Estrategia de seguridad ti apropiando el marco NIST con técnicas de gestión de riesgos y protección de redes para la transmisión de datos

Helber Leandro Baez Rodríguez

Asesor

Javier Medina Cruz

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Maestría en Gestión de Tecnología de Información

2025

Agradecimientos

Mención especial a los colegas (Docentes, directores, Ingenieros y Aliados) que desde su rol y conocimiento aportaron a que este proyecto se hiciera realidad y tomara el camino adecuado para el cumplimiento de los objetivos propuestos.

Dedicatoria

A todas las personas que me apoyaron, acompañaron y aportaron en el proceso. A mis hijos que son un pilar motivacional, aspecto fundamental para cada paso que doy en los proyectos propuestos, a mi madre mujer incondicional que ha estado ahí presente y a mi querida abuela que nos dejó hace poco, sin embargo, sigue presente en mi corazón.

Resumen

Generalmente se encuentran empresas que no destinan recursos a la seguridad de la información, es así como quedan expuestos a diferentes tipos de ataques que hacen que estén expuestos a que por medios de engaños les sean secuestrados sus datos, robados, o ataques que replican programas maliciosos de control de toda la infraestructura tecnológica, es así como se busca por medio del Marco de Ciberseguridad NIST (Instituto Nacional de Estándares y Tecnología) apoyar a las empresas, desde pequeñas hasta grandes compañías, a comprender los riesgos, de este modo poderlos administrar, reduciéndolos protegiendo sus redes e información.

Este marco permite ejecutar las buenas prácticas para definir en donde debe concentrar los recursos para la protección y aseguramiento de la información, con cinco fases fundamentales (Identificación, protección, detección, respuesta y recuperación). En cada fase se sugieren protocolos, técnicas y herramientas de protección que le permitirán seleccionar las más adecuadas para la organización, dependiendo del tipo de problema que este enfrentando, organizando los diferentes procedimientos para enfrentar los posibles ataques que se puedan presentar, generando confianza en que de algún modo ya tienen un norte frente a la preparación hacia posibles riesgos y vulnerabilidades que puedan afectar la gestión de los datos.

***Palabras clave*:** Seguridad, información, ataques, Marco de ciberseguridad (NIST), controles, protocolos.

Abstract

Companies that do not allocate resources to information security are often exposed to various types of attacks, leaving them vulnerable to having their data kidnapped, stolen, or attacked by malicious programs that can take control of their entire technological infrastructure through deception. This is where the National Institute of Standards and Technology (NIST) Cybersecurity Framework comes in to support businesses, from small to large companies, in understanding these risks so they can manage and reduce them, protecting their networks and information.

This framework allows for the implementation of best practices to define where resources should be concentrated for the protection and assurance of information, with five fundamental phases (Identification, Protection, Detection, Response, and Recovery). In each phase, protocols, techniques, and protection tools are suggested to help organizations select the most appropriate ones depending on the type of problem they are facing, organizing different procedures to confront potential attacks. This instills confidence that they have some direction in preparing for possible risks and vulnerabilities that may affect data management.

Keywords**:** Security, information, attacks, NIST Cybersecurity Framework, controls, protocols.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

Teniendo en cuenta la dinámica del mundo actual en temas de seguridad informática, las instituciones educativas de educación superior se encuentran en búsqueda de las mejores estrategias para el aseguramiento de la información. La gestión y protección efectiva de los datos se han convertido en prioridades críticas, especialmente con el aumento de amenazas cibernéticas sofisticadas y la creciente cantidad de información sensible que se transmite a través de redes tecnológicas. Es fundamental que estas instituciones implementen estrategias sólidas de seguridad de Tecnologías de la Información TI que no solo protejan los datos, sino que también preserven la integridad y confidencialidad de la información.

El título de este proyecto de investigación, "Estrategia de seguridad TI apropiando el marco NIST con técnicas de gestión de riesgos y protección de redes para la transmisión de datos.", encapsula la esencia de abordar este desafío mediante la aplicación de un enfoque integral y metodologías reconocidas internacionalmente.

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos proporciona un marco sólido y adaptable para la mejora de la seguridad de la información en diversos entornos, incluidas las instituciones educativas. Este marco, basado en mejores prácticas y estándares de la industria, ofrece una estructura para comprender, gestionar y comunicar los riesgos de seguridad de manera efectiva.

Al combinar el Marco NIST con técnicas de gestión de riesgos y protección de redes, se busca desarrollar una estrategia de seguridad de TI específicamente diseñada para las necesidades y desafíos únicos que enfrentan las instituciones educativas. Esto implica identificar evaluando los riesgos potenciales asociados con la transmisión de datos en entornos educativos, así como implementar controles con medidas de seguridad adecuadas para mitigar estos riesgos

de manera efectiva con técnicas de gestión de riesgos y protección de redes para abordar los desafíos de seguridad de la información en instituciones educativas. Al hacerlo, se fortalece la postura de seguridad con el fin de proteger los datos sensibles de estudiantes, docentes y personal administrativo contra las crecientes amenazas cibernéticas en el entorno educativo actual.

La protección de redes juega un papel crucial en esta estrategia, donde las redes son el eje central de la infraestructura tecnológica de una institución educativa y representan un punto crítico de vulnerabilidad si no se aseguran adecuadamente. Mediante la implementación de medidas de protección de redes, como firewalls, detección de intrusiones y cifrado de datos, se puede fortalecer la seguridad de las redes garantizando la integridad y confidencialidad de la información transmitida a través de ellas.

Planteamiento del Problema

Relación de problemáticas Internacionales

En este sentido, *"La información se constituye actualmente en un activo dentro de las instituciones sean públicas o privadas, y con el avance de la tecnología se pone en riesgo la seguridad de esta información, debido a la serie de amenazas que se presentan en el internet* (Rocha et al., 2020)*"*. Es importante que las instituciones se deben abastecer de herramientas para prevenir riesgos de seguridad.

Al respecto, s*i una empresa no administra adecuadamente su información, estará altamente vulnerable a los riesgos lo que podría afectar la continuidad del negocio* (Sulay et al., 2020). Las organizaciones deben considerar el manejo de la información como un aspecto fundamental para los intereses estratégicos.

Por tanto "Las plataformas de E-learning ofrecen numerosas ventajas a las instituciones y usuarios, su campo crece en ritmo acelerado y son considerables las iniciativas existentes para su impulso. Sin embargo, también se han detectado algunos problemas en la seguridad que dificultan su implantación en las plataformas virtuales (Roberto & Olmedo, 2020)". Se evidencia la necesidad de implementar estándares internacionales de seguridad de la información como la norma ISO/IEC 27001 enfocado en las plataformas virtuales.

Asimismo, *las medidas previenen violaciones de seguridad y garantizan la privacidad de los usuarios. Las aplicaciones prácticas incluyen políticas de contraseñas robustas, autenticación multifactorial y cifrado de datos* (Lezcano Gil et al., 2023). Donde se da gran valor a las estrategias de seguridad enfocándose en trabajar sobre estrategias y buenas prácticas de seguridad de la información.

Además, l*a información es necesaria en las empresas para el desarrollo de las estrategias organizacionales con bases sólidas, cualquier brecha de seguridad puede comprometer los datos sensibles de la organización y perjudicar gravemente a la misma* (Marreros et al., 2024). Determinando el activo de información a proteger teniendo en cuenta las herramientas digitales como elemento de valor en la protección.

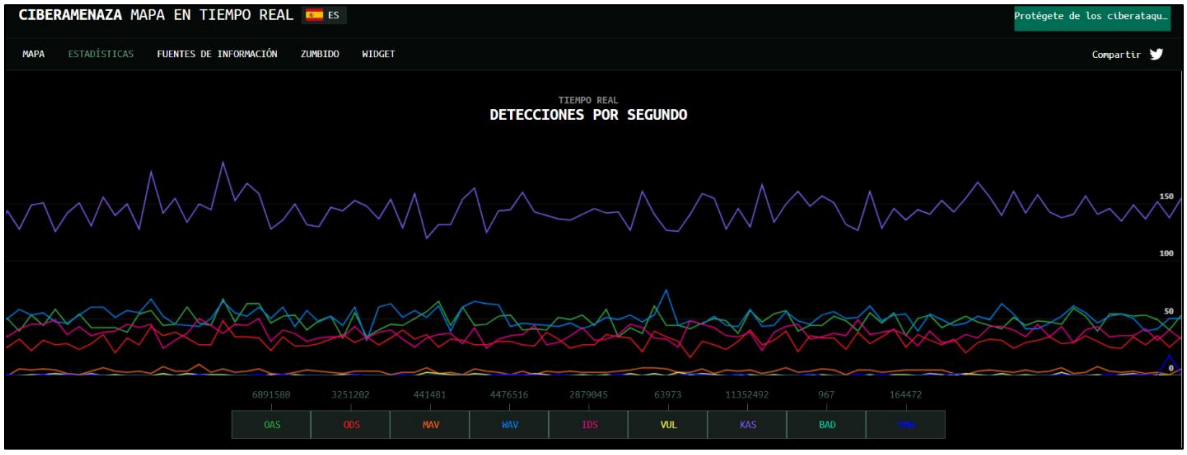
Incluso, *se establece la necesidad de herramientas innovadoras para contrarrestar amenazas híbridas en el ámbito de la seguridad de la información* (Nussipova et al., 2024). Es preciso destacar como la seguridad estable y sostenible de la información mantiene los componentes esenciales cuando se debe enfrentar a las amenazas.

Sin embargo, *En el dinámico escenario de la ciberseguridad actual, la gestión efectiva de accesos a sistemas y datos críticos es fundamental para salvaguardar la integridad y confidencialidad de la información* (Pacheco et al., 2023). El control de acceso a la información es una gran desafío para las organizaciones que tengan proyectada la inversión en la seguridad de la información sensible

A continuación, se relaciona el grafico estadístico tomado del cybermap de Kaspersky donde (kaspersky, 2024) identifica cuáles son las amenazas más recurrentes por segundo, la consulta se realiza el 01 de marzo del 2024

Figura 1

Amenazas Recurrentes a Nivel Mundial



Nota. Según los resultados el análisis más recurrente tiene que ver con el SPAM, en el segundo lugar se encuentran los virus, donde los troyanos son los más detectados. Tomado de. Ciber amenaza Mapa en Tiempo Real. KASPERSKY. (2024). https://cybermap.kaspersky.com/es/stats

Relación de problemáticas Nacionales

Al respecto, *La información es considerada actualmente uno de los recursos más importantes en las organizaciones, no solo como insumo fundamental de los procesos, sino como recurso que adecuadamente gestionado permite delimitar estrategias Organizacionales* (Carvajal Portilla et al., 2019). Es necesaria el desarrollo de una metodología que le permita a las Organizaciones establecer indicadores de gestión del riesgo y controles requeridos frente a los diferentes incidentes que se puedan presentar.

Por tanto, *La norma ISO/IEC 27001 aplica la metodología MARGERIT donde los resultados obtenidos de los cálculos de riesgos intrínseco y efectivo demuestran la presencia de salvaguardas y la evaluación de los impactos* (Guerra et al., 2021). Se menciona la necesidad de

implementar las diferentes normas y marcos de referencia con el fin de determinar el porcentaje de afectación en cada riesgo por proceso de calidad, identificando las medidas correctivas e incorporación de formatos de registros.

Asimismo, *La gestión documental es un proceso transversal encaminado a facilitar el uso de la información en las organizaciones para cumplir su objeto misional y preservar el patrimonio documental* (William et al., 2021). La información es un activo esencial dentro de la organización, por esta razón, es determinante generar un tratamiento adecuado de la misma y debe considerarse como un todo dentro de la organización.

No obstante, *se presenta un aumento notable en los casos de pérdida de datos, lo que puede resultar en grandes pérdidas económicas para las organizaciones* (Rojas Valiente et al., 2023). De esta manera, se deben evaluar el impacto al momento de implementar un modelo de gestión de seguridad con respecto a la prevención de la pérdida de datos.

En este sentido, *cualquier aparato tiene conexión a Internet, los usuarios deben ser responsables y conscientes de los riesgos que estos avances conllevan* (Rojas Bahamón et al., 2023). Se deben aplicar las políticas sobre la seguridad en el entorno digital teniendo en cuenta la legislación vigente como el Conpes, el plan TIC, entre otros.

Además, *la delincuencia aprovecha los entornos virtuales para intensificar delitos electrónicos como el phishing, las fake news y en general actividades como inyección de malware* (David Estrada-Esponda et al., 2021). Se deben generar campañas de concientización y sensibilización a los diferentes roles que interactúan en los entornos universitarios sobre buenas prácticas en la gestión de la información.

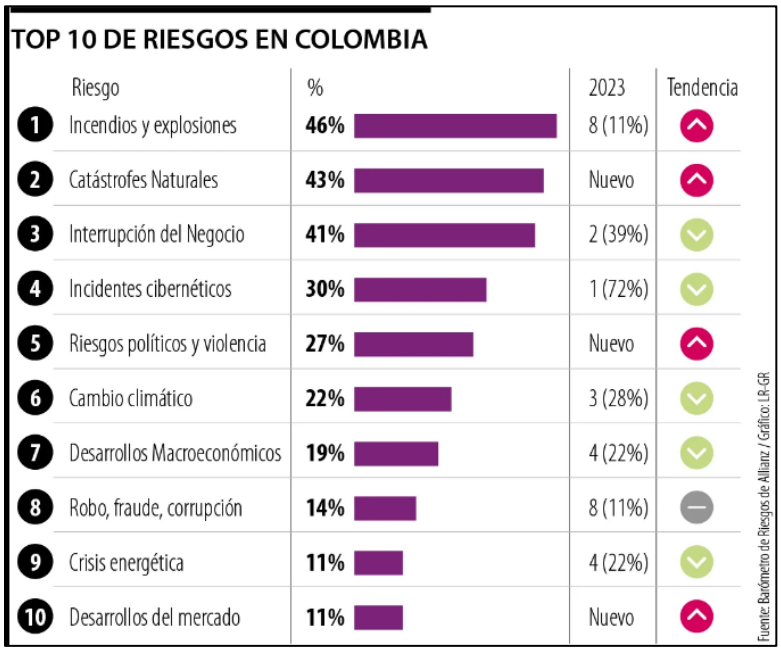
En consecuencia, *se propone un modelo de seguridad de la información bajo los principios de la gobernanza TI* (del Carmen Sagbini Echávez et al., 2024). Donde el primer paso

es desarrollar un análisis del negocio sobre los estándares requeridos de esta manera direccionar los proceso de TI con los objetivos estratégicos de la organización.

Según el diario la república (Sanchez, 2024) donde destaca el Barómetro de Riesgos de Allianz indicando "*los incidentes cibernéticos, como los ataques de ransomware, filtraciones de datos e interrupciones tecnológicas, son las mayores preocupaciones para las empresas a nivel global en 2024*".

Figura 2

Riesgos Recurrentes a Nivel Nacional



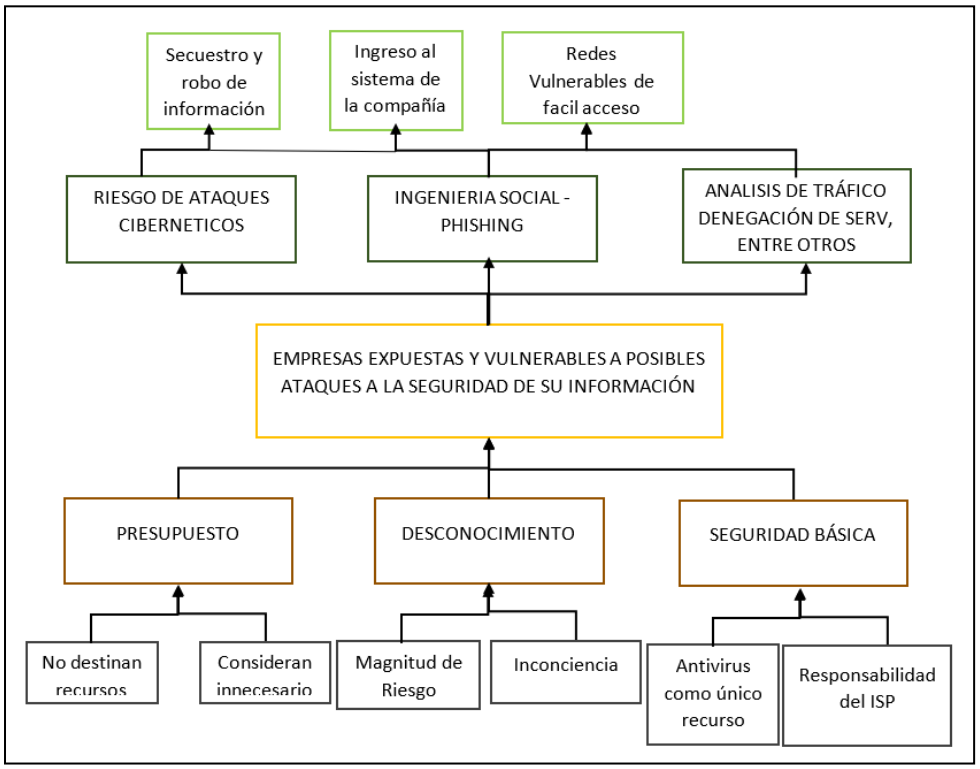
Nota. La amenaza cibernética más preocupante para los encuestados es la filtración de datos con 59%, seguida de ataques a infraestructuras críticas y activos físicos con 53% y ataques de ransomware. Tomado de. Los ataques cibernéticos serán el principal riesgo global para las empresas en 2024. Sanchez, V. (2024). https://www.larepublica.co/finanzas/los-ataques-ciberneticos-son-el-principal-riesgo-empresarial-global-para-2024-3783263

Descripción del Problema

Frente a las características desarrolladas en el planteamiento del problema se ve la necesidad de estudiar el escenario actual frente a las diferentes causas y efectos en la que una compañía puede enfrentarse, de esta manera en la Figura 3 Síntomas, causas y efectos se puede determinar el análisis frente a como las organizaciones se encuentran expuestas y vulnerables a los posibles ataques informáticos que impactan la seguridad de sus información.

Figura 3

Síntomas, Causas y Efectos



Nota. Identificación del problema central con la definición de las posibles líneas de cusas y efectos.

El problema de la seguridad informática en las empresas es una preocupación creciente debido a la frecuencia de los ataques cibernéticos y el secuestro de información, entre otros delitos, como lo documenta (Ibarra Imbachi, 2019) “Este conjunto de actividades o engaños que realizan los atacantes a las organizaciones y/o personas se usan para obtener información personal o de los bienes de las entidades utilizando las credenciales autorizadas para acceder a la información”, los cuales están perjudicando la productividad y la reputación de las compañías, todo parte de las vulnerabilidades que puedan tener en sus redes, adicional el desconocimiento de los empleados sobre las buenas prácticas para evitar que los ciberdelincuentes se apropien de sus cuentas o que por medio de sus equipos de cómputo ingresen y puedan apoderarse de los recursos o simplemente implementar ataques que destruyan los sistemas de información.

De acuerdo a lo anterior, es necesario tener en cuenta lo que menciona (Salgado & Osuna, 2019) quienes afirman que se deben establecer los parámetros a evaluar en una auditoria, teniendo en cuenta las actividades diarias, las reglas de control, entre otros aspectos que prevengan los diferentes conflictos en TI, lo anterior con el fin de salvaguardar los activos de las organizaciones, la integridad de la información, mediante políticas claras de gestión de la información y los métodos de seguridad de esta. Sin embargo, muchas compañías no realizan seguimientos adecuados al flujo de información en sus redes, lo que genera riesgos significativos para la seguridad de los datos lo cual se convierte en una problemática ya que las compañías tienden a no realizar los respectivos seguimientos al flujo de información en sus redes, generando riesgos en la seguridad de los datos.

En este sentido, las empresas se sienten seguras con las herramientas básicas, lo cual es un error, ya que por desconocimiento, pueden tener grandes vulnerabilidades sin identificar, como también, se encuentran compañías que invierten en seguridad con políticas claras de

gestión de la información, una de las estrategias que según (Benavides et al., 2020) se pueden implementar son las campañas de concientización las cuales son muy importantes para ser socializadas a los usuarios, de este modo se capacita para evitar que se usen de forma ineducada las herramientas tecnológicas y sistemas de información, también mencionan la aplicabilidad de técnicas como el MachineLearning y Deep Learning, las cuales hacen parte del mundo de la inteligencia artificial, permitiendo detectar de manera automática intrusiones a las redes de datos entre otros servicios de predicción.

Además, sobre la forma como las personas descuidan sus datos para (Sohrabi Safa et al., 2016) “Hackers target people, rather than computers, in order to create a breach; examples of user mistakes include inappropriate information security behaviour, such as taking a social security number as user name and password, writing passwords on sticky paper, sharing their username and pass-word with colleagues, opening unknown emails and downloading their attachments, as well as downloading soft-ware from the Internet.” [Los piratas informáticos se dirigen a personas, en lugar de computadoras, para crear una brecha; ejemplos de errores del usuario incluyen comportamiento inadecuado de seguridad de la información, como tomar un número de seguro social como nombre de usuario y contraseña, escribiendo contraseñas en papel adhesivo, compartir su nombre de usuario y contraseña con colegas, abrir correos electrónicos desconocidos y descargar sus archivos adjuntos, así como descargar software de Internet] (p. 70).

En consecuencia, es importante destacar la necesidad de tener en cuenta la seguridad de la información, enfatizando la importancia de mejorar los hábitos de seguridad de los usuarios, como evitar compartir contraseñas y abrir correos electrónicos desconocidos son un ejemplo de políticas que permitan concientizar al usuario con el fin de que mejore sus hábitos sobre el manejo de la información.

Por tanto, teniendo en cuenta lo que da a conocer (Esparza et al., 2020) “Una red informática puede ser vulnerada de distintas formas, tales como propagación de virus a través de las redes sociales, la facilidad de atacar e infectar dispositivos con sistemas operativos recién actualizados, uso de conectividad integrada, acoso cibernético, correo no deseado, denegación de servicio, fraude, intrusión, códigos maliciosos, spam, entre otros.” enumeran diversas formas en que una red informática puede ser vulnerada, lo que subraya la necesidad de realizar auditorías de seguridad informática para evaluar la gestión de la infraestructura TI y el manejo seguro de la información en las organizaciones. De este modo, es importante llevar a cabo una auditoria de seguridad informática que permita evidenciar como está la gestión de infraestructura TI frente al manejo seguro de la información en las organizaciones.

En este contexto, el problema de la seguridad informática en las empresas cumple con los criterios de ser interesante, relevante, vigente y factible de abordar con el método científico. Sin embargo, aún no ha sido adecuadamente resuelto, dejando un claro espacio para mejorar las prácticas de seguridad mitigando los riesgos asociados con los ataques cibernéticos.

¿En qué medida el desarrollo de una estrategia de seguridad TI, tomando como referencia el marco NIST con técnicas de gestión de riesgos y protección de redes, permitirá el control de vulnerabilidades y amenazas para las Fundación Universitaria Compensar en la ciudad de Bogotá**?**

Justificación

En el contexto actual, las entidades educativas enfrentan una creciente amenaza de ataques cibernéticos perpetrados por ciberdelincuentes que buscan secuestrar, robar información o vulnerar la seguridad de las compañías. (Ibarra Imbachi, 2019) lo menciona como una problemática para las organizaciones sobre este tipo de ataques, ejecutados mediante malware u otros programas maliciosos, tienen como objetivo principal el engaño de los empleados para acceder a la red corporativa comprometiendo la seguridad de la información. Ante esta situación, se hace evidente la necesidad de trabajar en pro de la seguridad mediante la adopción de protocolos con técnicas de protección de datos y de acuerdo con (Urrea et al., 2016) la importancia del desarrollo de sistemas de gestión de recursos.

Para abordar esta problemática, es esencial considerar la viabilidad técnica, económica y de recursos humanos para la ejecución del proyecto de investigación. Para esto se realizó una evaluación exhaustiva de los recursos disponibles, tanto tecnológicos como de personal, que garantiza la efectividad en la implementación de medidas de seguridad. Además, se analizó la importancia de apropiar este problema sobre el impacto que una solución óptima puede tener en la protección de la integridad de los datos sensibles para garantizar la estabilidad de la organización.

Al respecto, las características específicas del entorno de las entidades educativas hacen aún más imperativa la necesidad de abordar esta problemática (Albarrán, Silvia Pérez, Juan Salgado, Mireya Valero, 2019). Se llevó a cabo un análisis detallado de las amenazas actuales donde se destacó la importancia de implementar medidas de protección adecuadas en este contexto particular. Para asegurar la factibilidad del proceso de investigación, se evaluó el acceso a la información relevante, la disponibilidad de recursos sobre la viabilidad logística. Esto

garantizará la realización exitosa del proyecto con la obtención de resultados relevantes como aplicables.

Además, se espera que los resultados del proyecto contribuyan significativamente a la seguridad de las entidades educativas, como lo menciona (Barreño Gutiérrez & Lengerke, 2014) sobre la necesidad de generar escenarios de seguridad con políticas y mejores condiciones, proporcionando herramientas con protocolos para proteger la integridad de los datos de los sistemas de información de la institución. La implementación de medidas de seguridad basadas en el marco de referencia NIST permitirá comprender, administrar reduciendo los riesgos de seguridad, mitigando así la exposición de la información a posibles ataques informáticos.

En última instancia, este proyecto beneficiará a las empresas que aún no consideran la seguridad de la información como parte fundamental de su agenda empresarial (Hernández et al., 2019) consideran que las organizaciones se encuentran en riesgo y es vital generar estrategias de protección de los datos. Otro mecanismo es generar conciencia sobre las amenazas cibernéticas con herramientas para su mitigación, se espera que las entidades educativas puedan proteger sus activos de información fortaleciendo su posición en un entorno cada vez más digitalizado el cual se caracteriza por el riego de estar expuesto a los ataques informáticos.

Objetivos

Objetivo General

Desarrollar una estrategia de seguridad TI, tomando como referencia el marco NIST con técnicas de gestión de riesgos y protección de redes, para el control de vulnerabilidades y amenazas para las Fundación Universitaria Compensar.

Objetivos Específicos

Realizar un análisis diagnóstico, para la determinación de los diferentes tipos de ataques comunes que representa un riesgo alto, utilizando la técnica de análisis documental.

Diseñar los elementos de la Triada del modelo de gestión de seguridad TI, para la implementación de la estrategia, por medio de métodos de simulación con herramientas de pentesting “rapid7 Enterprise”.

Evaluar el impacto de la aplicación de la estrategia, en la determinación del mejoramiento de los indicadores de gestión en seguridad de la información, de acuerdo con la norma ISO/IEC 27001 y Guía 7 Min TIC.

Marco Referencial

Actualmente encontramos gran cantidad de virus y ataques informáticos que tienen como fin dañar la integridad de la información de las compañías, también buscan desintegrar la infraestructura de red, desprogramando todos los servicios y apoderándose de los sistemas de información, tomando control de los recursos tecnológicos de las organizaciones a nivel lógico.

En este sentido, (Benavides et al., 2020) mencionan que *un ataque recurrente en las compañías es la ingeniería social, destacan que la debilidad de los usuarios finales permiten que estos ataques sean cada vez más comunes y aplicados a este grupo de personas, es así como muestran que el Phishing es el ataque más recurrente donde por medio de páginas web falsas engañan a los usuarios con el fin de que suministren datos importantes, además que al dar clic en los enlaces hacen que se descarguen programas maliciosos en los equipos abriendo la puerta a los ciberdelincuentes.*

Al respecto, (Osorio-Sierra et al., 2020) establecen que *otro tipo de ataque común, son los relacionados con el secuestro de información o mejor conocido como "ransomware" que por medio del wannacry (programa tipo gusano dirigido al sistema de Windows que se encarga de propagarse en otros equipos), con el fin de encriptar las carpetas donde se encuentra la información, luego piden una gran suma de dinero para poder recuperarla, lo cual no hay garantía de que eso pueda pasar*.

En consecuencia, (Garcia et al., 2020) determinan *como los usuarios pueden ser víctimas de los ciberdelincuentes a través de estafas de tipo phishing, donde se engañan a las personas con el fin de que entreguen su información personal*, una de las formas más comunes es la de envíos de correos a las organizaciones donde hacen que los empleados tomen acciones frente a la

información, totalmente engañados acceden a las peticiones que allí se establecen porque el emisor es suplantado y al parecer el correo es de la organización.

Asimismo, (Rojas Valiente et al., 2023) Identifican *el aumento de los casos de perdida de datos estableciendo las consecuencias que puede generar a nivel económico en las organizaciones, a su vez, resaltan los motivos como fallos en el hardware, errores humanos, ataques maliciosos, desastres naturales, entre otros*. Lo anterior, permite identificar el impacto que pueden tener las estrategias de seguridad para minimizar el riesgo de la perdida de información.

Por tanto, (Hernández et al., 2019) Analizan *diferentes situaciones de riesgo, donde pueda verse afectada la información, basado en que los riesgos informáticos contienen dos elementos como lo son las amenazas y vulnerabilidades las cuales afectan los procesos de las organizaciones donde las consecuencias pueden resultar graves para la información generada.* Lo anterior, tiene como objetivo el de generar las diferentes estrategias para mitigar cualquier riesgo atendiendo los diferentes incidentes de seguridad que se puedan presentar con políticas claras y efectivas.

Además, (Quintero Tamayo et al., 2023) plantean *la necesidad de generar una base de conocimiento sobre incidentes de seguridad que busca mitigar las posibles vulnerabilidades de las universidades y que se tengan alternativas para actuar ante un caso que se pueda presentar en la institución.* En la actualidad existen varias plataformas con información de ataques recurrentes y actuales, sin embargo, lo que se plantea es la necesidad de generar una base de datos a la medida teniendo en cuenta las necesidades en seguridad.

Por último, (Sánchez-Sánchez et al., 2021) diseña *una herramienta que permite evaluar el estado actual de vulnerabilidades que tenga una empresa pequeña o mediana, de acuerdo con la medición sobre el nivel de seguridad se definen un esquema de recomendaciones de evaluación, mitigación y control.* Es satisfactorio evidenciar que se generan recursos de valor y de apoyo para las pequeñas empresas, las cuales no cuentan con los recursos suficientes para la inversión en seguridad.

Los anteriores son los ataques más frecuentes sin embargo también se encuentran procesos de intrusión de la infraestructura de red de las organizaciones, denegación de servicio, fuerza bruta, entre otros a los cuales también se les debe dar relevancia al momento de la búsqueda de estrategias de mitigación y gestión del riesgo.

Se debe trabajar en los controles, enfocados mediante metodologías y buenas prácticas que se ajusten a las necesidades de verificación, es así como encontramos la norma ISO/IEC 27001, estándar de seguridad de la información la cual es una de las normas que actúa como marco referencial para un buen manejo en el sistema de seguridad de la información para las compañías, teniendo en cuenta las vulnerabilidades, la gestión de los riesgos sobre los activos (sistemas de información y equipos que de algún modo tengan que ver con la gestión de datos), para luego dar a conocer los controles que se deben trabajar o implementar en la organización para asegurar la información, con el compromiso del personal y de los profesionales que manejan todas las políticas y control de los procesos y procedimientos relacionados con el manejo adecuado de la información; Metodologías como NIST las cuales establecen las buenas prácticas para comprender los riesgos, administrar, reducirlos y proteger la infraestructura de red y de datos.

Por tanto, (Leguizamón Páez et al., 2020) Indican que *los Honeypots (trampa o señuelo por medio de una red local desprotegida) los cuales son una alternativa que complementa la seguridad de las organizaciones, analizando y detectando ataques que amenazan la seguridad de la red y demás elementos de la infraestructura de red.* La estrategia es muy conocida, generalmente es usada en empresas grandes, las cuales tiene un riesgo alto por la cantidad de información que manejan.

Además, (Sotelo, 2020) *Desarrolló un clasificador que filtra líneas de logs de servidores web (registro o grabación secuencial de un archivo con todos los acontecimientos que afecten a un proceso) indicando comportamiento anómalo, este proceso reduce el tiempo de análisis, lo que lo hace un sistema ágil, obteniendo en menos tiempo, resultados referente a que logs contienen registros de comportamiento malicioso en la transferencia de datos de la red, o en eventos de procedimientos internos.* Este tipo de estrategias permiten establecer controles sobre la infraestructura de red evidenciando una ruta adecuada frente al deber ser de la seguridad de la información en las organizaciones.

En este sentido, (Guerra et al., 2021) establecen *un estudio sobre el proceso de implementación de un sistema de gestión de seguridad en un área de gran relevancia para las universidades como son las bibliotecas, de esta manera por medio de la* norma ISO/IEC 27001 *complementado con la metodología MAGERIT demuestran la presencia de salvaguardas y la evaluación de impactos.* Cuando las organizaciones aplican las normas de seguridad para desarrollar estrategias y políticas sobre el manejo de los activos, es una gran ventaja que les permite estar preparados ante un incidente o ataque informático.

Al respecto, (Carvajal Portilla et al., 2019) muestran *un claro ejemplo de cómo las medidas de protección son adoptadas por los entes gubernamentales teniendo en cuenta la norma ISO/IEC 27001 y teniendo en cuenta las guías generadas por el Ministerio de las TIC con el fin de establecer los controles necesarios, donde se obtiene el desarrollo de una metodología ajustadas a las necesidades de la entidad.* De esta manera es muy importante destacar que todos los entes del gobierno tienen una responsabilidad considerable debido al manejo de recursos públicos e información de los ciudadanos, la cual se enfoca en generar políticas para el aseguramiento de los activos de la información.

En consecuencia, (Roberto & Olmedo, 2020) verifica como *las plataformas virtuales ofrecen ventajas a los usuarios y a las instituciones educativas, también identifica problemas que se pueden presentar a nivel de seguridad de esta manera se trabaja sobre la normatividad vigente enfocada en estos espacios de trabajo con el fin de definir una marco de gestión de seguridad donde se concluye la importancia de asegurar la triada de la información y el material que se encuentre en los entornos de aprendizaje.* Las Universidades manejan estrategias de educación virtual las cuales van en crecimiento, de ahí la importancia de asegurar la disponibilidad, confidencialidad e integridad de la información.

Además, (Marreros et al., 2024) de acuerdo con el análisis referencial *se obtienen varios mecanismos desarrollados para la protección de la información organizacional, donde se identifican tres elementos de valor, el software, el hardware y las personas donde las estrategias más importantes son la gestión de contraseñas y doble factor, acceso limitado a el hardware según el tipo de usuarios y la capacitación del personal.* Se destacan las estrategias relacionadas con la capacitación, se puede tener las mejores estrategias de seguridad, sin embargo, el usuario

debe tener clara la implementación y el conocimiento de las políticas, de este modo vale la pena invertir en seguridad, un usuario puede abrir una brecha por desconocimiento.

Por último, (Esparza et al., 2020) de acuerdo con las diferentes problemáticas analizadas, *se determina que los incidentes de seguridad pueden ser mitigados por medio de la implementación de tecnologías de seguridad informática, renovación de licencias de hardware y software y capacitación al personal de seguridad dentro de la organización.* Como se puede evidenciar, las organizaciones establecen estrategias de inversión en seguridad a nivel de mejoras técnicas y de licenciamiento, monitoreo de la infraestructura TI y la capacitación del personal, lo cual es una visión asertiva frente a las amenazas del entorno.

Marco Teórico y Conceptual

Estrategia de Seguridad TI

De acuerdo con, (Pacheco et al., 2023) enfocan el concepto en donde *las estrategias de seguridad de la información pueden ayudar a salvaguardar la información sensible, teniendo en cuenta la importancia que genera para la digitalización actual.* De la misma manera (del Carmen Sagbini Echávez et al., 2024) dan a conocer *como las organizaciones tienen una mayor dependencia de las TIC (Tecnologías de la información y las comunicaciones) de manera interna en los procesos que manejan de esta manera se hace necesario implementar estrategias de seguridad basadas en los principios del Gobierno TI.* Teniendo en cuenta el planteamiento de los autores las Estrategias de seguridad permiten a las organizaciones establecer campos de acción y focalizar los entornos de protección sobre la aplicabilidad de las mismas, definiendo una ruta acorde a los objetivos y necesidades de mitigación.

Marco NIST

Según, (Handri et al., 2023) destacan los marcos de seguridad *como un factor fundamental en la protección de sistemas, infraestructura, ciberamenazas y ataques en donde predominan los componentes fundamentales del Marco NIST (identificar, proteger, detectar, responder y recuperar).* Al respecto (Safitri & Kabetta, 2023) establecen la necesidad de *llevar a cabo el diseño de un plan de riesgo cibernético sobre los activos de la organización, de esta manera el estándar de seguridad NIST es uno de los marcos principales para llevar a cabo y apoyar el proceso de identificación de vulnerabilidades.* Sobre lo anterior, se evidencia el marco de referencia NIST como un recurso de valor para el acompañamiento en el proceso de

generación de una estrategia de seguridad en las diferentes organizaciones donde se identifique la necesidad de generar un plan de aseguramiento de la información.

Técnicas de Gestión de Riesgos

Por tanto, (González H, 2018) determina el concepto de las técnicas en el momento en que *se analizan las capacidades para la detección de vulnerabilidades en aplicaciones web que proponen las principales metodologías de pruebas de penetración. El objetivo fue determinar hasta qué punto son válidos los procedimientos, herramientas y pruebas de seguridad propuestas en las metodologías*. En consecuencia, (Ricardo Ospina Díaz & Emilio Sanabria Rangel, 2020) las definen como el procedimiento donde se enfoca *particularmente en el componente de seguridad de la información, y se trabajan diversos aspectos al respecto (contextos, análisis de riesgos, sistemas de gestión y estándares de calidad) mientras se muestran los riesgos para las empresas, la sociedad y los países.* Teniendo en cuenta los conceptos de los autores, se destacan los elementos esenciales que aportan a la seguridad de la información de las organizaciones con el fin de desarrollar aspectos como (Evaluación de riesgos, tratamiento, controles, monitoreo y generación de planes).

Control de Vulnerabilidades

Al respecto, (Camero D, 2020) indica los elementos necesarios para el control de vulnerabilidades el cual se basa en *El modelo que consta de 3 fases: 1. Hacer el inventario de activos de información de la empresa, para poder realizar el análisis de riesgos de cada uno de ellos; 2. Evaluar el tratamiento que se debería dar a cada riesgo; 3. Una vez implementados los controles, diseñar indicadores que ayuden a monitorear las salvaguardas*

implementadas. Asimismo, (Diéguez M, 2021) identifica la necesidad de realizar controles debido a que *las organizaciones se han visto obligadas a definir y aplicar un conjunto de contramedidas que, basadas en criterios de expertos, permiten asegurar sus activos de información frente a ataques casuales o deliberados. Sin embargo, estas medidas se están demostrando insuficientes ante el aumento de ataques en el mundo*. Las definiciones permiten establecer la necesidad que tienen las organizaciones de aplicar medidas frente a los diferentes ataques informáticas basadas en políticas que permitan asegurar la información de manera eficaz.

Análisis Diagnóstico

En este sentido, (Chóez I, 2023) establece que *los análisis se realizan con la finalidad de verificar errores en la red, y realizar el mejoramiento en la misma, teniendo en cuenta las características, ventajas y desventajas de los recursos que se necesitaron*. Mientras que (Lorusso G, 2022) destaca que los análisis *surgen la necesidad de implementar nuevas herramientas de protección informática, de las cuales han destacado los "**Honeypots"**. Estos últimos ha tomado relevancia, además de proteger, proporcionar seguridad; se consideran sistemas de tipo "**trampa**" que sirve para observar los diferentes comportamientos de ciberataques para posteriormente analizar la intrusión, los métodos que se utilizaron.* Las reflexiones de los autores destacan la necesidad de implementar métodos y herramientas que contribuyan a la seguridad de la información de las organizaciones enfocado en la seguridad de la red.

Protección de Redes

En consecuencia, (Reyes H, 2020) recomienda la importancia de configurar los equipos de red de manera segura teniendo en cuenta que *los posibles atacantes pueden usar herramientas de escaneo, como Wireshark, para capturar dichas tramas y extraer información sobre las características de seguridad para descubrir vulnerabilidades*. De igual importancia, (Chillagana et al., 2023) destaca como en la seguridad de redes *es de vital importancia para conservar la integridad de los datos, disponibilidad de servicios, protección de la privacidad y sobre todo la protección contra amenazas cibernéticas, por tanto, la incorporación de mecanismos de seguridad es esencial y obligatorio.* En general, las organizaciones deben establecer mecanismos de control generando estrategias frente a los incidentes de seguridad que se puedan presentar enfocado en la infraestructura de red y los servicios implementados.

Amenazas

Entre tanto, (Balseca-Chávez et al., 2021) expone que *el uso masivo de las Tecnologías de la Información y Comunicaciones ha ocasionado la interdependencia de la sociedad respecto de estas; sumado a la ausencia de controles eficientes y efectivos a nivel general, incrementan la exposición a los ataques o amenazas informáticas, a las vulnerabilidades en los activos de información de las organizaciones.* De forma similar, (Pozo C, 2023) considera que *las amenazas y ataques en la red son cada vez más sofisticados y sus consecuencias más costosas para las personas y empresas.* Teniendo en cuenta lo que establecen los autores, las amenazas pueden afectar a las organizaciones con un impacto alto si no se tienen en cuenta los controles generando costos incalculables afectando los activos de información.

Tipos de Ataques Comunes

De acuerdo con, (Pantoja N, 2020) determina el punto de partida *sobre una necesidad de obtener más información en cuanto a ataques informáticos se trata, ya sean ataques de denegación de servicios o también ataques cross site scripting, entre otros más*. De la misma manera, (Leguizamón Páez et al., 2020) menciona estrategias como elementos que complementa *el servidor IDS (Intrusion Detection System), permitiendo con los registros almacenados crear reglas e implementarlo en Iptables. Este hecho permite que el servidor IDS se convierta en un nodo en una red de sensores que alimentan la base de datos globalmente para una investigación de los ataques en todas las computadoras conectadas y configuradas, obteniendo información para realizar un análisis complejo para el usuario final.* Para los autores, cualquier tipo de ataque genera alertas que deben ser tenidas en cuenta, con el fin de realizar el respectivo seguimiento recolectando la información, de esta forma analizar las posibles soluciones que a su vez deben ser efectivas.

Técnica de Análisis Documental

Según, (Martínez-Corona et al., 2023) la revisión y el análisis documental hace parte de *la calidad de una investigación se denota por esta cualidad en cada de sus etapas. El asumir una actitud de rigurosidad en cada tarea, como lo es la revisión documental, es una muestra del compromiso investigativo. Desarrollar competencias investigativas es un aspecto relevante para el profesor universitario.* Al respecto, (Chaparro-Prieto A, 2024) enfoca el concepto en la gestión del conocimiento el cual lo define como *un proceso fundamental para las organizaciones, ya que permite maximizar el capital intelectual, potenciando así la innovación y mejorando la competitividad. En instituciones de educación superior, la gestión del conocimiento se torna*

esencial para la promoción de la excelencia académica, más aún cuando se considera la variabilidad del entorno en el cual se encuentran inmersas estas organizaciones. Sobre lo anterior, se considera que la fortaleza de una investigación es el análisis de la documentación y evidencias, de esta manera, se tiene claridad sobre la aplicación de la gestión del conocimiento como aporte esencial al desarrollo de las instituciones universitarias.

Elementos de la Triada

Por tanto, (Pulgar & Quiñones, 2022) determinan *la asimilación de los delitos informáticos tipificados por el legislador con los delitos de impacto, para demostrar que los tipos penales de carácter informático requieren un tratamiento diferencial, mayor conocimiento y estrategias tendientes a mejorar las medidas de prevención y autoprotección de la sociedad.* En consecuencia, (Carvajal Portilla et al., 2019) la seguridad de la información está relacionada con *la integración de estándares internacionales de seguridad de la información y su contextualización en un ámbito gubernamental, dando respuesta a requerimientos regulatorios y permitiendo una vez finalizada la implementación, contar con un desarrollo metodológico pertinente que le permite a la organización pública desarrollar de forma continuada los procesos de gestión de seguridad de la información.* Los aportes de los autores permiten destacar la importancia de fortalecer la disponibilidad, la integridad y la confidencialidad de la información por medio de estrategias y normativas, las cuales, permiten generar un buen modelo de seguridad de la información sobre la infraestructura tecnológica de la organización.

Modelo de Gestión de Seguridad TI

Al respecto, (Ñañez, 2020) destaca el *modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, para mejorar la gestión de seguridad de la información sobre la evaluación de los riesgos y el tratamiento de estos; para cada uno de los activos de TI*. Asimismo, (Marchand-Niño & Vega Ventocilla, 2020) mencionan *en diversos sectores de las actividades humanas, las organizaciones están adoptando con mayor intensidad las tecnologías de la información TI. De este modo, exponen datos sensibles y confidenciales de empleados y clientes se formula un modelo de Cuadro de Mando Integral que vincula a los controles críticos de seguridad del CIS.* Los modelos de gestión permiten a las organizaciones establecer la ruta adecuada desde la identificación de activos hasta la generación de políticas y controles a las posibles vulnerabilidades, amenazas y la evaluación de riesgos. De esta manera la aplicabilidad de normas y metodologías como la norma ISO/IEC 27001, 27005, NIST, COBIT, entre otras, son de gran aporte para el desarrollo del modelo de seguridad.

Métodos de Simulación con Herramientas Pentesting

En este sentido, (Ferruzola Gómez et al., 2022) desarrollan pruebas teniendo en cuenta el *análisis sobre el uso y la efectividad de los sistemas centralizados en la seguridad informática con el objetivo de mostrar que con esta herramienta libre podemos hacer un monitoreo de amenazas, para el efecto se hizo un estudio general de la herramienta informática utilizada para proteger información denominada ALIENVAULT OSSIM.* Mientras que, (Sánchez-Sánchez et al., 2021) *diseña una herramienta que permite evaluar el estado actual de vulnerabilidad informática que tiene una pequeña y mediana empresa (PYME) a partir de la medición del nivel de seguridad de su software. Se definen y describen las componentes de la herramienta que,*

apoyado en la base de datos de vulnerabilidades y exposiciones comunes (CVE), ofrece un mecanismo para la evaluación eficaz del riesgo cibernético y un esquema de recomendaciones. Se evidencia el uso de herramientas de uso libre o desarrolladas con el fin de diagnosticar los sistemas organizacionales, de esta manera se genera un mecanismo de protección mediante el monitoreo constante del flujo de información en la red escaneando los servicios sobre la búsqueda de vulnerabilidades, mediante el escaneo de puertos o métodos que complementen el desarrollo de las diferentes pruebas.

Los enfoques de la investigación

En consecuencia, (Rodríguez, 2024) *analiza diversas perspectivas epistemológicas, tales como el positivismo, constructivismo y realismo, destacando su impacto en la formulación de preguntas de investigación y la interpretación de los resultados. Método: A partir de una revisión de la literatura sobre el tema, se sistematizan conceptos y postulados que demuestran la importancia de la epistemología en el marco de la investigación científica. Resultados: Al examinar los enfoques de investigación, se detalla el análisis de los paradigmas cualitativos, cuantitativos y mixtos, señalando sus características distintivas y aplicaciones específicas*. De igual importancia, (Carmona Rojas, 2020) aplica los enfoques de investigación donde *analiza los enfoques y perspectivas de la investigación sobre el problema del transporte informal en América Latina. Con base en la revisión de documentos académicos e institucionales, el texto da cuenta de la transformación en el abordaje del transporte informal en las últimas décadas. En la misma medida, sugiere que la falta de estudios de síntesis sobre el tema es un claro indicador de la posición subordina que este ha tenido con respecto a asuntos urbanos como la vivienda o el empleo.* Se refleja en los estudios, la dinámica de la investigación sobre la apropiación de

elementos que contribuyen a establecer el camino de recolección y de identificación de información sobre la problemática planteada partiendo de una necesidad de un sector como en el caso planteado en esta investigación.

Diseños de Investigación

Entre tanto, (Vergara, 2024) determina la ruta del diseño de investigación en dos puntos relevantes *en primer lugar, describimos las técnicas previstas y su forma de implementación junto con los obstáculos y cambios contextuales; en segundo lugar, damos cuenta de la reformulación del trabajo de campo y, finalmente en las Consideraciones Finales esbozamos posibles interpretaciones*. De forma similar, (Pereira Burgos, 2024) resalta el diseño de investigación sobre dos puntos, *la primera, que existen estudios donde se usan varios diseños, pues alguno de los objetivos puede tener abordaje documental mientras que otro puede tener un abordaje de campo, en este caso hablamos de estudios en su mayoría mixtos pues mezclan técnicas cualitativas y cuantitativas.* Lo anterior, establece la secuencia lógica del diseño de una investigación teniendo en cuenta de manera clara los elementos de análisis, recolección y resultados sobre los datos obtenidos producto de la indagación la cual es la base para continuar con el proceso de desarrollo de la problemática planteada.

Técnicas de Análisis de la Información (cuantitativa y cualitativa)

De acuerdo con, (Sánchez Solís & Coto Jiménez, 2021) indican que, *con el advenimiento de la Inteligencia Artificial, se ha observado cómo distintas técnicas relacionadas con el aprendizaje automático y la optimización se han incorporado a estas tareas de predicción, con las cuales se obtienen generalmente mejores resultados en los valores estimados que aquellos*

generados a partir de técnicas más tradicionales. De la misma manera, (Arenas Grisales et al., 2022) Determinan la ruta de investigación sobre *el método implementado en la investigación tuvo un enfoque principalmente cualitativo, se usaron tres técnicas de investigación: 1) el análisis de redes sociales de la producción científica, 2) la consulta de comunicados de organismos multilaterales e instituciones del área, el análisis de fuentes de mercado y 3) el desarrollo de entrevistas en profundidad con especialistas en el tema.* Se puede evidenciar los dos escenarios que se plantean sobre las técnicas tradiciones sobre el enfoque investigativo y la implementación de la IA para obtener resultados a nivel predictivo lo que permite mejores resultados sobre los valores estimados.

Metodología

El enfoque de la investigación es mixto, la cual nos permite analizar los datos para luego representarla por medio de tablas, protocolos de acuerdo con los registros y resultados que se den durante las pruebas de algunos ataques, estas tablas mostraran los registros de las bases de datos, como también los datos de las diferentes pruebas del prototipo en el momento de la detección del intruso. En donde se tendrán en cuenta la parte cuantitativa para determinar los datos más representativos a nivel de ataques, vulnerabilidades, riesgos y en general de seguimiento de las redes de la organización. Cualitativamente se tendrán en cuenta los diferentes fenómenos o tipos de ataques más recurrentes, entre otros aspectos relevantes para el análisis de la problemática planteada y de este modo alcanzar el objetivo propuesto.

En este sentido, la Investigación aplicada permite dar un enfoque frente a la realidad, relacionado con aquellas problemáticas que se evidencian en los procesos organizacionales y en donde se busca desarrollar el proyecto aplicando los parámetros el Método Experimental con sus pilares fundamentales (La reproducibilidad y la falsabilidad), donde se controlan las variables para realizar la delimitación de los resultados, basado en la metodología científica. Teniendo en cuenta las variables dependientes de trabajo.

Al respecto, el enfoque cuantitativo se centra en la recolección, análisis de datos numéricos y objetivos, con el fin de identificar patrones o relaciones entre las variables. En la estrategia de seguridad, los datos cuantitativos pueden incluir la cantidad de ataques, vulnerabilidades detectadas, puertos abiertos, porcentajes de éxito de las medidas de seguridad, entre otros.

Además, las variables dependientes son aquellas que el investigador mide y están sujetas a los cambios provocados por la manipulación de las variables independientes. En el contexto de la seguridad de la información, las variables dependientes pueden ser los resultados de los análisis de vulnerabilidades, como el número de intrusiones detectadas o la cantidad de puertos inseguros identificados. Las variables independientes son las que el investigador controla o manipula para observar cómo afectan a las variables dependientes. En un modelo de gestión de seguridad, las variables independientes podrían incluir la implementación de diferentes controles de seguridad (como firewalls o sistemas de detección de intrusiones), configuraciones de red, y otras medidas para proteger la red de la organización.

Asimismo, la variables intervinientes o extrañas son no controladas por el investigador que pueden influir en el resultado de la investigación, generando sesgos o alteraciones en los datos. Sobre el proyecto de seguridad, las variables intervinientes pueden incluir fluctuaciones en el tráfico de red, cambios en la configuración del sistema, o factores externos como ataques no previstos.

En consecuencia, frente al enfoque cualitativo se enfoca en la descripción de fenómenos no numéricos, observando y analizando el comportamiento, experiencias o situaciones. En el contexto de investigación en seguridad, este enfoque se utiliza para estudiar fenómenos como los tipos de ataques más recurrentes, el comportamiento de los atacantes, o la respuesta organizacional ante incidentes de seguridad.

Al respecto, los ámbitos de indagación en la investigación cualitativa abarcan las áreas o dimensiones donde se exploran los fenómenos. Estos ámbitos pueden incluir la percepción de los empleados sobre la seguridad de la red, el análisis de los tipos de ataques frecuentes, y el estudio de las políticas de seguridad implementadas. En tanto, las categorías de análisis se refieren a los

temas o conceptos clave que se extraen de los datos cualitativos para ser analizados y comparados. Estas categorías pueden incluir: tipos de ataques, vulnerabilidades más comunes, métodos de prevención implementados, y políticas de respuesta ante incidentes.

Además, la triangulación como técnica permite utilizar múltiples fuentes o enfoques para analizar un mismo fenómeno obteniendo una visión más completa y confiable. En la triangulación entre variables y categorías, se cruzan los datos cuantitativos (por ejemplo, la cantidad de ataques) con los cualitativos (como el análisis de los tipos de ataques o las experiencias de los usuarios) para validar y fortalecer los hallazgos del estudio. De este modo, se puede obtener una visión más integral de las vulnerabilidades y las estrategias de protección en la organización.

A su vez, este enfoque mixto en la investigación permite abarcar tanto la parte numérica (ataques detectados, vulnerabilidades, entre otros.) como la parte descriptiva (tipos de ataques, comportamiento de los intrusos), lo cual es clave para analizar la efectividad de un modelo de seguridad de la información en una organización.

Hipótesis

El Desarrollo de una estrategia de seguridad TI tomando como referencia el marco NIST con técnicas de gestión de riesgos y protección de redes permitirá controlar las vulnerabilidades y amenazas en la institución de educación superior “CASO DE ESTUDIO SEDE PRINCIPAL”, la anterior es la población sobre la base de que primero se realizara en un entorno de prueba, la muestra se enfoca en un ambiente de la universidad donde se concentra la mayoría de sus redes y sistemas de información.

Población y Muestra

La población incluye a todos los administrativos y estudiantes de la universidad para la percepción de seguridad y el manejo de la información por parte de la institución el departamento de TI tuvo en cuenta al personal activo y estudiantes matriculados con el correo institucional habilitado

Sobre la muestra seleccionada para el estudio es de 500 personas. Dado que la encuesta fue enviada a través del correo institucional, se podría inferir que la muestra es no probabilística por conveniencia donde según, (Taleb et al., 2023) la definen como la forma *which involves selecting sample units based on their accessibility to the selector, which could be influenced by various factors such as geographic proximity, availability during the study period, or willingness to participate in the analysis*. Debido a que se seleccionó a quienes respondieron a la invitación en función de su disponibilidad y la disposición en desarrollar el instrumento enviado de forma voluntaria.

En consecuencia, tomando como base lo descrito según (Pérez, s.f.) de la OBS Businees School es importante que durante el desarrollo del Proyecto se trabaje con el siguiente enfoque teniendo en cuenta las fases descritas en la Tabla 1, se toma como referencia varios documentos, sin embargo, se enfoca en las fases de acuerdo con las necesidades del prototipo estructurados como se evidencia en la siguiente tabla.

Tabla 1

Fases del Proyecto y del Procedimiento

Fase	Descripción
Analizar	Análisis de las necesidades de las organizaciones en cuanto a la seguridad de su infraestructura TI Análisis de los tipos de ataques más recurrentes que afectan la seguridad de la información
Planear	Planeación de las estrategias a implementar bajo la norma ISO/IEC 27001 y NIST
Diseñar	Diseño de los procedimientos de gestión de seguridad de la información y de protección de esta
Pruebas	Prueba de pentesting sobre posibles vulnerabilidades de la información con las diferentes herramientas.
Evaluar	Evaluación de los procedimientos mediante seguimiento de las técnicas utilizadas.
Ejecución y Verificación para nuevas pruebas	Ejecución y verificación, corrección de las posibles fallas presentadas durante el proceso y que limitaron las técnicas utilizadas.

Nota. Los procedimientos se desarrollan teniendo en cuenta las fases de la tabla con el fin de llevar a cabo las pruebas proyectadas

Al respecto, es un proyecto de investigación general, el cual será una guía de apoyo para las organizaciones que aún no ven la seguridad informática como algo de gran relevancia para la compañía, o para las que presentan inconvenientes con comprender el tema y no tienen la claridad de como empezar para la ejecución de procesos de protección de la información, se

empleara la metodología ágil (Scrum) como insumo de apoyo para la optimización del proyecto, donde se desarrollan reuniones periódicas con los diferentes actores involucrados en cada una de las fases. Teniendo en cuenta el concepto de scrum según (Onieva, 2018) método en el cual se trabaja por etapas o fases, donde por medio de procesos se gestionan proyectos y se motiva al grupo de trabajo, logrando eficiencia y mejorar continúa cumpliendo con el tiempo estipulado.

Instrumentos de recolección de datos

La encuesta en línea fue diseñada para recoger datos de manera eficiente promoviendo la participación de la comunidad educativa, utilizando el correo institucional como medio de envío. Este canal permite una comunicación directa, de confianza, asegurando que todos los miembros de la universidad tengan igual acceso a la encuesta donde puedan responder desde cualquier dispositivo con acceso a internet. La encuesta incluye preguntas cerradas, con una escala Likert (opciones de respuesta graduadas) para evaluar el nivel de percepción de la seguridad de la información, y preguntas abiertas para captar observaciones personales y detalladas. Este diseño mixto facilita la recolección tanto de datos cuantitativos, que pueden ser medidos y comparados objetivamente, como de datos cualitativos, que permiten explorar percepciones y experiencias específicas.

Instrumentos Cuantitativos y Cualitativos

El uso de una encuesta en línea distribuida por correo institucional es coherente con el enfoque mixto de este estudio, ya que permite la integración de instrumentos cuantitativos y cualitativos en un solo medio. Las preguntas cerradas proveen un enfoque cuantitativo al permitir el análisis de datos numéricos, mientras que las preguntas abiertas facilitan la recolección de

datos cualitativos al captar el contexto y los matices de las experiencias de los participantes. Este diseño mixto es adecuado para estudios de percepción en seguridad de la información, pues permite identificar tanto patrones numéricos generales como insights profundos (comprensión detallada sobre un tema) en las experiencias individuales, necesarios para comprender la complejidad del tema desde diferentes perspectivas.

Técnicas de Análisis Cuantitativo y Cualitativo

De acuerdo con el análisis cuantitativo para los datos obtenidos de las preguntas cerradas, se utilizan estadísticas descriptivas tales como promedios, frecuencias y desviaciones estándar. Esto permitirá observar las tendencias generales en las percepciones de seguridad, comparando el nivel de conocimiento sobre la práctica de seguridad en la Institución. Además, se llevará a cabo un análisis inferencial para identificar si existen diferencias significativas entre los grupos encuestados, en cuanto a su percepción de seguridad. Técnicas como la prueba t (comparativo de dos grupos) para muestras independientes serán útiles para contrastar estas diferencias y validar si se presentan de manera consistente en la muestra.

A su vez, en el análisis cualitativo las respuestas abiertas se analizarán mediante técnicas cualitativas como la codificación, donde se clasificarán las respuestas en categorías o temas que reflejen preocupaciones recurrentes, como la falta de capacitación o la exposición a riesgos. Posteriormente, se realizará un análisis de contenido para evaluar la frecuencia con la relevancia de los términos o frases relacionados con amenazas sobre las prácticas de seguridad, lo que permitirá identificar patrones obteniendo insights profundos sobre las experiencias de los encuestados en torno a la seguridad de la información.

Preguntas

Para abordar tanto los aspectos técnicos como perceptivos, la encuesta incluirá preguntas como tiempos de respuesta en navegación en Internet las cuales permiten entender cómo perciben los usuarios el rendimiento de los sistemas en términos de acceso y uso diario, lo cual puede influir en la seguridad si las demoras llevan a conductas de riesgo (como omitir pasos de verificación). Otro tipo de preguntas de orden lógico como el rendimiento de los equipos que busca identificar problemas de rendimiento que puedan ser indicativos de amenazas a la seguridad, como infecciones por malware o uso indebido de recursos, que afectan la percepción general sobre la seguridad de los sistemas y la información.

Procesos llevados a Cabo para el Desarrollo del Proyecto

Las instituciones educativas en Colombia son cada vez más vulnerables a los ataques informáticos, lo que puede resultar en la exposición de información confidencial, interrupción de operaciones diarias, daños financieros y reputacionales significativos. Los ataques más comunes incluyen las técnicas de ingeniería social de la cual hace parte el phishing, así también los tipos malware como ransomware y ataques de denegación de servicio distribuidos (DDoS).

En tanto, para evitar estos ataques, las instituciones educativas deben invertir en la seguridad de los sistemas informáticos capacitando a los usuarios en gestión de riesgos y seguridad cibernética. La educación y la concientización también son clave para mantener la seguridad de la información. Además, incluir la ciberseguridad como tema de estudio en universidades y centros de formación puede ser clave para mejorar la seguridad informática en el sector educativo.

Además, las instituciones han invertido poco presupuesto en ciberseguridad, lo que las convierte en un blanco fácil y atractivo para los ciberdelincuentes. Es necesario que las instituciones educativas aumenten la visibilidad de su postura de ataque para mejorar su ciberseguridad. La información que estas entidades salvaguardan tiene que ver con registros académicos, calificaciones, hojas de vida de docentes, programas y archivos. Los cibercriminales buscan robar identidades, datos personales de estudiantes, docentes y demás trabajadores, información financiera, datos de proveedores de las instituciones educativas, plagio de proyectos e investigaciones. Asegurar el entorno de TI en las organizaciones educativas permitirá no solo proteger la integridad de los datos de todos sus miembros, sino también promover el alto desempeño que requieren para empoderar a los alumnos y docentes.

En este sentido el sector educativo ha experimentado un aumento en los ciberataques en los últimos años, lo que ha expuesto información confidencial de la comunidad educativa, ha paralizado sistemas y ha causado pérdida de datos. Estos ataques pueden provenir de diferentes fuentes, como estudiantes, exalumnos, hackers externos y grupos organizados, uno de los objetivos comunes es obtener acceso a información financiera y personal de los estudiantes para cometer fraudes o robo de identidad.

No obstante, (Sociedad et al., 2021) indica que *los riesgos han aumentado la necesidad de que las instituciones educativas implementen soluciones digitales para la educación a distancia*, lo que ha hecho que sean más vulnerables a los ataques cibernéticos. Por lo tanto, es importante que las instituciones educativas en Colombia tomen medidas de seguridad informática adecuadas para protegerse contra estas amenazas potenciales. Algunas medidas que se pueden implementar incluyen, La implementación de políticas de seguridad de datos, La actualización regular de los sistemas de software y la capacitación a la comunidad educativa sobre cómo proteger sus datos personales y prevenir técnicas relacionadas con la ingeniería social como lo es phishing.

De acuerdo con esta necesidad, se genera la estrategia con los actores participantes del proyecto la Fundación Universitaria Compensar, el aliado JETURING división SEGRD y los Docentes Investigadores, con el fin de establecer las actividades que permitan cumplir con los objetivos del proyecto, en la tabla 2 Se describen cada una de ellas

Tabla 2

Actividades Desarrolladas en las Diferentes Fases del Proyecto

Fecha	Actividad	Descripción
Marzo 2023	Desarrollo de encuesta inicial de percepción de seguridad por parte del Departamento TI de la Institución	Mediante el correo institucional se desarrolla la encuesta a la comunidad educativa (Ver Apéndice A)
Marzo 2023	Análisis inicial y perfilado OSINT "DNS" "pruebas bloques IP"	Análisis Estructura de Red Proyección de análisis de verificación con los respectivos acuerdos de confidencialidad. (Ver Apéndice B)
Mayo 2023	Visita aliado de la Empresa Jeturing – SEGRD promoción y pruebas iniciales	Visita Experto alistamiento y configuración de equipo para acceso y desarrollo de pruebas de verificación de red. (Ver Apéndice C)
Junio 2023	Reunión y resultados de la auditoria	Presentación Informe de resultados (Ver Apéndice D)
Octubre 2023	Sobre las vulnerabilidades encontradas se presenta propuesta de controles	Por medio de la matriz de riesgos se dan a conocer algunas sugerencias generales sobre los controles que puede implementar la institución para mitigar los riesgos.
Durante el transcurso del proyecto	Capacitaciones y charlas a la comunidad educativa	Talleres Conferencias Charlas Comunidad Educativa (Ver Apéndice E)

Nota. Etapas de validación y resultados describiendo las evidencias recolectadas

Diagnóstico de la Situación

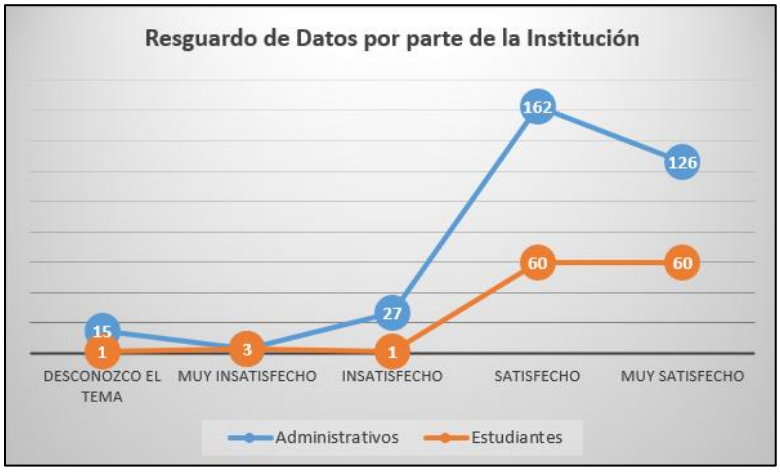
La institución desde el área de tecnología desarrolla una serie de encuestas de percepción sobre la seguridad de la información (personal administrativo donde se incluyen docentes y la perspectiva de los estudiantes), sobre los resultados se destacan los siguientes elementos:

A continuación, se identifica la percepción sobre el resguardo de la información en donde se destaca que el 16,6 % del personal administrativo se encuentra insatisfecho con el aseguramiento de la información en la institución y según los comentarios está enfocado a la necesidad de actualización de los equipos de cómputo y mejoras en la calidad en la velocidad de acceso a internet. Lo anterior evidencia que desde el rol de este tipo de usuarios hay una notable necesidad sobre la mejora de la capacidad tecnológica para garantizar un ambiente seguro.

En general, se muestra el trabajo hacia la confianza general en la comunidad educativa puesto que, a pesar de las limitaciones mencionadas, la percepción global no refleja un nivel de desconfianza crítica en los sistemas de seguridad, en donde puede relacionarse con la ausencia de incidentes cibernéticos significativos hasta el momento. A continuación, en la Figura 4, se puede identificar estos factores de percepción.

Figura 4

Percepción Comunidad Educativa Sobre la Seguridad de la Información



Nota. La gráfica permite interpretar la credibilidad de la comunidad sobre la seguridad de la institución

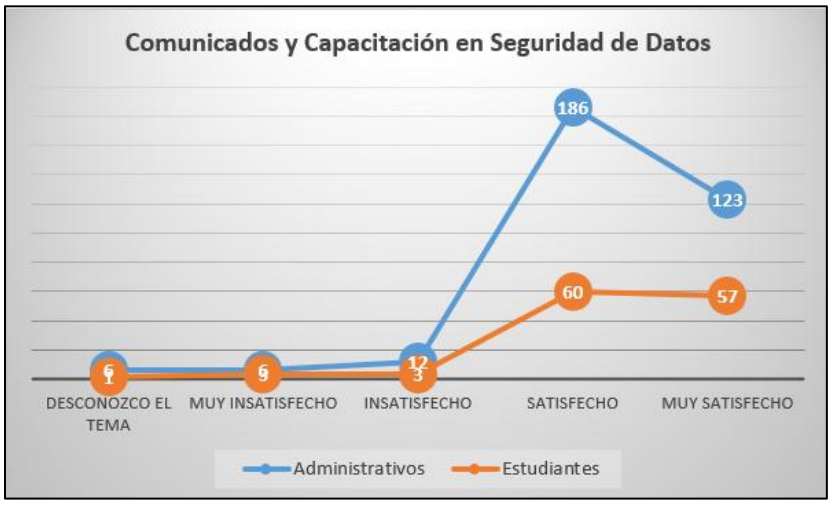
La identificación de equipos desactualizados representa un potencial punto de entrada para ataques informáticos. Este riesgo, aunque latente, es una alerta estratégica que debe abordarse para evitar posibles filtraciones o compromisos en la red. Es determinante diseñar estrategias que permitan actualizar la infraestructura tecnológica, considerando el impacto de estos equipos sobre la seguridad y funcionalidad general.

Como retos globales. la preparación para enfrentar brechas de seguridad sigue siendo limitada en muchas organizaciones. La falta de indicadores de gestión de riesgos y la alta incidencia de ataques cibernéticos refuerzan la importancia de adoptar enfoques preventivos. La necesidad de desarrollar capacidades para detectar brechas y gestionar riesgos de manera efectiva, lecciones que pueden guiar el fortalecimiento de la estrategia institucional.

En cuanto a los comunicados y capacitaciones sobre la seguridad de datos, se destaca en el gráfico, indicando que no hay niveles de insatisfacción considerables sobre este aspecto, además, no se evidencian comentarios enfocados con la seguridad de la información. Este resultado el cual se puede evidenciar en la Figura 5, sugiere que la institución ha logrado construir un proceso educativo sólido que fomenta la cultura de ciberseguridad, aunque no necesariamente garantiza la suficiencia técnica para mitigar vulnerabilidades.

Figura 5

Percepción Comunidad Educativa Sobre los Comunicados e Instructivos Recibidos



Nota. Los diferentes roles determinan que se está llevando a cabo un buen proceso de cultura en ciberseguridad.

Es importante tener en cuenta que los niveles de satisfacción son altos debido a que la institución no ha tenido casos de ataques informáticos, sin embargo, el factor de actualización de equipos identificado en la indagación permite generar una alerta con el fin de que se plantee la

forma de mitigar este aspecto. Los equipos desactualizados pueden ser vulnerados y actuar como entrada a que se filtre un posible ataque en la red.

En este sentido, (Camero D, 2020) indica que *de acuerdo con estudios de Ernst & Young, el 90% de las empresas del Perú no se encuentran preparadas para detectar brechas de seguridad, y el 51% de las empresas ya han sido atacadas. Además, de acuerdo con Deloitte, sólo el 10% de las empresas mantiene indicadores de gestión de riesgos.* Esta perspectiva internacional demuestra como a nivel global las empresas no toman medidas para el control y manejo de posibles ataques que se puedan presentar, generando un riesgo para las organizaciones sobre las amenazas existentes.

Con base en lo anterior, es necesario realizar una auditoría tecnológica que permita diagnosticar el estado actual de los equipos de cómputo. Esto facilitará la creación de un plan de actualización o sustitución que mitigue vulnerabilidades asociadas a dispositivos obsoletos. Además, se deben implementar mejoras en la infraestructura de red para optimizar la velocidad y estabilidad del internet, asegurando que cumpla con estándares modernos de seguridad que respalden tanto el desempeño como la protección de los datos institucionales.

En consecuencia, es importante promover una capacitación continua que, además de mantener la percepción positiva sobre los comunicados actuales, integre talleres prácticos y simulaciones diseñados para enfrentar amenazas reales. También se recomienda la adopción de indicadores claros de gestión de riesgos que permitan monitorear de manera constante el estado de la seguridad frente al actuar de forma proactiva ante posibles brechas. Finalmente, debe diseñarse un plan integral de contingencia y respuesta a incidentes que incluya protocolos detallados con simulacros periódicos, asegurando una preparación efectiva frente a potenciales ataques.

Propuesta Intervención y Componente Tecnológico

Lo planteado en el diagnostico nos lleva a determinar la mejor estrategia para evaluar las diferentes vulnerabilidades, por lo tanto, se establecen reuniones con los diferentes actores del proceso, (líder del departamento de seguridad de la información, líder de infraestructura TI, líder de soluciones, Socio compañía Jeturin SEGRD departamento de seguridad), todo enfocado en los siguientes pasos.

En el procedimiento de preparación se tiene en cuenta la base de la estrategia de verificación de vulnerabilidades la cual tiene como objetivo establecer los lineamientos iniciales para un análisis efectivo. En esta fase, se define el alcance de las actividades, identificando los activos tecnológicos clave que serán evaluados, tales como servidores, aplicaciones web, bases de datos, redes internas, subdominios y dispositivos conectados. Esto asegura que las pruebas sean específicas con enfoque en las áreas más críticas de la universidad.

Asimismo, es fundamental obtener los permisos y acuerdos formales necesarios para llevar a cabo estas actividades con los líderes de TI, garantizando el cumplimiento de las normativas legales y las políticas institucionales (acuerdo de confidencialidad). Como parte de esta preparación, se realizan perfiles iniciales mediante técnicas OSINT, centradas en el análisis de registros DNS y pruebas de bloques IP. Esto permite mapear la infraestructura tecnológica para detectar posibles configuraciones incorrectas o activos expuestos.

Al respecto, se realiza la identificación detallada de vulnerabilidades mediante el uso de herramientas avanzadas como Rapid7 InsightVM. Esta herramienta permite ejecutar escaneos exhaustivos para detectar software obsoleto, configuraciones inseguras, servicios abiertos no autorizados y parches faltantes en los sistemas. El análisis se enfoca en los activos críticos,

especialmente aquellos que manejan información confidencial, como datos estudiantiles y financieros.

En este sentido, los resultados obtenidos se presentan en reportes categorizados por niveles de riesgo (baja, media, alta, crítica) para facilitar la priorización. Además, se correlacionan los datos OSINT obtenidos previamente con los hallazgos de Rapid7, lo que permite identificar inconsistencias, sistemas sin monitoreo entre otros aspectos como accesos no autorizados. Este enfoque combinado maximiza la precisión del análisis lo que ayuda a identificar vulnerabilidades que podrían pasar desapercibidas con un único método.

Asimismo, luego de identificar las vulnerabilidades, se realiza un análisis exhaustivo de los resultados con el propósito de comprender los riesgos subyacentes y priorizar su mitigación. En esta etapa, se identifican patrones comunes, como la presencia de software desactualizado o configuraciones predeterminadas inseguras. Es importante tener en cuenta que, en el sector educativo en Colombia, se pueden encontrar varias vulnerabilidades que pueden ser explotadas por los ciberdelincuentes. Algunas de estas vulnerabilidades son, falta de seguridad física donde la mayoría de las instituciones educativas no tienen suficientes medidas de seguridad física para prevenir robos, vandalismo entre otros delitos.

En cuanto a la falta de protección de datos personales, Las instituciones educativas son fuente de una cantidad significativa de información personal sobre sus estudiantes, que empieza desde nombres o documentos de identidad hasta historiales académicos. Cuando las instituciones educativas no cuentan con protocolos sobre una buena arquitectura de seguridad adecuados, se exhiben a potenciales filtraciones de información. Por último, la divulgación no autorizada de la información puede llevar a resultantes graves como el robo de identidad y el uso de la información con fines maliciosos.

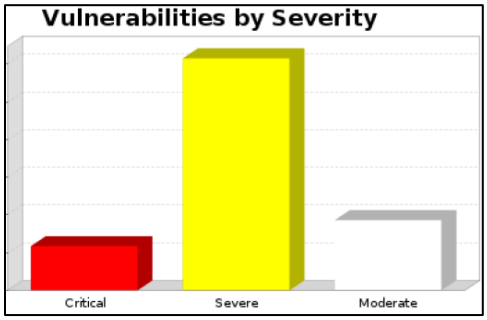
Al respecto, es muy frecuente que en las instituciones educativas tanto el personal administrativo como los estudiantes pueden no estar plenamente conscientes de la importancia de la protección de datos personales. Esto obedece posiblemente a la falta de formación específica sobre seguridad de la información; Otro factor importante que explica esta situación se debe a que muchas instituciones educativas no tienen suficiente financiamiento para implementar sistemas de seguridad de datos eficientes. Esto incluye la falta de herramientas tecnológicas, personal capacitado y medidas de seguridad adecuadas.

Por tanto, se debe considerar como una posible causa la no existencia de un modelo de seguridad implementado en las instituciones basado en las normas actuales sobre la protección de la información. Por consiguiente, utilizan software o hardware obsoleto debido a restricciones presupuestarias, esto puede dejar a los sistemas más vulnerables con posibles ataques cibernéticos y fugas de datos.

En la Figura 6, se evidencian los estados de las vulnerabilidades de la institución, la cantidad por motivos de confidencialidad no pueden ser revelados, sin embargo, se interpreta que la mayoría de las vulnerabilidades se presentan en un estado “severo”, seguido de las que se encuentran en estado “moderado” y en un menor porcentaje en estado “crítico”

Figura 6

Clasificación de las Vulnerabilidades Encontradas

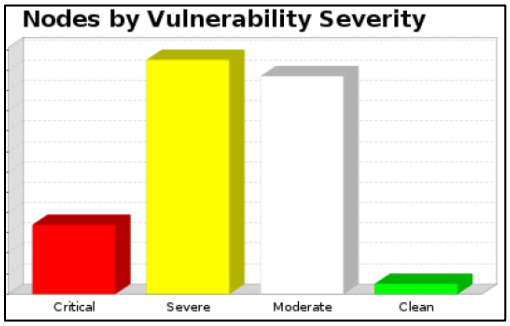


Nota. Relación de las vulnerabilidades resultado de las pruebas de pentesting y del informe de auditoría.

En relación con los nodos en riesgo sobre las vulnerabilidades encontradas según el reporte general de auditoría, en la Figura 7, se establecen vulnerabilidades en estado “Severo” con cantidad similar para las que se encuentran en estado “Moderado”, por otro lado, el estado “critico” no representa una cantidad representativa, mientras que puntos libres de vulnerabilidades se encuentra en un índice muy bajo.

Figura 7

Clasificación de las Vulnerabilidades Encontradas a Nivel de Nodos



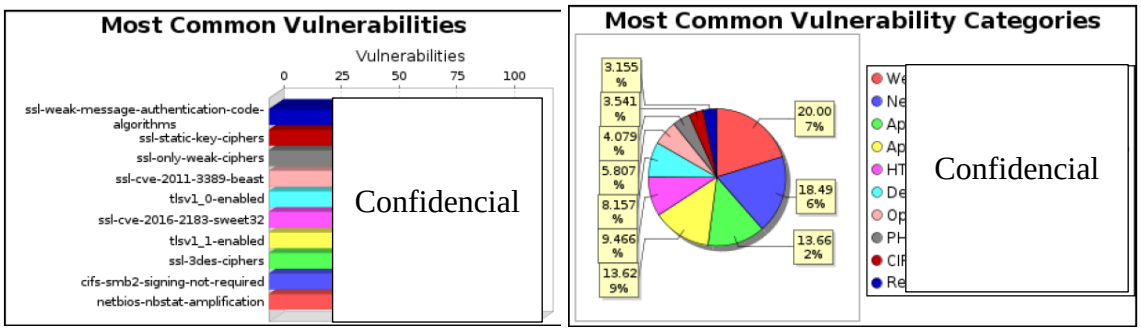
Nota. Cantidad de nodos de acuerdo con su nivel de riesgo sobre la infraestructura de red de la institución

Los problemas de seguridad en línea en las instituciones educativas son evidentes los cuales pueden atribuirse a varios factores entre ellos se encuentran, infraestructura tecnológica obsoleta o inadecuada donde pueden ser más vulnerables a los ataques cibernéticos generando riesgos para una amplia gama de tecnologías sobre la gestión de datos de los estudiantes, la entrega de contenido educativo y la comunicación.

Esto crea múltiples puntos de vulnerabilidad que pueden ser explotados por actores maliciosos. A continuación, en la Figura 8, se describen las vulnerabilidades más comunes y los porcentajes por categorías de acuerdo con los resultados encontrados en las pruebas. (se muestran resultados sobre la cantidad teniendo en cuenta la confidencialidad de los datos de la organización)

Figura 8

Vulnerabilidades más Comunes con los Porcentajes de Afectación

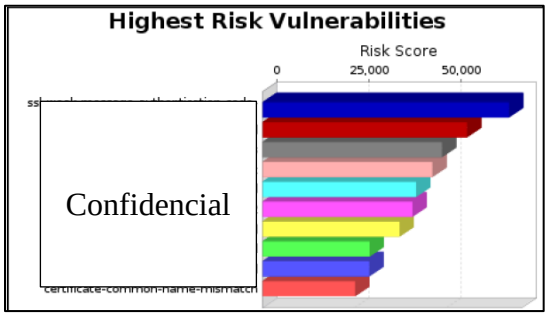


Nota. Relación del comportamiento de vulnerabilidades en la Institución sobre el comportamiento por medio de los gráficos de barras y segmentación de datos.

Además, las políticas y procedimientos para asegurar la información en línea son inadecuados no se implementan de manera efectiva. También el uso de redes y dispositivos personales para acceder a recursos educativos aumenta el riesgo de seguridad como se evidencia en la Figura 9. Estos elementos que hacen parte de los activos de la información a menudo carecen de las medidas de seguridad adecuadas y pueden ser fácilmente comprometidos.

Figura 9

Vulnerabilidades de Mayor Riesgo en la Institución

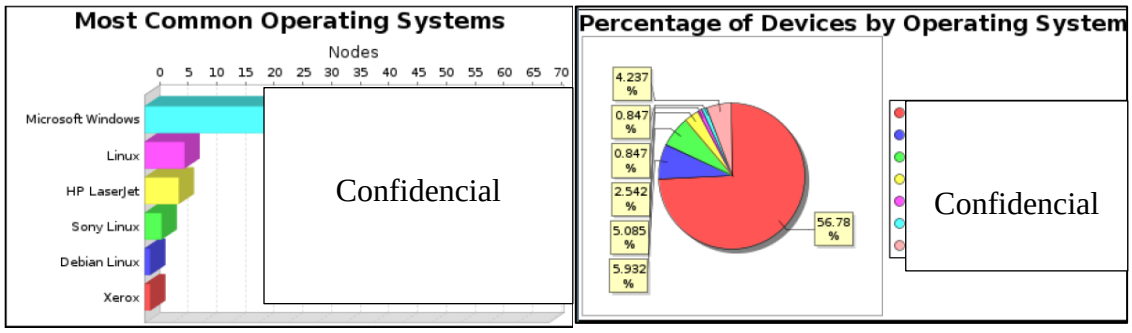


Nota. Se encuentran vulnerabilidades que representan un riesgo alto sobre la infraestructura tecnológica de la organización

Los sistemas informáticos de las instituciones educativas también pueden ser vulnerables a los ataques cibernéticos, especialmente si no se mantienen actualizados y protegidos con medidas de seguridad adecuadas. En la Figura 10, se dan a conocer los sistemas operativos que normalmente se proyectan como los más vulnerables. la falta de personal capacitado en tecnología y seguridad puede aumentar el riesgo de ataques cibernéticos entre otros problemas de seguridad.

Figura 10

Sistemas Operativos Propensos a Diversos Ataques Informáticos

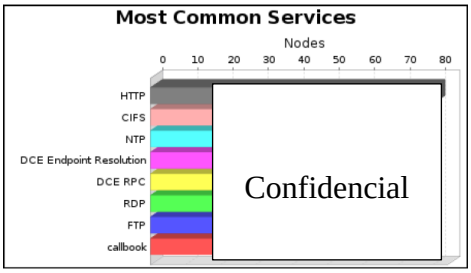


Nota. Relación de sistemas operativos organizados según el nivel de afectación ante un posible incidente de seguridad

Los usuarios de los sistemas informáticos también pueden ser una fuente de vulnerabilidades. Si no se les capacita en cómo mantener sus contraseñas seguras, por ejemplo, pueden poner en riesgo la seguridad de toda la institución. De esta manera se representa en la Figura 11, los servicios más comunes que pueden ser vulnerados por malas prácticas en la institución.

Figura 11

Servicios más Comunes Afectados en la Institución

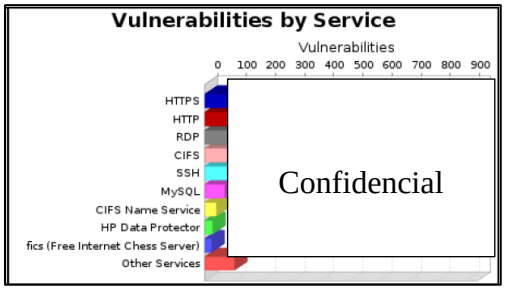


Nota. Según el informe de auditoría se encuentran los servicios más vulnerables

Por último, en este caso de estudio se encuentran los resultados con respecto a las pruebas de verificación de red desarrolladas por un tiempo determinado con el fin de analizar el tráfico sobre los servidores en servicio y en general de equipos que puedan estar vinculados en la red con actividades relevantes para la organización como se muestra en la Figura 12.

Figura 12

Vulnerabilidades por Servicio Encontradas en la Institución



Nota. La relación de servicios puede variar debido a que actualmente se trabaja en la mitigación de los riesgos encontrados.

Evaluación del Impacto de la Aplicación de la Estrategia

De acuerdo con las normas de gestión de seguridad y de buenas prácticas en el manejo de la información como la NIST y la norma ISO/IEC 27001, se establecen los parámetros de recomendaciones luego de los resultados obtenidos en las pruebas de identificación de vulnerabilidades, de esta manera se genera la matriz de riesgos con los diferentes controles como sugerencias para que la institución implemente cambios y estrategias en pro de la seguridad de la información.

Con el fin de no comprometer la seguridad de la institución a continuación se relaciona la ruta de identificación de vulnerabilidades, hasta el plan de acción recomendado. Se recomienda diseñar acciones correctivas enfocadas en solucionar estas problemáticas, tales como la actualización de sistemas operativos, la implementación de configuraciones seguras en servicios expuestos y la habilitación de protocolos de protección para servicios de red. En la Figura 13, se identifican con la respectiva descripción y el enlace donde se encontrará información detallada según el código correspondiente

Figura 13

Matriz de Evaluación de Vulnerabilidades

Nivel de criticidad	Id de Caso	Nombre	Descripción	Documentación
3	1	Vulnerabilidad de elusión de autenticación	Una vulnerabilidad en la función 802.1X de Cisco Catalyst 2960-L Series Switches y Cisco Catalyst CDB-8P Switches podría permitir a un atacante no autenticado y adyacente reenviar tráfico de difusión antes de ser autenticado en el puerto.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c2960L-DpWA9Re4 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3231
4	2	Una vulnerabilidad en el controlador criptográfico de hardware del software Cisco IOS XE	Los routers de servicios integrados Cisco 4300 Series y los controladores inalámbricos Cisco Catalyst 9800-L podrían permitir a un atacante remoto no autenticado desconectar sesiones legítimas de VPN IPsec en un dispositivo afectado.	https://www.cvedetails.com/cve/CVE-2020-3220/
5	3	Denegación de servicio - Remota CVE-2005-4258	Conmutadores Cisco Catalyst no especificados permiten a atacantes remotos provocar una denegación de servicio (fallo del dispositivo) a través de un paquete IP con las mismas IP y puertos de origen y destino, y con la bandera SYN activada (también conocida como LanD). NOTA: se desconoce la procedencia de este problema; los detalles se obtienen únicamente del BID.	https://www.cvedetails.com/cve/CVE-2005-4258/
4	4	Autenticación remota de usuarios - Denegación de servicio CVE-2012-1338	Cisco IOS 15.0 y 15.1 en Catalyst 3560 y 3750 interruptores de la serie permite a los usuarios remotos autenticados para causar una denegación de servicio (dispositivo de recarga), completando la autenticación web local rápidamente, aka Bug ID CSCts88664.	https://www.cvedetails.com/cve/CVE-2012-1338/

Nota. Se generan los diferentes recursos de información para la institución con las rutas de validación

Una vez identificadas las vulnerabilidades se proceden a determinar las posibles amenazas como se puede observar en la Figura 14, con la respectiva descripción y documentación externa. Adicionalmente, se da a conocer la importancia de fortalecer la seguridad mediante la segmentación de la red, limitando el acceso a servicios críticos únicamente a usuarios autorizados y restringiendo los rangos IP públicos a los activos estrictamente necesarios. Estas medidas reducen significativamente la exposición de la universidad a posibles ataques.

Figura 14

Identificación de Amenazas y Documentación

Nivel de criticidad	Id de Caso	Tipo	Descripción	Documentación
4	CVE-2020-3231	Amenaza de acceso no autorizado	Podría permitir a un atacante acceder a información confidencial de usuarios.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c2960L-DpWA9Re4
4		Amenaza de intercepción de datos	Podría permitir a un atacante capturar datos sensibles transmitidos entre el cliente y el servidor.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3231
5	CVE-2020-3220	Amenaza de denegación de servicio (DoS)	Un atacante podría explotar la vulnerabilidad para saturar los recursos del sistema y hacer que sea inaccesible para usuarios legítimos.	https://www.cvedetails.com/cve/CVE-2020-3220/
4	CVE-2005-4258	Amenaza de ejecución de código arbitrario	Un atacante podría aprovechar la vulnerabilidad para ejecutar código malicioso en el sistema comprometido.	https://www.cvedetails.com/cve/CVE-2005-4258/
4		Amenaza de escalada de privilegios	Podría permitir a un atacante aumentar sus privilegios de acceso en el sistema comprometido, obteniendo así un mayor control sobre el mismo.	
5	CVE-2012-1338	Amenaza de inyección de código SQL	Un atacante podría insertar comandos SQL maliciosos en las solicitudes de entrada de datos, lo que podría conducir a la extracción de información confidencial o a la modificación de la base de datos.	https://www.cvedetails.com/cve/CVE-2012-1338/
5		Amenaza de exposición de información confidencial	Podría permitir a un atacante obtener acceso a datos sensibles almacenados en la base de datos a través de consultas SQL manipuladas.	

Nota. Se establecen los parámetros sobre la forma en que actúa la amenaza mediante un posible ataque informático

Se procede con la identificación de riesgos y como afectan a los elementos de la triada según la descripción sobre el componente de seguridad o activo de la información expuesto lo cual puede verse evidenciado en la Figura 15. Es importante que se evalúe la efectividad de las medidas implementadas mediante revisiones periódicas con las herramientas trabajadas. Los escaneos regulares permiten detectar nuevas vulnerabilidades o confirmar la resolución de problemas previamente identificados.

Al mismo tiempo, se debe considerar actualizar los perfiles OSINT monitoreando los bloques IP, lo que permite a futuro asegurar un seguimiento continuo de la infraestructura tecnológica. Para medir el impacto de las acciones correctivas, se recomienda implementar indicadores clave de rendimiento, como la disminución de vulnerabilidades críticas sobre el

tiempo promedio de respuesta ante hallazgos. También es relevante fomentar la capacitación del personal de TI en el uso de herramientas con técnicas avanzadas, promoviendo un enfoque preventivo y ágil.

Figura 15

Identificación de Riesgos

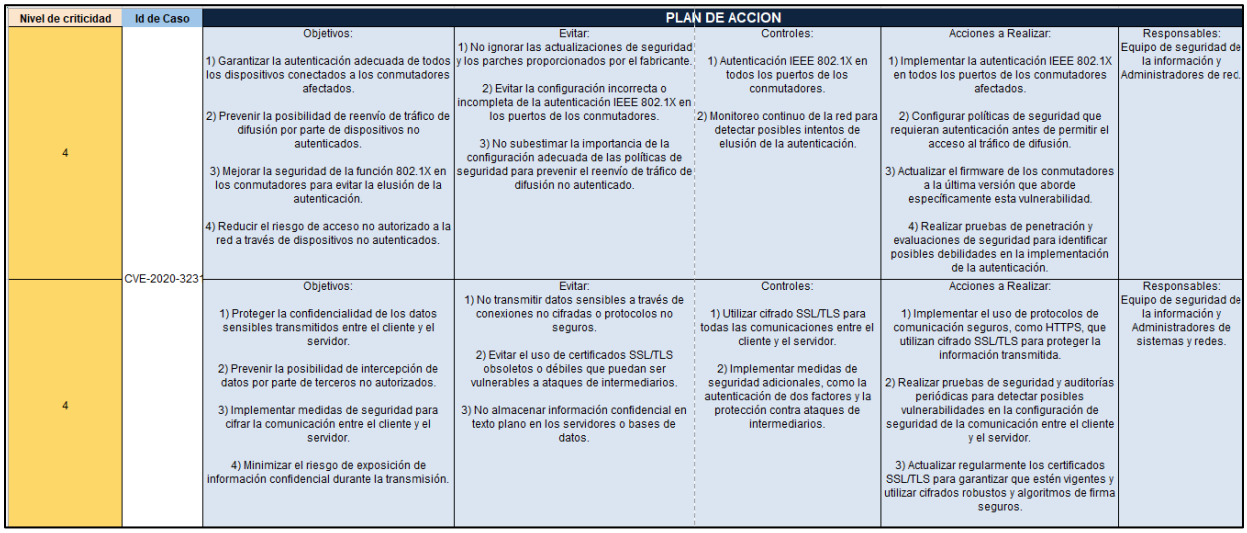
Nivel de criticidad	Id de Caso	Tipo	Descripción	Documentación
5	CVE-2020-3231	Confidencialidad	Riesgo de violación de la confidencialidad de la información debido a vulnerabilidades en la gestión de sesiones de usuario.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c2960L-DpWA9Re4
5		Integridad	Riesgo de pérdida de integridad de los datos almacenados o transmitidos debido a la explotación de vulnerabilidades en aplicaciones web.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3231
5	CVE-2020-3220	Confidencialidad	Riesgo de exposición a ataques de denegación de servicio (DoS) debido a vulnerabilidades en el protocolo de comunicación utilizado por la aplicación o sistema afectado.	https://www.cvedetails.com/cve/CVE-2020-3220/
5	CVE-2005-4258	Integridad	Riesgo de ejecución de código arbitrario o instalación de software malicioso debido a vulnerabilidades en la autenticación o gestión de privilegios de usuario.	https://www.cvedetails.com/cve/CVE-2005-4258/
5		Integridad y disponibilidad	Riesgo de compromiso de la integridad y disponibilidad de los datos almacenados en sistemas afectados.	
5	CVE-2012-1338	Integridad	Riesgo de exposición a ataques de inyección de código SQL debido a vulnerabilidades en la validación de entrada de datos en aplicaciones web o sistemas de bases de datos.	https://www.cvedetails.com/cve/CVE-2012-1338/
5		Confidencialidad	Riesgo de pérdida de confidencialidad y manipulación de información crítica almacenada en bases de datos.	

Nota. Se establecen los elementos de la triada relacionados con el riesgo identificado

Desarrollados los pasos anteriores se realiza la propuesta del plan de acción para la mitigación en caso de ocurrencia del evento documentando los objetivos, que se debe evitar, establecimiento de controles, acciones a realizar y por último los responsables en función de roles como equipo de respuesta, esto permite obtener una línea de trabajo claro que permite responder de manera eficiente ante un incidente de seguridad relacionado con los activos de la información más propensos a ser atacados, lo anterior se puede identificar con una muestra en la Figura 16.

Figura 16

Propuesta del Plan de Acción



Nivel de criticidad	Id de Caso	PLAN DE ACCION				
4	CVE-2020-323	Objetivos: 1) Garantizar la autenticación adecuada de todos los dispositivos conectados a los conmutadores afectados. 2) Prevenir la posibilidad de reenvío de tráfico de difusión por parte de dispositivos no autenticados. 3) Mejorar la seguridad de la función 802.1X en los conmutadores para evitar la elusión de la autenticación. 4) Reducir el riesgo de acceso no autorizado a la red a través de dispositivos no autenticados.	Evitar: 1) No ignorar las actualizaciones de seguridad y los parches proporcionados por el fabricante. 2) Evitar la configuración incorrecta o incompleta de la autenticación IEEE 802.1X en los puertos de los conmutadores. 3) No subestimar la importancia de la configuración adecuada de las políticas de seguridad para prevenir el reenvío de tráfico de difusión no autenticado.	Controles: 1) Autenticación IEEE 802.1X en todos los puertos de los conmutadores. 2) Monitoreo continuo de la red para detectar posibles intentos de elusión de la autenticación.	Acciones a Realizar: 1) Implementar la autenticación IEEE 802.1X en todos los puertos de los conmutadores afectados. 2) Configurar políticas de seguridad que requieran autenticación antes de permitir el acceso al tráfico de difusión. 3) Actualizar el firmware de los conmutadores a la última versión que aborde específicamente esta vulnerabilidad. 4) Realizar pruebas de penetración y evaluaciones de seguridad para identificar posibles debilidades en la implementación de la autenticación.	Responsables: Equipo de seguridad de la información y Administradores de red.
4		Objetivos: 1) Proteger la confidencialidad de los datos sensibles transmitidos entre el cliente y el servidor. 2) Prevenir la posibilidad de intercepción de datos por parte de terceros no autorizados. 3) Implementar medidas de seguridad para cifrar la comunicación entre el cliente y el servidor. 4) Minimizar el riesgo de exposición de información confidencial durante la transmisión.	Evitar: 1) No transmitir datos sensibles a través de conexiones no cifradas o protocolos no seguros. 2) Evitar el uso de certificados SSL/TLS obsoletos o débiles que puedan ser vulnerables a ataques de intermediarios. 3) No almacenar información confidencial en texto plano en los servidores o bases de datos.	Controles: 1) Utilizar cifrado SSL/TLS para todas las comunicaciones entre el cliente y el servidor. 2) Implementar medidas de seguridad adicionales, como la autenticación de dos factores y la protección contra ataques de intermediarios.	Acciones a Realizar: 1) Implementar el uso de protocolos de comunicación seguros, como HTTPS, que utilizan cifrado SSL/TLS para proteger la información transmitida. 2) Realizar pruebas de seguridad y auditorías periódicas para detectar posibles vulnerabilidades en la configuración de seguridad de la comunicación entre el cliente y el servidor. 3) Actualizar regularmente los certificados SSL/TLS para garantizar que estén vigentes y utilizar cifrados robustos y algoritmos de firma seguros.	Responsables: Equipo de seguridad de la información y Administradores de sistemas y redes.

Nota. Se desarrollan los elementos de mitigación en caso de ocurrencia del incidente de seguridad

La propuesta se centra en establecer una capacidad de respuesta efectiva frente a incidentes y en ajustar la estrategia según los nuevos desafíos de seguridad. Es necesario diseñar protocolos claros que garanticen una intervención rápida y coordinada ante potenciales ataques. A su vez, se debe revisar la estrategia regularmente, considerando cambios en la tecnología, tendencias emergentes y resultados de auditorías previas. Este enfoque adaptativo permite a la institución mantenerse preparada frente a amenazas dinámicas, fortaleciendo su entorno tecnológico de manera sostenida.

Conclusiones

De acuerdo con el análisis de vulnerabilidades realizado, se encuentran hallazgos relevantes frente a la oportunidad de mejora continua sobre la protección de la infraestructura de red de la institución, aunque en el momento de la verificación no se han presentado ataques informáticos o incidentes de seguridad de gran riesgo, es necesario que se desarrolle un modelo de seguridad que permita preparase generando barreras para responder ante incidentes que puedan surgir a corto plazo.

La falta de inversión, actualización en tecnología y software de las instituciones del sector es una de las principales debilidades que afecta la seguridad de la información. Es importante generar estrategias con políticas claras para la gestión de los datos, donde trabajen en colaboración con empresas de seguridad de la información, expertos en ciberseguridad y proveedores.

En cuanto a la formación y concienciación de los usuarios en la comunidad educativa, es un factor decisivo en la seguridad de la información. El desconocimiento sobre prácticas seguras en factores como el comportamiento en línea puede poner en riesgo la privacidad afectando en gran medida la protección de datos sensibles. La necesidad de una cultura de seguridad en la cual se integran medidas de seguridad en las prácticas cotidianas de los usuarios de la institución en los diferentes roles que representan.

Por último, los problemas de seguridad pueden exponer a la institución a diferentes ataques informáticos. Estos pueden incluir en intentos de phishing (uno de los más comunes puesto que todos los roles educativos tienen acceso a una cuenta institucional), ataques de malware, entre otros vectores de amenaza que buscan robar información o comprometer la integridad de los datos y medios de los usuarios.

Recomendaciones

Para prevenir estos riesgos que contribuyen en el esquema de protección, las instituciones educativas en Colombia y en la Institución donde se desarrolla este proyecto es necesario invertir en la seguridad de los sistemas informáticos, como también en formación capacitando a los usuarios en gestión de riesgos y seguridad cibernética. Además, es importante que se implementen medidas de seguridad física y se proteja la información personal de los diferentes roles mediante la actualización de políticas sobre los procedimientos para un manejo eficiente de la información asegurando los recursos necesarios para implementar medidas de seguridad efectivas. También es fundamental que se actualicen y protejan los sistemas informáticos contratando personal capacitado en tecnología y seguridad.

Para el proceso de identificación de vulnerabilidades en la red educativa, se recomiendan las pruebas de verificación relacionadas con el escaneo de puertos donde esta prueba consiste en analizar todos los puertos que están abiertos y vinculados a los servicios en la red educativa, para identificar si alguno de ellos presenta vulnerabilidades. A nivel de Inspección de tráfico se puede llevar a cabo una evaluación del tráfico de red para detectar patrones de comportamiento sospechosos, como por ejemplo transmisiones de paquetes malintencionados o intentos de acceso no autorizados.

De acuerdo con lo anterior, para la Fundación Universitaria Compensar, la auditoria desarrollada mediante las pruebas de identificación de vulnerabilidades permite conocer el estado actual de la institución y a partir de los resultados obtener elementos de valor que les permite interiorizar las buenas prácticas en seguridad y las estrategias a desarrollar a futuro frente a la dinámica en seguridad de la información.

El enfoque de la prueba de penetración debe ser hacia verificar cómo el software se comporta y resiste ante diferentes tipos de ataque en la red educativa para identificar los puntos débiles y comprobar si es posible violar la seguridad de la red. Loa anterior, se complementa con el análisis de vulnerabilidades a través de herramientas especiales, se pueden analizar las cuales existen en la red, como errores en la configuración, actualizaciones de software pendientes, contraseñas inseguras, entre otros aspectos relevantes según la necesidad de la organización sobre la profundidad de lo que se quiere evaluar.

Por último, en cuanto a la revisión de estrategias de seguridad se pueden desarrollar evaluaciones con auditorias periódicas en la red educativa de la Fundación para comprobar si se están siguiendo las mejores prácticas en materia de seguridad informática. Es importante destacar que las instituciones educativas en Colombia han invertido poco presupuesto en ciberseguridad, lo que las convierte en un blanco atractivo para los ciberdelincuentes. Por lo tanto, es necesario que las instituciones educativas aumenten la visibilidad de su postura de ataque para mejorar su ciberseguridad. Además, es fundamental que se actualicen, protejan los sistemas informáticos, donde uno de los aspectos fundamentales es contratar personal capacitado en aseguramiento de la infraestructura tecnológica como tambien educar a la comunidad educativa sobre cómo mantener sus contraseñas seguras y evitar prácticas inseguras en línea.

Referencias Bibliográficas

Albarrán, Silvia Pérez, Juan Salgado, Mireya Valero, L. (2019). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares* (Vol. 1).

Arenas Grisales, S. P., Giraldo Lopera, M. L., Gutiérrez, J. O., & Tangarife Patiño, A. M. (2022). Possibility, Risk and Uncertainty: Analysis of Trends in the Information Sciences. *Revista Interamericana de Bibliotecologia*, *45*(3). https://doi.org/10.17533/UDEA.RIB.V45N3E347313

Balseca-Chávez, F., Colina-Vargas, A. M., & Espinoza-Mina, M. A. (2021). Identificación de amenazas informáticas aplicando arquitecturas de Big Data. *INNOVA Research Journal*, *6*(3.2), 141–167. https://doi.org/10.33890/innova.v6.n3.2.2021.1860

Barreño Gutiérrez, R., & Lengerke, O. (2014). *Voto electrónico con SSL/TLS e IPSEC*. 391–402.

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, *13*(1), 97–104. https://doi.org/10.18779/cyt.v13i1.357

Camero D, C. M. A. J. M. J. (2020). *Modelo de gestión de riesgos de seguridad de información para mitigar el impacto en las PYMEs en Perú*.

Carmona Rojas, M. Y. (2020). Problemas y enfoques de la investigación sobre el transporte informal en América Latina. *Revista Transporte y Territorio*, *23*, 159–181. https://doi.org/10.34096/rtt.i23.9661

Carvajal Portilla, D. L., Cardona Londoño, A., & Valencia Duque, F. J. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre ciencia e ingeniería*, *13*(25), 68–76. https://doi.org/10.31908/19098367.4016

Chaparro-Prieto A, P.-V. I. (2024). *La gestión del conocimiento en la educación superior colombiana: un análisis documental*.

Chillagana, J., Simbaña, J., & Suntaxi, K. (2023). *Design and Deployment of a WAN/LAN/WLAN Network Infrastruc-ture with Security using FortiGate in GNS-3*. *VIII*(3), 68–76. https://doi.org/10.24133/RCSD.VOL08.N03.2023.05

Chóez I, M. K. (2023). *EVALUACIÓN DE DIVERSAS HERRAMIENTAS TECNOLÓGICAS PARA EL ANÁLISIS DE TRÁFICO DE LA RED DE DATOS EN LA CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN*.

David Estrada-Esponda, R., Luis Unás-Gómez, J., & Oleskyenio, |. (2021). *Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá*. https://doi.org/10.22335/rlct.v13i3.1446

del Carmen Sagbini Echávez, J., Velásquez Perez, T., & Espinel Blanco, E. (2024). Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero. *Journal of Engineering Sciences*, *21*, 9–12. https://doi.org/10.22463/2011642X.3588

Diéguez M. (2021). *Enfoque Metodológico para la Selección de Controles de Seguridad de la Información*.

Esparza, D. E. I., Diaz, F. J., Echeverria, T. K. S., Hidrobo, S. R. A., Villavicencio, D. A. L., & Ordonez, A. R. (2020). Information security issues in educational institutions. *Iberian Conference on Information Systems and Technologies, CISTI*, *2020-June*(June), 24–27. https://doi.org/10.23919/CISTI49556.2020.9141014

Ferruzola Gómez, E. C., Bermeo Almeida, O. X., & Arévalo Gamboa, L. M. (2022). Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim. *Ecuadorian Science Journal*, *6*(1), 23–31. https://doi.org/10.46480/esj.6.1.181

Garcia, S. G., Centurion, J. B., & Silva, J. S. (2020). Seguridad De La Información : Phishing Y Coronavirus. *Bol Inst Nac Salud*, *26*, 17–21. http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=143705990&lang=es&site=ehost-live

González H, M. R. (2018). *Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web*. 52–65.

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

Handri, E. Y., Putro, P. A. W., & Sensuse, D. I. (2023). Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, 82–87. https://doi.org/10.1109/ICoCICs58778.2023.10277024

Hernández, M., Cantero, Z., Giseth, L., Vidal, R., & Marcela, D. (2019). *Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia*. https://www.redalyc.org/articulo.oa?id=29063446029

Ibarra Imbachi, M. Y. (2019). *Delitos informáticos asociados a la ingeniería social en Colombia y Latinoamérica (tesis especialización)*. https://repository.unad.edu.co/handle/10596/27420

kaspersky. (2024, marzo 2). *CIBERAMENAZA MAPA EN TIEMPO REAL*. https://cybermap.kaspersky.com/es/stats

Leguizamón Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas. *Ingeniería Y Competitividad*, *22*(2), 1–13. https://doi.org/10.25100/iyc.v22i2.8483

Lezcano Gil, A. J., Geronimo Dionicio, P. O., & Mendoza De Los Santos, A. C. (2023). Principales medidas de seguridad para la protección de información y datos en la nube: una revisión sistemática. *INGENIERÍA INVESTIGA*, *5*. https://doi.org/10.47796/ing.v5i0.796

Lorusso G, R. C. (2022). *EVALUACIÓN DEL RENDIMIENTO DE HONEYPOT EN REDES TELEMÁTICAS*.

Marchand-Niño, W.-R., & Vega Ventocilla, E. J. (2020). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS). *Interfases*, 57–76. https://doi.org/10.26439/interfases2020.n013.4876

Marreros, J., Acosta, D., & Mendoza, A. (2024). Mecanismos de seguridad de la información en una organización: una revisión sistemática. *Revista Científica Ciencias Ingenieriles*, *4*(1), 79–90. https://doi.org/10.54943/ricci.v4i1.384

Martínez-Corona, J. I., Palacios-Almón, G. E., & Oliva-Garza, D. B. (2023). Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo. *Ra Ximhai*, 67–83. https://doi.org/10.35197/rx.19.01.2023.03.jm

Nussipova, A., Khussainova, G., Kabilova, R., Aliyarov, E., & Nuralina, B. (2024). Information Security Communications Strategy as a Prerequisite to Counteracting Hybrid Warfare: World Experience. *Revista Latina de Comunicacion Social*, *2024*(82), 1–20. https://doi.org/10.4185/rlcs-2024-2134

Ñañez, O. (2020). *Modelo de gestión de riesgos de ti para mejorar la gestión de seguridad de la información en la*.

Onieva, J. (2018). *2 (Abril- Junio, 2018)SCRUM COMO ESTRATEGIA PARA EL APRENDIZAJE COLABORATIVO A TRAVÉS DE PROYECTOS. PROPUESTA DIDÁCTICA PARA SU IMPLEMENTACIÓN EN EL AULA UNIVERSITARIA*. *2*.

Osorio-Sierra, A. F., Mateus-Hernández, M. J., & Vargas-Montoya, H. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*, *19*(3), 131–142. https://doi.org/10.18273/revuin.v19n3-2020013

Pacheco, J., Chavez, J., & Mendoza De los Santos, A. (2023). Control de accesos en seguridad de la información: Una revisión sistemática de las técnicas actuales. *Campus*, *28*(36), 163–176. https://doi.org/10.24265/campus.2023.v28n36.01

Pantoja N, A. S. M. K. M. E. (2020). *Determinación de técnica de inteligencia para la detección de un tipo de ataque en un IDS*. 317–329.

Pereira Burgos, M. (2024). *TRABAJO DE GRADO: ELABORAR Y PUBLICAR SUS RESULTADOS UNA GUÍA PARA LOGRARLO*.

Pozo C, R. R. M. R. (2023). *COMERCIO ELECTRÓNICO Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DURANTE LA PANDEMIA DE COVID-19*.

Pulgar, J. O. G., & Quiñones, K. S. C. (2022). Una mirada a la cibercriminalidad en Colombia y su asimilación con los delitos de impacto A look at cybercrime in Colombia and its

assimilation with impact crime. *Revista Criminalidad*, *64*(3), 203–307. https://doi.org/10.47741/17943108.373

Quintero Tamayo, J. F., Nuñez Alvarez, Y. S., & Cuevas Nuñez, N. A. (2023). Estructuración de ataques informáticos por medio de playbooks. *Publicaciones e Investigación*, *17*(4). https://doi.org/10.22490/25394088.7498

Reyes H, M. L. O. A. (2020). *Survey of the security risks of Wi-Fi networks based on the information elements of beacon and probe response frames*.

Ricardo Ospina Díaz, M., & Emilio Sanabria Rangel, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*.

Roberto, M., & Olmedo, M. (2020). *Seguridad de la Información en plataformas virtuales de E-learning*.

Rodríguez, J. A. (2024). *LA EPISTEMOLOGÍA Y ENFOQUES DE LA INVESTIGACIÓN*.

Rojas Bahamón, M. J., Pulido Jiménez, A., & Serrato Rodríguez, Y. I. (2023). Prácticas de seguridad de la información en estudiantes de escuela secundaria en Colombia. *Entre ciencia e ingeniería*, *17*(33), 16–23. https://doi.org/10.31908/19098367.2832

Rojas Valiente, M. J., Castillo Sarmiento, J. M. H., & Mendoza De Los Santos, A. C. (2023). Seguridad de la información en la prevención de perdida de datos: una revisión sistemática. *Innovación y Software*, *4*(2), 182–200. https://doi.org/10.48168/innosoft.s12.a92

Safitri, E. H. N., & Kabetta, H. (2023). Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and*

Challenges, ICoCICs 2023, 332–338. https://doi.org/10.1109/ICoCICs58778.2023.10277652

Salgado, C., & Osuna, C. (2019). *La Auditoría Informática en las organizaciones The Computer Audit in organizations*. *4*.

Sánchez Solís, J., & Coto Jiménez, M. (2021). Estado del Arte de la Predicción de Variables en Sistemas de Ingeniería Eléctrica Basada en Inteligencia Artificial. *e-Ciencias de la Información*. https://doi.org/10.15517/eci.v12i1.47628

Sanchez, V. (2024, enero 18). *Los ataques cibernéticos serán el principal riesgo global para las empresas en 2024*. https://www.larepublica.co/finanzas/los-ataques-ciberneticos-son-el-principal-riesgo-empresarial-global-para-2024-3783263

Sánchez-Sánchez, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información tecnológica*, *32*(5), 121–128. https://doi.org/10.4067/s0718-07642021000500121

Sociedad, U. Y., Raquel, M., Paredes, Z., José, E., Arias, J., Ernestina, M., Olmedo, A., Leonardo, J., & Chango, G. (2021). *ANALYSIS OF COMPUTER SECURITY IN VIRTUAL ENVIRONMENTS OF THE AUTONOMOUS REGIONAL UNIVERSITY OF THE ANDES EXTENSION QUEVE-DO IN TIMES OF COVID-19 ANÁLISIS DE SEGURIDAD INFORMÁTICA Cita sugerida (APA, séptima edición)*.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Sotelo, R. (2020). *ciberseguridad Customized access log classifier for cybersecurity incident detection*. *18*, 47–52.

Sulay, L., Baca, R., Francisco, C., Puente De La Vega, C., Corredor, C. M., Alberto, M., Diaz, A., & Corredor, M. (2020). *Application of ISO 27001 and its influence on the information security of a Peruvian private company*. *8*, 786. https://doi.org/10.20511/pyr2020.v8n3.786

Taleb, R., Hallé, S., & Khoury, R. (2023). Uncertainty in runtime verification: A survey. En *Computer Science Review* (Vol. 50). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2023.100594

Urrea, S. E. C., Núñez, W. N., Gutiérrez, R. B., & Osorio, H. E. S. (2016). *Gestión de conocimiento soportado en TIC para entidades educativas de formación por competencias SENA – CEET*.

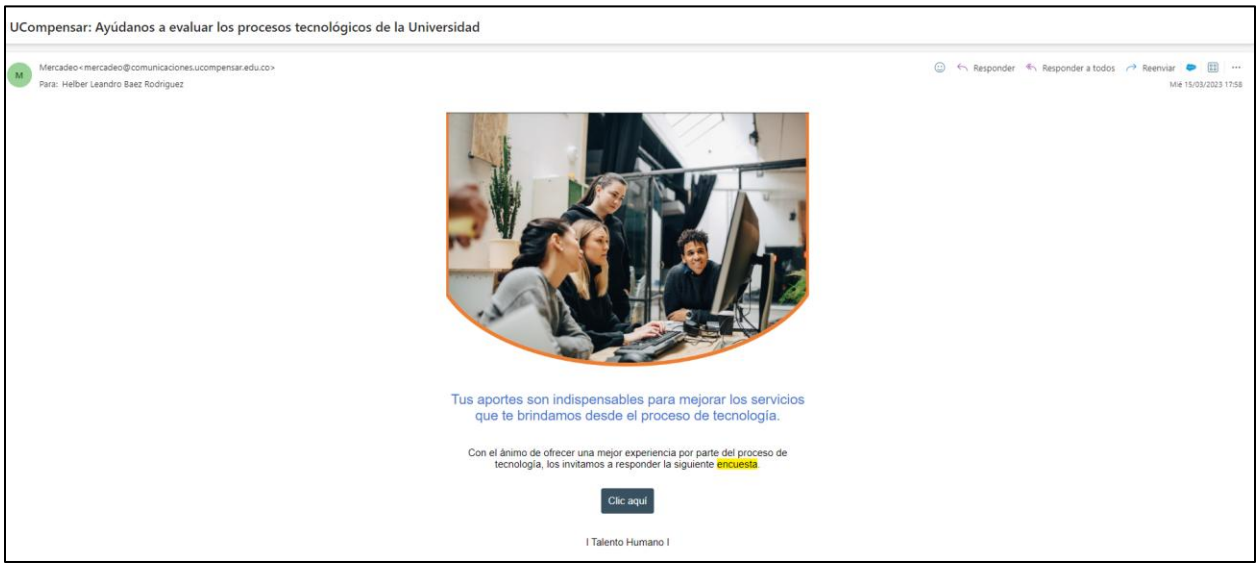
Vergara, G. (2024). *La flexibilidad del diseño de investigación: reflexiones acerca de los desafíos y oportunidades de investigar en/desde el aula*.

William, J., Torres, T., Ingrid, **, Moreno, C., & *** R. (2021). *Armonización entre la gestión documental, la calidad y la seguridad de la información en una institución de educación superior*. https://doi.org/10.15332/24631140

Apéndices

Apéndice A

Evidencias de Promoción y Difusión de Encuesta de Percepción



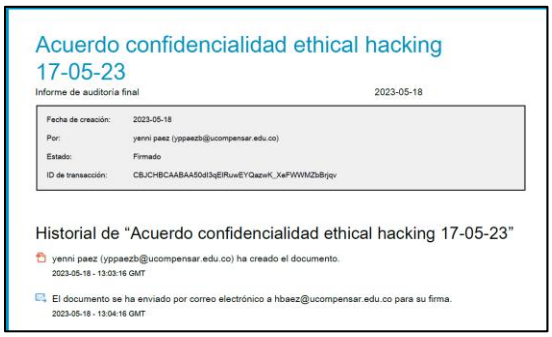
J	K	L	M	N	O	P	Q	R	S
La actitud, disposici	Puntos: La actitud, d	Comentarios: La acti	Los diferentes canal	Puntos: Los diferent	Comentarios: Los dif	Las soluciones brind	Puntos: Las solucion	Comentarios: Las so	Tiempo de respuest
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Satisfecho			Satisfecho			Satisfecho			Insatisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Muy satisfecho			Insatisfecho			Satisfecho			Satisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Satisfecho			Muy satisfecho			Insatisfecho			Insatisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Satisfecho			Insatisfecho			Satisfecho			Insatisfecho
Satisfecho			Satisfecho			Satisfecho			Insatisfecho
Satisfecho			Muy Insatisfecho			Satisfecho			Muy Insatisfecho
Muy satisfecho			Satisfecho			Satisfecho			Insatisfecho
Satisfecho			Muy satisfecho			Satisfecho			Insatisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Satisfecho			Satisfecho			Insatisfecho			Insatisfecho
Muy satisfecho			Muy satisfecho			Muy satisfecho			Muy satisfecho
Muy satisfecho			Satisfecho			Muy satisfecho			Muy satisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Satisfecho			Satisfecho			Satisfecho			Satisfecho
Insatisfecho			Insatisfecho			Insatisfecho			Muy Insatisfecho

Apéndice B

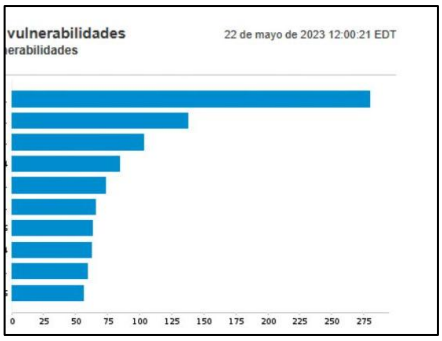
Acuerdos de Confidencialidad Rangos IP y Pruebas Iniciales

Evidencias acuerdos de confidencialidad


CONTRATO DE INVESTIGACIÓN SUSCRITO ENTRE LA SEGRD Y LA FUNDACIÓN UNIVERSITARIA COMPENSAR

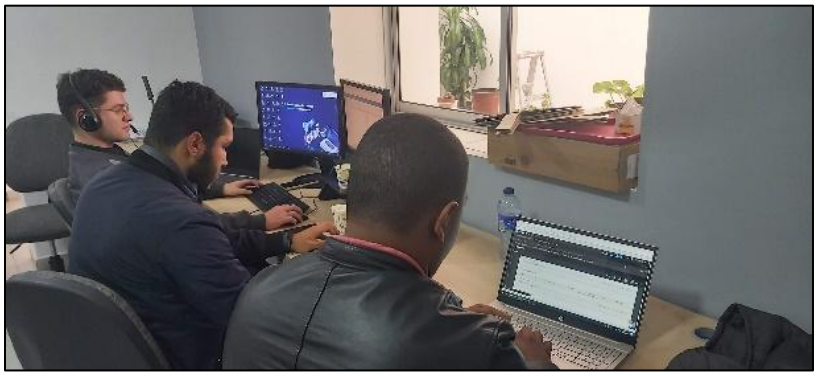


Resultados pruebas iniciales



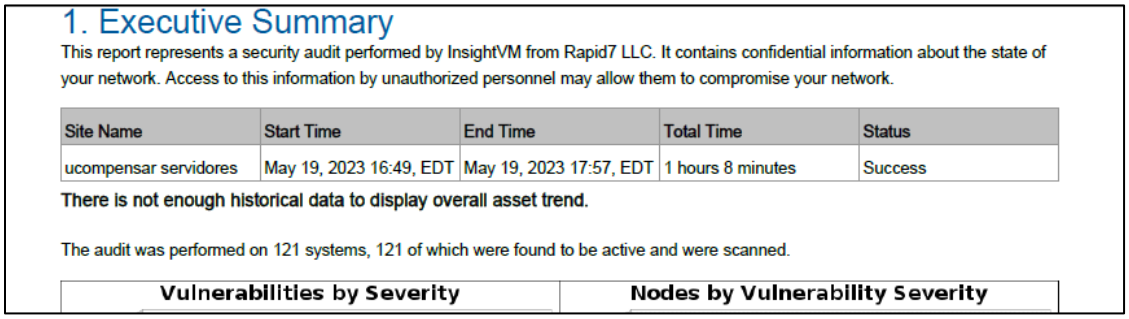
Apéndice C

Visita Experto Internacional Ejecución Pruebas



Apéndice D

Presentación de Informe de Auditoría Sobre los Resultados Obtenidos



1. Executive Summary

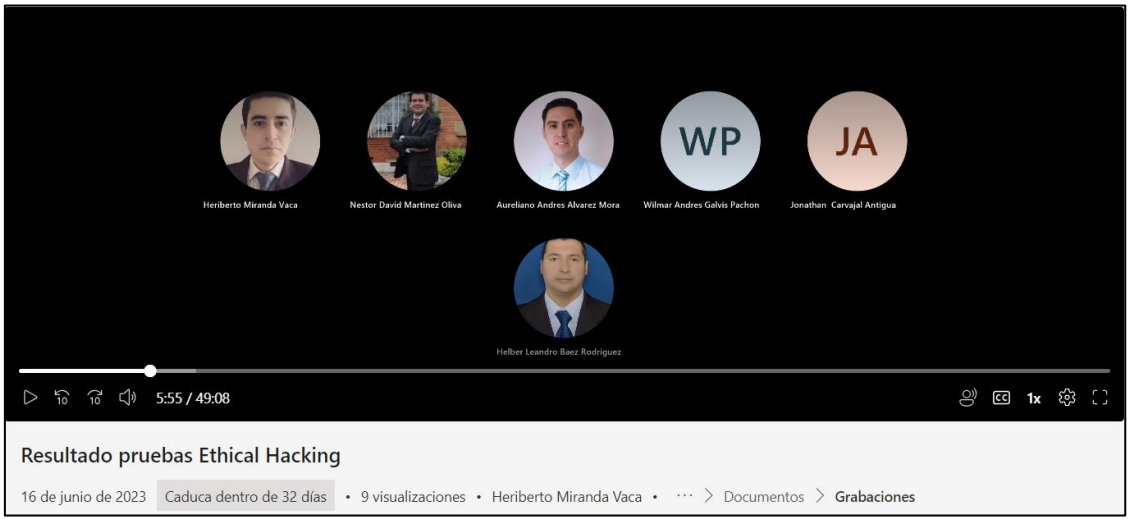
This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
ucompensar servidores	May 19, 2023 16:49, EDT	May 19, 2023 17:57, EDT	1 hours 8 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on 121 systems, 121 of which were found to be active and were scanned.

Vulnerabilities by Severity	Nodes by Vulnerability Severity



Apéndice E

Proceso de Divulgación con la Comunidad Educativa