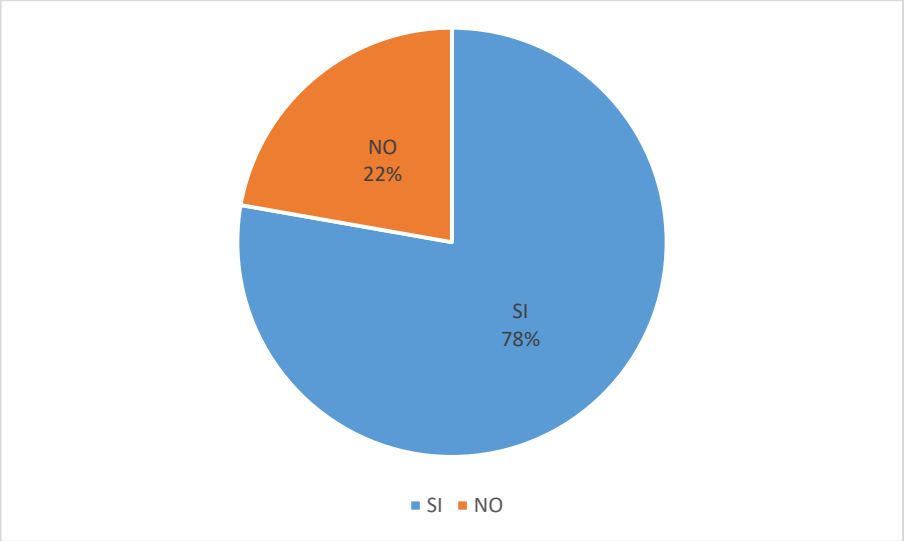

Figura 28 N°10- Encuesta - Resultados Políticas