UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2023**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS
Línea de Investigación:
SISTEMAS DE INFORMACIÓN E INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)
Autor:
Guilcapi Mainato Jhonny Ricardo
Tutor:
Mg. Recalde Varela Pablo Marcel

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS.

Elaborado por: JHONNY RICARDO GUILCAPI MAINATO, de C.I: 1723181309, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, JHONNY RICARDO GUILCAPI MAINATO con C.I: 1723181309, autor del proyecto de titulación denominado PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

Firma

ORCID: 0009-0007-5908-7621

Tabla de contenidos

Contenido

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Los ataques informáticos son hechos maliciosos llevados a cabo por personas o grupos con el único objetivo de comprometer sistemas informáticos. La ciberseguridad es crucial para prevenir y mitigar estos ataques, implicando prácticas y medidas para proteger los sistemas y datos, así como la educación de los usuarios en la detección mediante la seguridad informática.

Contextualización del tema

En la actualidad, los ataques cibernéticos y la sustracción de información sensible son frecuentes en las organizaciones, desde los inicios de la década de los sesenta y setenta basados en el surgimiento de los sistemas de computadoras, se dieron los primeros indicios de ciberataques, en los que se buscaba obtener acceso no autorizado a sistemas y robar datos confidenciales. A medida que la tecnología avanzaba, en los años noventa, los ataques cibernéticos se hicieron más relevantes y sofisticados, propagándose globalmente mediante virus (Sain, 2019).

Según (Guaña, y otros, 2022), el motivo primordial de los ataques informáticos es afectar directamente a las partes financieras de las organizaciones además de varios fines lucrativos más, tales como estructura política y estructura militar. La mayoría de estos daños son por adware, ataques de denegación de servicio, ataques de doxing, phishing, gusanos, ransomware, troyanos, spyware, entre otros. Para ello, diversas organizaciones utilizan varias soluciones para prevenir los daños causados por los ciberataques, haciendo uso de la seguridad informática.

Basado en todos estos diferentes tipos de ataques que se pueden dar a una empresa, se debe considerar la implementación de un plan de prevención que fortalezca la seguridad de la información sensible. Por lo que, para mitigar el robo de información, el área de TI podría optar por la aplicación de buenas prácticas de seguridad, tales como son: instalar un firewall, mantener el servidor actualizado, garantizar la protección de endpoints, encriptar los datos, hacer copias de seguridad, crear políticas de ciberseguridad, charlas y documentación.

Problema de investigación

El problema reside en que en la actualidad la mayoría de organizaciones, tienen un escaso conocimiento sobre ataques informáticos. La falta de conciencia y preparación en materia de seguridad informática constituye un problema grave hasta el día de hoy.

La creciente dependencia de la tecnología y los procesos digitales comerciales han hecho que las amenazas cibernéticas sean una preocupación, lo que con lleva al fácil acceso y posterior robo de información.

El verdadero inconveniente se presenta cuando datos confidenciales de una empresa, tales como: base de datos, cuentas bancarias, claves de acceso, datos financieros, estrategias internas, en fin, toda la información sensible es hurtado por agentes ilícitos. Lo que implica una serie de impactos negativos que pueden afectar significativamente en entornos financieros, jurídicos y su reputación de imagen. Con un plan de prevención de ataques basados en IPS e IDS y buenas prácticas internas se puede proteger a las áreas financieras de una empresa (Mostacero, 2020).

¿Con la prevención de ataques informáticos basado en sistemas de detección de intrusos, se puede mejorar la seguridad en las áreas financieras?

Objetivo general

Prevenir los ataques informáticos basado en IPS e IDS para minimizar el impacto en las áreas financieras.

Objetivos específicos

- Identificar los métodos más frecuentes de ataques informáticos en el ámbito empresarial.
- Determinar cuáles son los procesos internos y datos sensibles que maneja el departamento financiero.
- Desarrollar una estructura lógica y sistemática en el contenido del plan de prevención de ataques informáticos.
- Valorar el impacto que tendrá el área financiera, con esta nueva cultura de protección de datos**.**

Vinculación con la sociedad y beneficiarios directos

La seguridad informática en el ámbito empresarial es un tema que radica de manera más notable en el mundo tecnológico, ya que las personas están más conectados que antes a través de los diferentes dispositivos y plataformas. Debido a esto, se debe tener una cultura de seguridad más que todo en el tema de manejo de datos sensibles. Por ello la presente investigación toma como referencia a los objetivos de desarrollo sostenible basándose en el trabajo decente y crecimiento económico (Guevara, 2023).

Según la Onu (2019), en el octavo objetivo sostenible que habla de “promover el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo y el trabajo decente para todos”. Para tal efecto el uso de medidas de prevención de ataques cibernéticos, aportaría al trabajo sostenible y potencializa la tranquilidad en la sociedad digital.

Dentro de los beneficios sociales se puede destacar lo siguiente:

Protección de la infraestructura de la red. - Asegura que los sistemas estén resguardados contra accesos no deseados o no autorizados.

Mejor control de acceso a la información. - Determina el personal autorizado para tener acceso a determinados datos, aplicaciones y recursos.

Confianza de los clientes al entregarnos sus datos. - Se basa en las estrategias enfocadas en desarrollar una relación comercial duradera con el cliente.

Control del riesgo de pérdidas financieras. – Permite determinar las consecuencias de la inversión que puede incidir sobre las finanzas de una empresa.

Para culminar se enfatiza la importancia de aplicación del plan de seguridad informática para las empresas, previniendo los efectos negativos que produce un ciberataque.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Hoy en día es esencial implementar medidas de prevención contra las amenazas informáticas, ya que el aumento de la conectividad digital ha llevado consigo un incremento en los ciberataques y el robo de información.

1.1 Contextualización general del estado del arte

Información

Según Campuzano (2021), menciona que la información desempeña un papel sumamente significativo tanto en las instituciones de nivel público como en las instituciones de nivel privado, además de ser crucial para las actividades cotidianas de la sociedad. Las entidades reconocen la importancia de proteger la información de sus organizaciones y han establecido medidas para hacer frente a posibles ataques cibernéticos. Existen diversas formas de amenazas, muchas de las cuales implican un riesgo considerable para la entidad y requieren una evaluación exhaustiva.

Seguridad Informática

La información desempeña un papel sumamente significativo tanto en las organizaciones públicas como también en las privadas, además de ser crucial para las actividades cotidianas de la sociedad. Las entidades reconocen la importancia de proteger la información de sus organizaciones y han establecido medidas para hacer frente a posibles ataques cibernéticos. Existen diversas formas de amenazas, muchas de las cuales implican un riesgo considerable para la entidad y requieren una evaluación exhaustiva (Arcos, 2023).

Delincuencia financiera

La criminalidad financiera engloba desde el simple hurto o engaño perpetrado por individuos con malas intenciones hasta maniobras a gran escala dirigidas por grupos delictivos bien organizados que tienen alcance en todos los continentes. Estas actividades ilícitas de gravedad no deben subestimarse, ya que van más allá de su impacto en la comunidad y las finanzas. La delincuencia financiera impacta a la sociedad en su conjunto y esta forma de delincuencia ha adquirido una nueva dimensión gracias al rápido progreso de la tecnología digital. Los mismos que operan internacionalmente para evitar detección, y los recursos sustraídos atraviesan múltiples fronteras físicas y digitales antes de llegar a su destino final (Interpol, 2022)

Ataques Informáticos

El principal propósito de los ataques informáticos es causar daños financieros tanto a individuos como a organizaciones de diversos sectores. Estos ataques se originan a partir de una amplia gama de programas maliciosos, generalmente conocidos como malware.

Como resultado de este acontecimiento, las empresas implementan distintas estrategias o maniobras para prevenir los daños ocasionadas por los ciberataques. Estas estrategias se basan en el conocimiento de la seguridad informática, que recopila información día a día sobre los datos más recientes relacionados con la seguridad de los programas informáticos.

El propósito es identificar los tipos más comunes de ataques informáticos en el ámbito digital, con el propósito de comprender cómo se realiza y en qué consisten estas amenazas cibernéticas. Este entendimiento del tema permitirá implantar métodos y técnicas para minimizar las consecuencias que tienen sobre la seguridad de la información, como también es importante considerar que la principal debilidad en los métodos digitales radica en el factor humano (Lino, 2022).

Técnicas de ataques informáticos más frecuente

Existen varias técnicas utilizadas para llevar a cabo actos delictivos en contra de nuestra privacidad. Por ejemplo, podríamos caer en engaños de phishing, ser víctimas de ataques xploits o ser infectados con troyanos y otros tipos de software malicioso (Benavides, 2020).

Ingeniería Social

La Ingeniería Social describe una amplia variedad de técnicas que son ampliamente utilizadas por los ciberdelincuentes. Estas técnicas incluyen estrategias como los cebos, donde se presenta al usuario algo atractivo para inducirlo a descargar un archivo no deseado.

En este caso, los usuarios reciben correos electrónicos con la intención de obtener su información personal o datos valiosos de manera fraudulenta. Además, el scareware se emplea para engañar a los usuarios, haciéndoles creer que sus computadoras están infectadas con malware y ofreciéndoles supuestas soluciones que, en última instancia, terminan introduciendo más elementos maliciosos en el sistema (Tobar, 2022).

Robos de Información

Según Villegas (2022), La reorganización de la educación en ciberseguridad, es de extrema importancia en la actualidad, la gran parte del tiempo dedicamos a explorar el Internet y todos los conocimientos que nos brinda, ya sea para fines de estudio, laborales o simplemente para entretenimiento personal. Pero lastimosamente en estos instantes, existe la posibilidad de que los datos sean sustraídos.

Prevención ante ciberataques

Dado que los delincuentes cibernéticos operan en el anonimato y son difíciles de identificar, es posible que pase un período considerable antes de que los problemas se vuelvan evidentes para una organización. Aunque ciertas amenazas puedan ser descubiertas, la mayoría pasará inadvertida. Por lo tanto, la detección temprana siempre será un aspecto fundamental. Por lo tanto, se presenta algunos pasos preventivos para estar listo: supervisa el uso de correos electrónicos, estar alerta del tráfico anormal, reconoce las conexiones sospechosas, mantén tu sistema actualizado.

1.2 Proceso investigativo metodológico

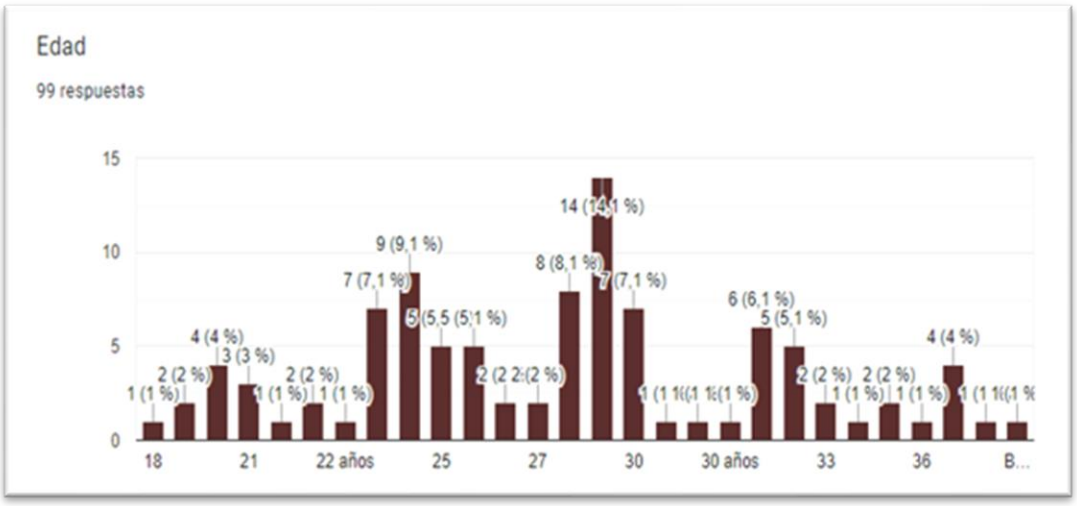
La presente investigación es basaba en una metodología cualitativa - descriptiva, que permitió recopilar, simplificar, estructurar y presentar datos provenientes de diversas fuentes bibliográficas y sitios web. Al reunir información relacionada con estrategias de prevención de ciberataques comunes en empresas, se identificaron los posibles riesgos que enfrentan y las formas de mitigarlos. Para llevar a cabo esta labor, se empleó la técnica de encuesta, en la cual se utilizaron preguntas cerradas y de selección múltiple para identificar los métodos más frecuentes de ataques cibernéticos.

Adicionalmente, se adoptó el enfoque de investigación deductiva. La línea de investigación seleccionada para este estudio se centra en Sistemas de Información y Comunicación, Emprendimiento e Innovación, con una sublínea específica en redes y tecnología de software y hardware (Aguirre, 2015).

1.3 Análisis de resultados

En la actual investigación se realizó la recopilación de datos mediante encuestas, utilizando la plataforma de Google Forms con preguntas estructuradas en Escala Likert. La cual obtuvo resultados importantes para la investigación que se detallan a continuación.

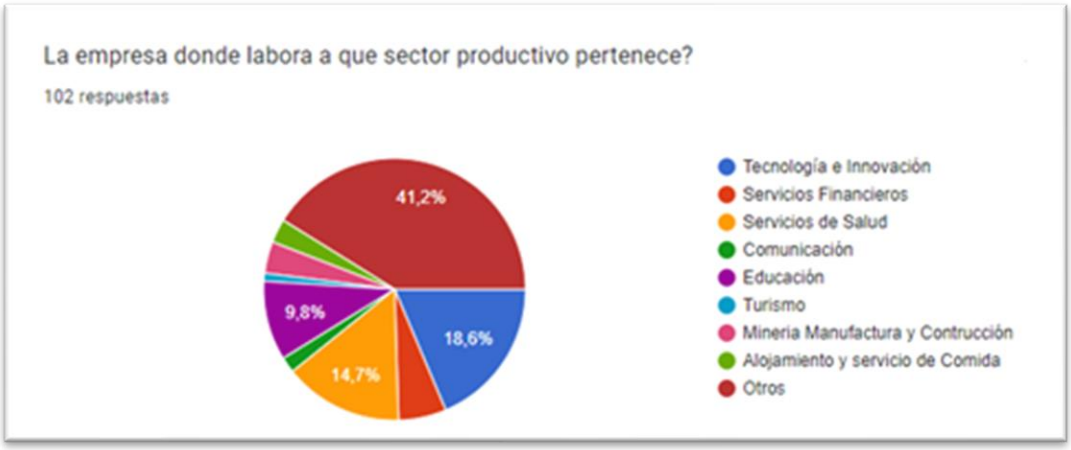
Figura 1.
Tabla de edades de encuestados



Nota: Gráfico de barras de edades de encuestados.

Dentro de los encuestados se toma en cuenta un promedio de edad entre 18 y 38 años. Los mismos que cumplen con características relevantes como conocedores de los avances tecnológicos y que se desempeñan en un ámbito laboral, de esta manera con su experiencia y conocimiento del tema, aportan a la investigación.

Figura 2.
Sector producto de investigación



Nota: Representación de Pastel de sectores productivos encuestados.

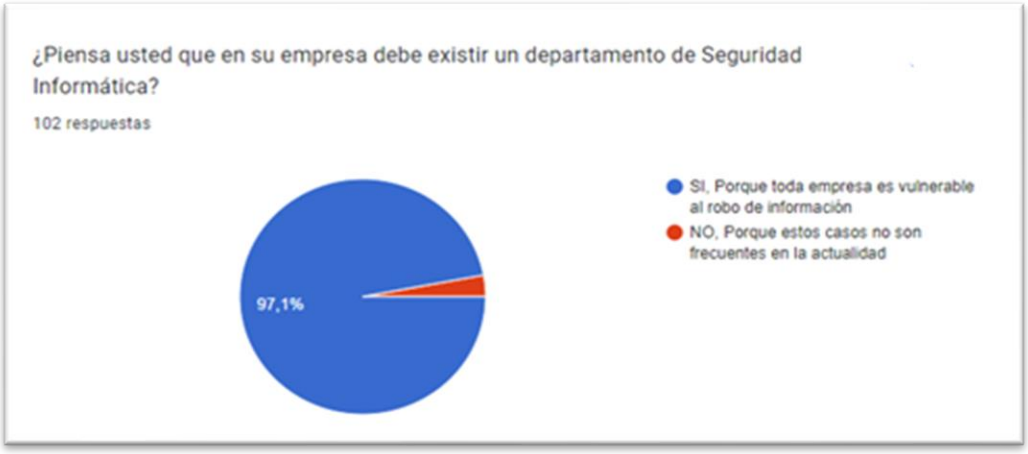
En la figura número 2 se puede apreciar que la mayor cantidad de los encuestados está inmersa en el Sector Financiero, por lo que la información contenida refleja la situación verdadera en el campo laboral y por ellos resultan ser datos muy relevantes para esta investigación.

Figura 3.
Área de trabajo

Nota: Participación de áreas de trabajo encuestadas.

El mayor grupo de encuestados correspondiente al 28.4% pertenecen al área de producción, seguido del 18.6% que corresponde al departamento de tecnología de la información y en tercer lugar está el área contable financiera. En base a estos resultados se describe que el grupo de encuestados forman parte de un segmento clave para la recopilación de datos en el sector empresarial.

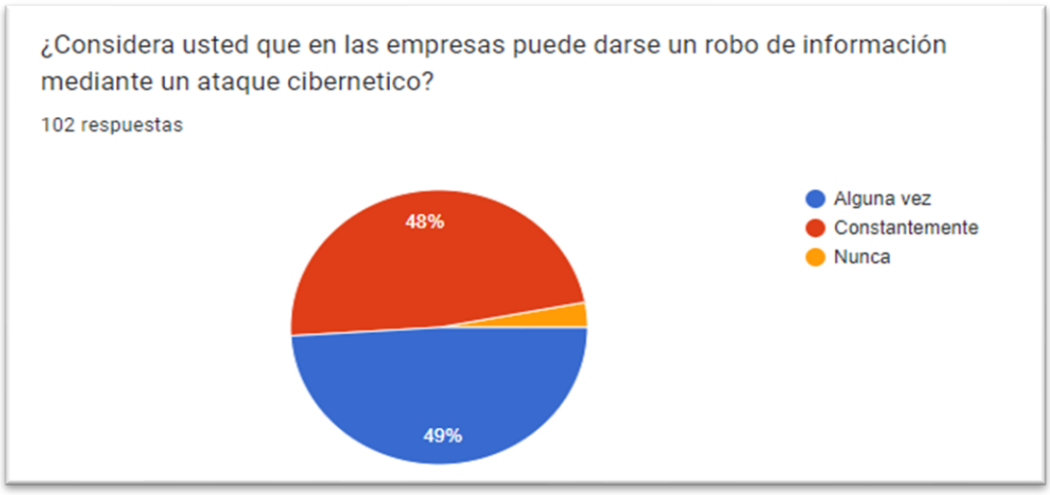
Figura 4.
Existencia de Seguridad Informática en las empresas



Nota: Recomendación de la implementación de un departamento financiero.

Los resultados mencionan que el 97.1% corroboran la importancia de la existencia de un departamento de seguridad informática en una empresa, ya que esta área está destinada a salvaguardar la estabilidad de la información.

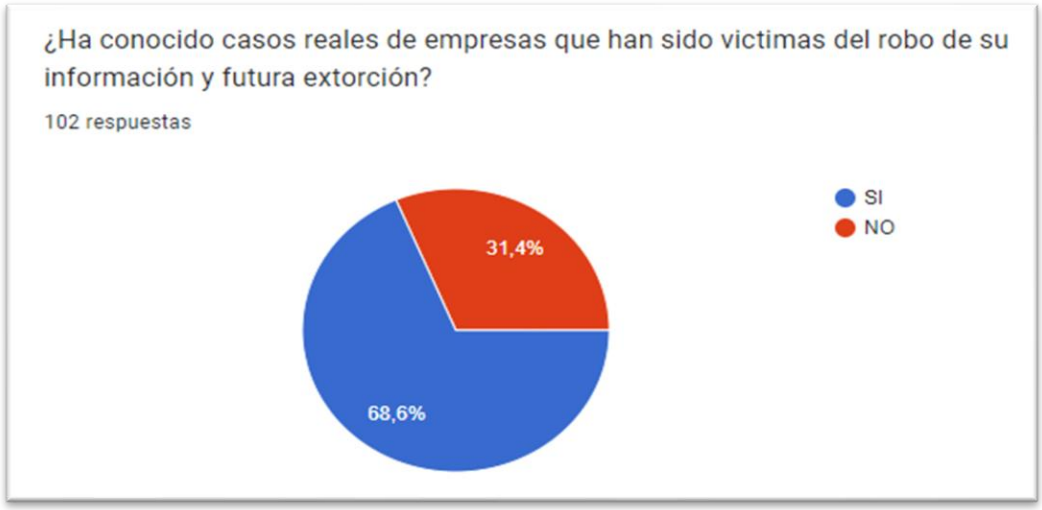
Figura 5.
Nivel de frecuencia de robo de información



Nota: Conocimiento general de las personas a los ataques cibernéticos.

En los resultados del nivel de frecuencia para que se dé un robo de información, el 49% de encuestados considera que ocurre de manera irregular. Es decir, alguna vez se ha dado en la historia de una empresa. Mientras que el 48% considera que se da con mayor frecuencia.

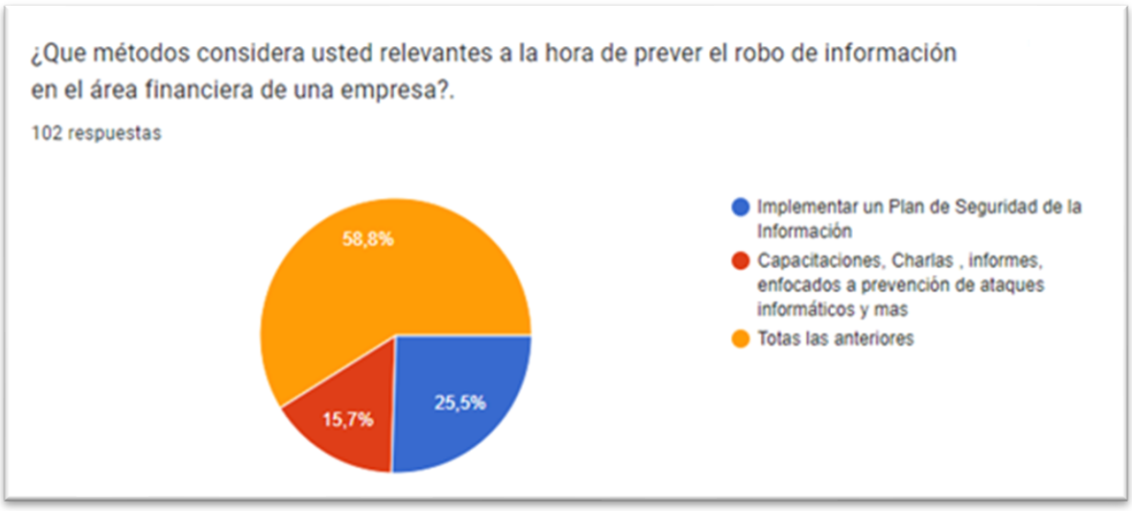
Figura 6.
Realidad de casos existentes



Nota: Conocimiento de casos reales de ataques informáticos a las empresas.

El 68.5% de los encuestados mencionan haber conocido algún tipo de robo o ataque cibernético a una empresa. Esto refleja que el caso no es aislado en el ámbito laboral y a su vez se debe dar mayor atención y protección a esta amenaza.

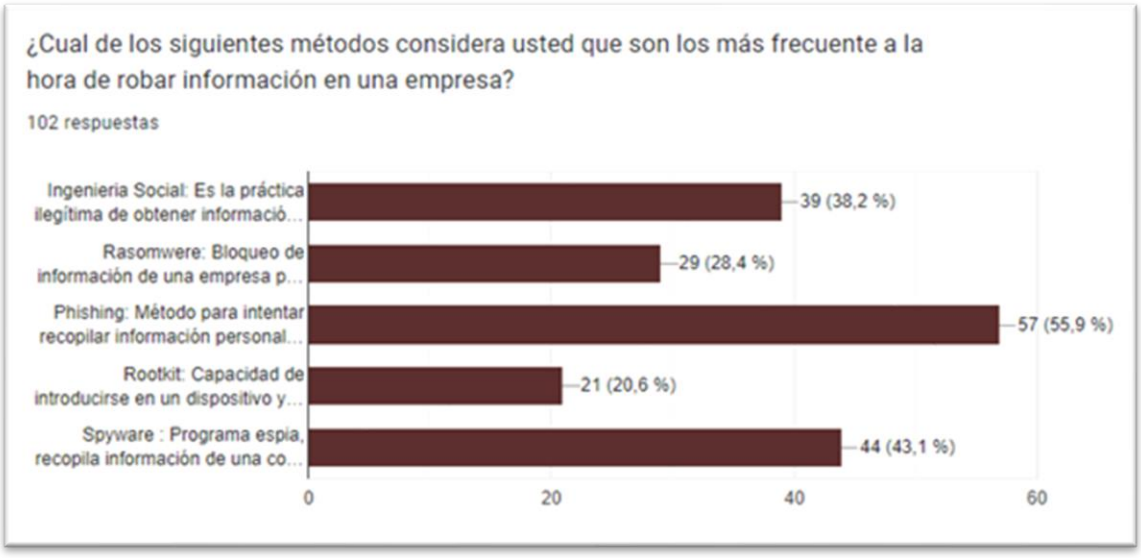
Figura 7.
Métodos para mitigar el robo de información



Nota: Tips para la mitigación del robo de datos.

Más del 50% de los encuestados, concuerdan que se debe aplicar algún tipo de métodos para prever el robo de información. El resultado de esta pregunta es una evidencia precisa de la relevancia que hay a la hora de crear un Plan de prevención de ataques informáticos.

Figura 8.
Formas más frecuentes para robar información



Nota: Ataques informáticos más conocidos.

La figura número 8 representa el tipo de métodos aplicables por la ciberdelincuencia para hurtar información financiera de una empresa. El 55.9% de encuestados mencionaron que el método más utilizado para este tipo de delitos es Phishing, que representa el estudio y

análisis de intentar recopilar información personal y por medio de ella desarrollar el acto ilícito.

Figura 9.
Buenas prácticas de protección de datos.

Nota: Buenas prácticas para proteger nuestros datos.

El 52.9% de los encuestados afirman que No conocen de las buenas prácticas para proteger sus datos financieros. Esto refleja un gran porcentaje de desconocimiento y vulnerabilidad en la sociedad.

Figura 10.
Seguridad informática

Nota: Bases del concepto de la seguridad informática.

Los resultados reflejan que el 83.3% de personas analizadas, aciertan con la definición de Seguridad Informático. Por lo que se entiende que la población está al tanto de la existencia de esta disciplina, pero no conoce de la funcionalidad y beneficios.

CAPÍTULO II: PROPUESTA

Dada la gestión de datos confidenciales que las empresas manejan en la actualidad, resulta imperativo reducir la posibilidad de que los ciberdelincuentes roben información empresarial, es por esto que se debe implementar un plan de seguridad informática para salvaguardar toda la información.

2.1 Fundamentos teóricos aplicados

Según Farro (2020), la seguridad informática mediante el Sistemas de Prevención de Intrusos y el Sistemas de Detección de Intrusos implica la implementación de herramientas y tecnologías diseñadas para identificar y alertar sobre actividades anormales de una red o sistema.

Un Sistemas de Prevención de Intrusos (IPS) no solo detecta las actividades maliciosas, sino que también toma medidas activas para prevenir o detener los ataques. Puede bloquear el tráfico o aplicar reglas de seguridad en tiempo real, para evitar que una amenaza se materialice en un ataque exitoso.

En cambio, un IDS monitorea y analiza todo el tráfico de la red en busca de códigos y firmas asociadas con actividades maliciosas. Cuando detecta esta actividad sospechosa, genera alertas para que los administradores de seguridad tomen acción.

Desarrollo e Implementación con IPS e IDS

Según Pardo (2019), describe el enfoque integral de seguridad informática utilizando un Sistemas Detección de Intrusos, para detectar, mitigar y analizar ataques informáticos en las empresas.

Planificación y Diseño IPS:

Con un Sistema de Prevención de intrusos (IPS) podemos evitar en su gran mayoría que los hackers accedan a la red empresarial y ataquen al área financiera. Sin embargo, se debe considerar los siguientes puntos para tener una planificación y minimizar el impacto de los ataques:

Identificar activos críticos: Determinar qué activos y sistemas son más valiosos y deben ser protegidos con mayor énfasis en el área financiera como: bases de datos, cuentas bancarias, documentos, firmas, estados de cuenta, estrategias de negocio, entre otros.

Topología de red: Se debe comprender la arquitectura de la red y decidir dónde colocar los sensores de IPS, para cubrir los puntos de entradas y salidas más críticos.

Reglas y firmas: Se debe configurar las reglas y firmas del IPS para detectar y bloquear patrones de tráfico maliciosos específicos.

Software y Hardware: Decidir si implementar un IPS como dispositivo hardware independiente o como software en un servidor.

Capacidad de rendimiento: Asegurar que el IPS pueda manejar la carga de tráfico de la red sin degradar el rendimiento.

Vigilancia continua: Configurar el IPS para monitorear constantemente el tráfico en busca de patrones de comportamiento malicioso o actividades sospechosas.

Alertas y notificaciones: Configurar el sistema para que genere alertas en tiempo real cuando se detecten amenazas.

Acción automática**:** Configurar el IPS para que tome medidas automáticas en función de las reglas y firmas configuradas. Se puede bloquear direcciones IP, detener conexiones, entre otros.

Planificación y Diseño IDS:

Cuando un ciberdelincuente ya ha podido vulnerar la seguridad de una empresa se aplica un Sistema de Detección de intrusos (IDS), donde alerta al centro de seguridad las amenazas capturadas. Se debe considerar los siguientes puntos para tener una planificación y contrarrestar el impacto de los ataques:

Ubicación Estratégica: Colocar los sensores de IDS en ubicaciones estratégicas dentro de la red para cubrir puntos de entrada y salida, así como segmentos críticos.

Selección de IDS: Elegir entre IDS de red e IDS de host, dependiendo de tus necesidades y los sistemas que deseas proteger.

Configuración y Personalización:

Ajustar las reglas y firmas del IDS para adaptarlas a tu entorno y amenazas específicas.

Configurar umbrales y niveles de alerta para evitar falsos positivos y negativos.

Monitoreo Continuo: Asegurar que el IDS monitoree el tráfico y la actividad de manera constante en busca de patrones sospechosos.

Generación de Alertas: Configurar el IDS para enviar alertas en tiempo real cuando se detecten actividades sospechosas o potencialmente maliciosas.

Respuesta a Incidentes: Definir procedimientos claros para responder a las alertas de IDS, lo que podría incluir el aislamiento de sistemas afectados, la recopilación de evidencia y la mitigación de la amenaza.

La seguridad informática basado en IPS e IDS garantiza una estrategia estructurada para prevenir, detectar y responder a posibles amenazas cibernéticas, fortaleciendo la defensa de la infraestructura tecnológica de la organización.

2.2 Descripción de la propuesta

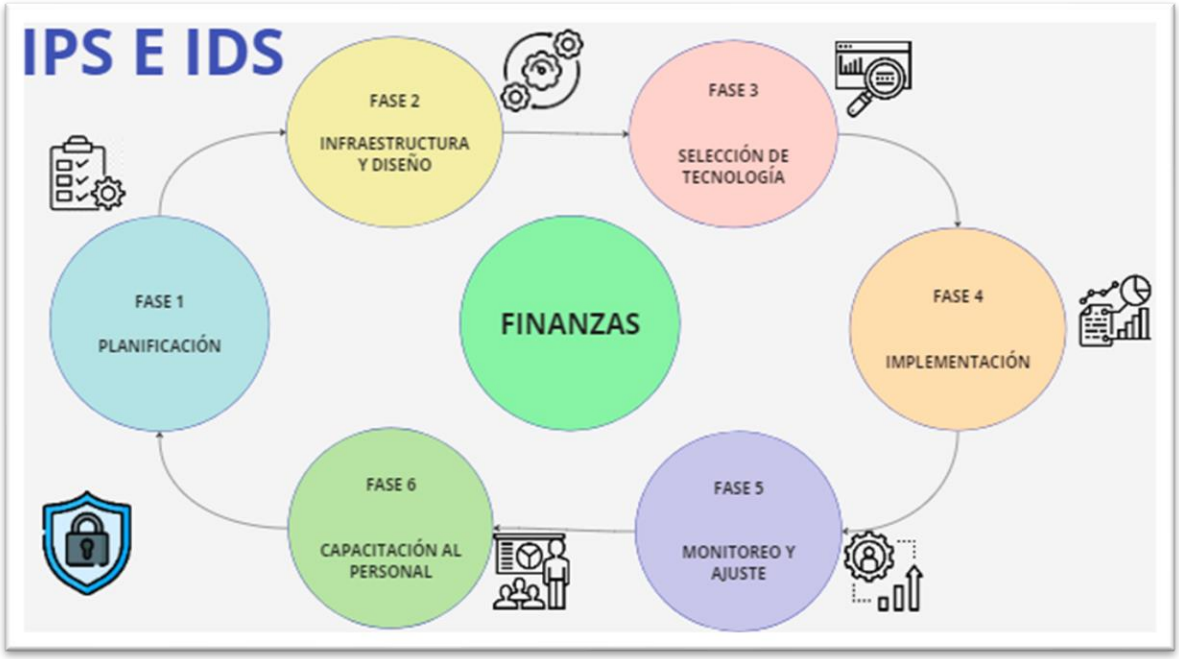
El proyecto se fundamenta en la presentación de un plan de seguridad preventiva, el cual se deriva de los resultados recopilados a través de encuestas, que identifican los diferentes tipos de ataques informáticos en el departamento financiero. Estos ataques abarcan áreas como sitios web confiables, correos electrónicos, plataformas de redes sociales y la gestión de claves de acceso, así como el control de información delicada.

a. Estructura general

Según Suárez, Sotomayor , & Medina (2021), afirma que entender el ciclo de evolución de un ciberataque es esencial para identificar y poner fin al mismo. Esto implica comprender cómo se desarrolla y progresa un ataque informático.

Esta comprensión permite establecer una serie de acciones y precauciones que aseguran cierto grado de protección en caso de ser blanco de un ciberataque. A continuación, se establecen 6 fases para el plan de prevención.

Figura 11.
Planificación por Fases



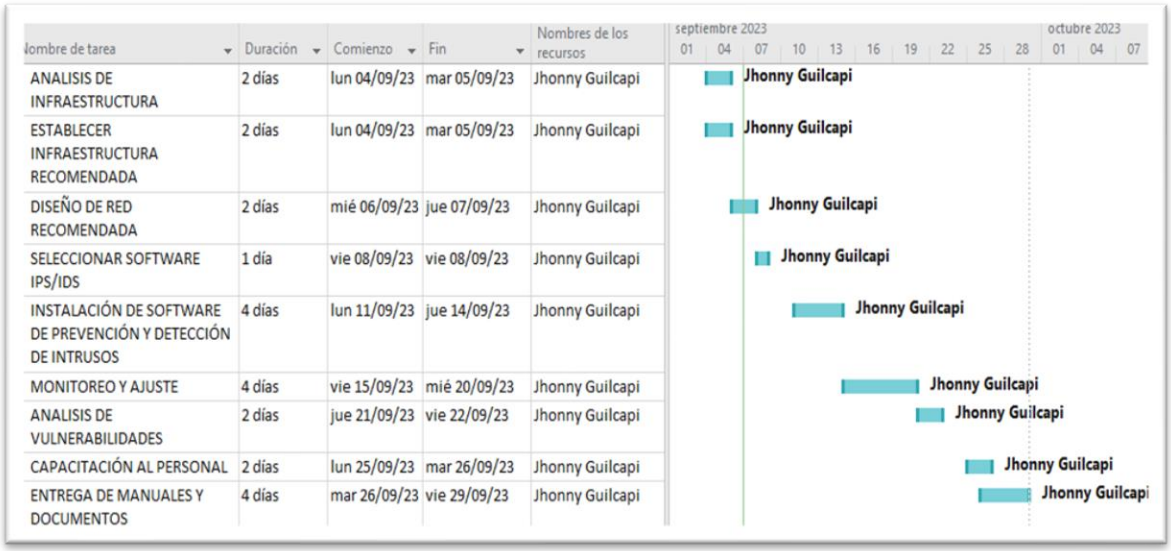
Nota: Elaboración Propia, fases de la implementación.

b. Explicación del aporte

La implementación de sistemas de intrusiones IPS e IDS implica varias fases para asegurar de que estos sistemas estén configurados y funcionen de manera efectiva. A continuación, se da a conocer las fases para implementar en el área financiera:

Fase_1: Planificación

Figura 12.
Cronograma de actividades



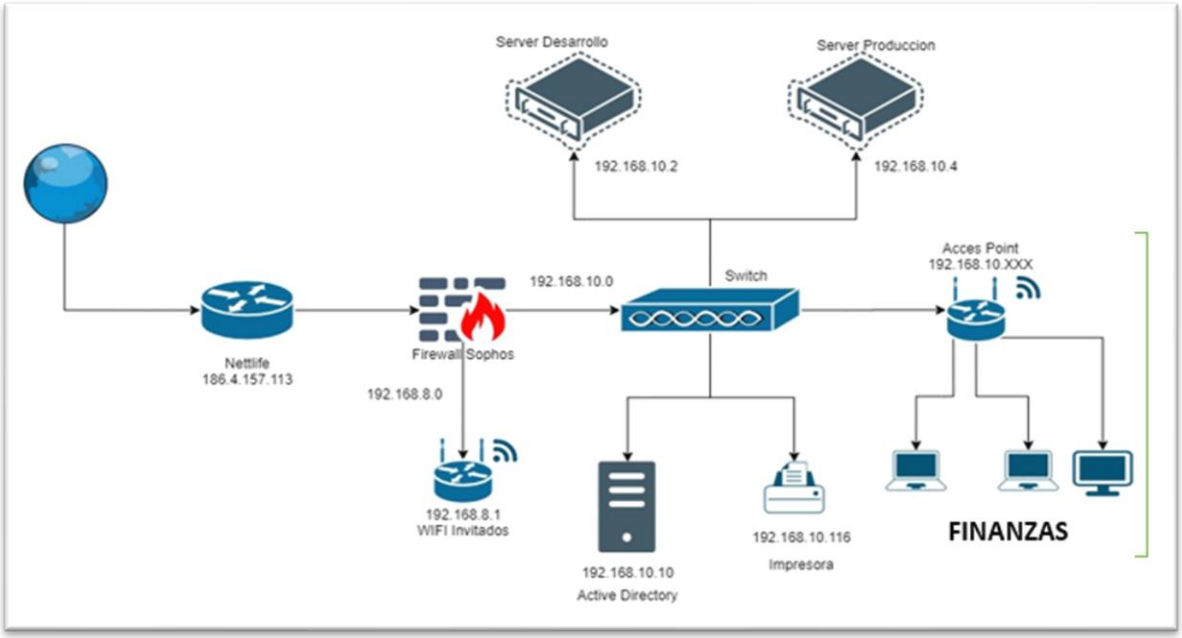
Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
ANALISIS DE INFRAESTRUCTURA	2 días	lun 04/09/23	mar 05/09/23	Jhonny Guilcapi
ESTABLECER INFRAESTRUCTURA RECOMENDADA	2 días	lun 04/09/23	mar 05/09/23	Jhonny Guilcapi
DISEÑO DE RED RECOMENDADA	2 días	mié 06/09/23	jue 07/09/23	Jhonny Guilcapi
SELECCIONAR SOFTWARE IPS/IDS	1 día	vie 08/09/23	vie 08/09/23	Jhonny Guilcapi
INSTALACIÓN DE SOFTWARE DE PREVENCIÓN Y DETECCIÓN DE INTRUSOS	4 días	lun 11/09/23	jue 14/09/23	Jhonny Guilcapi
MONITOREO Y AJUSTE	4 días	vie 15/09/23	mié 20/09/23	Jhonny Guilcapi
ANALISIS DE VULNERABILIDADES	2 días	jue 21/09/23	vie 22/09/23	Jhonny Guilcapi
CAPACITACIÓN AL PERSONAL	2 días	lun 25/09/23	mar 26/09/23	Jhonny Guilcapi
ENTREGA DE MANUALES Y DOCUMENTOS	4 días	mar 26/09/23	vie 29/09/23	Jhonny Guilcapi

Nota: Elaboración Propia.

En el cronograma que se muestra de la figura 12 se establece toda la planificación por actividades, fechas y responsables para la implementación de la herramienta de prevención y detección de intrusos. Esta planificación de actividades es de vital importancia para llevar a cabo una implementación adecuada y segura.

Fase_2: Infraestructura y Diseño

Figura 13.
Diseño de Red



Nota: Elaboración Propia.

En la figura 13, se establece un diseño de red recomendado, ya que esta tiene una base organizacional y estructurada. Así podemos observar todos los componentes de la red empresarial desde la entrada del internet, hasta llegar al área financiera.

Tabla 1.
Recomendación de Infraestructura

Componentes	**Características**
Servidores	Modelo: System x3550 M5 Capacidad: 1,81 TB Dimensiones Físicas: (aproximadamente) Ancho: 43 cm Profundidad: 73
Componentes	**Características**

Dominio	NIC EC
Certificado SSL	GoDaddy
Seguridad de red	Sophos XG125
Switch	Switch hp 1910 48 puertos jg540a
Estaciones de trabajo	Modelo: Lenovo
	Procesador: Intel Corei7
	RAM: 16 GB
	Disco SSD: 460 GB
	Sistema Operativo: Windows 10
Seguridad estaciones de trabajo	Microsoft Security Esentials,
	antivirus de archivos y trabaja
	con el firewall de Windows 10
Antivirus estaciones de trabajo	Norton Licenciado
Internet	Netlife
	Ancho de banda de 100 Mbps

Nota: Elaboración Propia.

Para llevar a cabo la instalación de un sistema de prevención de intrusos es recomendable varias características a nivel de componentes físicos y lógicos, ya que al tener una infraestructura adecuada se minimizan los ataques informáticos.

Fase_3: SELECCIÓN DE TECNOLOGÍA

Tabla 2.
Tipos de Software de monitoreo

Nombre de herramienta	Compatibilidad del SO	Costo	Monitoreo en tiempo real
Wazuh	Linux/Windows	Gratis/Open Source	SI
Solarwinds Security Event manager	Linux/Windows	$1,995 anual	SI
Suricata	Linux Free BSD/Windows	Gratis/Open Source	SI
McAfee Enterprise Security Manager	Linux/Windows	$1,500 anual	SI
OpenVas	Linux	Gratis/Open Source	NO

Nota: Elaboración Propia.

Tabla 3.
Software Suricata

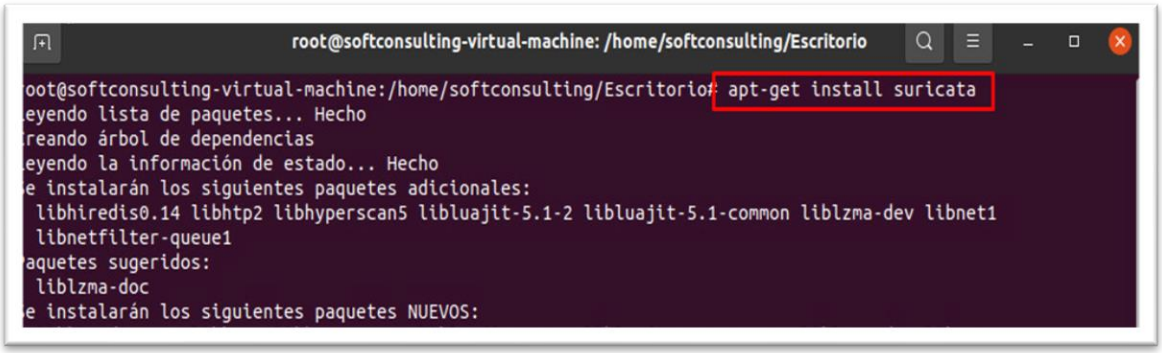
Detalle	IPS-IDS
Software	SURICATA
Creador	OSIF (Open Information Security Foundation)
Licencia	Open-Source
¿Que detecta?	Esta herramienta puede analizar paquetes, y también revisar certificados TLS, SSL, peticiones DNS y solicitudes HTTP.
Ventajas	Tiene una arquitectura multi hilos. Se beneficia con los procesadores multi-núcleo Si se descargan malware en los equipos, con esta herramienta es posible capturarlos y estudiarlos desde Suricata.
Desventajas	No existe un parche para la mayoría de los bugs de seguridad, se requiere de un tiempo de espera para su solución por parte de las comunidades que lo desarrollan No es sustituto para un Firewall.
Costo	Gratuito

Nota: Elaboración Propia.

Basado en el análisis de herramientas de detección de intrusos IPS e IDS, podemos observar que una de las mejores herramientas es el software de Suricata, ya que al ser Open-Source y sin costo nos da uno de los mayores beneficios para la implementación y mitigación de ataques informáticos.

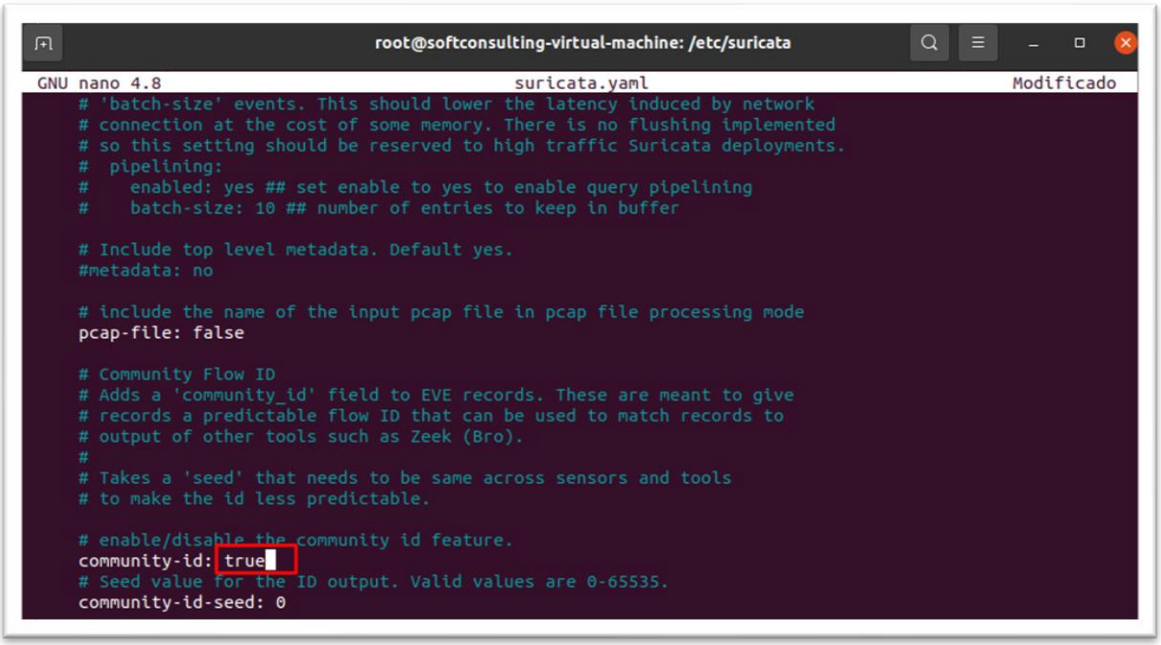
Fase_4: IMPLEMENTACIÓN

Figura 14.
Instalación Suricata



Nota: Elaboración Propia.

Figura 15.
Identificación de comunidad

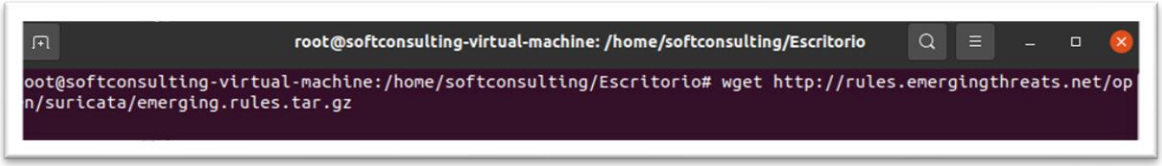


Nota: Identificación de comunidad, editar directiva “community-id” con valor de “true” en archivo /etc/suricata/suricata.yaml. Elaboración Propia

Figura 16.
Interfaz

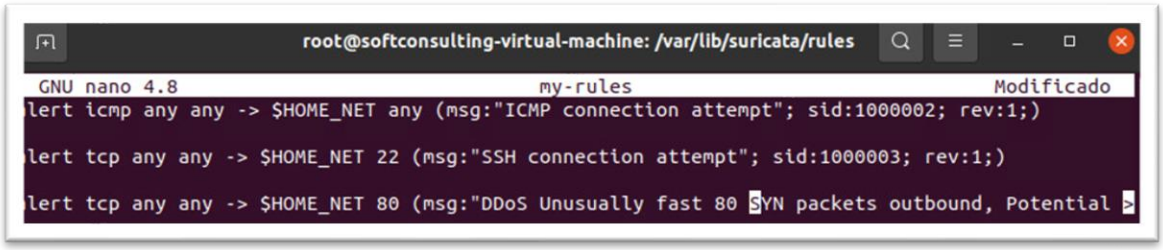
Nota: Definiendo que interfaz de red se debe monitorear: Elaboración personal.

Figura 17.
Descarga de reglas de la comunidad de Suricata



Nota: Elaboración propia.

Figura 18.
Creamos reglas personalizadas para probar Suricata



Nota: Elaboración propia

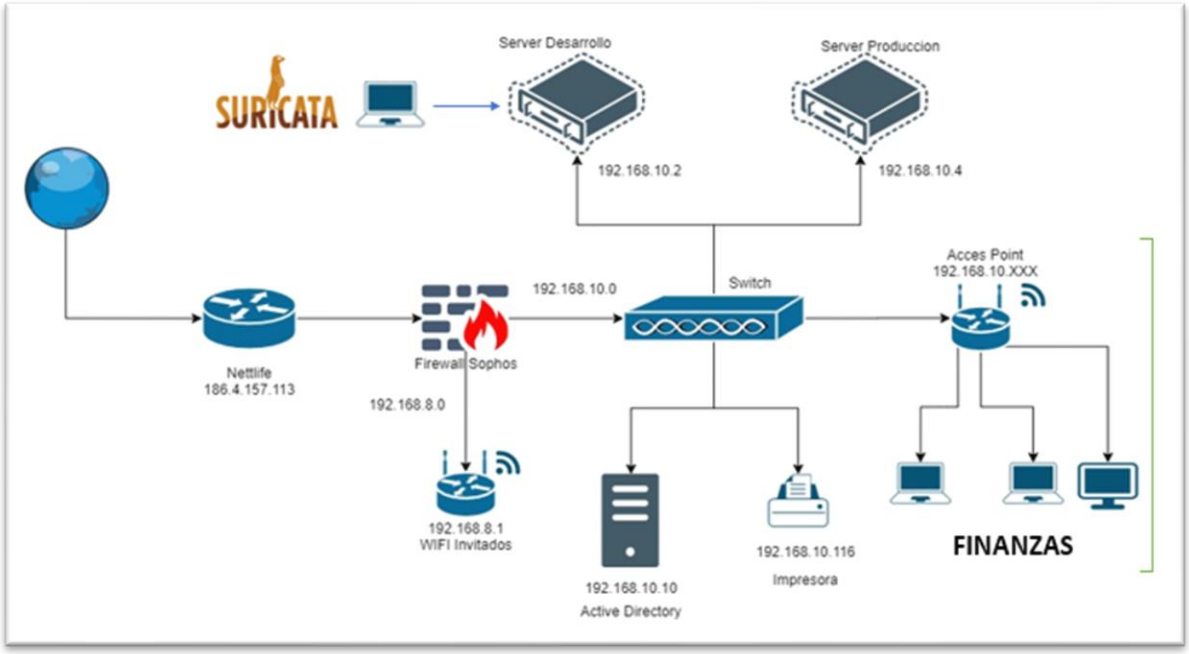
Figura 19.
Reglas de la comunidad

Nota: Elaboración propia

Figura 20.
Ejecutar suricata

Nota: Elaboración propia.

Figura 21.
Implementación de Software



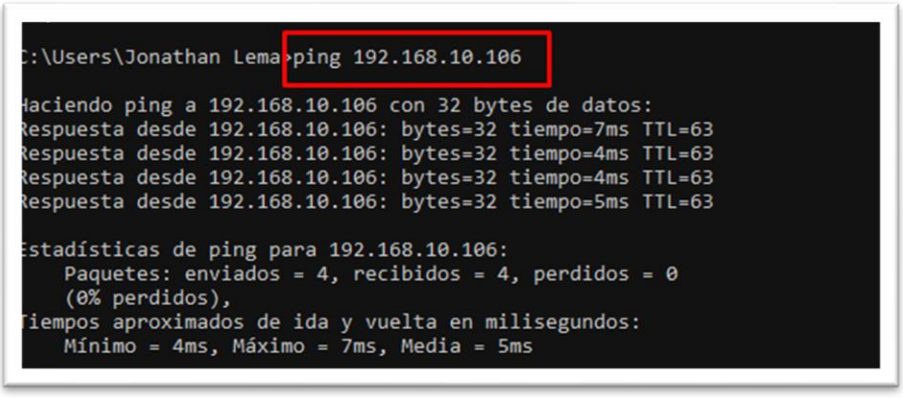
Nota: Elaboración Propia.

En base a la implementación del software Suricata instalado en una máquina virtual dentro de los servidores de una empresa, se ejecuta el monitoreo en la red para monitorear el área de finanzas.

Fase_5. MONITOREO Y AJUSTE

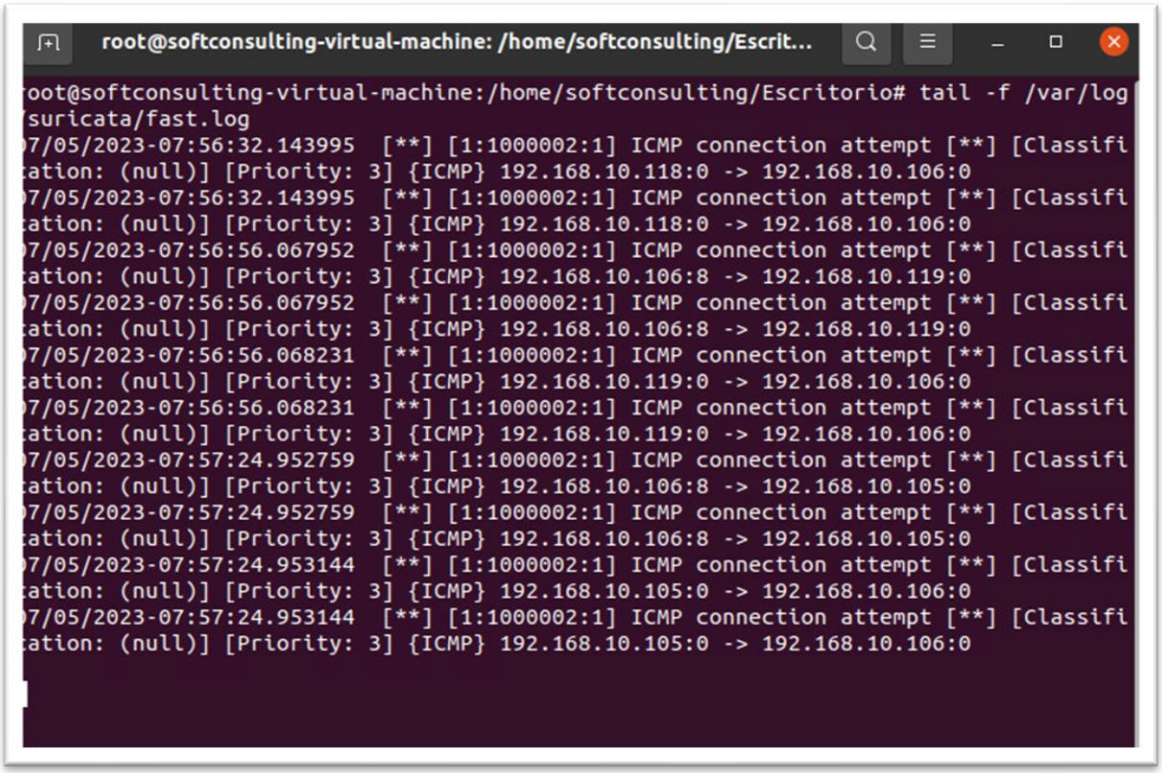
Para realizar el respectivo monitoreo desde el área de finanzas lo primero que se hace es desde un computador que se encuentra en dicha área, realizar un ping hacia la máquina virtual 192.168.10.106 donde se encuentra instalado el software de suricata.

Figura 22.
Conexión mediante ping



Nota: Elaboración Propia.

Figura 23.
Análisis del log de eventos de suricata en tiempo real



Nota: Elaboración Propia.

Tabla 4.
Componentes del monitoreo

Activo	Código	Nombre	Detalle
1	ACT-SC-1	ROUTER ISP	Huawei HG8545H
2	ACT-SC-2	Firewall	Sophos XG125
3	ACT-SC-3	Servidor Desarrollo	IBM X3650 M4
4	ACT-SC-4	Servidor Producción	Lenovo X3550 M5
5	ACT-SC-5	Servidor Active Directory	Lenovo
6	ACT-SC-6	Impresoras	LaserJet
7	ACT-SC-7	Switch	HP
8	ACT-SC-8	Access Point LAN	Aruba
9	ACT-SC-9	Computadoras de Empleados	Windows 10
10	ACT-SC-10	Computadoras de Empleados	Windows 10
11	ACT-SC-11	Computadoras de Empleados	Windows 10

Nota: Elaboración Propia.

Se realizo el análisis y monitorización en base a los distintos componentes que tienen la red, y son los siguientes:

ACT-SC-1 no fue posible realizarlo ya que, si bien es cierto, forma parte de la infraestructura tecnológica de la organización y se encuentra definida en la topología de la red. Esta pertenece al proveedor de Internet y por el momento no se cuenta con acceso para poder obtener datos y monitorizarlo.

Se realizó la monitorización para el activo ACT-SC-2 mediante él envió de logs con el protocolo syslog y no se encontraron vulnerabilidades.

Para el análisis de resultados de los activos ACT-SC-3 y ACT-SC-4 se realizó el envío de logs por syslog a una máquina virtual con distribución de Linux, en la cual se instaló Suricata para la recolección de los logs.

En el caso del activo ACT-SC-5, la monitorización no fue posible debido a que el activo se encuentra dentro de la infraestructura tecnológica de la organización, pero no está en uso y se encuentra apagado.

En el caso del activo ACT-SC6, la monitorización no fue posible debido a que el activo se encuentra dentro de la infraestructura tecnológica de la organización, pero es una Impresora.

Para los activos de ACT-SC-7 y ACT-SC-8 se realizó la monitorización mediante él envió de logs con el protocolo syslog y no se encontraron vulnerabilidades.

Para el análisis de los activos ACT-SC-9, ACT-SC-10, ACT-SC-11 se realizó la monitorización con la herramienta suricata para el envío de datos y parámetros que mediante reglas definidas en su archivo de configuración permite su análisis, por medio de su módulo de detección de vulnerabilidades nos informó las incidencias encontradas.

Tabla 5.
Vulnerabilidades

Siglas	Monitorización	Vulnerabilidad	Detalle
ACT-SC-1	N/A	N/A	Forma parte de la infraestructura tecnológica, pero pertenece al proveedor de Internet y por el momento no se cuenta con acceso.
ACT-SC-2	Syslog	N/A	N/A
ACT-SC-3 y ACT-SC-4	Syslog	$HOME_NET 22 msg:"SERIALIZINGME SCAN OpenSSH Based SSH Connections Allowed" (SSH ABIERTO)	Mitigación: Deshabilitar el protocolo SSH para evitar intrusiones en los servidores de manera remota. Solo habilitar cuando sea necesario.
ACT-SC-5	N/A	En el caso del activo ACT-SC-5, la monitorización no fue posible debido a que el activo se encuentra dentro de la infraestructura, pero no está en uso y se encuentra apagado.	N/A
ACT-SC-6	Syslog	No se realizó la monitorización del equipo debido a que no es posible la instalación de un agente de monitorización	N/A
ACT-SC-7	Syslog	Se ha realizado la monitorización mediante Syslog y no se encontró vulnerabilidades.	N/A
ACT-SC-8	Syslog	Se ha realizado la monitorización mediante Syslog y no se encontró vulnerabilidades.	N/A
ACT-SC-9, 10, 11	Syslog	No se encontraron vulnerabilidades.	N/A

Nota: Elaboración Propia.

Culminadas todas las pruebas necesarias para la evaluación de las soluciones se encontraron resultados de vulnerabilidades que después de investigar representan un riesgo tolerable a alto para la infraestructura de TI.

Entre los resultados se encontraron puertos TCP y UDP abiertos, información como correos electrónicos empresariales detectados por aplicaciones de reconocimiento de dominios y una vulnerabilidad que podría ser causar una denegación de servicios, pero la cual después de verificar ya ha sido corregida.

Fase_6. CAPACITACIÓN AL PERSONAL

La capacitación del personal es esencial para maximizar la efectividad de los sistemas IPS e IDS y garantizar que tanto el equipo financiero como las demás áreas esté preparados para enfrentar las amenazas cibernéticas de manera eficaz. A continuación, veremos puntos importantes para la mitigación de dichas amenazas:

Contraseñas Fuertes: Se debe crear contraseñas únicas y complejas para cada cuenta, utilizando una composición entre mayúsculas y minúsculas, caracteres especiales y números.

Educa a los Empleados: Proporcionar información en ciberseguridad a los empleados para que puedan reconocer las señales de posibles ataques, como phishing, ingeniería social, entro otras y eviten caer en trampas.

Realiza Backups Regularmente: Crear backups de seguridad periódicas de tus datos críticos en sistemas separados y seguros. Esto les permitirá recuperar fácilmente de ataques de ransomware u otros problemas.

Segmenta la Red: Dividir la red en segmentos para limitar la propagación de ataques. Esto asegura que, si un segmento se ve comprometido, el atacante no tenga acceso inmediato a toda la red.

Controla los Privilegios de Acceso: Otorgar acceso solo a aquellos empleados que realmente necesitan ciertos recursos o datos. Limitar los privilegios reduce el impacto potencial de un ataque.

Realiza Pruebas de Penetración y Evaluaciones de Seguridad: Contrata profesionales de seguridad o utiliza herramientas automatizadas para evaluar tus sistemas y redes en busca de vulnerabilidades.

La seguridad informática es un esfuerzo continuo y colaborativo. Al aplicar estas medidas y mantener una actitud proactiva hacia la seguridad, se puede reducir significativamente el riesgo de ser víctima de ataques informáticos.

c. Estrategias y/o técnicas

Determinación de una estructura para el plan de prevención.

Análisis de riesgos

Realizar un análisis de riesgos de los recursos valiosos de la organización a nivel informático, con el propósito de ajustar las directrices de seguridad de acuerdo a la situación actual y real de la empresa. Este proceso implica identificar los activos de

información críticos de la empresa, como datos confidenciales, sistemas esenciales y procesos clave. Luego, se analizan las posibles amenazas y vulnerabilidades que podrían comprometer la integridad, confidencialidad y disponibilidad de estos activos.

Identificar las amenazas potenciales

Una vez que se han identificado las amenazas potenciales y las debilidades en la seguridad, se procede a evaluar la probabilidad de que ocurran incidentes de seguridad y el impacto que tendrían en la organización en términos de pérdida financiera, daño a la reputación y perturbación de operaciones.

Calcular el nivel de riesgo asociado y priorizar los riesgos asociados.

Con esta información, se puede calcular el nivel de riesgo asociado a cada amenaza y activo. Posteriormente, se priorizan los riesgos en función de su impacto y probabilidad, lo que ayuda a la empresa a asignar recursos de manera efectiva para mitigar las amenazas más críticas.

Ajustar e implementar nuevas medidas de seguridad.

En base a los resultados de esta evaluación de riesgos, se ajustan las políticas de seguridad existentes o se implementan nuevas medidas de seguridad. Esto garantiza que las prácticas de seguridad sean adecuadas y proporcionales a las amenazas reales que enfrenta la empresa, lo que a su vez contribuye a proteger sus activos de información y a mantener la continuidad de sus operaciones de manera más efectiva.

Difusión de medidas de seguridad informática a la organización.

Informar a todos los empleados involucrados acerca de las directrices, ventajas y posibles riesgos relacionados con los activos, recursos y componentes de seguridad. Se debe utilizar medios de comunicación oficiales, y recopilar evidencias que garantice la recepción de información completa al personal.

Definir el alcance de las políticas.

Definir de manera precisa y específica la extensión y limitaciones de las políticas con el propósito de prevenir situaciones tensas al implementar sistemas de seguridad. Además, es crucial identificar las razones que podrían obstaculizar la implementación efectiva de las políticas de seguridad informática. La claridad en la descripción del alcance de las políticas es esencial para evitar malentendidos y conflictos al implementar medidas de seguridad. Al tener una comprensión clara de lo que las políticas abarcan y lo que no, se minimiza la posibilidad de desacuerdos o tensiones entre los distintos departamentos y niveles de la organización.

Las dificultades en la aplicación de las políticas de seguridad informática pueden surgir debido a varias razones, tales como:

Resistencia al Cambio: La implementación de nuevas medidas de seguridad puede encontrarse con resistencia si los empleados están acostumbrados a métodos anteriores o consideran que las nuevas políticas son inconvenientes.

Complejidad Tecnológica: Si las políticas de seguridad requieren tecnologías o procesos complicados, puede haber dificultades en su implementación y mantenimiento.

Finalmente, para evitar tensiones al implementar medidas de seguridad en línea con las políticas establecidas, es crucial definir el alcance de manera clara y anticipar y abordar las posibles razones que puedan dificultar la aplicación de las políticas de seguridad informática.

2.3 Valoración de la propuesta

La elaboración de un plan de prevención contra ataques informáticos no solo evita la pérdida de información, sino que también establece una cultura de precaución a la hora de manipular y entregar datos por medio de cadenas digitales.

Haciendo un énfasis al cuidado que debe tener el área financiera, hay que implementar los sistemas que monitorean los eventos en tiempo real, buscando códigos de comportamiento inusuales que puedan indicar ataques o intrusiones. Los IPS e IDS contribuyen a fortalecer la protección contra accesos no autorizados, ataques informáticos y el robo de información sensible. Trabajando en conjunto con otras medidas de seguridad, los sistemas de detección de intrusos desempeñan un papel esencial en la defensa informática.

Es importante elegir las herramientas adecuadas según las necesidades de seguridad de la empresa, en este caso elegimos el software Suricata por su gran ayuda con la comunidad opensource y licencia gratuita. Cabe recalcar que Suricata no es para todos los usuarios ya que la respuesta de las vulnerabilidades que muestra, se enfoca en un aspecto bastante técnico, a diferencia de otras herramientas con más nivel gráfico, pero con un costo anual adicional. Es por eso que es viable implementar un plan de prevención de intrusos con el software de Suricata, así protegeremos al área financiera y sus intereses.

Finalmente, en base a la propuesta de este documento, se realizará un análisis con expertos en el área de seguridad informática, que permita valorar según su nivel de expertis la viabilidad de implementar un plan de prevención basados en IPS e IDS para el área financiera. Estos resultados se adjuntarán en el apartado de anexos.

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 6.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Conceptualización de términos	Términos como la información, seguridad informática, delincuencia financiera, ataques informáticos	Metodología enfoque cualitativo – descriptivo. Análisis de revisión documental.	Determinación de técnicas utilizadas para llevar a cabo actos delictivos en contra de nuestra privacidad.	Identificar los tipos más habituales de ciberataques en el entorno digital actual, con el objetivo de comprender cómo se llevan a cabo y en qué consisten estas amenazas.	Artículos de revista. Libros Trabajos Curriculares
IPS E IDS	Importancia de la aplicación para detectar actividades maliciosas tomar medidas activas de prevención y monitoreo.	Metodología enfoque cualitativo – descriptivo. Análisis de revisión documental.	Enfoque integral de seguridad informática utilizando IPS e IDS, para detectar y mitigar ataques informáticos	Define procedimientos claros para responder a las alertas de IPS e IDS, lo que podrá incluir el aislamiento de sistemas afectados, la recopilación de evidencia y la mitigación de la amenaza.	Artículos de revista. Libros Trabajos Curriculares
Encuestas al grupo objetivo referentes del	Conocimiento previo de la	Proceso de investigación	Elaboración de encuestas. Aplicación	Los resultados el alto nivel de vulnerabilidad de las	Plataformas digitales y Excel

sector productivo involucrado.	familiarización de los términos IPS E IDS en la población.	cualitativa mediante encuestas en Google Forms	de preguntas estructuradas en Escala Likert,	empresas ante un ataque informático.	
Evaluación y planificación	Identificar activos que se encuentren en riesgo y Establecer reglas y políticas para detectar intrusos	Observación, Análisis de Casos	Implementación de sistemas IPS e IDS es un paso crucial para asegurar la efectividad de la seguridad de una red	Altos niveles de seguridad en la red. Determina los activos críticos los flujos de tráfico principales y las amenazas potenciales a las que te enfrentas.	Análisis de casos

Nota: Elaboración propia

CONCLUSIONES

En conclusión, podemos mencionar que se reconocen las tácticas más comunes utilizadas para llevar a cabo un ataque informático, la elaboración de un sólido plan de seguridad al departamento financiero es crucial para prevenir los perjudiciales ataques que acechan constantemente a las empresas en la era digital.

Se identificaron cuáles son los procesos internos y datos más sensibles que maneja el departamento financiero, así pudimos crear reglas en nuestro IPS e IDS para salvaguardar los datos y mitigar los ataques más comunes con ciberdelincuentes.

Se ha desarrollado una estructura lógica y sistemática para el plan de prevención de ataques informáticos, basándonos en 6 fases principales, las cuales son: planificación, estructura y diseño, selección de tecnología, implementación, monitoreo y capacitación al personal. Es importante destacar que este plan de seguridad debe ser implementado de manera integral, involucrando a todas las partes dentro de la empresa. La asociación entre los departamentos de TI, recursos humanos y finanzas resulta crucial para asegurar la efectividad de estas medidas.

Se ha resaltado la necesidad de educar a los miembros del departamento financiero sobre las tácticas utilizadas por los ciberdelincuentes, para que puedan identificar y evitar posibles amenazas, con esta nueva cultura prevención a sus datos no solo protegerá los activos del departamento financiero, sino que también preservará la confianza de los clientes y socios comerciales. Esto se traducirá en una mayor estabilidad financiera y una reputación sólida dentro del mercado. Así que, ante la creciente sofisticación de los ciberataques, es imperativo que el departamento financiero se mantenga siempre alerta y sea proactivo en la implementación de medidas de seguridad efectivas.

RECOMENDACIONES

Antes de implementar los sistemas de IPS e IDS, se debe realizar una planificación exhaustiva, como definir los objetivos principales, comprende las necesidades específicas de seguridad y establecer políticas y reglas.

Es de vital importancia evitar confiar únicamente en reglas genéricas que nos brindan la herramienta de detección de intrusos, debemos de monitorear y crear continuamente nuevas reglas en el software de suricata para minimizar los falsos positivos (alertas erróneas) y falsos negativos (amenazas no detectadas).

Es indispensable que no solo se utilice un programa de monitoreo tal como lo hicimos con software de suricata que, a pesar de ser un software potente a la hora de la detección de intrusos, no nos brinda los resultados obtenidos de una manera gráfica, es de vital importancia conocer los análisis de una manera rápida y eso lo podemos hacer si unimos suricata con wazuh.

Desarrollar y documentar un plan de respuesta a incidentes que especifique cómo se manejarán las alertas y los eventos de seguridad, también definir roles y responsabilidades para un enfoque coherente, como también capacitar al personal técnico constantemente para analizar y comprender las alertas que nos brinda el software de detección de intrusos.

BIBLIOGRAFÍA

Aguirre, J. C. (2015). El papel de la descripción en la investigación cualitativa. Revista Scielo, 181.

Arcos, M. (2023). Propuesta de estrategia para evitar la fuga de información en empresas constructoras utilizando detección por comportamiento (ueba) caso de estudio: scmi inc (usa). Universidad Israel.

Benavides, E. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Revista Cientifica OJS Univerdidad de Quevedo, 97.

Campuzano, P. S. (2021). Modelos de Seguridad para prevenir riesgos de ataques informáticos. Universidad Salesiana, 6.

Farro, M. (2020). Análisis y Técnicas de seguridad en Redes. Universidad Privada del Norte, 8.

Guaña, J., Sánchez, A., Cherrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2022). Ataques informáticos más comunes en el mundo. Revista Ibérica de Sistemas y Tecnologias de Informacíon, 88.

Guevara, E. M. (2023). Vulnerabilidades y amenazas en los activos de información: una revisión sistemática. Universidad Nacional San Matín, 1.

Interpol. (2022). Organización International de Policía. Obtenido de Informe anual: https://www.interpol.int/es/Delitos/Delincuencia-financiera

Lino, J. (Septiembre de 1 de 2022). Herramientas para mejorar la seguridad. Obtenido de Sciencedirect: https://www.sciencedirect.com/science/article/abs/pii/S1130239922000736

Mostacero, N. (2020). Controles y mecanismo en la gestión de seguridad de red. Universidad Peruana Union, 2.

Olmedo, J. I. (15 de 09 de 2018). Análisis de los ciberataques realizados en América Latina. Innova research journal, 172.

Onu. (2019). Naciones Unidas. Obtenido de https://www.un.org/es/chronicle/article/objetivo-8-analisis-del-objetivo-8-relativo-al-trabajo-decente-para-todos

Pardo, A. (2019). Blockchain Aplicado a Retos de Ciberseguridad. Repositorio Digital, Escuela Colombiana de Ingenieria Julio Garavito, 8.

Sain, G. (2019). Evolución histórica de los delitos. Revista Pensamiento Penal, 2.

Suárez, E. A., Sotomayor , E. R., & Medina, M. (2021). Implementación de un sistema de prevención de perdida de datos, con políticas de seguridad, mediante el control de dominio por medio de una herramienta de terceros. Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Villavicencio, 20.

Tobar, J. D. (2022). Ingeniería Social: Técnicas utilizadas por los ciberdelincuentes y cómo protegerse. La Red de Repositorio de Acceso Abierto del Ecuador, 6.

Villegas, J. C. (2022). Ciberseguridad y robo de información. Universidad Catolica Santo Toribio Mogrovejo, 5.

ANEXOS

FORMATO DE ENCUESTA

Encuesta sobre Seguridad Informática

La información adquirida es netamente para ambitos académicos

jhonnyguilcapi@gmail.com Cambiar de cuenta

No compartido

* Indica que la pregunta es obligatoria

Nombre

Tu respuesta

Edad

Tu respuesta

La empresa donde labora a que sector productivo pertenece? *

- ◯ Tecnología e Innovación
- ◯ Servicios Financieros
- ◯ Servicios de Salud
- ◯ Comunicación
- ◯ Educación
- ◯ Turismo
- ◯ Mineria Manufactura y Contrucción
- ◯ Alojamiento y servicio de Comida
- ◯ Otros

¿En que área de la empresa se desempeña? *

- ◯ Tecnologías de la Información
- ◯ Contable Financiero
- ◯ Talento Humano
- ◯ Producción
- ◯ Marketing y Ventas
- ◯ Logística
- ◯ Administración
- ◯ Otros

¿Piensa usted que en su empresa debe existir un departamento de Seguridad Informática? *

- ◯ SI, Porque toda empresa es vulnerable al robo de información
- ◯ NO, Porque estos casos no son frecuentes en la actualidad

¿Considera usted que en las empresas puede darse un robo de información mediante un ataque cibernetico? *

- ◯ Alguna vez
- ◯ Constantemente
- ◯ Nunca

¿Ha conocido casos reales de empresas que han sido victimas del robo de su información y futura extorción? *

- ◯ SI
- ◯ NO

¿Que métodos considera usted relevantes a la hora de prever el robo de información en el área financiera de una empresa?. *

- ◯ Implementar un Plan de Seguridad de la Información
- ◯ Capacitaciones, Charlas , informes, enfocados a prevención de ataques informáticos y mas
- ◯ Totas las anteriores

¿Cual de los siguientes métodos considera usted que son los más frecuente a la hora de robar información en una empresa? *

- ☐ Ingenieria Social: Es la práctica ilegítima de obtener información confidencial a través de la manipulación de las personas
- ☐ Rasomwere: Bloqueo de información de una empresa para futura extorción
- ☐ Phishing: Método para intentar recopilar información personal utilizando correos electrónicos y sitios web engañosos
- ☐ Rootkit: Capacidad de introducirse en un dispositivo y hacerse con el control del mismo
- ☐ Spyware : Programa espia, recopila información de una computadora transmite esta información a una entidad externa

¿Conoce usted de las buenas prácticas a la hora de proteger sus datos financieros? *

- ◯ SI
- ◯ NO

¿Cuál cree usted que se asemejan más al concepto de seguridad informática? *

- ◯ Procesos y Prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque
- ◯ Es un conjunto de actividades que apoyan a la poblacion en zonas vulnerables para hacer frente a los desastres naturales
- ◯ Es la elaboración de aplicaciones y sistemas informáticos

¿Ha escuchado de la nueva de protección de datos personales en el Ecuador? *

- ◯ SI
- ◯ NO

Enviar Borrar formulario

Preguntas Respuestas 102 Configuración

102 respuestas

Vincular con Hojas de cálculo

Se aceptan respuestas

Resumen Pregunta Individual

Nombre

99 respuestas

- Amanda
- Alex Dario Ushiña Llulluna
- Jhonny
- Jonathan Lema
- Ronmel tinitana
- Mishel
- Dayana
- CESAR VINICIO ZURITA TORO
- Sebastián

JUICIO DE EXPERTOS

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA LA VALORACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para valorar la siguiente propuesta del proyecto de titulación: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Valorado por: María Gabriela Arcos

Contacto: 0983745483

Título obtenido
Maestría en Seguridad Informática
Cédula de Identidad
1725532582
E- mail
gabrielaarcos0@gmail.com
Institución de Trabajo
Mobilvendor
Cargo
Calidad QA
Años de experiencia en el área
4

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	x	x			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		x			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	x				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*		x			
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		x			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	x				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	x				
Total		**4**	**4**	**0**	**0**	**0**

Recomendaciones

1. Se recomienda tener más énfasis en las 6 fases de planificación abordar temas como el mejoramiento de la infraestructura y diseño de la red.
2. Dependiendo de la organización los sistemas de detección de intrusos IPS e IDS de pago tiene más beneficios que los gratis, por ello deben de ser contemplados en la implementación.

Lugar, fecha de validación: Quito, 04 de septiembre del 2023

Firma del especialista

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA LA VALORACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para valorar la siguiente propuesta del proyecto de titulación: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Valorado por: Santiago Javier Caranqui Cobo

Contacto: +1 (929) 622-0608

Título obtenido
Ingeniería en sistemas informáticos
Cédula de Identidad
0401800115
E- mail
Santiago_javiercc@hotmail.com
Institución de Trabajo
Corporación GPF
Cargo
Auditor en Sistemas
Años de experiencia en el área
3 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		***X***			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		***X***			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
	Total	*32*	3	0	0	0

Recomendaciones

La solución expuesta en este caso puede ser aplicable en algunas otras situaciones, siempre y cuando cumplan con los requisitos mínimos para la implementación.

Evaluar posibles problemas si existe una falla en la disponibilidad de la solución, y las opciones de continuidad del negocio me garantiza esta solución.

Considerar que al no ser un firewall cómo tal se debe mantener la infraestructura de Firewall para la evitar ataques informáticos.

Lugar, fecha de validación: Quito 02 de septiembre de 2023

Firma del especialista

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA LA VALORACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para valorar la siguiente propuesta del proyecto de titulación: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Valorado por: Tnlgo. Guevara Caza Byron Alexis

Contacto: 0996110409

Título obtenido
Tecnólogo en Análisis de Sistemas
Cédula de Identidad
1720743911
E- mail
alex_1guevara@hotmail.com
Institución de Trabajo
Agencia Metropolitana de Tránsito
Cargo
Agente Civil de Tránsito
Años de experiencia en el área
8 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: PREVENCIÓN DE ATAQUES INFORMÁTICOS BASADOS EN IPS E IDS PARA EL DEPARTAMENTO FINANCIERO DE EMPRESAS

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		X			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*			X		
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		X			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		X			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado*		X			
	Total	*2*	*3*	*1*	*0*	*0*

Recomendaciones

Detallar la información del hardware externo tales como sensores y equipos de IPS con el fin de conocer más a detalle se sus funcionamientos.

Lugar, fecha de validación: Quito, 1 de septiembre del 2023

Firma del especialista