SISTEMA DE PREVENCIÓN Y DETECCIÓN DE ATAQUES PARA CORREDOR EMPRESARIAL S.A.

Jimmy Rogelio Soto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2024

SISTEMA DE PREVENCIÓN Y DETECCIÓN DE ATAQUES PARA CORREDOR EMPRESARIAL S.A.

Jimmy Rogelio Soto

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Christian Reynaldo Angulo
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2024

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá. 8 de agosto 2024

DEDICATORIA

Está tesis está dedicada en primer lugar a Dios, porque gracias a él no estaría dónde estoy, a mi familia, con su amor, apoyo incondicional y paciencia siempre me han acompañado a cumplir todas mis metas y quiénes durante años facilitaron mi estudio, de una u otra forma.

En memoria de mi madre Consuelo Soto, quien me ayudó con su apoyo a estar donde estoy.

Agradezco además a la empresa Corredor Empresarial, por confiar en mí, y permitirme realizar el proceso investigativo en sus instalaciones.

AGRADECIMIENTOS

Agradezco a la Universidad Abierta y a distancia UNAD, directivos, tutores y asesores que mediante sus enseñanzas y conocimientos siempre han aportado dirección enseñanza y sobre todo colaboración durante todo este proceso.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Análisis heurístico: Definido como la detección proactiva y Autónoma del malware, es una amenaza mediante la utilización de técnicas heurísticas, mediante técnicas de comparación de ficheros con fragmentos de códigos de virus, y se asemejan en su comportamiento y pueden detectar actividades dañinas, su esencia es detectar nuevos virus.[1]

Ataque activo: Este tipo de ataque se caracteriza por modificar en parte el contenido de la información, ya sea de un mensaje, archivo del sistema, recursos, entre otros muchos, siempre tratando de dañar el sistema.[2]

Ataque combinado: Definido como uno de los ataques más completo tipos y métodos y técnicas sofisticadas, combina virus, gusanos, troyanos y códigos entre muchos otros, inicia el proceso de ataque desde un servidor, conectándose a través de internet transmitiendo y a su vez difundiendo el ataque de forma automática, sus características principales son: la gran variedad de ataques de tipo DDos, direccionamiento IP, con distintas formas de propagación utilizando vulnerabilidades en redes de ordenadores y granjas de servidores para buscar contraseñas por defecto o infinidad brechas informáticas.[3]

Brecha de seguridad: Es definido como la violación de la seguridad y trata de destruir, eliminar o alterar, ya sea información o archivos, afectando también a las comunicaciones y accesos no autorizados tratando de eliminar la información almacenada.[4]

---

[1] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.15.

[2] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.15.

[3] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.16.

[4] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.23.

Certificado digital: Archivo informático generado por una entidad denominada autoridad certificadora, asocia los datos de identidad de una empresa, organismo o persona, dándole a conocer in internet, por este medio es fácil autenticar la validez y existencia, una página web y verificando si es de confianza, auténtica y sirve además para sirve para cifrar comunicaciones y firmar digitalmente documentos.[5]

Centro de respaldo: Definido como definido como de procesamiento de datos CPD, en él se toma el control en caso de contingencia, la localización debe ser totalmente distinta como mínimo 20 km, los servidores y servicios además del respaldo electrónico debe ser compatible con el existente, el software en toda su extensión debe ser idéntico, contener una base de datos idéntica cola que se trabaja en producción.[6]

Datacenter: Centro de procesos de datos, instalación que se utilizada para alojar sistemas informáticos y dispositivos asociados, consta de un espacio definido en una edificación, el cual permite instalar mecanismos de hardware, comunicación e interconexión, bajo la norma que dicta las directrices y requerimientos de los centros de cómputo TIA-942. Dentro de este espacio se integran telecomunicaciones, sistemas de almacenamiento, servidores, sistemas de respaldo de fluido eléctrico y están divididos en 4 componentes, telecomunicaciones, arquitectura, electricidad, Mecánico.[7]

Escaneo de vulnerabilidades: Acción de búsqueda de vulnerabilidades en servidores, computadores y redes mediante técnicas y aplicaciones especializadas, identificar y así mismo cualquier tipo de Brecha de inseguridad en una red, especializado principalmente en aplicaciones, puertos y servicios de cualquier empresa.[8]

IDS: Evolución de seguridad que protege datos e información, es una herramienta para el administrador de red que detectar en lo posible actividades maliciosas y alertan al administrador para tomar labores eficaces. Pero que es una intrusión es un acceso no autorizado que manejando recursos de informáticos. Diferente a un

---

[5] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.26.

[6] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.25.

[7]Concepto Definición. [Página Web]. (2023, 23 de febrero). Data center. https://conceptodefinicion.de/. https://conceptodefinicion.de/data-center/

[8] INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.42.

atacante que es un sujeto real que trata de hallar una forma de acceder a información, con el resultado de dañar[9]

Snort: Software creado con el fin de detectar intrusos basado en red (NIDS), de uso libre. Funciona parecido a un sniffer, revisa el tráfico de red, explorando posibles intrusiones. Por medio de reglas detecta ataques e inspecciona, alertas y reconoce anomalías anticipadamente por medio de patrones.[10]

Política de seguridad: Son todas aquellas medidas de seguridad que nacen en una compañía con el fin de generar ciertas reglas para implementar, protocolos ceñidos a análisis y normas de amplio conocimiento qué una empresa crea, para la seguridad en sus sistemas y datos, luego de evaluar cada uno de sus activos y riesgos expuestos, representa un documento de seguridad de la información.[11]

Vulnerabilidad: Se entiende como una debilidad en un sistema está falla puede ser aprovechada con fines maliciosos normalmente existe y cuál se denomina exploit, llama también agujero de seguridad.[12]

9 INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.49.

10 Gomez, V. (s/f). Analizando la seguridad de la red con snorby – DOJOConf Panamá 2022. Dojoconfpa.org. Recuperado el 2 de octubre de 2022, Disponible en Internet: <https://dojoconfpa.org/analizando-la-seguridad-de-la-red-con-snorby/>.

11 INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.63.

12 INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>. p.77.

RESUMEN

Hoy en día los ataques en el mundo y especialmente en Colombia, son rutina necesaria, por lo tanto, es ineludible qué las empresas protejan de cualquier tipo de daño a la información.

En el mundo actual es necesario tomar en cuenta los nuevos retos como la inmediatez, gran cantidad de información a la mano y el desarrollo mismo de las tecnologías, la información o datos se cuenta como el activo más significativo, hoy en día para una compañía no importa su ubicación o dimensión, la defensa siempre es y será necesaria, evitando con esto una alta posibilidad de escape de información y privacidad de la misma.

Día tras día se crean, virus, diferentes formas de ataque y en general formas de amenazas, dado que internet es el sitio de encuentro de toda red, la red empresarial se presenta miles de amenazas externas, por lo tanto, es importante proteger cada extremo de la red, mediante un estudio de debilidades o fragilidades de instalaciones de rede, físicas y de activos más valioso.

Por medio de estudios, análisis se detectarán, comportamientos anómalos, eventos no apropiados o inusuales los cuales deben ser bloqueados, definidos o aplicados.

El horizonte de este proyecto es implementar herramientas para examinar, detectar y advertir por medio de monitoreo del tráfico de la red, para impedir ataques o accesos no autorizados, ante cualquier característica de inteligencia IA u ocultamiento avanzado, ante amenazas o fuga de información, nace el proyecto de la necesidad en ser un primer recurso de protección (IPS-IDS).

ABSTRACT

Nowadays attacks in the world and especially in Colombia, are necessary routine, therefore it is unavoidable that companies protect from any kind of damage to information.

In today's world it is necessary to take into account new challenges such as immediacy, large amount of information at hand and the very development of technologies, information or data is counted as the most significant asset, today for a company no matter its location or size, it is always and will be necessary defense, thus avoiding a high possibility of escape of information and privacy of the same.

Day after day are created, viruses, different forms of attack and in general forms of threats, since the internet is the meeting place of any network, the corporate network is presented thousands of external threats, therefore it is important to protect each end of the network, through an analysis of vulnerabilities of both physical facilities, as more important assets will be detected, anomalous behavior, inappropriate or unusual events which must be blocked, defined or applied.

The horizon of this project is to implement tools to examine, detect and warn by monitoring network traffic, to prevent attacks or unauthorized access, to any feature of AI intelligence or advanced concealment, to threats or information leakage, the project is born of the need to be a first resource protection (IPS-IDS).

INTRODUCCIÓN

En el ambiente actual de amenazas cibernéticas que siempre se encuentra en constante evolución, las empresas se enfrentan a riesgos relativamente nuevos y significativos para la seguridad de la información confidencial. Sin un análisis y abordaje adecuados de estos riesgos, las empresas pueden sufrir consecuencias graves. Los ataques cibernéticos pueden conducir a la pérdida de datos sensibles, daños a la reputación de la empresa e interrupción de sus operaciones comerciales, entre muchas otras repercusiones. Además, los ataques exitosos pueden resultar en la explotación de vulnerabilidades en los sistemas de la organización y la filtración de información confidencial, lo que puede tener consecuencias legales y financieras significativas.

En Colombia el campo de la ciberseguridad se ha tomado de manera responsable últimamente, planeando, evaluando, exigiendo políticas y procedimientos para todo tipo de ataques cibernéticos ante potenciales amenazas de los ciberdelincuentes, es necesario crear un entorno digital, abierto y confiable involucrando la gestión del riesgo permitiendo a las empresas e individuos maximizar la seguridad digital, como un reto económico, empresarial, sobre los conocimientos y a nivel personal de retos constantes.

La ciberseguridad es la piedra angular de toda información, sobre la cual se verifican evaluaciones de todo tipo de amenazas, los ciberataques son los más denunciados, ante esta situación surgen controles para salvaguardar los activos más valiosos y analizar la transferencia o tráfico de información, estas herramientas cuentan con monitoreo en tiempo real y alerta como (IDS e IPS) que pueden identificar, revisar y remediar el impacto. Ataques a la disponibilidad del servicio y/o fuga de información o, en casos extremos, evitar denuncias por fuga de información crítica o pérdida de clientes, todo ello en conjunto con firewalls, antivirus y otras herramientas de protección de la red.[13]

Enfocados en una de esas herramientas clave para proteger las redes internas de una compañía es la implementación de sistemas de prevención y detección de intrusiones (IPS/IDS, por sus siglas en inglés), muchas empresas en Colombia no cuentan con sistemas de IPS/IDS adecuado o realmente implementado, entre las posibles causas puede encontrarse falta de conocimiento, recursos o la creencia errónea de que las medidas de seguridad existentes son suficientes.

13 CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Estudio semestral Tendencias del cibercrimen: Ciberseguridad en la era de la movilidad digital. www.ccit.org.co [página web]. (julio, 2022). [Consultado el 12, octubre, 2022]. Disponible en Internet: <https://www.ccit.org.co/estudios/estudio-semestral-tendencias-del-cibercrimen-ciberseguridad-en-la-era-de-la-movilidad-digital/>.

Como resultado, puede entre muchas otras consecuencias exponerse ataques, fugas de información, robar datos sensibles de los clientes o interrumpir las operaciones comerciales lo cual repercutiría en incumplimientos normativos y legales, así como daños económicos, reputacionales, significativos.

El interés de este proyecto es proponer soluciones efectivas y realistas para proteger las redes internas de una empresa en particular por medio de un sistema de defensa eficiente que identifique, evite y prevenga incidentes de seguridad y posibles fugas de información en tiempo real en la red interna de la organización.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La organización dónde se iniciará el proceso tiene como actividad principal desarrollo de sistemas informáticos, soporte ti y operaciones, se encuentra el área de desarrollo varias herramientas las cuales representan el Core del negocio, que son las apuestas en línea, constantemente, la empresa se expone a Miles de amenazas de diferentes partes del mundo, incrementando el riesgo de protección de la información el software y la red en general, actualmente la empresa posee un sistema de cortafuegos antivirus efectivo, pero recibe ataques combinados de forma variada, tratando de encontrar una brecha de seguridad, se realizan escaneo de vulnerabilidades constantemente por parte de terceros y dentro de la empresa la área de auditoría y seguridad, hoy en día las herramientas de uso cotidiano cómo son impresoras dispositivos y IOT, aumenta la productividad Y como siempre la eficiencia en todas las empresas, con esto aumentan los riesgos debido a que estos presentan software o firmware que no se actualizan constantemente, solamente el 11% de las pymes puse una solución de seguridad y más de 52 porciento no tienen estrategias de seguridad para los dispositivos[14]

La globalización asociada con la evolución tecnológica aumenta las cifras de ataques cibernéticos siempre en aumento según información de fiscalía general de la Nación se han registrados más casos de abuso informático, con 6407 más de 46% con respecto al año 2021.

Existe un estudio de tendencias en cibercrimen enfocado en Colombia llamado “Seguridad Aplicada al Fortalecimiento empresarial (SAFE)”, recomiendan indagar varios recursos humanos y tecnológicos para reforzar y salvaguardar la información.

Este estudio informa que el acceso abusivo a redes y computadoras registra 6.407 eventos es decir 46% más que año anterior, solo el primer semestre de este año, ubicándolo con el mayor crecimiento, además se incrementó el hurto por medios informáticos con un 15% con 11.078 casos reportados.[15]Dell Technologies realizo encuesta sobre la confianza en la protección de datos en las empresas hibridas,

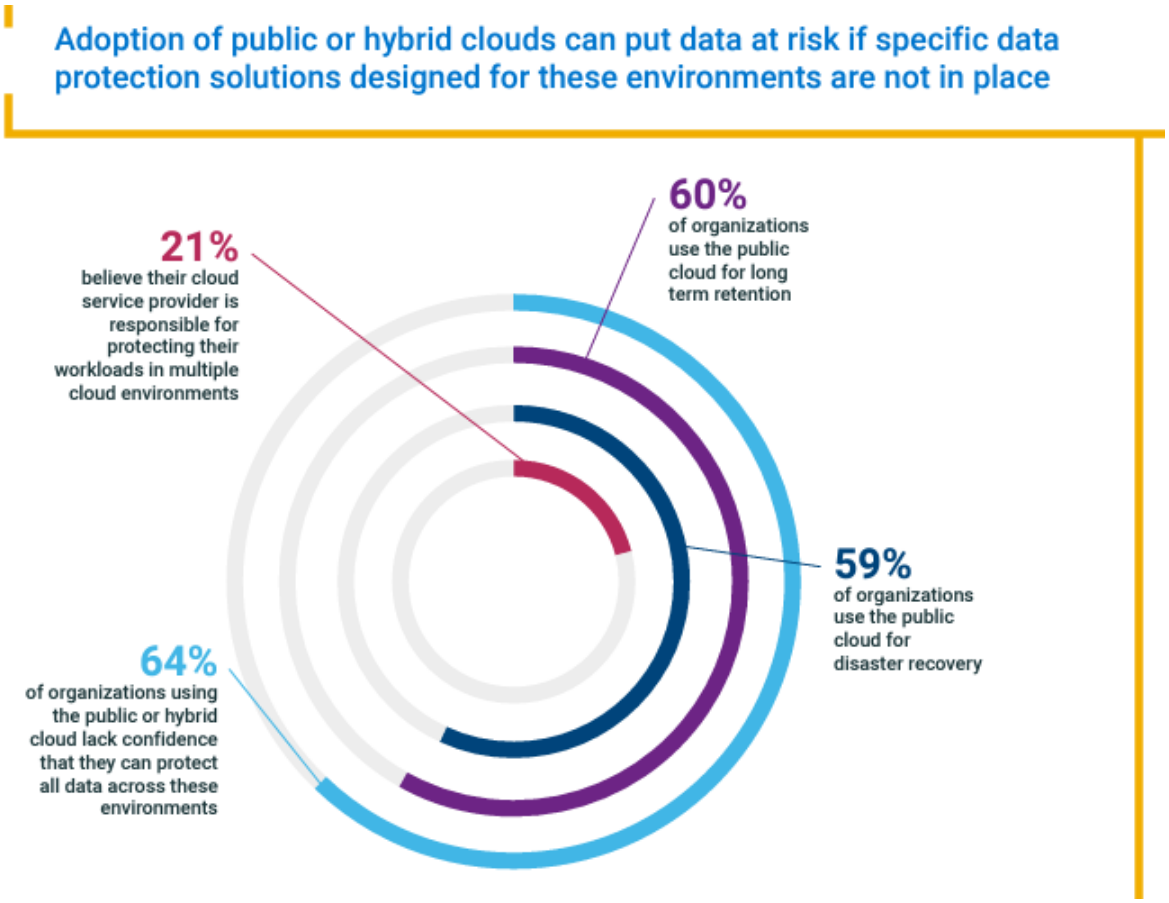
14 OSORES, Melisa. Solo 11% de las pymes tiene una solución completa de seguridad IoT. www.computerweekly.com [página web]. (14, octubre, 2022). [Consultado el 25, octubre, 2022]. Disponible en Internet: <https://www.computerweekly.com/es/noticias/252526128/Solo-11-de-las-pymes-tiene-una-solucion-completa-de-seguridad-IoT>.

15 CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Estudio semestral Tendencias del cibercrimen: Ciberseguridad en la era de la movilidad digital. www.ccit.org.co [página web]. (julio, 2022). [Consultado el 12, octubre, 2022]. Disponible en Internet: https://www.ccit.org.co/estudios/estudio-semestral-tendencias-del-cibercrimen-ciberseguridad-en-la-era-de-la-movilidad-digital/

revelando que existe una perdida global de USD$ 959.493 dólares por ataques informáticos en solo el continente americano.[16]

Y se aumenta este riesgo y la percepción de inseguridad al tener la plataforma en la nube o de forma hibrida en las empresas ya que no son conscientes de la cantidad de riesgos y el proceso de protección, análisis y prevención.

Figura 1 Protección en Cloud Hibrida



Fuente: Dell Technologies(2021), Data Protection in a Time of Digital Transformation, descargado de:https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm#pdf-overlay=//www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/global-data-protection-index-infographic-ams.pdf

16 DELL TECHNOLOGIES. Data Protection in a Time of Digital Transformation. www.dell.com [página web]. (abril, 2021). [Consultado el 28, octubre, 2022]. Disponible en Internet: <https://www.dell.com/es-es/dt/data-protection/gdpi/index.htm#scroll=off&pdf-overlay=//www.delltechnologies.com/asset/es-es/products/data-protection/briefs-summaries/global-data-protection-index-infographic-global.pdf>.

Es necesario si no primordial que las empresas evolucionen de un enfoque fragmentado al atender riesgos internos a uno holístico, para tomar en cuenta riesgos potenciales desde múltiples enfoques reforzando la táctica de defensa de datos complementado con la aceptación de un liderazgo múltiple.[17]

Se deduce que al materializarse un riesgo el impacto según informe de Microsoft son en porcentajes los siguientes impactos:

Figura 2 Impactos de eventos de riesgos en empresas

Fuente : Microsoft, (2022), Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft, Tomado de: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE58Ymd>

la implementación de un sistema más reforzado de seguridad ayudará a reducir el riesgo latente, garantizar a la protección, pérdida de datos, peligros reputacionales, o pérdida de datos por culpa de los usuarios y evitará problemas legales, medio la implementación de un sistema de prevención y detección confiable se eliminará y

17 MICROSOFT. Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft. www.microsoft.com/es-co/security/ [página web]. (junio, 2022). [Consultado el 22, octubre, 2022]. Disponible en Internet: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE58Ymd>.

disminuirá, la mayoría de las amenazas y afinar al mismo tiempo las políticas de seguridad en la empresa.[18]

1.2 FORMULACIÓN DEL PROBLEMA

¿En qué forma es posible implementar un sistema de prevención de ataques IPS E IDS, mediante recursos tecnológicos qué analicen, prevengan, detecten y bloqueen mediante monitoreo constantemente ataques cibernéticos a la empresa, asegurando los activos más importantes de la organización Corredor Empresarial?

18 GÓMEZ, V. (s/f). Analizando la seguridad de la red con snorby – DOJOConf Panamá 2022. Dojoconfpa.org. [Consultado el 16, octubre, 2022] https://dojoconfpa.org/analizando-la-seguridad-de-la-red-con-snorby/

2 JUSTIFICACIÓN

Hoy en día ante el creciente aumento de ataques informáticos qué se producen, que no solamente buscan robar información confidencial, sino una gran variedad de daños a nivel tecnológico, se encuentra una sofisticación de herramientas utilizadas para realizar ataques y algunas son capaces de eludir medidas de seguridad tradicionales causando daños importantes. Por tanto, es esencial que los gobiernos, empresas y todos los actores, tomen medidas necesarias para garantizar que los sistemas son seguros y que los datos que se almacenan están protegidos. Hacerlo contribuirá a evitar que sigan creciendo las ciber amenazas y minimizar el riesgo de generar una caída del sistema de ventas o crear una campaña de desprestigio, o enfrentar pérdidas económicas y de reputación, este proyecto procura delinear e implementar un recurso estable, fiable y unido al sistema de protección actual complementando las herramientas de seguridad actuales IDS e IPS en la red de la empresa Corredor Empresarial.

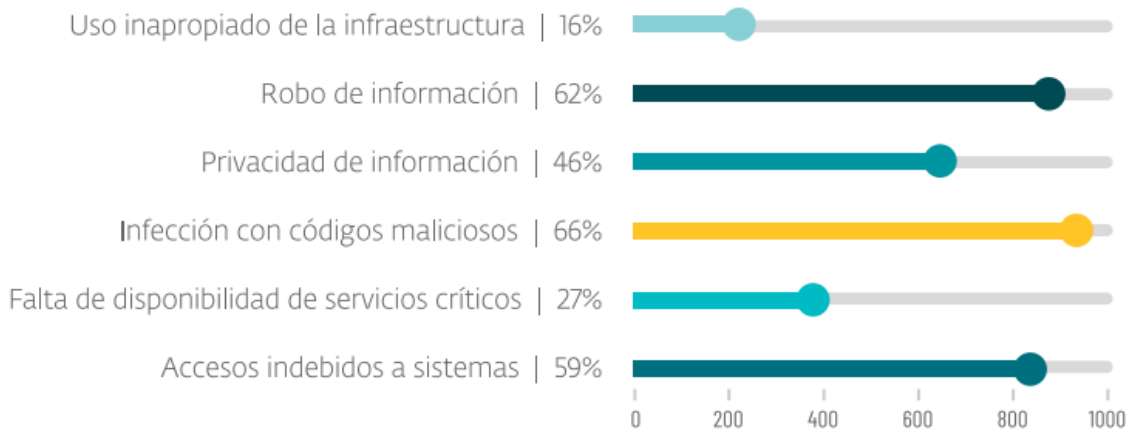
Según informes del reporte de ESET SECURITY REPORT,[19] después de realizar más de 1800 encuestas a personal en el ámbito de la ciberseguridad en el último año, se encuentra que, una de cada dos compañías en Latinoamérica confirmo sufrir algún tipo de incidente de seguridad y que uno de cada cuatro eventualidades se relacionó con malware,

Existe una preocupación latente sobre el tipo de ataques que pueden llegar sobre una empresa entre los más importantes se encuentra que la infección por códigos maliciosos son la mayor preocupación con el 66% y le sigue el robo de información seguido de accesos indebidos a sistemas[20]:

[19] ESET SECURITY REPORT. El 48% de las empresas de América Latina sufrió algún tipo de incidente de seguridad. https://www.welivesecurity.com/ [página web]. (4, agosto, 2022). [Consultado el 1, junio, 2023]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2022/08/04/empresas-america-latina-incidentes-seguridad/>.

[20] ESET SECURITY REPORT. Security Report Latinoamérica 2022. https://www.welivesecurity.com/ [página web]. (2022). [Consultado el 1, junio, 2023]. Disponible en Internet: < https://www.welivesecurity.com/wp-content/uploads/2022/10/ESET-security-report-LATAM2022.pdf>.

Figura 3 Preocupación sobre ataques

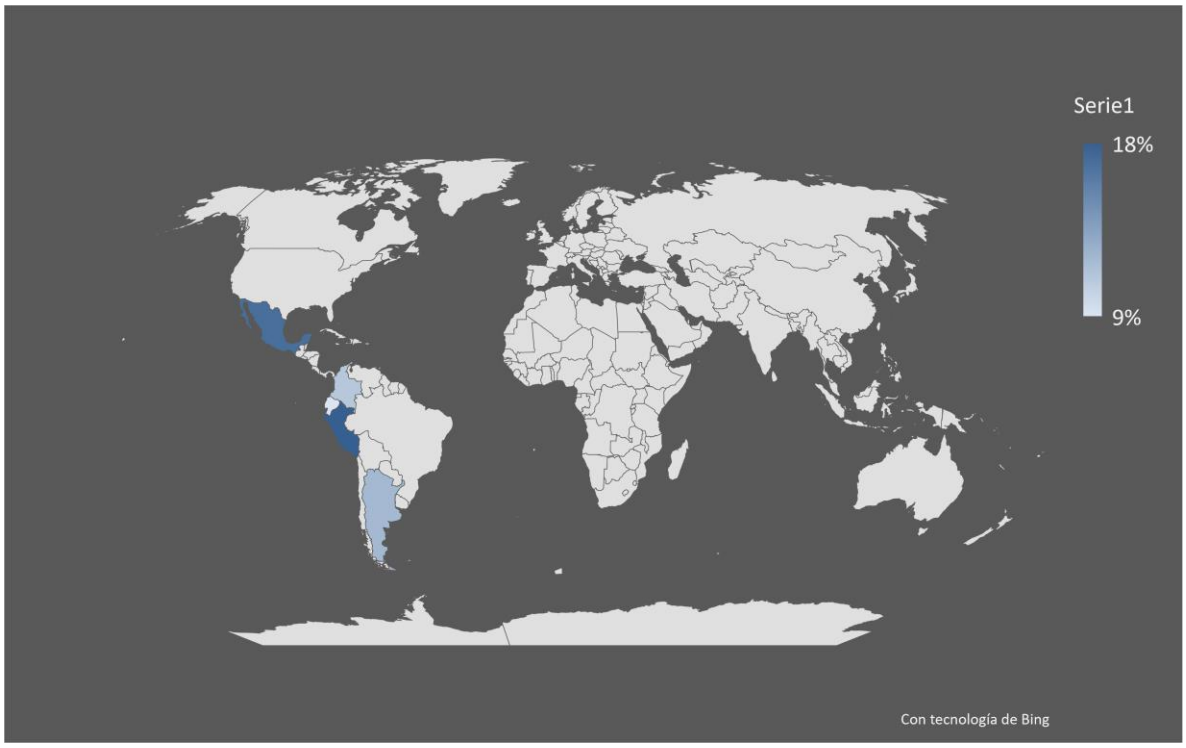


Fuente : www.welivesecurity.com, (2022), Security Report 2022, descargado de : < https://www.welivesecurity.com/wp-content/uploads/2022/10/ESET-security-report-LATAM2022.pdf>

Por países en Latinoamérica se muestra como Colombia ocupa el 3er lugar en cuanto detecciones de todo tipo de virus:

Países con mayor cantidad de detecciones Perú (18%), México (17%), Colombia (12%), Argentina (11%) y Ecuador (9%).

Figura 4 Detecciones Por Países



Fuente : Creación Propia

Con los ataques en aumento, unido al crecimiento cibernético que experimenta la humanidad y la creciente necesidad económica de estar interconectados especialmente en Latinoamérica, existe ahora una mayor dependencia de los dispositivos conectados a Internet, que permiten que los ciberdelincuentes lleven a cabo actividades con mayor facilidad, siempre al avanzar la tecnología, lo hacen las herramientas utilizadas para acceder a datos e información sensibles, esto genera mayor necesidad de adoptar medidas de seguridad para proteger a usuarios y empresas de ciberataques, al reducir los riesgos latentes, continuos y contrarrestar problemas de información del uso o mal uso, unidas a nuevas formas de teletrabajo actualmente, debe aumentar el control con más seguridad de datos personales, monitorizar el tráfico entrante y saliente de correspondencias, datos, recursos y algo no menor la utilización del ancho de banda.

Al implementar un IDS e IPS tiene como ventajas ver el tráfico en tiempo real de la red, logs de escaneado, alerta sobre posibles agresiones, precisar por lo tanto modelos de búsqueda y de examen al tráfico, esto nos sirve para estar al corriente quién como y cuando se genera una agresión o realizar estudios más exhaustivos.

Agregando una capa de seguridad, protege las conexiones de intranet e internet, estos servicios deben estar activos en todo momento, para clientes y usuarios, optimizando recursos, reforzando tácticas de defensa, políticas de seguridad y asegurando activos de información.

Por lo tanto, la implementación será beneficiosa para Corredor Empresarial, optimizando recursos, reforzando tácticas de defensa y garantizando seguridad de activos de información, este proyecto generará conocimientos sobre la implantación de un sistema IPS/IDS, que podrán servir de referencia para futuros proyectos.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Proponer un sistema de defensa que identifique, evite y prevenga incidentes de seguridad y posibles fugas de información en tiempo real en la red interna de la organización.

3.2 OBJETIVOS ESPECÍFICOS

Realizar la identificación de equipos de comunicación y servidores de la organización con posibles fallos de seguridad que puedan ser afectados con diferentes vectores de ataque y diseñar un plan para la mitigación de brechas de seguridad en la empresa.

Realizar un análisis de tráfico con el fin de garantizar y mejorar monitoreo, ante situaciones de ataques y reforzar la seguridad.

Proponer la implementación y configuración de políticas de seguridad en el IDS e IPS con el fin de asegurar la eficacia y aumentar el funcionamiento correcto de la plataforma actual, bloqueando intentos de ataques, vulnerabilidades y amenazas.

Elaborar manual de implementación IDS e IPS que sirva de punto de referencia ante la compañía, que servirá para que la organización proteja sus redes internas de incidentes de seguridad y fugas de información en tiempo real, de manera eficaz asegurando la eficiencia, garantizando así operaciones seguras.

4 MARCO REFERENCIAL

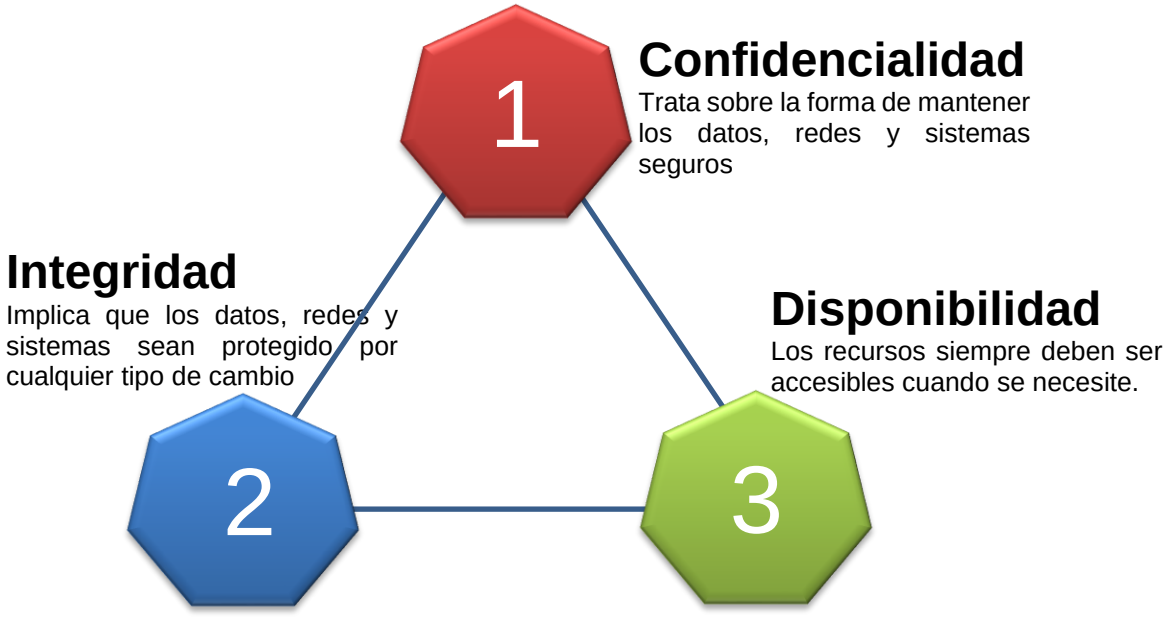
4.1 MARCO CONCEPTUAL Y TEÓRICO

La seguridad informática se crea por la preocupación creciente en la era digital, donde existe y se crean todo tipo de amenazas cibernéticas y como se ha verificado evolucionan constantemente. En este contexto, las herramientas de Detección y Prevención de Intrusiones (IDS/IPS) desempeñan un papel fundamental en la protección de las redes contra ataques maliciosos.

En este contexto, este tipo de soluciones son esenciales porque salvaguardan la integridad, confidencialidad y disponibilidad de la información, que son los pilares de la seguridad informática y con esto se garantiza que los procesos se completen para alcanzar un nivel de confiabilidad alto y estable ante cualquier tipo de amenaza.[21]

Estos pilares deben garantizar que sea segura la información.

Figura 5 Pilares de Seguridad Informática.



Fuente : Creación Propia.

21 GOODMAN, Seymour; DETMAR W. STRAUB y RICHARD BASKERVILLE. Information security : policy, processes, and practices. (2017). [Consultado el 1, noviembre, 2023]. Disponible en Internet: <https://eds-p-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/ebookviewer/ebook/ZTAwMHh3d19fMjc1NTEzX19BTg2?sid=d87ca403-93ad-4b3f-816c-49faf1ffa4e6@redis&vid=2&format=EB&rid=4>.

4.1.1 Seguridad Informática

Proceso de prevención a cualquier tipo de detección, ataque o virus a cualquier tipo de sistema informático en la empresa que proteja la información como activo más preciado. Su objetivo principal es la protección en contra de intrusos para dañar la información, el uso constante del internet tiene como punto importante el acceso a todo tipo de información, pero conlleva un riesgo para la seguridad, por eso es necesario, tener una solución que resguarde el sistema de todo tipo de virus, spyware o malware.

Como se generar la protección de la información por medio de la detección de infecciones, este concepto es la aplicación del procesamiento electrónico de datos EDP, qué utiliza mecanismos de identificación por medio de patrones y a su vez métodos estadísticos con tecnologías, qué aplican esquemas de funcionamiento para analizar los datos basados en políticas de seguridad.

Esto se logra monitorizando con precisión y aplicando pautas de control qué generan confianza este término se acuño en los años 70 por parte del departamento de defensa de Estados Unidos, llamado iniciativa de seguridad 1977, este sistema procesaba una cantidad de información respecto a la confidencialidad y permitía generar mecanismos de auditoría, resumido en cinco objetivos son:

- Permitir revisar patrones de acceso y mecanismos para la protección.
- Revisar intentos externos y internos de burlar la protección.
- Descubrir si los usuarios realizan elevación de privilegios, en una red.
- Bloquear usuarios para proteger el sistema.
- Garantizar a los administradores que los ataques o instrucciones fueran controlados de posibles daños.

Estas pautas generaron un base que llegaron a crear un conjunto de controles mediante políticas, procesos, gestión, estructuras empresariales, funciones en el hardware y software, procedimientos, que deben y tienen que asegurar y proteger la información como son:

- Proteger la información, registros y propiedad intelectual.
- Crear una política de seguridad de la información.
- Gestionar la continuidad del negocio, las vulnerabilidades técnicas e incidentes y mejoras con respecto a la seguridad de la información.
- Conocer, educar y capacitar sobre la seguridad de la información.
- Procesar correctamente las aplicaciones.

Basado en estos datos y controles se crea un diseño de arquitectura de seguridad informática que incremente la seguridad de la información de la compañía Corredor

empresarial, inicialmente en forma experimental que se base en recopilar los tipos de ataques, formas de ataques, más comunes y crear reglas efectivas y que estén acordes a la empresa y tipos de virus con el fin de verificar a una variable independiente como lo es la arquitectura de seguridad informática qué impactará directamente la variable dependiente seguridad de información, es necesario aumentar el alcance de protección a la información, evaluar por medio de software de seguridad con un perfil y características que cumplan la integridad confidencialidad y disponibilidad necesarias.[22]

Terán Bustamante, Antonia; Dávila Aragón, Griselda y otros [23]elaboran un modelo que identifica y cuantifica diversos factores que impactan en la gestión adecuada de tecnologías e impacto en innovación, enfocadas eficiencia de la gestión de la tecnología e innovación en la seguridad informática.

Los riesgos informáticos se muestran como una amenaza para toda organización, dependiendo de la forma que se maneja. Toda empresa debe y tiene que implementar estrategias para prevenir y minimizar situaciones de peligro en seguridad de información y que las mismas sean aplicadas integralmente.[24]

Como ya hemos visto el principal objetivo es prevenir que las filtraciones de datos se generen. Pero para llegar en ultimas a este objetivo, es esencial dividirlo en objetivos más detallados.

Una primera etapa incluye identificar los activos de información de una empresa en este caso de Corredor Empresarial y cómo o en qué forma pueden verse comprometidos. Esto debe permitir categorizar los riesgos en componentes separados, como vulnerabilidad, amenaza, probabilidad e impacto.

Esto sirve como segundo paso para diseñar estrategias de seguridad informática efectivas, para poder mitigar riesgos y fortalecer la resistencia de los sistemas frente a posibles ataques como vulnerabilidades que puede considerarse como una debilidad en el diseño, implementación o configuración de un sistema, dejándolo expuesto a amenazas potenciales.

---

22 ASURZA CACERES, Josue David. Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa bafing S.A.C. en 2021. repositorio.cientifica.edu.pe [página web]. (2022). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://repositorio.cientifica.edu.pe/handle/20.500.12805/2414>.

23 BUSTAMANTE, Antonia Terán; ARAGÓN, Griselda Dávila y CASTAÑÓN IBARRA, Rosario. Gestión de la tecnología e innovación: un modelo de redes bayesianas. www.redalyc.org [página web]. (7, enero, 2019). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://www.redalyc.org/journal/2811/281161618004/movil/>.

24 GOMEZ, Diego González. Sistema de detección de intrusiones. https://dgonzalez.net/ [página web]. (1, julio, 2007). [Consultado el 5, noviembre, 2023]. Disponible en Internet: <https://dgonzalez.net/papers/ids/ids_v1.0.pdf>.

Las Amenazas que representan escenarios o eventos que podrían explotar esas vulnerabilidades y su respectiva probabilidad de que una amenaza se materialice está unida y ligada a la efectividad de los mecanismos de defensa implementados para evaluar esta probabilidad que implica anticipar posibles escenarios y entender la sofisticación de las amenazas existentes. Por ultimo y no menos importante, el impacto que se refiere a las consecuencias derivadas de una explotación exitosa de una vulnerabilidad.

Comprender los diversos elementos del riesgo permite a las organizaciones desarrollar el tercer paso que son estrategias efectivas, gestionar los riesgos, así como la implementación y el mantenimiento de medidas de seguridad adecuadas que, sumado a los empleados, que deben comprender los riesgos y su papel en el mantenimiento de la seguridad de la información.

La gestión de la seguridad de la información garantiza que en ultimas los activos de información estén protegidos contra el acceso, uso, divulgación, interrupción, alteración o destrucción no autorizados.[25]

4.1.2 Categorización de IDS

Como herramienta los IDS son la base para proteger de forma proactiva redes para monitorear el tráfico y detectar códigos maliciosos en sistemas digitales, este tipo de herramienta se basa en modelos y patrones de comportamiento que detecta por medio de análisis de estadísticas de uso, este es un elemento crítico para proteger la integridad, la confidencialidad y la disponibilidad de la información en todas las empresas con respecto a amenazas cibernéticas.

Los IDS son esencialmente un conjunto de herramientas y mecanismos diseñados para identificar y responder a actividades anómalas o potencialmente maliciosas dentro de una red o sistema. Sus operaciones se basan en el monitoreo continuo de patrones de tráfico, comportamientos anómalos sobre firmas específicas, utilizando firmas heurísticas, soportado con técnicas de análisis estadístico para detectar posibles intrusos o violaciones.

Existen enfoques en distinguir diferentes sistemas de descubrimiento de intrusos en función de qué sistemas revisan y en función en cómo lo realizan, por lo tanto, en

25 IRWIN, Luke. What is information security management? - IT governance UK blog. IT Governance UK Blog [página web]. (22, febrero, 2022). [Consultado el 12, noviembre, 2023]. Disponible en Internet: <https://www.itgovernance.co.uk/blog/what-is-information-security-management>.

función de qué sistemas revisan existen grupos centralizados.[26]que buscan mediante un análisis de acciones un único servidor en búsqueda de agresiones a una subred o dominio completo.

Los IDS basados en red revisan y verifican paquetes que circulan en búsqueda de elementos que se vean como un ataque contra alguna ip, servidor o pc que se encuentra en su subred, Tienen una función protegiendo una sola plaza de forma análoga a un antivirus en forma de background investigando patrones que puedan indicar una tentativa de intrusión y alertar, para tomar medidas eficaces y oportunas.

A su vez se divide en 3 grandes grupos:

SIV: Sistemas que monitorizar información en búsqueda de posibles modificaciones.

LFM: Sistemas que revisan log generados por algún tipo de programa en una red en búsqueda de patrones alterados.

Honeypots o DTK: Sistemas que simulan falencias en servicios con inconvenientes de seguridad aprovecha al registrar todas actividad del atacante.

La otra clase IDS basados en un host en cómo actúan.

Detección de anomalías, basado en suponer que una intrusión es una anomalía, crea un perfil de conducta del sistema y revelaría infracciones por patrón, denominado discernimiento positivo.

Detección en uso indebido en esta busca patrones para ataques ya conocidos y diferenciaciones y se basa en estar al tanto de lo anormal para detectar la agresión, como conocimiento negativo.

Propiedades de un IDS:[27]

IDS sin continuidad y sin supervisión;
Bajo grado de intrusión sin afectar el sistema general y no crea un exceso sin generar falsos positivos.

---

26 OSTEC. DS:historia, concepto y terminología. https://ostec.blog/ [página web]. (1, octubre, 2015). [Consultado el 5, noviembre, 2023]. Disponible en Internet: <https://ostec.blog/es/seguridad-perimetral/ids-conceptos/>.

27 Joel Esler, PulledPork 3 — Actualización de reglas para Snort 3 [Sitio Web]. [Consultado 19, septiembre, 2022]. Disponible En:<https://blog.snort.org/2021/06/pulledpork-3-rule-updating-for-snort-3.html>

Adaptabilidad a modelos dinámicos o cambios en el entorno de trabajo en la empresa, tolerancia a Fallas, entre otras la capacidad ante eventos de improviso.

Estos sistemas son instalados monitoreando la actividad local y detectan cambios inusuales en archivos, registros del sistema y configuraciones. Pueden basarse en firmas para identificar patrones de ataque específicos o en anomalías para detectar comportamientos anómalos dentro de un sistema.

IDS híbridos estos combinan las capacidades de la red y los sistemas basados en host, aprovechando tanto el análisis del tráfico de la red como el comportamiento del sistema local para brindar una cobertura más completa.

En definitiva, los IDS monitorean el tráfico entrante a través de análisis de la red y aumenta su protección escaneando los puertos, una vez terminado compara esta información con elementos maliciosos, si detecta actividad potencialmente sospechosa, el sistema de detección proporciona una alerta temprana que se envía al administrador del sistema u soporte, según análisis se encuentra el mejor IDS asi:

Figura 6 Mejor Software de detección IDS

		Free Trial Description	Product Best Use	Product Top Features			Bottom Line
SolarWinds Security Event Manager	solarwinds	30-Days	Small Business, Enterprise	Automated remediation capabilities	Real-time alerts	Compliance and audit reports	Powerful intrusion prevention system with exceptional log file management tools.
Papertrail	solarwinds papertrail	Free with optional upgraded plans	Small Business, Enterprise	Centralized log file storage	Uses anomaly and signature-based detection methods	Different payment plans	Cloud-based log management service with high levels of security.
ManageEngine Event Log Analyzer	ManageEngine	Personalized demo available	Small Business, Enterprise	Customizable dashboards	Easily restore from backups	Runs on Windows or Linux	A HIDS and NIDS with robust log management.
OSSEC	OSSEC	Free with optional upgraded plans	Home, Small Business	Effective log file processing	Anomaly-based detection	Runs on Windows, Linux, Unix, or Mac OS	Open-source HIDS with system monitoring features normally found in NIDS.
Sagan	QUADRANT	Free	Home, Small Business	Light CPU usage	Uses anomaly and signature-based detection methods	Runs on Unix, Linux, and Mac OS	A HIDS with several unique features that more prominent HIDS tools lack.
Splunk	splunk>	Free	Home, Small Business	Clean and attractive interface	Data analyzer	Runs on Unix, Linux, and Mac OS	Strong anomaly-based HIDS with workflow automation features.
Snort		Free	Home, Small Business	Real-time traffic analysis	Packet logging	Integrates with Sagan	Leading open-source intrusion prevention system with extensive rule customization.
Samhain		Free	Home, Small Business	Rootkit detection	Stealth monitoring	Manages multiple operating systems	Free HIDS with a variety of unique and useful functions.

Fuente : dnsstuff.com, (2022), Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft, descargado de : <https://www.dnsstuff.com/host-based-intrusion-detection-systems>

4.1.3 Categorización de IPS

Utilizados con el fin de proteger todo tipo de sistemas internos de posibles ataques o entradas no acreditadas, se utiliza como un instrumento qué analiza en todo momento conexiones que ingresan y presentan un análisis mediante variadas técnicas patrones y políticas de seguridad el tráfico de la red, este sistema detecta al actuar previniendo daños de ataques denomina reactivo, este sistema implementa varias estrategias de defensa informa de manera automática con base en detección es umbrales de alerta, creando alertas personalizadas.[28]

Existen como formas de detección establecida en firmas que verifica constantemente el tráfico de red en busca de ataques y revisa estándares de ataque de firmas predefinidos.[29] Además en forma de detección de examen de protocolo estado que se asemeja a incoherencias en un protocolo revisando eventos presentes con actividades correctas y predefinidas.

Existe en forma de detecciones establecidas por anomalías que monitorea todo tipo de paquetes cotejándolos con comportamientos normales y posibilita identificar nuevas amenazas, con la mala fortuna de crear falsos positivos.

4.1.4 Áreas comprometidas con la Seguridad Informática.

Confidencialidad: Implica exclusivamente a personal no acreditados que ingresan a sistemas de datos e información que no tienen ningún tipo de permiso . [30]
Integridad: Solo personal autorizado puede ser capaz de cambiar datos cuando lo amerite.
Disponibilidad: los datos e información siempre deben permanecer disponibles ante cualquier circunstancia para usuarios en el momento adecuado.
Autenticación: se debe estar completamente inequívoco qué la información entregada sea la persona indicada.

---

28 WWW.DNSSTUFF.COM. 7 Best Intrusion Detection Software and Latest IDS Systems. www.dnsstuff.com [página web]. (18, febrero, 2020). [Consultado el 13, octubre, 2022]. Disponible en Internet: <https://www.dnsstuff.com/network-intrusion-detection-software>.

29 PATHAK, Amrita. 8 herramientas IDS e IPS para una mejor seguridad y conocimiento de la red. geekflare.com [página web]. (16, febrero, 2022). [Consultado el 28, octubre, 2022]. Disponible en Internet: <https://geekflare.com/es/best-ids-and-ips-tools/>.

30 RAMÍREZ MÁRQUEZ, Jimmy Fernando. Análisis, desarrollo e implementación de un sistema de seguridad para el fortalecimiento de vulnerabilidades e integridad de aplicaciones web académicas. http://dspace.espoch.edu.ec/ [página web]. (12, marzo, 2022). [Consultado el 29, octubre, 2022]. Disponible en Internet: <http://dspace.espoch.edu.ec/handle/123456789/15708>.

4.2 MARCO HISTÓRICO

En 1980 James P. Anderson, documento la necesidad de un proyecto automatizar a la revisión de eventos en seguridad, se llamó Monitor de referencia redacta un informe sobre detección de intrusiones, subjetiva eliminación de información redundante mediante la revisión de registros de sucesos, según su investigación era necesario la clasificación, la cual distinguía algún tipo de ataque interno y externo verificando si el usuario tenía permiso de acceso o no al PC.

Algunos de objetivos debían entregar información a los encargados de seguridad, obtener datos distintas partes en el sistema, evitar algún tipo de ataque interno o indebido fuera de lo normal usuarios o recursos, además detectaría de diseño el mecanismo el capaz de verificar la estrategia usada.

Entre 1984 y 1986 Dorothy Denning y Peter Newman crearon un modelo llamado "Instrusion Detection Expert System", que definía un sistema de detección de intrusiones en tiempo real creado por la marina estadounidense buscaba la actividad de abuso, indebida o no particular por cuenta de un usuario indebido, este sistema establecía métodos estadísticos como pautas de comportamiento que según reglas presentaba posibles diferencias detectaba un nivel de seguridad adicional qué podría minimizar instrucción en caso dado este prototipo llamado SRI internacional.

Durante los comienzos de detección de intrusiones estos sistemas monitorizaban HOST o máquinas, fue solo a partir de los años noventa qué se creó DIDS "Distributed Intrusion Detection System", Qué fue la unión entre la revisión de un Host y una red, A partir de 1990 qué se crean los primeros programas de detección de intrusiones informe comercial inició con "computer watch" desarrollado por la empresa AT&T.[31]

4.3 ANTECEDENTES O ESTADO ACTUAL

Existe en la empresa un sistema de seguridad desarrollado para salvaguardar los datos y mejorar la seguridad en la sede principal la cual cuenta con herramientas de monitoreo cortafuegos, antivirus, DA básico del cortafuegos, está en proceso implementación de la norma ISO 27000, las cuales después de realizar diferentes tipos de análisis son necesarias varias mejoras en herramientas de seguridad, detectando en tiempo real posibles intentos de ataque a la red, creando y renovando reglas y políticas de seguridad establecidas, monitoreando la actividad de la red,

31 GONZÁLEZ GÓMEZ, Diego. Sistemas de Detección de Intrusiones. dgonzalez.net [página web]. (julio, 2003). [Consultado el 29, octubre, 2022]. Disponible en Internet: <https://dgonzalez.net/papers/ids/ids_v1.0.pdf>.

existe la herramienta de cortafuegos la cuál es una aproximación de un IDS, pero como tal no cumple las expectativas de la organización.

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

Al iniciar la presente investigación fue necesario verificar varios textos de estudio, viendo como tal los complementos teóricos de un como identificar intrusos, fue necesario después de analizar la documentación y red, la implementación de un IDS E IPS, los cuales se complementarían, para identificar en la red y en el sistema cualquier tipo de ataque.[32]

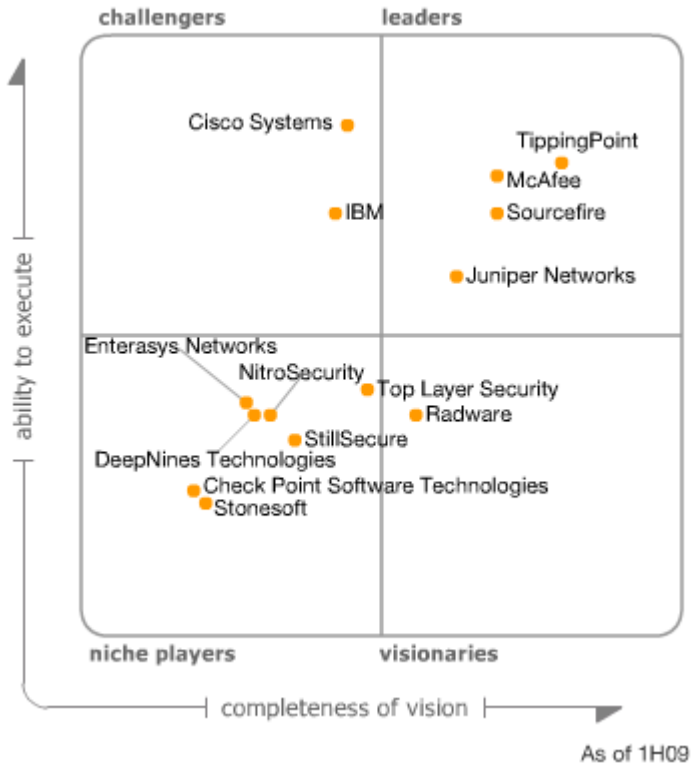
Fue necesario comparar las principales arquitecturas sus respectivos funcionamientos, tipos de sistema de detección de intrusos actuales, capas de red dónde se puede procesar y detectar paquetes de información y confirmar sí existe algún tipo de anomalía en los protocolos.

Se identifica características esenciales sobre el proyecto, las cuáles deben ser como mínimo una reacción automática acciones de ataques, filtros que detecten ataques en progreso, realizar monitoreo de falsos positivos y un bloqueo automático de ataques tiempo real, es necesario qué la herramienta proteja el sistema si no está debidamente parcheado y como acción fundamental optimizar el rendimiento de la red sin afectar la misma.

Mediante el cuadro de Gartner identificamos que la herramienta snort (Sourcefire) se encuentra entre las mejores de su ámbito por lo tanto se adecuara en la empresa respectiva.

32 INGALLS, Sam. Best intrusion detection and prevention systems (IDPS) for 2022. www.esecurityplanet.com [página web]. (6, octubre, 2022). [Consultado el 29, octubre, 2022]. Disponible en Internet: <https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/>.

Figura 7 Cuadro Garther mejores herramientas IDS/IPS



Fuente : www.neteye-blog.com,(2022), Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft, descargado de : <https://www.neteye-blog.com/2009/11/intrusion-detection-con-snort-leader-per-la-gartner/>

El sistema Snort actúa como prevención y detección en una red bajo licencia gpl, estudia e indaga el tráfico en tiempo real por medio de filtros buscando ataques.

Inicia su proceso capturando tráfico de red por medio de los protocolos udp, icmp, tcp/IP, paso seguido procesa y analiza por medio un motor de detección comparando paquetes, basado en reglas preestablecidas, su configuración es guardada en archivos que describe cada uno de los módulos, Módulo de captura de paquetes, monitoreados en vivo indirecto se crea un decodificador Libpcap este se encarga identificar protocolos de red, se complementa con un preprocesador encargado de analizar y almacenar todos los datos, ip de origen y destino, puertos y protocolos sigue el módulo de detección, que revisa paquetes entregados por el preprocesador, comparándolos en las reglas predefinidas y esperando una acción con respecto a las mismas.

Se complementa con el sistema de alertas e informes, que genera alertas en caso de detectar algún tipo de paquete en forma de ataque y por último el módulo de

reglas, que se identifica como patrones o comportamientos los cuales se deben Buscar y los paquetes capturados.[33]

4.5 MARCO LEGAL

Este proyecto es basado en leyes que protejan los datos y la integridad de los sistemas informáticos de la empresa, las sanciones al personal qué de manera incorrecta utilice los sistemas informáticos y las redes en Colombia.

Con base en este precepto se identifica la ley 1273 de 2009, que dicta normas y requisitos legales y se adecuan la actualidad, en esta ley se preservan los sistemas tecnología de la información y con y mediante artículos el acceso actualización Estación canción vicioso personales canción de sitios web acarrearan penalidades y muchas más tipificaciones.[34]

Algunos artículos de la ley que aplican al proyecto son: [35]

Artículo 269A: Acceso ilegal a un sistema informático.

Artículo 269B: Obstaculización ilegítima de sistema informático o red.

Artículo 269D: Perjuicio Informático.

Artículo 269E: Uso de software indebido.

Además, se tiene muy en cuenta la Ley 1581 del 2012, que habla de datos sensibles si existiera uso indebido de datos o revelen datos sensibles o privados.

33 ZAMBRANO, Farias. Diseño de un sistema de detección de intrusos usando SNORT a través del análisis de tráfico en tiempo real y el análisis de protocolos [en línea]. Tesis doctoral. Guayaquil: Universida de Guayaquil, 2022 [consultado el 13, noviembre, 2022]. Disponible en Internet: <http://repositorio.ug.edu.ec/handle/redug/59777>.

34 POLICÍA NACIONAL DE COLOMBIA. Normatividad sobre delitos informáticos. www.policia.gov.co [página web]. (30, octubre, 2022). [Consultado el 22, octubre, 2022]. Disponible en Internet: <https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos>.

35 POLICÍA NACIONAL DE COLOMBIA. Normatividad sobre delitos informáticos. www.policia.gov.co [página web]. (30, octubre, 2022). [Consultado el 22, octubre, 2022]. Disponible en Internet: <https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos>.

Es necesario las respectivas autorizaciones en todo caso de los titulares por medio de consulta.

5 DISEÑO METODOLÓGICO

5.1.1 Investigación aplicada

Su objetivo es solucionar un inconveniente específico, enfocándose en la investigación y fortalecimiento del conocimiento para aplicarlo en el desarrollo del proyecto, los hallazgos tecnológicos encontrados basados en la recopilación de primera medida de datos y patrones en la empresa para generar conocimiento por medio de la aplicación directa del problema abordado.

Al analizar los datos se trabajará en el desarrollo de implementación de dicha tecnología y la aplicación en la red real, las experiencias con la aplicación de esta nueva tecnología, analizar y recolectar posibles fallas en todo el modelo de solución implantado definirá cambios y adaptaciones para su aplicación en la empresa para dar respuesta a una dificultad especifica.

6 DESARROLLO DEL OBJETIVO 1

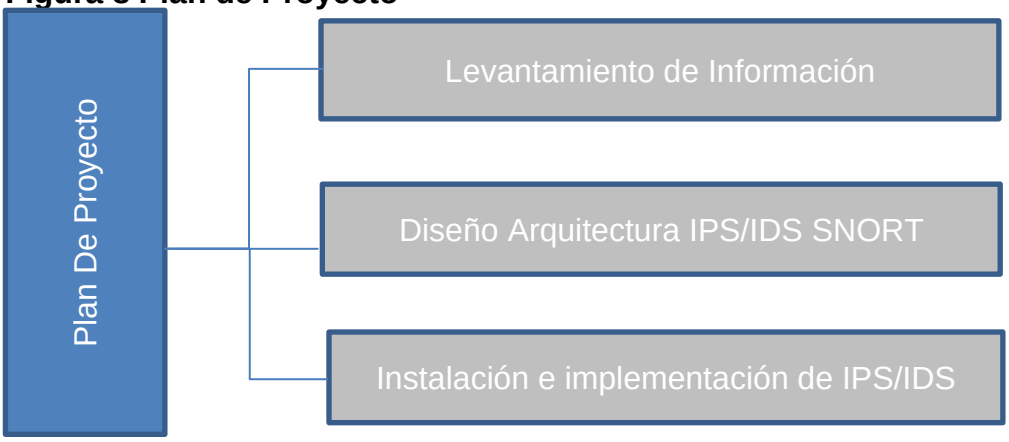
6.1 Identificación de equipos de comunicaciones y servidores de la organización con posibles fallas de seguridad que pueden ser afectados por distintos vectores de ataques.

Iniciamos el proceso reconociendo la infraestructural actual mediante la recopilación de diferentes servidores y equipos, los cuales son elementos necesarios para desarrollar la instalación e implementación del proyecto, está documentación se enfoca en los sistemas de información y su debida importancia, es necesario documentar y recolectar datos técnicos necesarios para tomar decisiones y facilitar a futuro la administración del mantenimiento de la plataforma y obviamente de los servidores, tomando decisiones sobre la implementación y uso debido de las herramientas.[36]

Recolectamos información básica sobre elementos que conforman el Data Center en la empresa, los servicios de la compañía están basados en creación e implementación de software y aplicaciones web empresariales, soporte a usuarios internos y externos de empresas, servidores de rack, virtualizados, equipos de almacenamiento NAS, bases de datos.

Está primer fase nos muestra información con el fin de conocer la infraestructura de red, comunicaciones, servidores, computadores de oficina y los diferentes servicios que operan sobre la misma y el sistema de seguridad actual.

Figura 8 Plan de Proyecto



Fuente: Propia

36 MARTÍNEZ RAMÍREZ, CARLOS ANDRÉS. DOCUMENTACIÓN TÉCNICA Y PROTOCOLO PARA LEVANTAMIENTO DE INFORMACIÓN EN CENTROS DE DATOS. /repositorio.ucp.edu.co [página web]. (2020). [Consultado el 26, noviembre, 2022]. Disponible en Internet: <https://repositorio.ucp.edu.co/bitstream/10785/3027/1/CDPEIST48.pdf>.

Adjunto diagrama de Rack actual:

Figura 9 Rack Servidores 1

Nombre / Descripción
Servidor 1
Servidor 2
Servidor 3
Servidor 4
Servidor 5
Switch 1
PatchPanel
Organizador
Servidor 6
Organizador
Patch Panel
Patch Panel
Patch Panel
Servidor 7
Servidor 8
Servidor 9
Servidor 10
Servidor 11
Servidor 12
Servidor 13
Servidor 14

Fuente: Propia

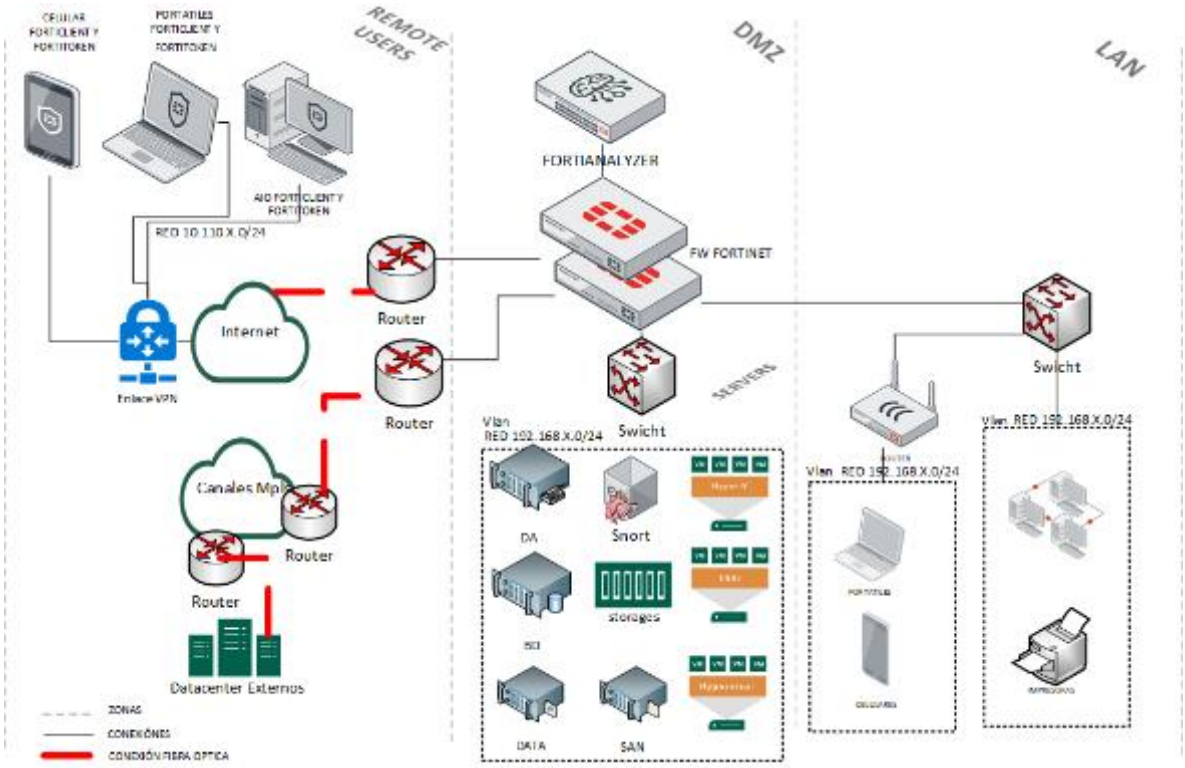
Figura 10 Rack Servidores 2

Nombre / Descripción
Firewall 1
Firewall 2
Fortyanalizer 1
Switch 1
Organizador
Switch 2
Patch Panel
Patch Panel
Patch Panel
Switch 3
Switch 4
Patch Panel
Organizador
Switch 5
Patch Panel
Patch Panel
Patch Panel
Patch Panel
UPS 1
UPS 2

Fuente: Propia

El siguiente esquema describe el sistema seguridad actual las oficinas de la empresa, conformado por un cortafuegos pasivo activo, canales de internet dedicado principal y contingencia, mpls principal y contingencia, switches para conexión entre servidores y equipos de la oficina, replicador de wi-fi, planta telefónica IPs, impresoras, servidores físicos y de virtualización, con una unidad de almacenamiento San.

Figura 11 Diagrama De Topología Red De Empresa



Fuente: propia

Tabla 1 Inventario de Servidores Físicos

HOSTNAME	Tipo	datacenter	Ubicación	Memoria GB	CPUs - Core	Sistema Operativo
SERVIDOR 1	Físico	PROPIO	Bogota	16	4	Windows Server 2012 R2 Std
SERVIDOR 2	Físico	PROPIO	Bogota	128	20	Windows Server 2012 R2 Std
SERVIDOR 3	Físico	PROPIO	Bogota	16	4	Windows Server 2012 Std
SERVIDOR 4	Físico	PROPIO	Bogota	36	4	Windows Server 2012 Std
SERVIDOR 5	Físico	PROPIO	Bogota	256	24	Vmware Esx 7.0
SERVIDOR 6	Físico	PROPIO	Bogota	32	12	Oracle Linux 7.7
SERVIDOR 7	Físico	PROPIO	Bogota	256	24	Vmware ESX 7.0
SERVIDOR 8	Físico	PROPIO	Bogota	256	24	Vmware ESX 7.0
SERVIDOR 9	Físico	PROPIO	Bogota	126	12	Oracle Linux 7.7
SERVIDOR 10	Físico	PROPIO	Bogota	256	12	Vmware ESX 7.0
SERVIDOR 11	Físico	PROPIO	Bogota	256	12	Vmware ESX 6.7
SERVIDOR 12	Físico	PROPIO	Bogota	126	12	Oracle Linux 7.7
SERVIDOR 13	Físico	PROPIO	Bogota	32	12	Oracle Linux 7.7
SERVIDOR 14	Físico	PROPIO	Bogota	32	12	Linux nas

Fuente: propia

La empresa cuenta con varios servidores físicos que se utilizan para virtualización, un equipo que se utiliza como servidor dns y de dominio, servidor para copias de seguridad, servidor para datos.

Existen políticas de red, implantadas por medio del dominio con autenticación del usuario qué evita acceso a terceros sin autorización el cual restringen acceso a carpetas, según la matriz roles y procedimientos, se restringe según el cargo acceso a internet, los usuarios tiene antivirus que verifican y restringe el acceso a páginas web, existen Vlan para servidores, DMZ, red wi-fi interna, empresarial e invitados, voz, además tiene servicios de red como, VPN, servidor de archivos, página web, ftp, smtp, telefonía IP, desactivado servicio DHCP.

Tabla 2 Inventario de Servidores Virtuales

Cod Maquina	MAQUINA VIRTUAL	Powersta	CPU	Memori	Memory	NICs	Disks	OS according to the configuration file
SERVIDOR 1	HYPERV 1	poweredOn	2	6	6144	1	1	Other 3.x Linux (64-bit)
SERVIDOR 2	HYPERV 2	poweredOn	2	16	16384			Windows Server
SERVIDOR 2	HYPERV 3	poweredOn	2	4	4096			Windows Server
SERVIDOR 3	VMWARE 1	poweredOn	1	2	2048			Windows Server
SERVIDOR 3	VMWARE 2	poweredOn	1	8	8192			Windows Server
SERVIDOR 3	VMWARE 3	poweredOn	4	6	6144			Windows Server
SERVIDOR 3	VMWARE 4	poweredOn	1	2	2048			Windows Server
SERVIDOR 3	VMWARE 5	poweredOn	4	12	12288			Windows Server 2012R2
SERVIDOR 3	VMWARE 6	poweredOn	2	24	24576			Windows Server
SERVIDOR 3	VMWARE 7	poweredOn	2	2	2048			Windows Server
SERVIDOR 3	VMWARE 8	poweredOn	2	6	6144			Windows Server
SERVIDOR 4	VMWARE 9	poweredOn	4	32	32768			Windows Server 2016
SERVIDOR 4	VMWARE 10	poweredOn	4	8	8192			Centos 7 Linux
SERVIDOR 4	VMWARE 11	poweredOn	10	16	16384			Windows Server 2016
SERVIDOR 4	VMWARE 12	poweredOn	4	8	8192			Windows Server 2016
SERVIDOR 4	VMWARE 13	poweredOn	24	32	32768			Centos 7 Linux
SERVIDOR 4	VMWARE 14	poweredOn	6	16	16384			Windows Server 2016
SERVIDOR 4	VMWARE 15	poweredOn	2	8	8192			Windows Server 2016
SERVIDOR 4	VMWARE 16	poweredOn	8	16	16384			Windows Server 2019
SERVIDOR 4	VMWARE 17	poweredOn	8	8	8192			Microsoft Windows Server 2019 (64-bit)
SERVIDOR 4	VMWARE 18	poweredOn	8	16	16384			Microsoft Windows 10 (64-bit)
SERVIDOR 4	VMWARE 19	poweredOn	5	8	8192			Microsoft Windows Server 2016 (64-bit)
SERVIDOR 4	VMWARE 20	poweredOn	4	32	32768			Microsoft Windows Server 2016 or later (64-bit)
SERVIDOR 4	VMWARE 21	poweredOn	4	12	12288			Other Linux (64-bit)
SERVIDOR 4	VMWARE 22	poweredOn	6	20	20480			Microsoft Windows Server 2016 (64-bit)
SERVIDOR 4	VMWARE 23	poweredOn	6	16	16384			Microsoft Windows Server 2016 (64-bit)
SERVIDOR 4	VMWARE 24	poweredOn	10	16	16384			Microsoft Windows Server 2016 (64-bit)
SERVIDOR 5	VMWARE 25	poweredOff	8	20	20480			Ubuntu Linux (64-bit)
SERVIDOR 5	VMWARE 26	poweredOn	2	16	16384			Ubuntu Linux (64-bit)
SERVIDOR 5	VMWARE 27	poweredOn	2	16	16384			Oracle Linux 7 (64-bit)
SERVIDOR 5	VMWARE 28	poweredOff	8	16	16384			Ubuntu Linux (64-bit)
SERVIDOR 5	VMWARE 29	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 5	VMWARE 30	poweredOff	4	4	4096			Ubuntu Linux (64-bit)
SERVIDOR 5	VMWARE 31	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 5	VMWARE 32	poweredOff	8	20	20480			Ubuntu Linux (64-bit)
SERVIDOR 5	VMWARE 33	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 5	VMWARE 34	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 6	HYPERV 4	poweredOn	2	4	4096			Windows 7
SERVIDOR 6	HYPERV 5	poweredOn	4	8	8192			Oracle Linux 7 (64-bit)
SERVIDOR 6	HYPERV 6	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 7	VMWARE 35	poweredOn	8	20	20480			Oracle Linux 7 (64-bit)
SERVIDOR 7	VMWARE 36	poweredOn	2	16	16384			Ubuntu Linux (64-bit)
SERVIDOR 7	VMWARE 37	poweredOn	4	16	16384			Oracle Linux 7 (64-bit)
SERVIDOR 8	VMWARE 38	poweredOn	4	16	16384			Centos 8 Linux
SERVIDOR 8	VMWARE 39	poweredOn	8	4	4096			Oracle Linux 7 (64-bit)
SERVIDOR 8	VMWARE 40	poweredOn	8	12	12288			Oracle Linux 7 (64-bit)
SERVIDOR 8	VMWARE 41	poweredOn	8	12	12288			Oracle Linux 7 (64-bit)
SERVIDOR 9	VMWARE 42	poweredOff	2	8	8192			Windows Server 2012
SERVIDOR 9	VMWARE 43	poweredOn	4	8	8192			Oracle Linux 7 (64-bit)
SERVIDOR 9	VMWARE 44	poweredOn	4	16	16384			Oracle Linux 7 (64-bit)
SERVIDOR 9	VMWARE 45	poweredOn	4	8	8192			Oracle Linux 7 (64-bit)
SERVIDOR 9	VMWARE 46	poweredOn	4	8	8192			Oracle Linux 7 (64-bit)
SERVIDOR 9	VMWARE 47	poweredOn	6	6	6144			Oracle Linux 7 (64-bit)
SERVIDOR 10	VMWARE 48	poweredOn	2	2	2048			Centos 7 Linux
SERVIDOR 10	VMWARE 49	poweredOn	2	4	4096			Centos 8 Linux
SERVIDOR 10	VMWARE 50	poweredOn	2	4	4096			Centos 8 Linux
SERVIDOR 10	VMWARE 51	poweredOff	1	4	4096			Windows 7
SERVIDOR 10	VMWARE 52	poweredOff	2	4	4096			Oracle Linux 7 (64-bit)

Fuente: propia

Tabla 3 Componentes de Red

PRODUCTO	TIPO	DATACENTER	Familia de servicios	Descripción
Firewall	Físico	Oficina	Servicios de Seguridad	Firewall perimetral de acceso y control
Firewall	Físico	Oficina	Servicios de Seguridad	Firewall perimetral de acceso y control
FortyAnalizer	Físico	Oficina	Servicios de Seguridad	Control de logs de Cortafuegos

Fuente: propia

Tabla 4 Inventario Swichts

SWITCH´S	MODELO
SWITCH 1	Cisco Catalyst 50P-Port Gigabit
SWITCH 2	Cisco Catalyst 50P-Port Gigabit
SWITCH 3	Cisco Catalyst 50-Port Gigabit
SWITCH 4	Cisco Catalyst 50-Port Gigabit
SWITCH 5	Cisco Catalyst 50-Port Gigabit
SWITCH 6	Cisco Catalyst 50-Port Gigabit
SWITCH 7 - AREA 1	Cisco Catalyst 26-Port Gigabit
SWITCH 8 - AREA 1	Cisco Catalyst -26P-Port Gigabit
SWITCH 9 - AREA 2	Cisco Catalyst -26P-Port Gigabit
SWITCH 10 - AREA 2	Cisco Catalyst -26P-Port Gigabit
SWITCH 11 MERAKI	Cisco MS120-24P-Port Gigabit

Fuente: propia

7 DESARROLLO DEL OBJETIVO 2

7.1 REALIZAR UN ANÁLISIS DE TRÁFICO CON EL FIN DE GARANTIZAR Y MEJORAR MONITOREO, ANTE SITUACIONES DE ATAQUES Y REFORZAR LA SEGURIDAD.

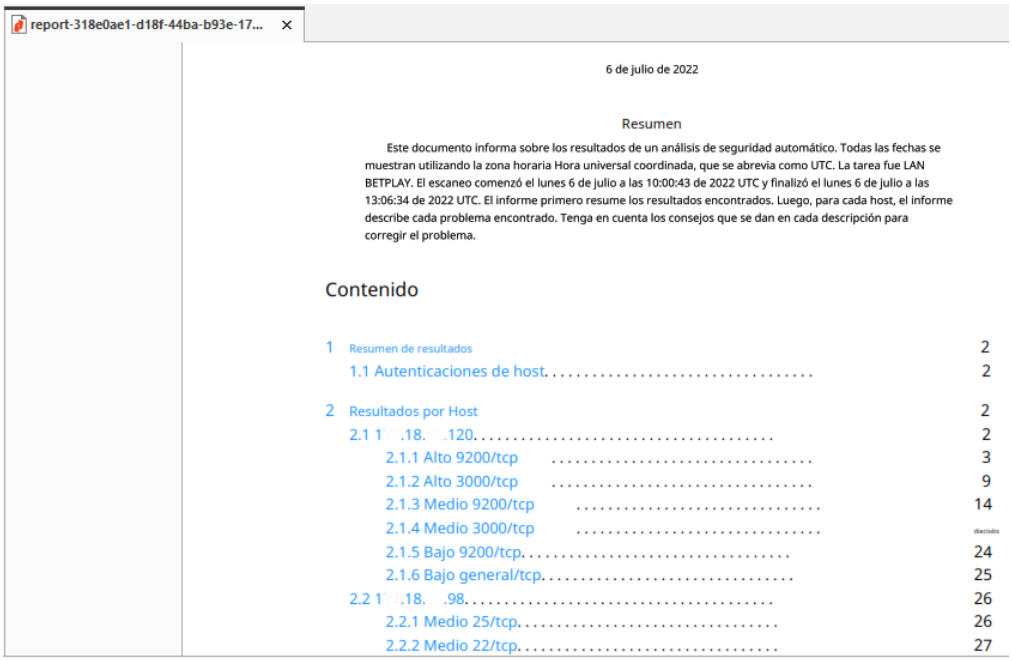
Realizada la identificación de diagrama de red se realizó mediante herramienta de escaneo de red ip- scanner buscando los distintos equipos conectados a la red con verificación de administradores de área de TI, se mostrarán datos básicos de los servidores, no es factible entregar información detallada de la red interna, el segmento de red trabaja sobre clase C 192.168.x.0/24, con subredes donde se identifican activos.

Como producto de la actividad se pueden establecer las siguientes vulnerabilidades y observaciones por parte del equipo consultor:

7.2 REPORTE OPENVAS – JULIO 2022

A continuación, se relacionan los segmentos de red y las páginas web escaneadas, se mencionan la cantidad de vulnerabilidades, el nivel de la vulnerabilidad, las IP anonimizadas que más resaltan y cuál es la vulnerabilidad que presenta, imagen de informe generado en pdf:

Figura 12 Informe PDF Openvas



Fuente: propia

7.3 Reporte OpenVas Pagina Web Betxlay.com.co Julio 2022

Reporta solo dos (2) vulnerabilidades nivel bajo

Tabla 5 Web Betxxx.Com.Co

Vulnerabilidad	Gravedad ▼	QoD	Anfitrión		Ubicación
			IP	Nombre	
TCP timestamps	**2.6 (Low)**	80 %	192.1X.2X.3X	www.bXX.com.co	general/tcp
TCP timestamps	**2.6 (Low)**	80 %	10X.1X.XX.3X	www.bXX.com.co	general/tcp

Fuente: propia Openvas

7.4 Reporte OpenVas Pagina Web Superx.Com.Co Julio 2022

Reporta 31 vulnerabilidades nivel medio separadas por vulnerabilidad y visualizando el puerto

Tabla 6 Web Supexx.com.co

Vulnerabilidad	Gravedad	QoD	Anfitrión		Ubicación
			IP	Nombre	
SSL/TLS: falta el atributo de cookie `seguro`	**6.4 (Medio)**	99 %	6X.4X.23.1XX	supXXXXX.com.co	2087/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	www.supXXXXX.com.co	2083/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	supXXXXX.com.co	2083/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	host.ceXXXXXX.co	2087/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	www.supXXXXX.com.co	2087/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	host.ceXXXXXX.co	2083/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	supXXXXX.com.co	2096/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	www.supXXXXX.com.co	2096/tcp
	6.4 (Medio)	99 %	6X.4X.23.1XX	host.ceXXXXXX.co	2096/tcp
Algoritmo(s) de clave de host débil (SSH)	**5.3 (Medio)**	80 %	6X.4X.23.1XX	host.ceXXXXXX.co	22555/tcp
Algoritmo(s) compatible(s) de intercambio de clave débil (KEX) (SSH)	**5.3 (Medio)**	80 %	6X.4X.23.1XX	host.ceXXXXXX.co	22555/tcp
SSL/TLS: informe conjuntos de cifrado débiles	**5.0 (Medio)**	98 %	6X.4X.23.1XX	host.ceXXXXXX.co	587/tcp
	5.0 (Medio)	98 %	6X.4X.23.1XX	host.ceXXXXXX.co	465/tcp
SSL/TLS: vulnerabilidad DoS de renegociación (CVE-2011-1473, CVE-2011-5094)	**5.0 (Medio)**	70 %	6X.4X.23.1XX	supXXXXX.com.co	587/tcp
	5.0 (Medio)	70 %	6X.4X.23.1XX	host.ceXXXXXX.co	587/tcp
Inicio de sesión de texto claro sin cifrar de FTP	**4.8 (Medio)**	70 %	6X.4X.23.1XX	supXXXXX.com.co	21/tcp
	4.8 (Medio)	70 %	6X.4X.23.1XX	www.supXXXXX.com.co	21/tcp
	4.8 (Medio)	70 %	6X.4X.23.1XX	host.ceXXXXXX.co	21/tcp
Inicio de sesión de texto claro sin cifrar SMTP	**4.8 (Medio)**	70 %	6X.4X.23.1XX	host.ceXXXXXX.co	587/tcp
	4.8 (Medio)	70 %	6X.4X.23.1XX	host.ceXXXXXX.co	25/tcp
SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso	**4.3 (Medio)**	98 %	6X.4X.23.1XX	host.ceXXXXXX.co	993/tcp
Algoritmos de cifrados débiles admitidos (SSH)	**4.3 (Medio)**	95 %	6X.4X.23.1XX	host.ceXXXXXX.co	22555/tcp
SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso	**4.3 (Medio)**	98 %	6X.4X.23.1XX	host.ceXXXXXX.co	995/tcp
SSL/TLS: Vulnerabilidad de fuerza de grupo DH insuficiente de intercambio de claves Diffie-Hellman	**4.0 (Medio)**	80 %	6X.4X.23.1XX	supXXXXX.com.co	995/tcp
	4.0 (Medio)	80 %	6X.4X.23.1XX	www.supXXXXX.com.co	
	4.0 (Medio)	80 %	6X.4X.23.1XX	host.ceXXXXXX.co	
	4.0 (Medio)	80 %	6X.4X.23.1XX	supXXXXX.com.co	993/tcp
	4.0 (Medio)	80 %	6X.4X.23.1XX	www.supXXXXX.com.co	
	4.0 (Medio)	80 %	6X.4X.23.1XX	host.ceXXXXXX.co	

Marcas de tiempo de TCP	**2.6 (Bajo)**	80 %	6X.4X.23.1XX	host.ceXXXXXX.co	general/tcp

Fuente: Propia Openvas

7.5 Reporte OpenVas Segmento Red Lan Julio_2022 – 192.168.X.0/24

Reporta 35 vulnerabilidades nivel medio separadas por vulnerabilidad y visualizando el puerto

Tabla 7 Vulnerabilidades LaN Interna

Vulnerabilidad	Severidad▼	QoD	Host	Localización
			IP	
Algoritmo(s) compatible(s) de intercambio de clave débil (KEX) (SSH)	**5.3 (Medium)**	80 %	192.168XX.X	22/tcp
	5.3 (Medium)	80 %	192.168.X.X	22/tcp
	5.3 (Medium)	80 %	192.168.X.X	22/tcp
	5.3 (Medium)	80 %	192.168.X.X	22/tcp
SSL/TLS: vulnerabilidad DoS de renegociación (CVE-2011-1473, CVE-2011-5094)	**5.0 (Medium)**	70 %	192.168.X.X	443/tcp
	5.0 (Medium)	70 %	192.168.X.X	5580/tcp
	5.0 (Medium)	70 %	192.168.X.X	443/tcp
SSL/TLS: informe conjuntos de cifrado débiles	**5.0 (Medium)**	98 %	192.168.X.XX	3389/tcp
SSL/TLS: vulnerabilidad DoS de renegociación (CVE-2011-1473, CVE-2011-5094)	**5.0 (Medium)**	70 %	192.168.X.XX	5500/tcp
	5.0 (Medium)	70 %	192.168.X.XX	9080/tcp
	5.0 (Medium)	70 %	192.168.X.X	5989/tcp
	5.0 (Medium)	70 %	192.168.X.XX	5989/tcp
	5.0 (Medium)	70 %	192.168.X.X	443/tcp
	5.0 (Medium)	70 %	192.168.X.X	8084/tcp
	5.0 (Medium)	70 %	192.168.X.XX	636/tcp
Informes de enumeración de servicios DCE/RPC y MSRPC	**5.0 (Medium)**	80 %	192.168.X.XX	135/tcp
SSL/TLS: Detección de autoridad certificadora (CA) no confiable/peligrosa conocida	**5.0 (Medium)**	99 %	192.168.X.XX	4353/tcp
	5.0 (Medium)	99 %	192.168.X.XX	443/tcp
SSL/TLS: vulnerabilidad DoS de renegociación (CVE-2011-1473, CVE-2011-5094)	**5.0 (Medium)**	70 %	192.168.X.XX	5500/tcp
	5.0 (Medium)	70 %	192.168.X.X	9080/tcp
Transmisión de texto sin cifrar de información confidencial a través de HTTP	**4.8 (Medium)**	80 %	192.168.X.X	4414/tcp
	4.8 (Medium)	80 %	192.168.X.XX	4414/tcp
Algoritmos de cifrados débiles admitidos (SSH)	**4.3 (Medium)**	95 %	192.168.X.XX	22/tcp
SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso	**4.3 (Medium)**	98 %	192.168.X.X	5500/tcp
	4.3 (Medium)	98 %	192.168.X.X	4353/tcp
	4.3 (Medium)	98 %	192.168.X.X	443/tcp
	4.3 (Medium)	98 %	192.168.X.XX	5500/tcp
	4.3 (Medium)	98 %	192.168.X.X	3389/tcp
	4.3 (Medium)	98 %	192.168.X.XX	5500/tcp
SSL/TLS: Vulnerabilidad de fuerza de grupo DH insuficiente de intercambio de claves Diffie-Hellman	**4.0 (Medium)**	80 %	192.168.X.X	3389/tcp

Fuente: Propia Openvas

7.6 Reporte OpenVas Interna Julio 2022 – 192.168.X.0/24

Reporta el escaneo 113 vulnerabilidades a nivel alto y 401 nivel medio separadas por vulnerabilidad y visualizando el puerto

Tabla 8 Vulnerabilidades Dominios Internos

Vulnerabilidad	Gravedad	QoD	Anfitrión		Ubicación
			IP	Nombre	
Detección de fin de vida de PHP (Windows)	**10.0 (Alto)**	80 %	XX.XX.2x0	puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad de desbordamiento de búfer de pila de PHP Mar18 (Windows)	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidades múltiples de PHP (febrero de 2019) - Windows	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 7.0.x < 7.0.23, 7.1.x < 7.1.9 Vulnerabilidad Use-After-Free - Windows	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Múltiples vulnerabilidades de PHP: 19 de marzo (Windows)	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad de desbordamiento de enteros PHP Aug18 (Windows)	**9.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 7.1.x < 7.1.28, 7.2.x < 7.2.17, 7.3.x < 7.3.4 Múltiples vulnerabilidades - Windows	**9.1 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Vulnerabilidades múltiples: 20 de enero (Windows)	**9.1 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 7.1.x < 7.1.29, 7.2.x < 7.2.18, 7.3.x < 7.3.5 Vulnerabilidad de divulgación de información/DoS - Windows	**9.1 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 7.1.x < 7.1.30, 7.2.x < 7.2.19, 7.3.x < 7.3.6 Múltiples vulnerabilidades - Windows	**9.1 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP Múltiples Vulnerabilidades May18 (Windows)	**8.8 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad no especificada de la función 'Análisis HTTP' de PHP (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 Vulnerabilidad de libcurl - May20 (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad de divulgación de memoria de PHP (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad de desbordamiento de búfer basado en montón PHP 'timelib_meridian' (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP 'CVE-2018-19935' - Vulnerabilidad de denegación de servicio 'imap_mail' (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Informes de salida de phpinfo()	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 Vulnerabilidad DoS - 20 de abril (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidades múltiples de PHP: 19 de agosto (Windows)	**7.5 (Alto)**	80 %		puexxxxx.coxxxxx.com.co	8070/tcp
HP Integrated Lights-Out (iLO) 4 Múltiples vulnerabilidades remotas	**10.0 (Alto)**	80 %	XX.XX.1C		80/tcp
	10.0 (Alto)	80 %			443/tcp
Detección de fin de vida útil (EOL) de OpenSSL (Windows)	**10.0 (Alto)**	80 %	XX.XX.2C	corredor-cxxx.com.co	80/tcp
	10.0 (Alto)	80 %		corredor-cxxx.com.co	443/tcp

Detección de fin de vida útil (EOL) de jQuery (Windows)	**9.9 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	9.9 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
OpenSSL: el script c_rehash permite la inyección de comandos (CVE-2022-1292) - Windows	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Apache HTTP Server <= 2.4.52 Múltiples vulnerabilidades - Windows	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Servidor Apache HTTP <= 2.4.51 Vulnerabilidad de desbordamiento de búfer - Windows	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Apache HTTP Server < 2.4.49 Múltiples vulnerabilidades - Windows	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Apache HTTP Server 2.4.0 - 2.4.46 Múltiples vulnerabilidades - Windows	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Apache HTTP Server 2.4.32 < 2.4.44 mod_proxy_uwsgi Vulnerabilidad de desbordamiento de búfer (Windows)	**9.8 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	9.8 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Vulnerabilidad de acceso a la memoria del servidor Apache HTTP (Windows)	**9.1 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	9.1 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Apache HTTP Server 2.4.7 - 2.4.51 Múltiples vulnerabilidades - Windows	**8.2 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	8.2 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
OpenSSL: desbordamiento de enteros en CipherUpdate (CVE-2021-23840) - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Apache HTTP Server < 2.4.39 mod_ssl Vulnerabilidad de omisión de control de acceso (Windows)	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Apache HTTP Server 2.4.30 < 2.4.49 Vulnerabilidad DoS - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Apache HTTP Server < 2.4.48 Vulnerabilidad de desreferencia de puntero NULL - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp

Apache HTTP Server 2.4.17 < 2.4.49 Vulnerabilidad de contrabando de solicitudes HTTP/2 'mod_proxy' - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
OpenSSL: Bucle infinito en BN_mod_sqrt() accesible al analizar certificados (CVE-2022-0778) - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Apache HTTP Server 2.4.20 - 2.4.39 Varias vulnerabilidades (Windows)	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	443/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	80/tcp
Servidor HTTP Apache < 2.4.39 mod_auth_digest Vulnerabilidad de omisión de control de acceso (Windows)	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
OpenSSL: Lectura de desbordamientos del búfer Procesamiento de cadenas ASN.1 (20210824) - Windows	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Apache HTTP Server 2.4.20 < 2.4.44 Varias vulnerabilidades (Windows)	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Vulnerabilidad de desbordamiento de pila del servidor Apache HTTP (Windows)	**7.5 (Alto)**	80 %		corredor-cxxx.com.co	80/tcp
	7.5 (Alto)	80 %		corredor-cxxx.com.co	443/tcp
Detección de fin de vida útil (EOL) del sistema operativo (OS)	**10.0 (Alto)**	80 %	XX.XX.1C2		general/tcp
Centreon <= 2.8.23 Múltiples vulnerabilidades	**9.8 (Alto)**	80 %			443/tcp
Ejecución remota de código de Centreon	**7.5 (Alto)**	99 %			443/tcp
	7.5 (Alto)	99 %			443/tcp
osTicket < 1.14.8, 1.15.x < 1.15.4 Múltiples vulnerabilidades	**9.8 (Alto)**	80 %	XX.XX.1X6	intranet.cxxx.netxx.co	443/tcp
PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Actualización de seguridad (febrero de 2022) - Windows	**9.8 (Alto)**	80 %		intranet.cxxx.netxx.co	443/tcp
	9.8 (Alto)	80 %	192.168.X.X	puexxxxx.coxxxxx.com.co	8070/tcp
Vulnerabilidad de ejecución remota de código de Microsoft Windows Remote Desktop Services 'CVE-2019-0708' (BlueKeep) - (remoto activo)	**9.8 (Alto)**	99 %	192.168.X.XX		3389/tcp
	9.8 (Alto)	99 %	192.168.X.XX	puexxxxx.coxxxxx.com.co	3389/tcp
Vulnerabilidad de ejecución remota de código de IBM WebSphere Application Server (comprobación activa)	**9.8 (Alto)**	95 %	192.168.X.XX	sisxxx-prueba.cxx.netxx.co	8880/tcp
Vulnerabilidad de inyección de encabezado HTTP del servidor GoAhead	**8.6 (Alto)**	99 %	192.168.X.X		80/tcp
	8.6 (Alto)	99 %			443/tcp
	8.6 (Alto)	99 %			443/tcp
	8.6 (Alto)	99 %			80/tcp
Vulnerabilidad de validación de entrada incorrecta de PHP 'CVE-2017-7189' (Windows)	**7.5 (Alto)**	80 %	192.168.X.X	intranet.cxx.netxx.co	443/tcp
	7.5 (Alto)	80 %	192.168.X.X	puexxxxx.coxxxxx.com.co	8070/tcp

SSL/TLS: Informar conjuntos de cifrado vulnerables para HTTPS	**7.5 (Alto)**	98 %	192.168.X.XXC		443/tcp
	7.5 (Alto)	98 %	XX.XX.CX		443/tcp
	7.5 (Alto)	98 %	XX.XX.CC		443/tcp
	7.5 (Alto)	98 %	192.168.X.X		443/tcp
	7.5 (Alto)	98 %	192.168.X.X	escritorio-bxxxxxx.corredorxxxxxl.com.co	443/tcp
	7.5 (Alto)	98 %	192.168.X.X	lansxxxr.corredorxx.com.co	82/tcp
	7.5 (Alto)	98 %	192.168.X.X		5500/tcp
	7.5 (Alto)	98 %	192.168.X.X		443/tcp
	7.5 (Alto)	98 %	192.168.X.X		443/tcp
	7.5 (Alto)	98 %	192.168.X.X		9001/tcp
	7.5 (Alto)	98 %	192.168.X.X		8080/tcp
	7.5 (Alto)	98 %	192.168.X.XX		443/tcp
	7.5 (Alto)	98 %	192.168.X.X	sisxxxx-prueba.cexxx.netxx.co	8880/tcp
	7.5 (Alto)	98 %	192.168.X.XX	saxolarwinds.corredorxxxxl.com.co.	443/tcp
	7.5 (Alto)	98 %	192.168.X.X	sisxxxx-prueba.cexxx.netxx.co	9443/tcp
	7.5 (Alto)	98 %	192.168.X.XX	corredor-cxxx.com.co	443/tcp
	7.5 (Alto)	98 %	192.168.X.X		443/tcp
	7.5 (Alto)	98 %	192.168.X.XX		443/tcp
PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Actualización de seguridad (JULIO de 2022) - Windows	**7.5 (Alto)**	80 %	192.168.X.XXX	puexxxxx.coxxxxx.com.co	8070/tcp
	7.5 (Alto)	80 %	XX.XX.13X	intranet.cexxx.netxx.co	443/tcp
PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 Vulnerabilidad de deferencia NULL (febrero de 2021) - Windows	**7.5 (Alto)**	80 %	XX.XX.2CC	puexxxxx.coxxxxx.com.co	8070/tcp
	7.5 (Alto)	80 %	192.168.X.X36	intranet.cexxx.netxx.co	443/tcp
Credenciales predeterminadas de la interfaz web de la tarjeta de administración de red de APC	**7.5 (Alto)**	98 %	XX.XX.C5		80/tcp
Vulnerabilidad de Eclipse Jetty DoS (GHSA-26vr-8j45-3r4w) - Windows	**7.5 (Alto)**	80 %	XX.XX.2C5	microexxx.corredorxxxx.com...	3333/tcp
	7.5 (Alto)	80 %	XX.XX.2C5	microexxx.corredorxxx.com...	3334/tcp
Vulnerabilidad de omisión de autenticación de sesión nula SMB/NETBIOS de Microsoft Windows	**7.5 (Alto)**	99 %	XX.XX.174	cem-0x9.corredorxxx.com.co	445/tcp
	7.5 (Alto)	99 %	XX.XX.1X4	xem-9.corredorxxxx.com.co	445/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	**7.5 (Alto)**	70 %	XX.XX.4X		443/tcp
PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Actualización de seguridad (octubre de 2021) - Windows	**7.5 (Alto)**	80 %	XX.XX.1XX	intranet.cexxx.netxx.co	443/tcp
	7.5 (Alto)	80 %	XX.XX.2XX	puexxxxx.coxxxxx.com.co	8070/tcp

Fuente: propia Openvas

El hallazgo inicial una vez recolectada la información de los elementos antes descritos nos demuestra falencias en varios servidores en cuanto a actualización de firmware, actualización de sistema operativos, actualización de software, actualización de configuraciones de seguridad en servidores entre otros, se ha

identificado e instalado medidas para iniciar el proceso de endurecimiento en los servidores y red.

Al realizar los análisis de riesgos encontramos exposición de información o fuga de datos, generados a partir del uso de discos extraíbles o USB, usuarios autorizados que tienen privilegios dentro de una organización para ingresar a carpetas, es necesario identificar eventos, fallas en infraestructura, caídas de internet, canales mpls qué pueden afectar la operación normal de la empresa, fallas humanas y además es necesario como recomendación que el personal de la organización conozca el plan para salvaguardar en cualquier tipo de novedad el drp, logrando generar un ambiente de seguridad informática y cultural, ante el personal creando un sentido de responsabilidad y mejora.[37]

Identificadas las vulnerabilidades es necesario crear un plan donde se gestione riesgos de tipo informático a partir de peligros y vulnerabilidades con sus respectivas consecuencias, detallar el funcionamiento y operación dentro de la organización creando reglas en la herramienta de snort que reduzca y solucione en parte amenazas y vulnerabilidades con el fin de mitigar en lo posible riesgos informáticos, con el fin de reducir en gran parte las falencias encontradas.

Valoración Cuantitativa de Activos

ELEMENTO	TIPO	RIESGO	VULNERABILIDAD
Servidores	Hardware	Permisos a carpetas de usuarios no autorizados, firmware desactualizado, fallas por obsolescencia tecnológica.	Revisar permisos de personal con respecto al cargo, servidores vulnerables, políticas obsoletas
Equipos de Personal	Hardware y Software	Actualizaciones de drivers no controladas, fuga de información	Controladores desactualizados, revisión constante de permisos en consola de antivirus y directorio activo sobre permisos de acceso a USB y páginas web
Aplicaciones internas	Datos	Perdida de información, ataques externos e internos	Servidores sin actualizaciones, cifrado obsoleto, puertos abiertos

37 CARDENAS RODRIGUEZ, Diego Alejandro. Diseño de un sistema de seguridad para la protección y prevención de intrusos ids/ips en la red empresarial de puntoqom minimizando el riesgo y asegurando los activos de información de la organización. repository.unad.edu.co [página web]. (2022). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://repository.unad.edu.co/bitstream/handle/10596/51475/dacardenasrod.pdf?sequence=1&isAllowed=y>.

Swicht´s	Comunicaciones	Obsolescencia tecnológica, actualización de firmware	Contraseñas débiles, sin actualizaciones, Backus y políticas obsoletas
Portales WEB	Datos	Ataques externos e internos	Servidores sin actualizaciones, cifrado obsoleto, puertos abiertos, peligro potencial de acceso no autorizado.
Canales mpls	Datos	Caída de servicio	Sin acceso a internet o sitios de servidores principales.

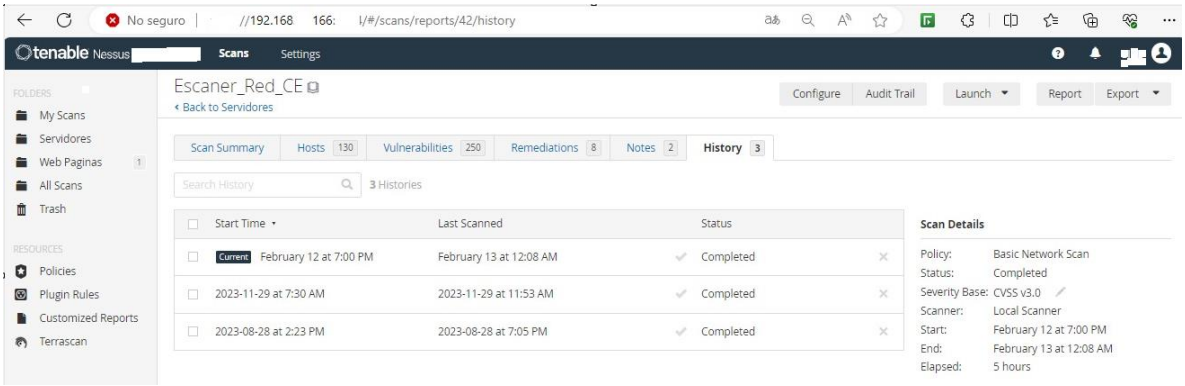
Fuente: propia

7.7 REPORTE DE NESSUS – FEBRERO 2024

En respuesta a los hallazgos y recomendaciones derivados del análisis inicial realizado en 2022, se ha llevado a cabo una actualización integral de herramientas de vulnerabilidades en la infraestructura de la empresa. El objetivo primordial de esta actualización es fortalecer la seguridad de la red y garantizar un monitoreo efectivo frente a posibles amenazas y ataques cibernéticos, tanto en nuestras páginas web y redes.

Para mantener un panorama actualizado de las vulnerabilidades presentes en la red de la empresa, se implementó un escaneo exhaustivo utilizando una combinación de herramientas avanzadas de análisis de seguridad. En este sentido, se ha incorporado un nuevo scanner de red de última generación, junto con las diferentes páginas web propias de la empresa, adjunto encontraran evidencias del reporte generado y envió posteriores áreas de la empresa.

Figura 13 Reporte Nessus 1.



Fuente: propia

En la imagen anterior se evidencia generación de escaneo a red empresarial y servidores.

Figura 14 Reportes Nessus 2.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Count
MEDIUM	51192	SSL Certificate Cannot Be Trusted	74
MEDIUM	57582	SSL Self-Signed Certificate	68
MEDIUM	157288	TLS Version 1.1 Protocol Deprecated	40
MEDIUM	104743	TLS Version 1.0 Protocol Detection	25
MEDIUM	45411	SSL Certificate with Wrong Hostname	24
HIGH	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	18
HIGH	35291	SSL Certificate Signed Using Weak Hashing Algorithm	16
HIGH	63155	Microsoft Windows Unquoted Service Path Enumeration	16
MEDIUM	57608	SMB Signing not required	14
MEDIUM	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	14
LOW	26194	Web Server Transmits Cleartext Credentials	6

Fuente: propia

El informe anterior muestra una estructura ordenada que enumera cada vulnerabilidad por tipo de ataque, lo cual facilita la priorización de las mismas. Sin embargo, se solicita una revisión para actualizar o eliminar las vulnerabilidades identificadas, con el fin de garantizar la eficacia de la solución.

Figura 15 Reportes Nessus3

Severity (CVSS v3.0)	All	Windows	MacOS	Linux	Other
CRITICAL	4	3	0	0	1
HIGH	39	24	0	7	8
MEDIUM	20	18	0	2	0
LOW	6	0	0	6	0
INFO	41	37	1	1	2
Totals	110	82	1	16	11

Fuente: propia

En la evidencia anterior se describe una tabla de detecciones de sistemas operativos por familia proporcionando al equipo de seguridad una vista resumida del riesgo basado en el sistema operativo y su vulnerabilidad con la severidad indicada.

Figura 16 Reportes Nessus4.

Top 10 Critical Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent critical vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	9.8	Yes	2023/01/29	4
179364	PHP 8.0.x < 8.0.30 Multiple Vulnerabilities	CGI abuses	9.8	Yes	2023/08/03	4
169630	PHP 8.0.x < 8.0.27	CGI abuses	9.1	-	2023/01/05	4
170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	9.0	-	2022/07/12	4
20007	SSL Version 2 and 3 Protocol Detection	Service detection	9.8	-	2005/10/12	1
55786	Oracle Database Unsupported Version Detection	Databases	10.0*	-	2011/08/09	1

Fuente: propia

La última imagen nos muestra las 10 principales vulnerabilidades agrupadas según su gravedad, según un análisis de amenazas exhaustivo, se consideran las más críticas para mitigar, sobre el método CVSS v3.0.

7.8 RESULTADOS DEL ESCANEO

El análisis revela una serie de vulnerabilidades y áreas de mejora en la seguridad de la red. Se han identificado vulnerabilidades de diversa gravedad, desde aquellas de bajo riesgo hasta aquellas que representan una amenaza inminente para la integridad y confidencialidad de los datos. Los resultados detallados se presentan a continuación:

Vulnerabilidades de Bajo Nivel: Se han identificado únicamente 6 vulnerabilidades de bajo nivel, las cuales han sido categorizadas como riesgos menores para la seguridad de la red.

Vulnerabilidades de Medio: Se han detectado un total de 20 vulnerabilidades de nivel medio.

Vulnerabilidades de Nivel Alto y criticas: Se han detectado un total de 39 vulnerabilidades de nivel alto y 4 vulnerabilidades de nivel críticox. Estas vulnerabilidades abarcan una variedad de áreas, desde falencias en la actualización de firmware y sistemas operativos hasta configuraciones inseguras en servidores y dispositivos de red.

7.9 ACCIONES CORRECTIVAS Y PLAN DE GESTIÓN DE RIESGOS

Basándonos en los hallazgos del análisis de vulnerabilidades, se ha diseñado un plan integral de gestión de riesgos informáticos. Este plan incluye medidas correctivas específicas para abordar las vulnerabilidades identificadas, así como la implementación de políticas y procedimientos para fortalecer la seguridad de la red a largo plazo.

Entre las acciones correctivas se incluyen:

Actualización de firmware, sistemas operativos y software en todos los dispositivos de la red.
Implementación de configuraciones de seguridad robustas en servidores y dispositivos de red.
Reforzamiento de medidas de seguridad física y lógica para prevenir la fuga de datos y ataques internos.
Capacitación continua del personal en prácticas de seguridad informática y concienciación sobre la importancia de la seguridad de la información.

8 DESARROLLO DEL OBJETIVO 3

8.1 PROPONER LA IMPLEMENTACIÓN Y CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD EN EL IDS E IPS CON EL FIN DE ASEGURAR LA EFICACIA Y AUMENTAR EL FUNCIONAMIENTO CORRECTO DE LA PLATAFORMA ACTUAL, BLOQUEANDO INTENTOS DE ATAQUES, VULNERABILIDADES Y AMENAZAS.

Todo sistema de detección de intrusos comprende una herramienta de seguridad que permite observar, analizar, detectar y bloquear todo tipo de tráfico no autorizado, esta función se basa en una base de datos de firmas de ataques que compara el tráfico y determina si debe estar bloqueado o no, categorizándolos según el tipo generar alertas ante tráfico anómalo, esta arquitectura de la solución se basa en la norma ISO 27001, la cual recomienda planificar, implementar, medir y mejorar por medio de la monitorización del tráfico, se instalará el servidor en sistema virtual vmware y sobre la red WAN de servidores 192.168.x.0/24, el servidor se configurará con dos interfaces virtuales red Lan e interfaz de red de servidores WAN.

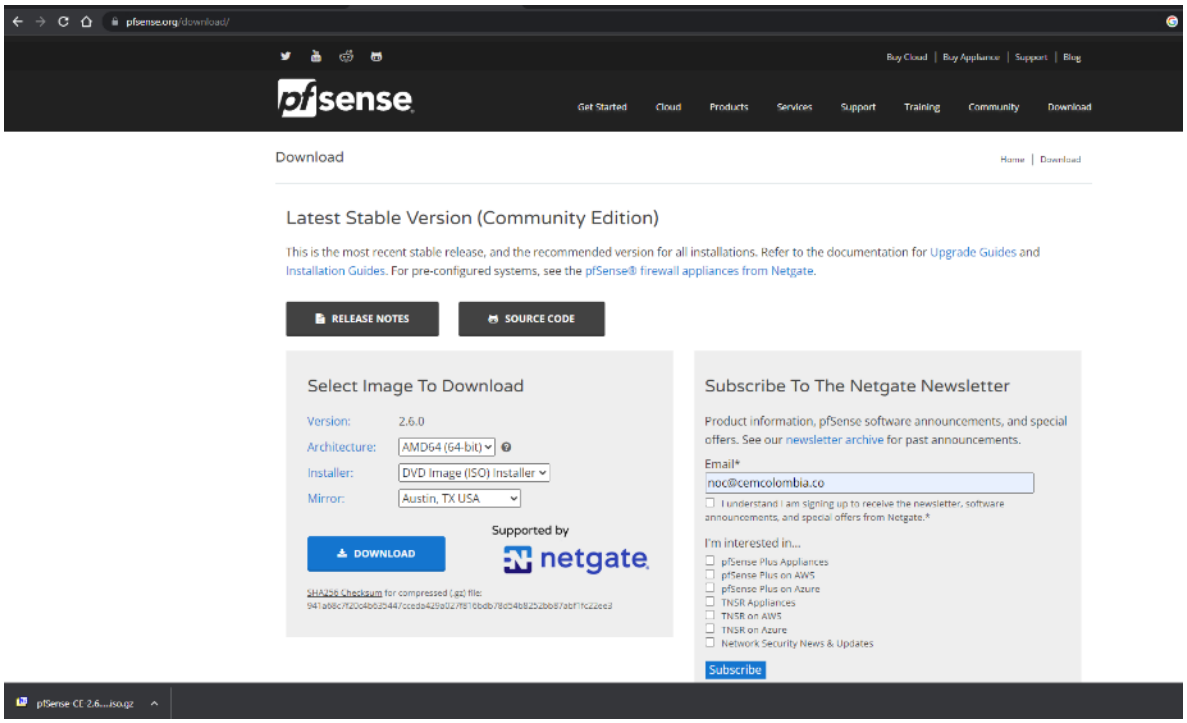
El monitoreo constante y oportuno de los sistemas de seguridad, utilizando las herramientas actuales son pocas y se necesita definir objetivos claros para el monitoreo como la detección de posibles intrusos o identificación de patrones de tráfico sospechosos, mediante los escáneres establecidos en reportes se encuentran patrones y permiten iniciar con una parametrización a evaluar que no afecte el rendimiento del sistema de seguridad, sino que refuerce el mismo.

Esta configuración debe evitar reporte de falsos positivos y para garantizar una respuesta oportuna y efectiva, contemplando simulación de ataques para evaluar el rendimiento de los sistemas de seguridad y de identificar posibles debilidades en la red y procedimientos de respuesta.

Reconociendo las características y basado en su alta efectividad, como herramienta y con documentación de referencia en soporte y gestión además de interfaz gráfica se elige implementar (SNORT), como medio de prevención y detección.

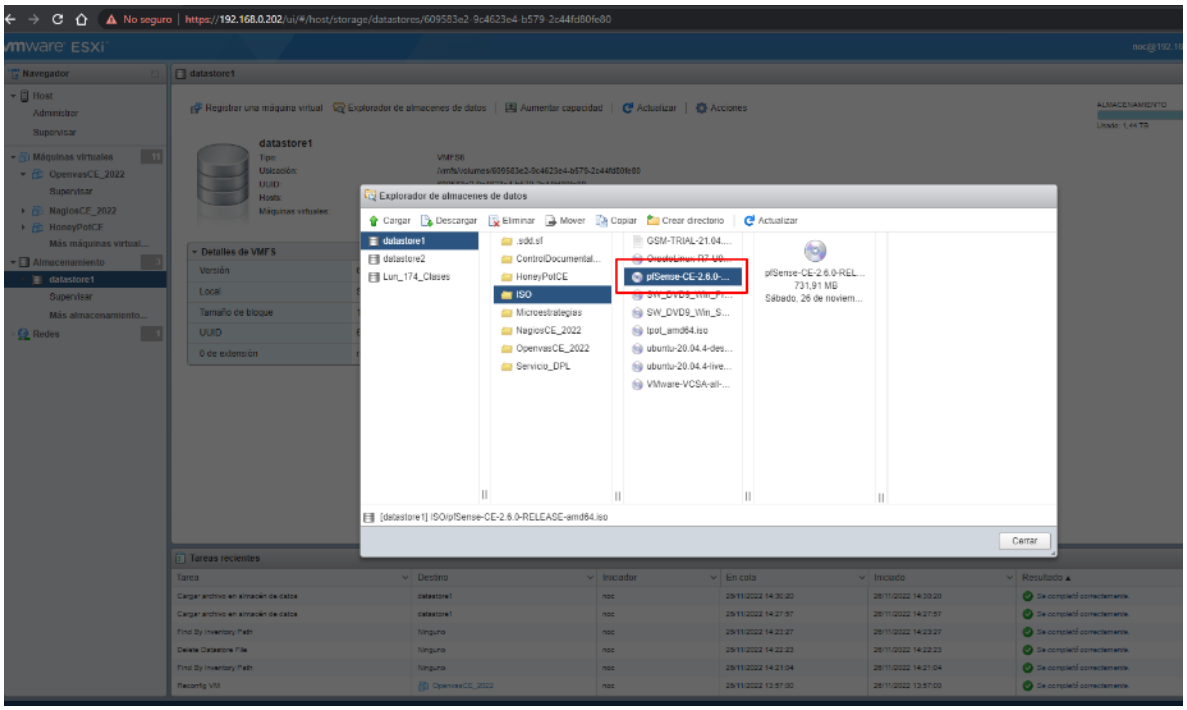
Iniciando el proceso de recopilación de información para su respectiva instalación e implementación con recursos en una máquina virtual en servidor one premise de la empresa.

Figura 17 Descarga sistema operativo en Vmware



Fuente: propia

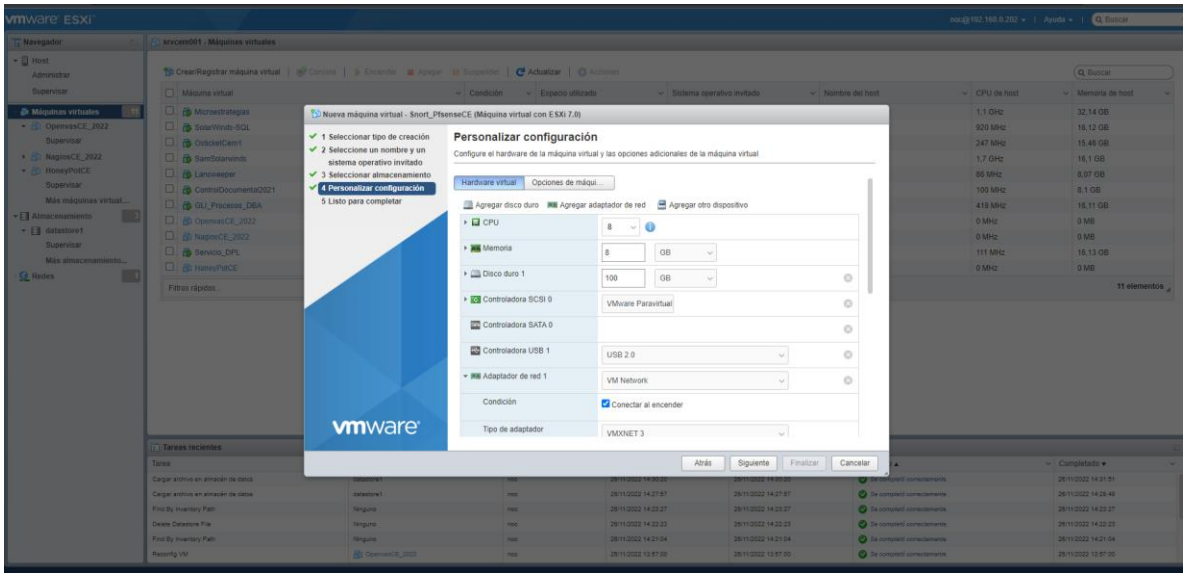
Descarga desde página web de pfsense directamente para arquitectura de 64 bits.
Figura 18 Carga de archivo iso en Vmware.



Fuente: propia

Adjunto repositorio de vmware en servidor carpeta iso imagen de pfsense.

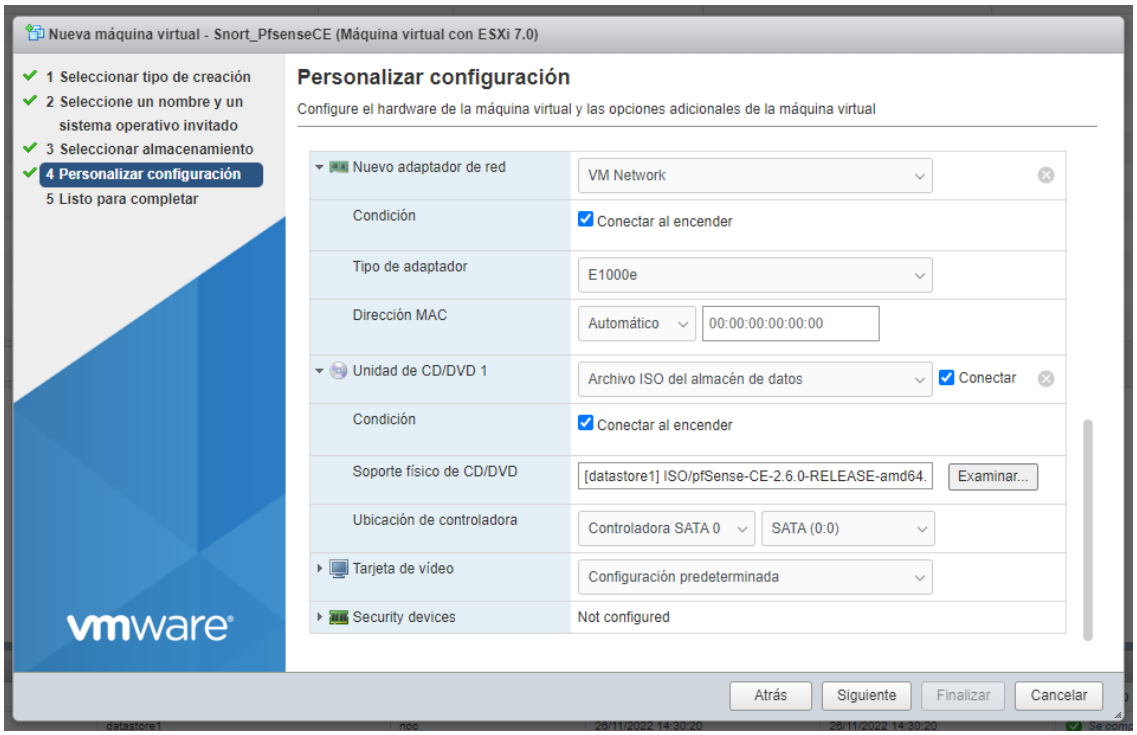
Figura 19 Creación de máquina virtual en Vmware.



Fuente: propia

Inicio configuración de parámetros de cpu 8 , memoria mínimo 8 gigas, espacio de disco duro 100 gb y agrego tarjeta de red para configurar interfases físicas WAN y lan.

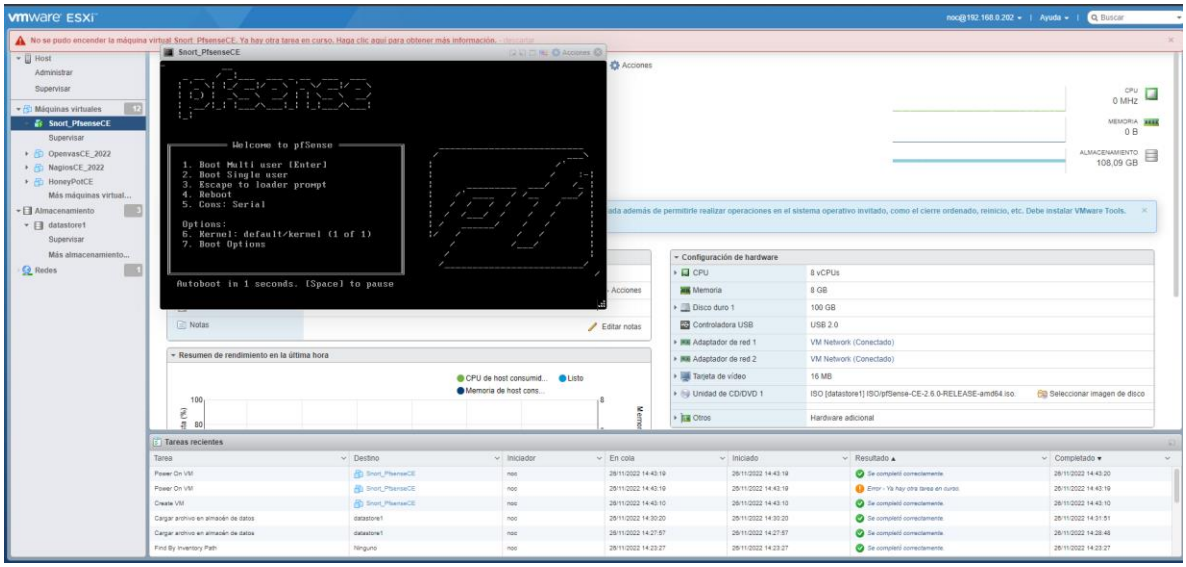
Figura 20 Creación y puesta en marcha de VM



Fuente: propia

Iniciamos la puesta en marcha del proceso de instalación en servidor vmware

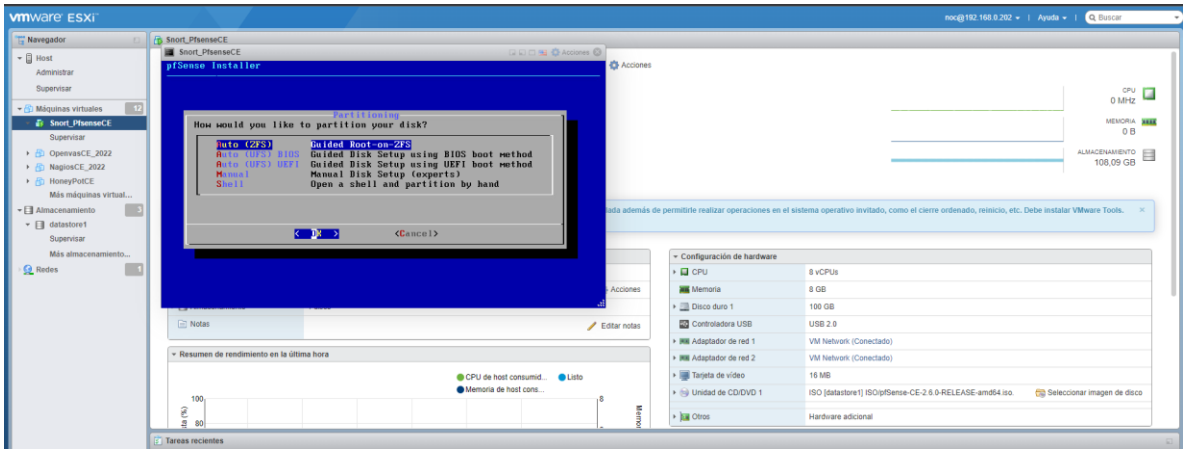
Figura 21 Inicio de instalación VM.



Fuente: propia

El proceso de instalación inicia automáticamente la instalación en pocos pasos.

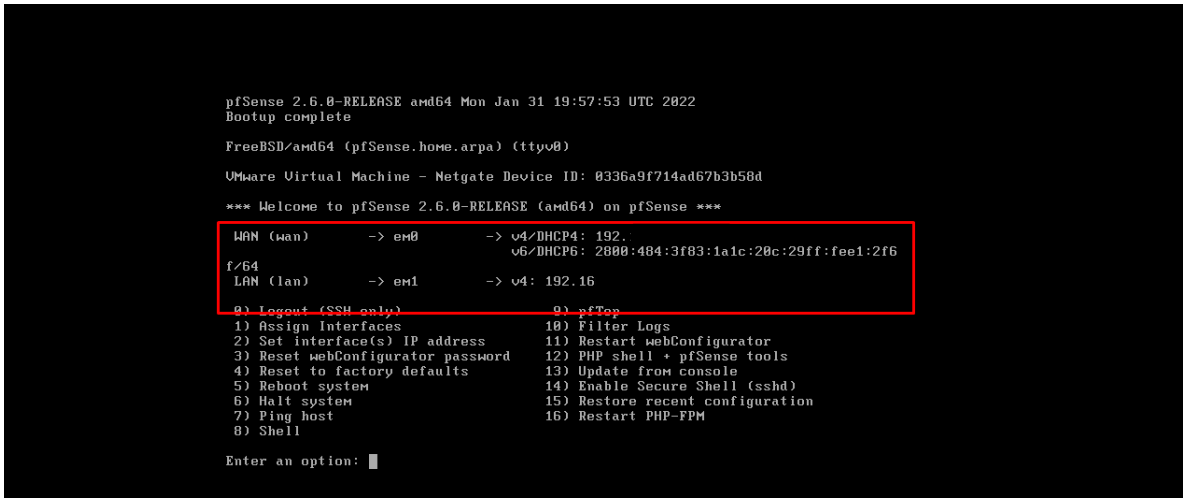
Figura 22 Configuración de interfase y creación de particiones en DD virtual



Fuente: propia

Elegimos configuración de particiones automáticamente cifrada ZFS y proseguimos instalación de sistema operativo en máquina virtual al reiniciar es necesario remover medio de instalación iso del sistema.

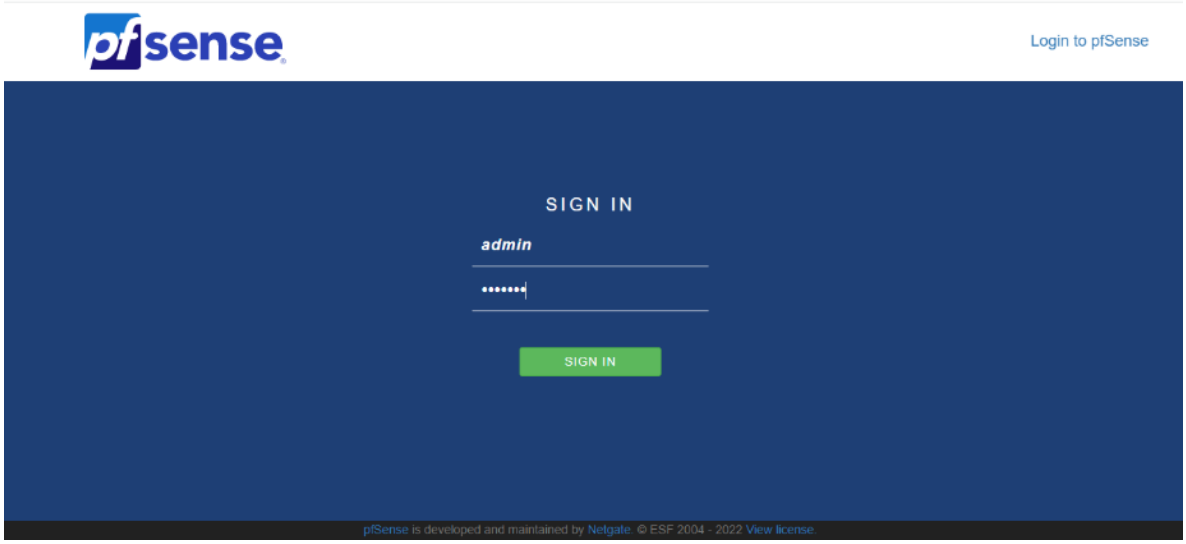
Figura 23 Terminación proceso de Instalación PfSense



Fuente: propia

Al reiniciar máquina virtual, verificamos la asignación correcta de ip tanto para la WAN como la red interna LAN, en este apartado realizamos tareas de admiración y configuración directamente sobre el sistema operativo pfsense.[38]

Figura 24 Ingreso a Consola Web Inicial

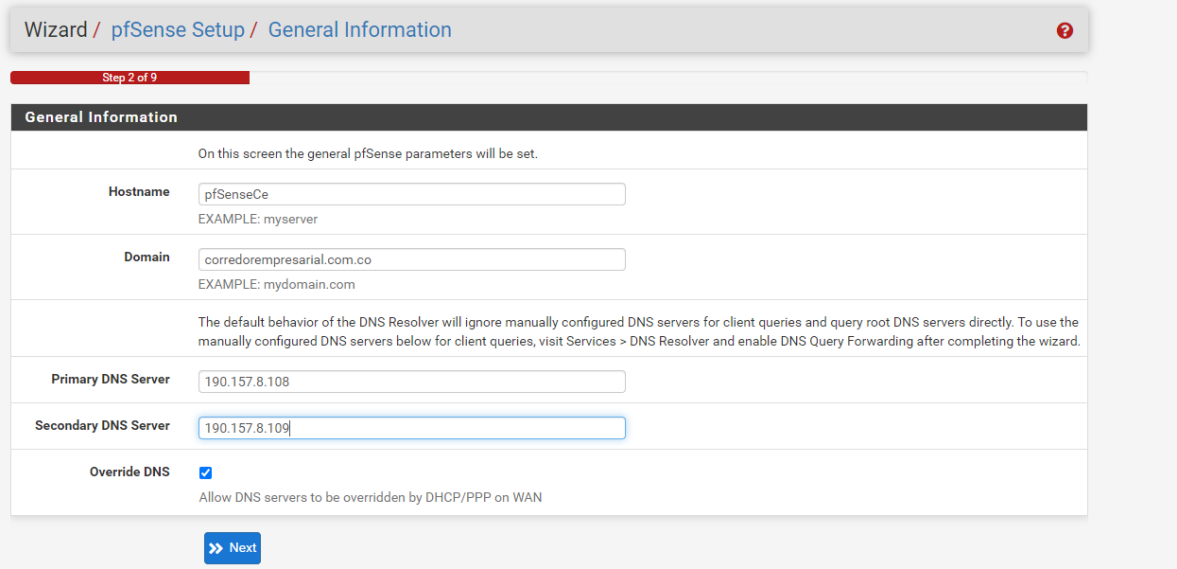


Fuente: propia

38 De Luz, S. (2022, 22 de mayo). Configura pfSense para proteger tu hogar o empresa con este firewall. www.redeszone.net. https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/

Una vez asignada WAN y LAN de la red en sistema inicial de Linux ingresamos por medio de consola web usuario y clave por defecto al sistema.

Figura 25 Acceso a consola de administración PfSense.



Fuente: propia

Configuración de nombre de dominio, dns del servidor y cambio de contraseña de administración.

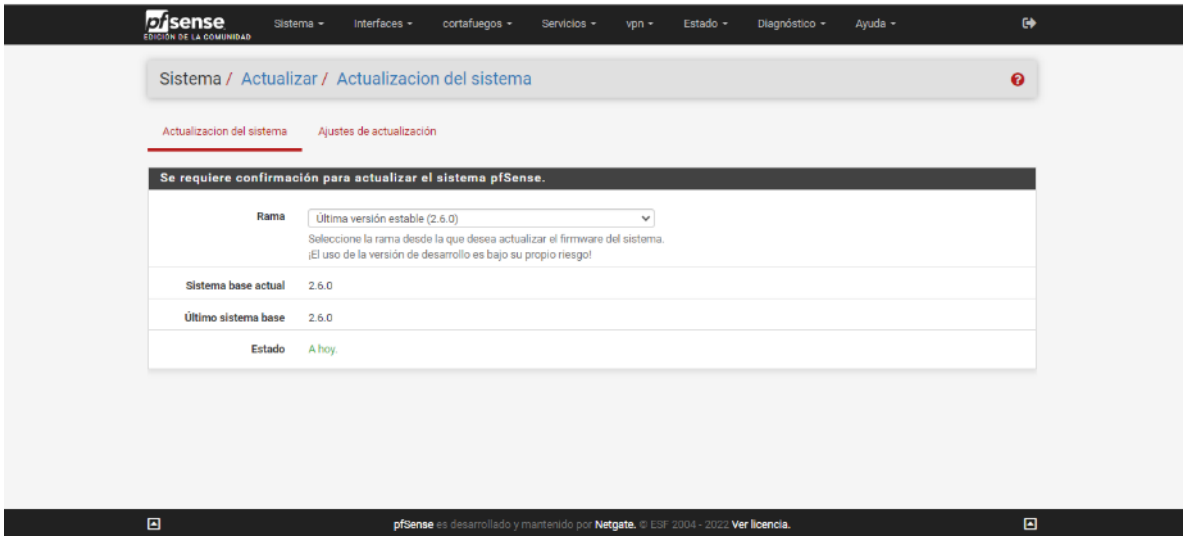
Figura 26 Acceso a Consola Web Pfsense

Fuente: propia

Reiniciamos máquina virtual con nueva ip definida en segmento de clase c de vlan de servidores y verificamos acceso a consola web de sistema operativo pfsense con

nueva clave y configuración de nombre en dominio de la empresa, cabe aclarar por seguridad.

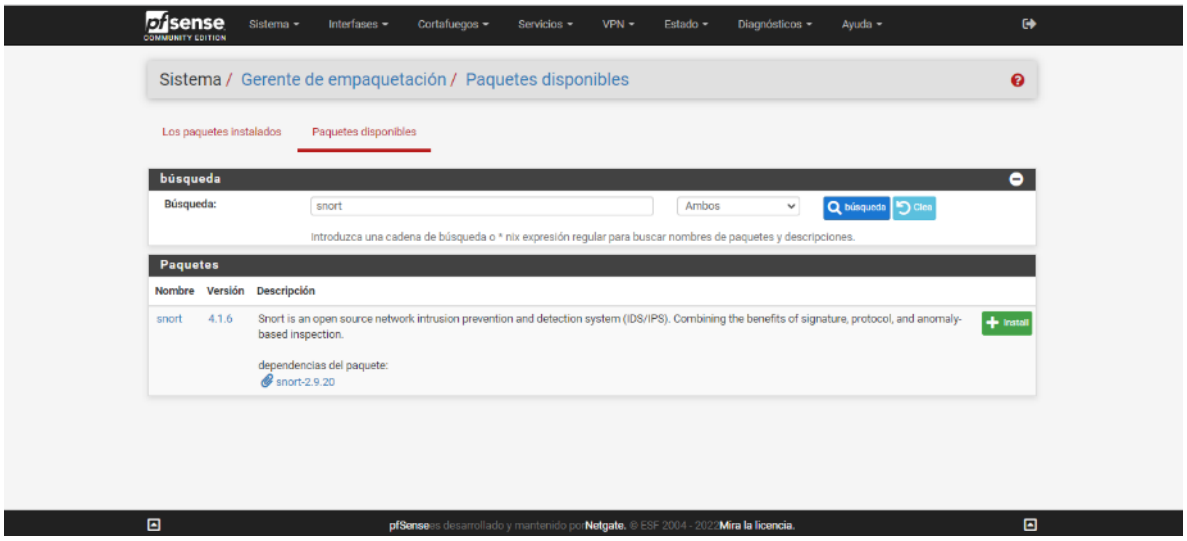
Figura 27 Verificación actualización SO.



Fuente: propia

Verificamos actualizaciones del sistema paso a seguir instalación de recurso de snort.

Figura 28 Instalación de paquete Snort.

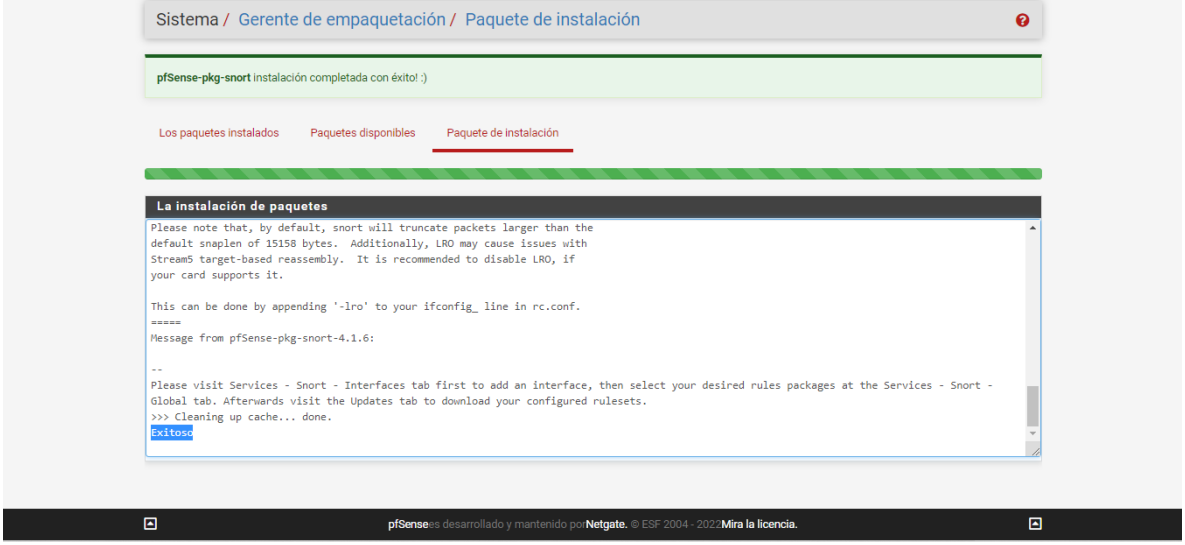


Fuente: propia

Verificando los pasos anteriores instalaremos el paquete snort el cual puede ser descargado desde la consola web del sistema pfsense. [39]

Una vez instalado el paquete la información de sus paquetes y pasos son los siguientes:

Figura 29 Instalación exitosa Snort

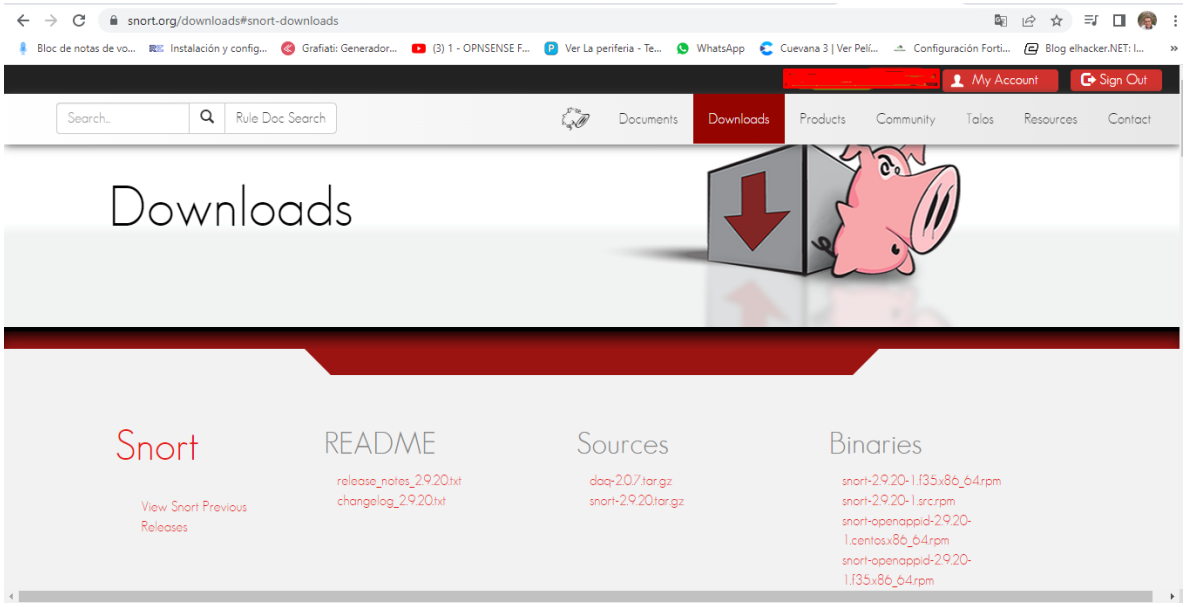


Fuente: propia

Esta es la verificación que el proceso de instalación del paquete fue exitoso a continuación es necesario la configuración inicial del ids/ips snort, pero antes es necesario seguir unos pasos en la página web de snort.

Figura 30 Acceso a Snort.org

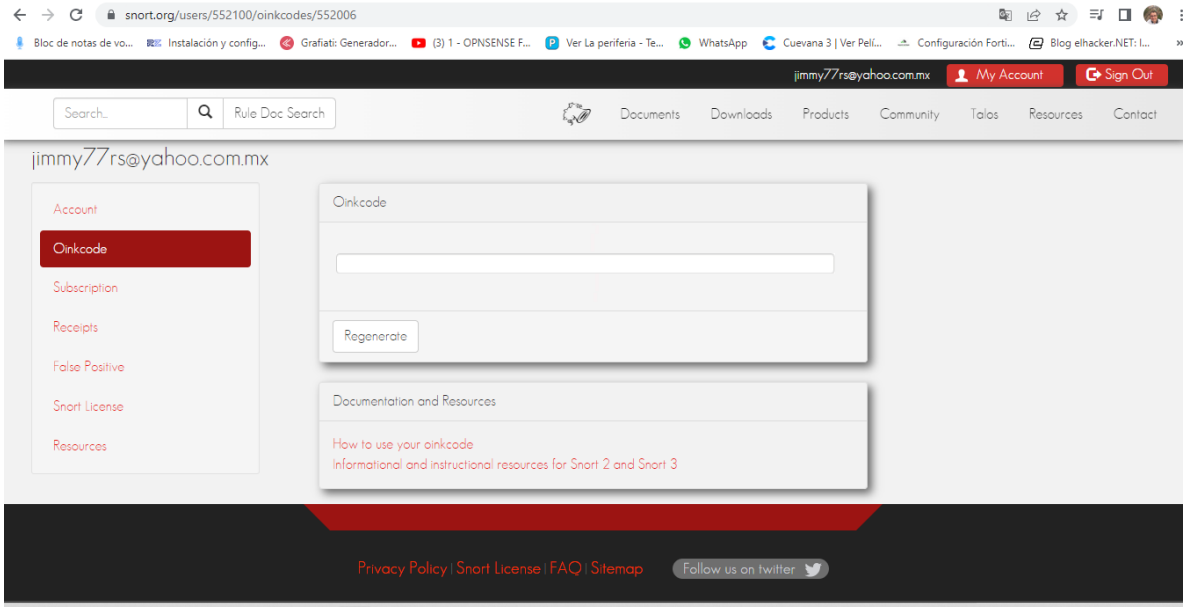
39 Pentester77. (2021, 24 de septiembre). PfSense 2.5 + SNORT (sistema de detección de intrusos) [Video]. www.youtube.com. https://www.youtube.com/watch?v=gvpwuk9ysCw



Fuente: propia

Es necesario crear una cuenta para descargar reglas y algunas configuraciones básicas del sistema ids e ips de snort para lo cual se tiene una cuenta del dominio para descargar este tipo de actualizaciones.

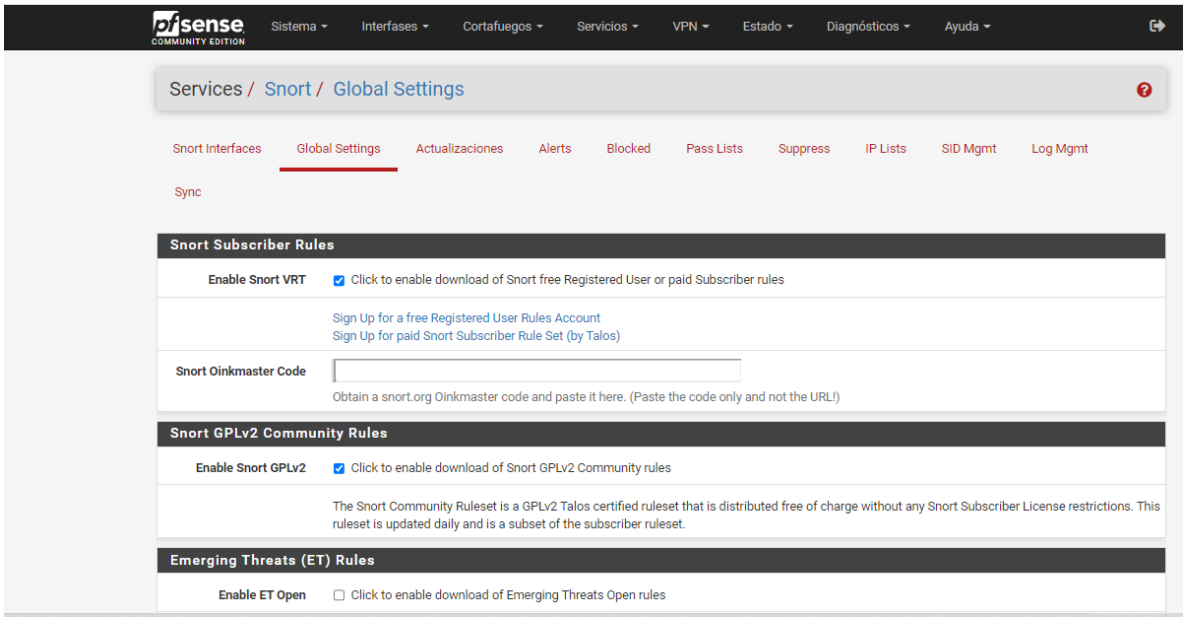
Figura 31 Descarga de código OinkCode



Fuente: propia

Luego de ingresar es necesario descargar el código oinkcode de la página web de snort directamente este código permite descargar actualizaciones y reglas.

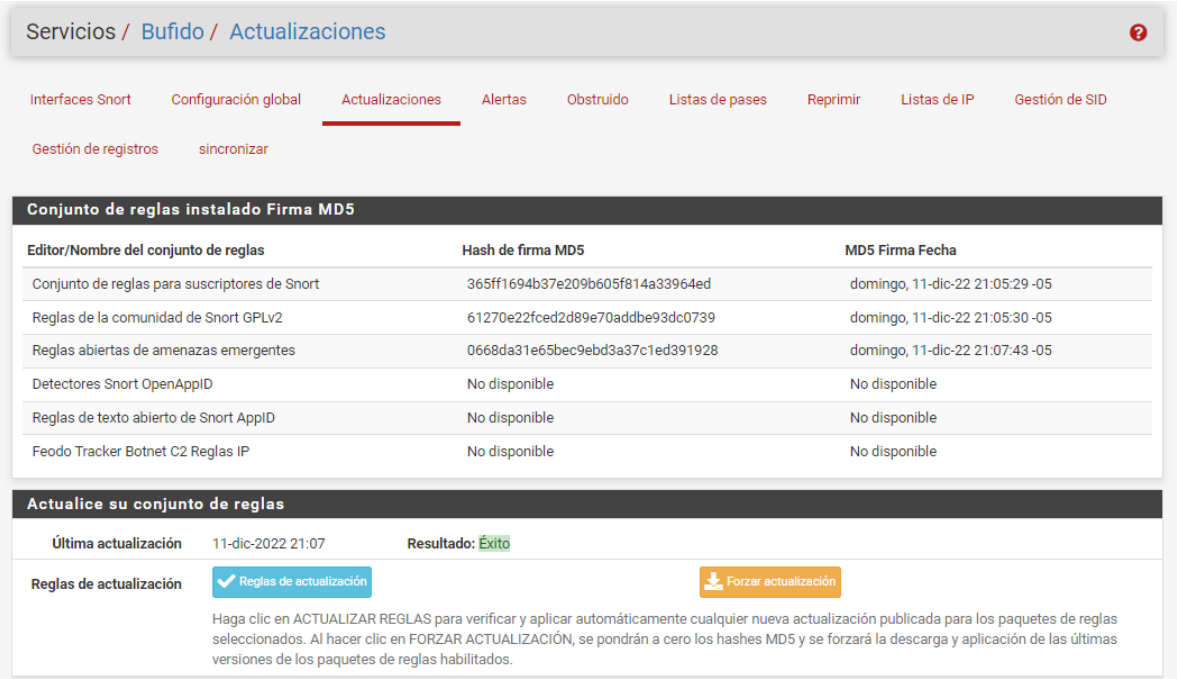
Figura 32 Activación VRT Snort



Fuente: propia

En este paso agregamos el código oinkcode y activamos VRT en la configuración inicial del sistema snort dentro de la consola web de pfsense, para loguearse como usuario libre por ahora, además activamos en el menú GPLV2 para descargar reglas libres de la comunidad, activamos reglas de amenazas emergentes (ET) además actualizaciones de reglas cada 12 horas y desde las 4 am.

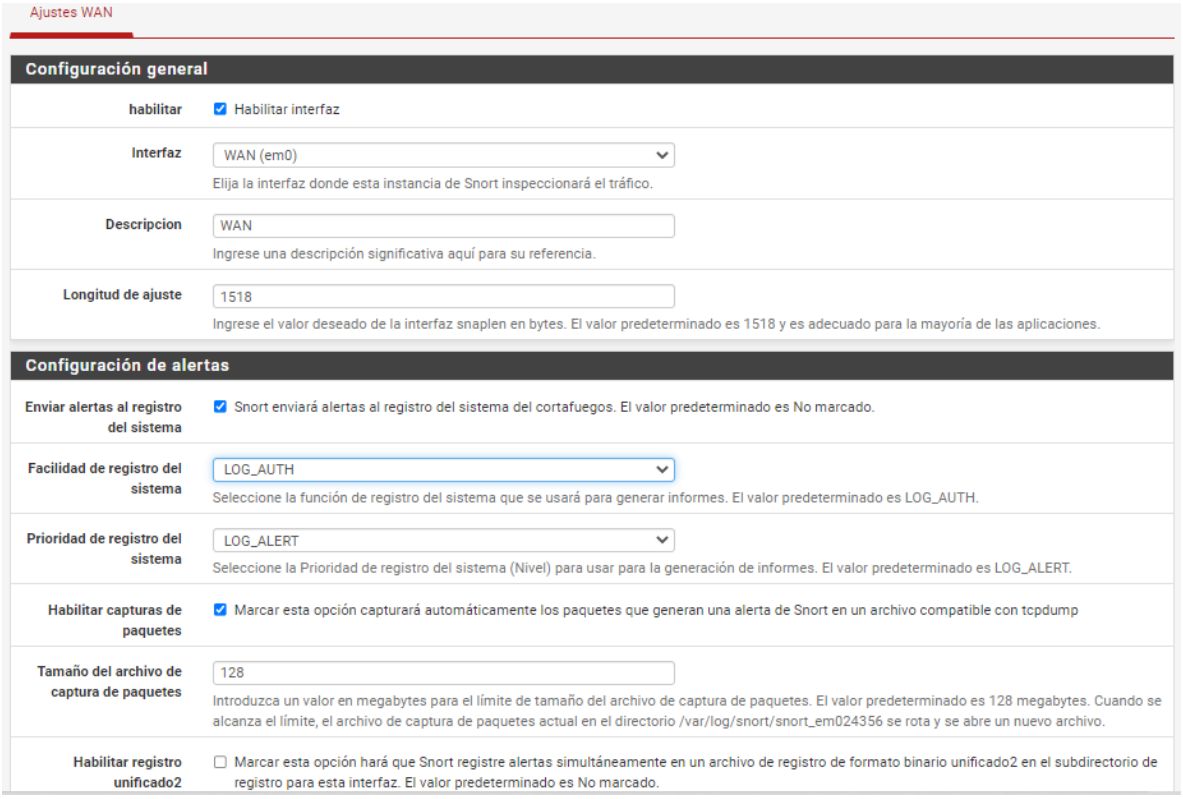
Figura 33 Actualización de Snort.



Fuente: propia

Iniciamos actualización y nos muestra al finalizar un hash la correcta descarga de reglas de la comunidad, GPL2 y amenazas emergentes que se revisa de manera periódica para afinar implementar verificar reglas y configuraciones instaladas.

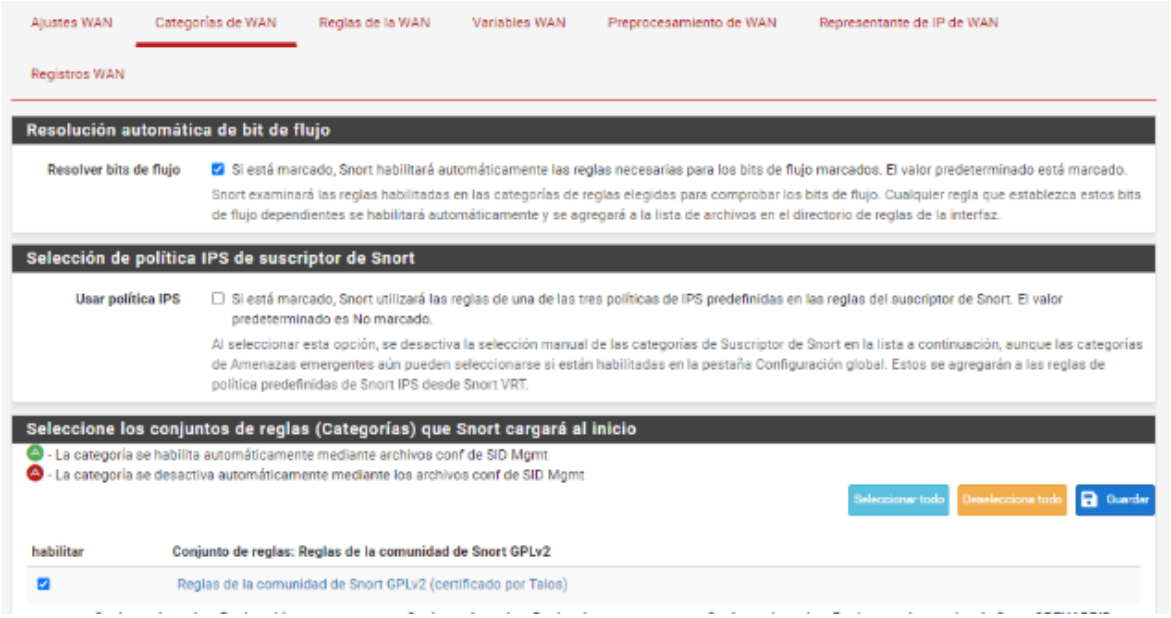
Figura 34 Activación WAN Snort.



Fuente: propia

Activamos interfase WAN lógicamente debido a que los ataques en su mayoría son externos, además activamos alertas captura de paquetes para lectura de tcpdump para analizar tráfico de origen a destino, se deja por defecto el algoritmo AC-BNFA que es una matriz de verificación de consulta de estado por medio de verificación de patrones, control de rendimiento del sistema.

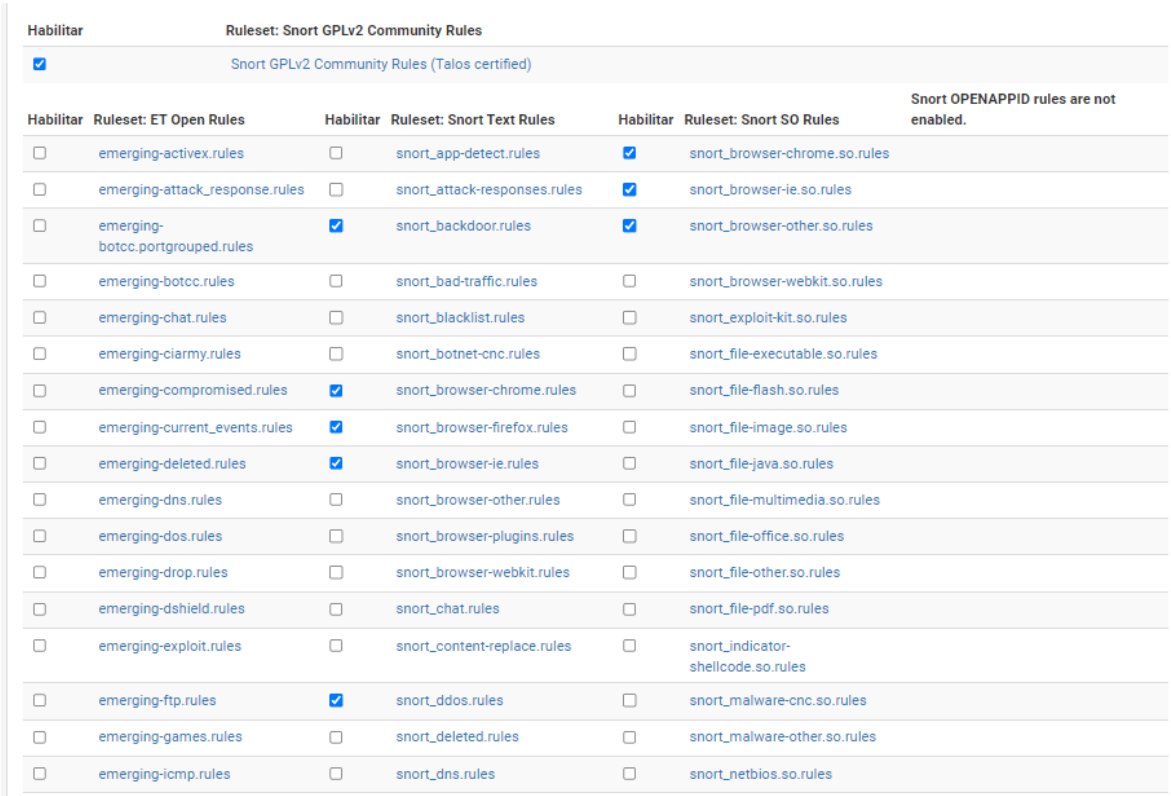
Figura 35 Activación Categorías WAN.



Fuente: propia

Verificamos categorías básicas de reglas por defecto está marcado los bits de flujo marcados, en la parte del menú se activan reglas de la comunidad, para iniciar este primer paso es necesario realizar un análisis granular sobre que necesitamos verificar, se consultó con administrador de red, grupo de Ti para activar algunas reglas esenciales en la red sin cargar el sistema en general y verificar el respectivo impacto en el rendimiento.

Figura 36 Activación de reglas básicas Snort



Habilitar	Ruleset: Snort GPLv2 Community Rules
☑	Snort GPLv2 Community Rules (Talos certified)

Habilitar	Ruleset: ET Open Rules	Habilitar	Ruleset: Snort Text Rules	Habilitar	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
☐	emerging-activex.rules	☐	snort_app-detect.rules	☑	snort_browser-chrome.so.rules	
☐	emerging-attack_response.rules	☐	snort_attack-responses.rules	☑	snort_browser-ie.so.rules	
☐	emerging-botcc.portgrouped.rules	☑	snort_backdoor.rules	☑	snort_browser-other.so.rules	
☐	emerging-botcc.rules	☐	snort_bad-traffic.rules	☐	snort_browser-webkit.so.rules	
☐	emerging-chat.rules	☐	snort_blacklist.rules	☐	snort_exploit-kit.so.rules	
☐	emerging-ciarmy.rules	☐	snort_botnet-cnc.rules	☐	snort_file-executable.so.rules	
☐	emerging-compromised.rules	☑	snort_browser-chrome.rules	☐	snort_file-flash.so.rules	
☐	emerging-current_events.rules	☑	snort_browser-firefox.rules	☐	snort_file-image.so.rules	
☐	emerging-deleted.rules	☑	snort_browser-ie.rules	☐	snort_file-java.so.rules	
☐	emerging-dns.rules	☐	snort_browser-other.rules	☐	snort_file-multimedia.so.rules	
☐	emerging-dos.rules	☐	snort_browser-plugins.rules	☐	snort_file-office.so.rules	
☐	emerging-drop.rules	☐	snort_browser-webkit.rules	☐	snort_file-other.so.rules	
☐	emerging-dshield.rules	☐	snort_chat.rules	☐	snort_file-pdf.so.rules	
☐	emerging-exploit.rules	☐	snort_content-replace.rules	☐	snort_indicator-shellcode.so.rules	
☐	emerging-ftp.rules	☑	snort_ddos.rules	☐	snort_malware-cnc.so.rules	
☐	emerging-games.rules	☐	snort_deleted.rules	☐	snort_malware-other.so.rules	
☐	emerging-icmp.rules	☐	snort_dns.rules	☐	snort_netbios.so.rules	

Fuente: propia

Una vez consultado y verificado se activa las siguientes reglas básicas, que se relacionan con distintos tipos de ciberataques que pueden prevenirse utilizando las capacidades de detección y prevención de intrusiones de Snort como primera medida, algunas son:

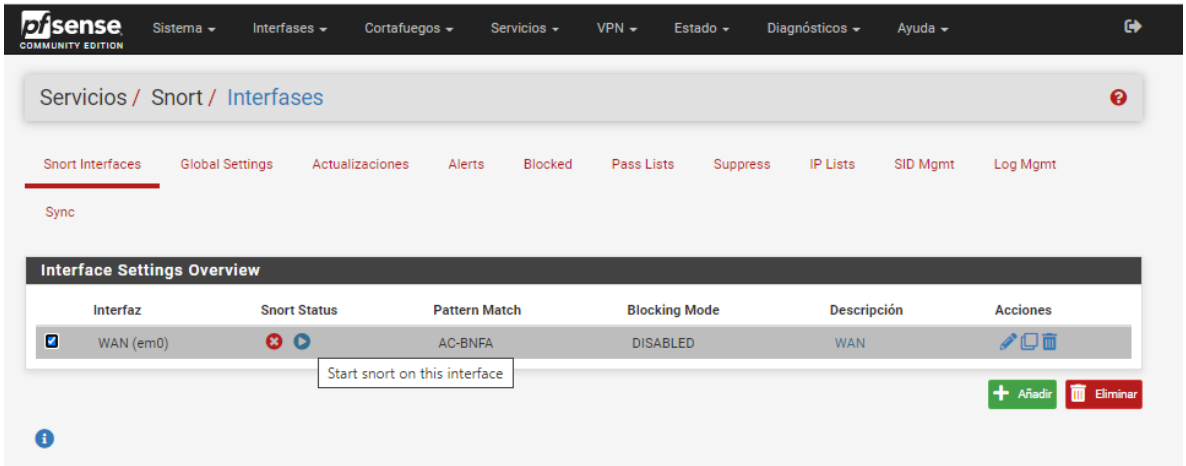
Tabla 9 Reglas Básicas Snort

Regla	Descripción
BACKDOOR RULES	Identifica y bloquea tráfico de puertas traseras, que son programas maliciosos que permiten a los atacantes acceder a un sistema en forma remota, al identificar el tráfico bloque el tráfico malicioso
BROWSER-CHROME RULES,	Diseñada para detectar y prevenir ataques dirigidos Chrome identifica y bloquear tráfico que explota vulnerabilidades en Chrome.
BROWSER-FIREFOX RULES,	Detecta actividades inusuales que afecten al navegador Mozilla Firefox, por medio de patrones de tráfico, comportamientos anómalos sobre ataques, explotaciones o compromisos al navegador.

BROWSER-IE RULES	Diseñada para detectar y prevenir actividades sospechosas sobre el navegador Internet Explorer (IE), identifica patrones de tráfico sobre ataques y explotación de vulnerabilidades sobre IE.
DDOS RULES	Detecta y controla ataques de tipo (DDoS), identificando patrones de tráfico sospechosos mitigando el impacto del ataque.
DOS RULES	Detecta e impide ataques de denegación de servicio que se originan desde una única fuente, por medio de patrones de tráfico bloquea tráfico malicioso.
EXPLOIT RULES	Detecta intentos de explotación de vulnerabilidades conocidas en sistemas, aplicaciones o protocolos, controla exploits para evitar de brechas desde pdf, Word, Excel o desde correo electrónico.
ICMP RULES	Evita ataques con la herramienta hping3, Activación de SHELLCODE RULES que es un tipo de exploit y detecta el tráfico sobre el protocolo de Mensajes de Control de Internet identificando patrones inusuales.
MYSQL RULES	Revisa el sistema de gestión de bases de datos sobre MySQL, Detectando y previniendo ataques
ORACLE RULES	Se enfoca en verificar el sistema de gestión de bases de datos, revisando el tráfico con intentos para explotar vulnerabilidades para bloquear el tráfico malicioso.

Fuente: propia

Figura 37 Inicio de Escaneo Snort

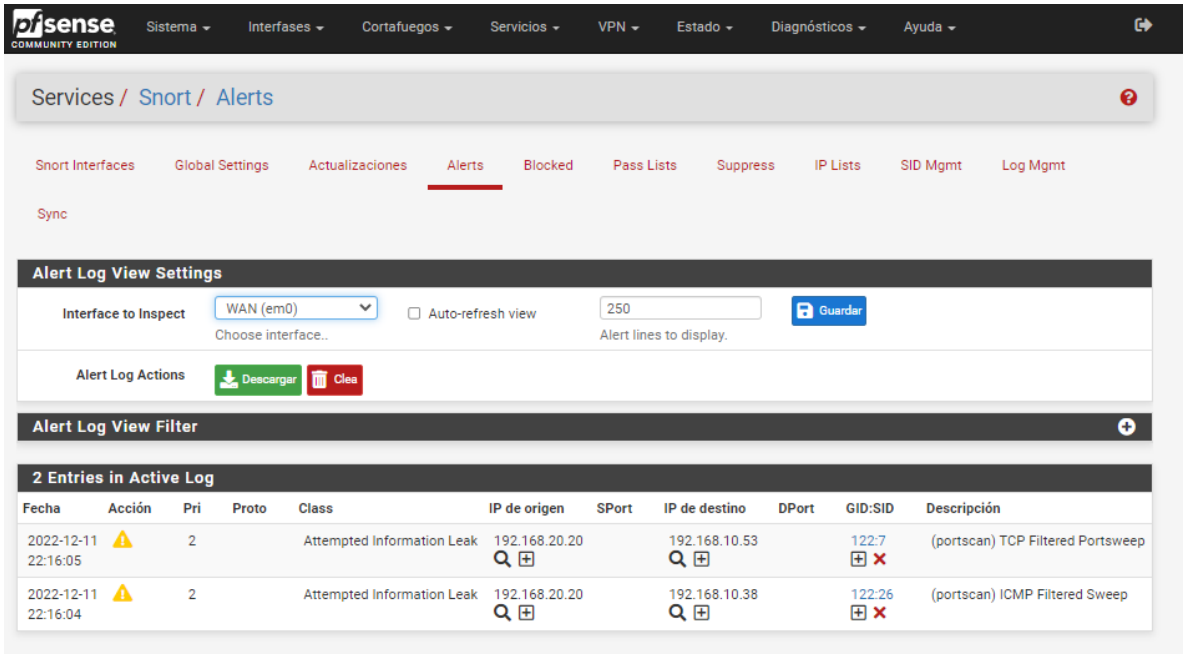


Fuente: propia

Al dar clic en icono azul se activa las reglas activas anteriormente en la interfase WAN, tener en cuenta que el preprocesador activa la revisión del SSH y detecta varios intentos de explotación de Secure Shell, se activa por defecto HTTP Inspect

que verifica y decodifica para detectar tráfico HTTP y anomalías de protocolo, activamos Portscan Detection que detecta escaneos de puertos.

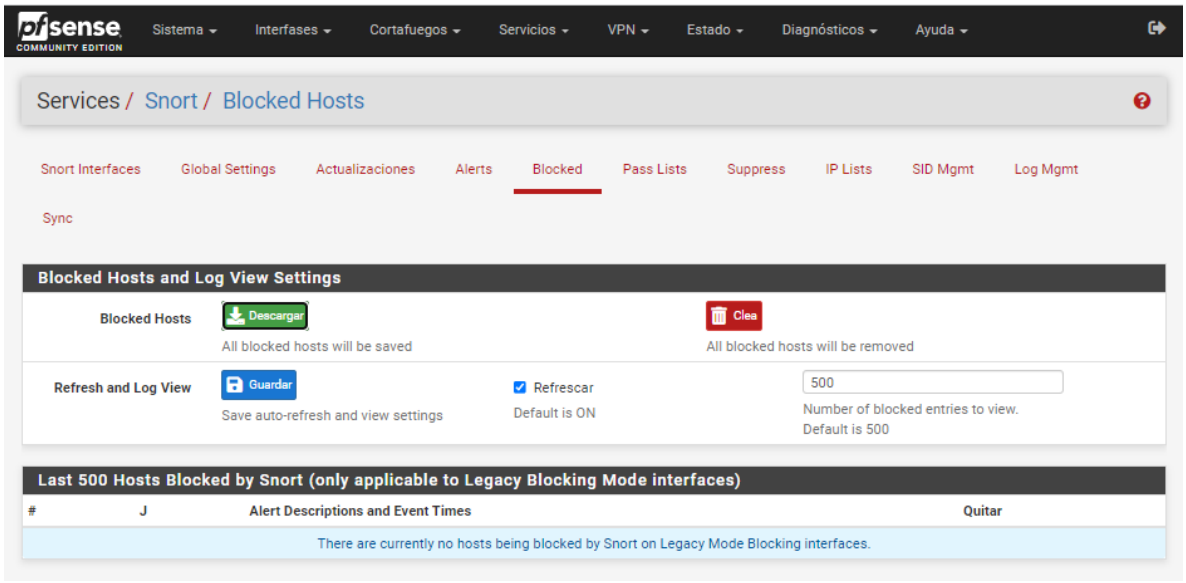
Figura 38 Detección de alertas Snort.



Fuente: propia

Inicia el proceso de revisión y trafico sospechoso en menú de alertas.

Figura 39 Bloqueo de Ips o Host.



Fuente: propia

Esta arquitectura llega a través de un cortafuegos fortigate, pasa por un switch a el nuevo servidor snort, nuestro y IDS/IPS verificar el tráfico y seguirá el proceso, este enfoque está basado en 4 etapas planear el cual tiene como objetivo analizar y diseñar reglas según las amenazas más frecuentes verificadas en el escaneo tanto el estor como del fortianalyzer, esto mejora la seguridad de la información tanto la organización como para los usuarios y evalúa las reglas generales.

Implementar como objetivo principal la instalación y configuración de un motor avanzado de amenazas Ids/Ips de tipo Snort, utilizando la plataforma virtual esxi 7.2 denominador como un hypervisor qué utiliza el hardware del sistema directamente, snort y de reglas por defecto se adquirió un oinkcode creando una cuenta para descargar reglas básicas de la comunidad.

Medir es el objetivo fundamental para realizar el análisis y monitoreo de todo el tráfico mediante el reporte de snort verificando los logs bloqueos.

Mejorar, es un objetivo para realizar pruebas al análisis del tráfico, sí tomaron acciones correctivas y preventivas de manera primordial desarrolladas con el grupo de TI y su respectivo administrador, para esta segunda fase es necesario analizar las reglas del reporte del tráfico malicioso de las diferentes herramientas de monitoreo, tener en cuenta que las reglas activadas son alertas básicas y las diferentes bibliotecas adicionales permiten trabajar algunos tipos de ataques básicos es necesario revisar de la implementación Y configuración por medio de una investigación.

9 DESARROLLO DEL OBJETIVO 4

9.1 ELABORAR MANUAL DE IMPLEMENTACIÓN IDS E IPS QUE SIRVA DE PUNTO DE REFERENCIA ANTE LA COMPAÑÍA, QUE SERVIRÁ PARA QUE LA ORGANIZACIÓN PROTEJA SUS REDES INTERNAS DE INCIDENTES DE SEGURIDAD Y FUGAS DE INFORMACIÓN EN TIEMPO REAL, DE MANERA EFICAZ ASEGURANDO LA EFICIENCIA, GARANTIZANDO ASÍ OPERACIONES SEGURAS.

Se realiza un manual, que presenta una guía para la implementación de IDS e IPS en la red interna de la compañía Corredor Empresarial, con la herramienta Snort.

Esta guía se dirige tanto a los usuarios finales como a los administradores de la empresa, con el objetivo de ofrecer una descripción detallada de los pasos necesarios como fue la implementación y como debe ser la gestión de este sistema de seguridad, este manual no es solo una guía para la implementación de Snort, sino que brinda información valiosa sobre la importancia de la seguridad informática en la empresa.

Además, se ha enfatizado la importancia de mantener actualizado y bien administrado el sistema de detección y prevención de intrusiones, ya que las amenazas evolucionan constantemente y los sistemas de seguridad deben estar preparados para hacer frente a ellas.[40]

Adjunto link de acceso a manual creado de la herramienta snort fácil de entender para el usuario final.

https://flipbookpdf.net/web/site/5b9febd54bd1810bb3ca281c73de417d62589dd1202304.pdf.html

[40] SNORT.ORG. Manual de usuario de Snort 3. (22, marzo, 2023). [Consultado el 14, abril, 2023]. Disponible en Internet: < http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>.

10 CONCLUSIONES

La implementación de Snort IDS/IPS ha reforzado considerablemente nuestra postura de seguridad en Corredor Empresarial.

Inicialmente se llevó a cabo una identificación de equipos de comunicación y servidores de la organización que presentaban posibles fallos de seguridad susceptibles de ser explotados por diversos vectores de ataque que proporcionó una visión clara y actualizada de la infraestructura de red, lo que permitió mitigar proactivamente posibles amenazas y fortalecer la capacidad de proteger los activos críticos de información. Esto no solo mejoro la seguridad, sino que también aporta a la capacidad para adaptarse a las situaciones adversas.

Asimismo, se realizó un análisis y monitoreo de tráfico que mejoro significativamente la gestión de riesgos permitiendo una comprensión profunda de las actividades de red de la empresa, que fortaleció la detección temprana de actividades sospechosas y la prevención de intrusiones no autorizadas que han reducido de manera significativa las amenazas cibernéticas. Esto ha generado una mayor confianza tanto en el equipo de TI como entre los stakeholders de la empresa.

No obstante, es importante reconocer que este proceso no estuvo exento de desafíos. La configuración inicial de los sistemas IPS/IDS requirió un esfuerzo considerable y una cuidadosa adaptación a las necesidades específicas de Corredor Empresarial. Además, se identificaron falsos positivos que, aunque disminuyeron con el tiempo, requirieron una atención constante por parte del equipo de seguridad. Además, con base en la información recopilada se crearon políticas de seguridad a la medida de Corredor Empresarial enfocadas en sus activos y trafico especifico, mejorando y aumentando el nivel de protección de la plataforma. A través del análisis, se verificaron los reportes de tráfico malicioso generados por Snort. Se registraron accesos a los sistemas y aplicaciones críticas, lo cual llevó a la revisión de los protocolos de acceso para el personal de la compañía. Además, se establecieron políticas claras para el manejo de contraseñas y se mejoró el proceso de autenticación, garantizando que solo los usuarios autorizados puedan acceder a los sistemas.

Por último, la creación de un manual de uso eficiente y compacto para la herramienta Snort y la implementación de programas de formación para nuestro personal ha elevado la cultura de seguridad de la información. Al empoderar a los empleados para que sean parte activa de la estrategia de seguridad, transformado la seguridad de la información en una responsabilidad compartida, lo que aumenta aún más la resiliencia y crea una inversión estratégica que ha aportado valor en todas las áreas para detectar y mitigar amenazas en la red, proporcionando una capa adicional de seguridad que resulta fundamental en el entorno actual de ciberamenazas.

11 RECOMENDACIONES

Al realizar un análisis del trabajo realizado se hace relevante describir aspectos que no se agregaron al trabajo entre estas recomendaciones al evaluar los resultados para medir su efectividad, se han encontrado el establecer un plan de contingencia claro y preciso en caso de que ocurra un incidente de seguridad, el cual debe incluir procedimientos claros a seguir en caso de una violación de seguridad, así como los contactos clave a los que se debe notificar a nivel técnico y empresarial.

Además es necesario establecer un equipo dedicado a la gestión y mitigación de incidentes de seguridad, con herramientas efectivas y preventivas como el factor de doble autenticación en los sistemas actuales creados a medida de la compañia, sistemas dlp, que permita mejorar el proceso de protección y disponibilidad de datos

Contemplar realizar simulaciones periódicas para evaluar la efectividad de la herramienta y hacer mejoras necesarias y de actualización a la herramienta snort, que reforzaran el sistema de seguridad.

Además se necesita establecer políticas claras de acceso a la red interna y asegurarse de que sean cumplidas permanentemente y reforzar sistemas de autenticación fuerte para garantizar que solo el personal autorizado tenga acceso a la red.

Abordando el tercer objetivo se hace necesario capacitar al personal, contra riesgos de seguridad informática para evitar por negligencia o falta de conocimiento, relacionados con la seguridad informática, amenazas y técnicas utilizadas por los atacantes.

Por último el documento creado debe ser retroalimentado y discutido para verificar los diversos métodos para implementar un sistema de prevención de ataques IPS e IDS en Corredor Empresarial, incluido el uso de recursos tecnológicos para analizar, advertir, descubrir y bloquear ataques cibernéticos.

Crear seguimiento a casos para afinar reglar respectivas actualizándolas constantemente, basados en la norma ISO 27001:2022, es necesario mejorar la calidad e implementación de este proyecto.

Realizar pruebas periódicas del sistema y componentes que evalúen la efectividad y detectar posibles vulnerabilidades, generar auditorías externas que deben ser realizadas por expertos en seguridad informática.

12 BIBLIOGRAFÍA

ALMANZA, Andrés. XIX Encuesta Nacional de Seguridad Informática: Evolución del perfil del profesional de seguridad digital. sistemas.acis.org.co [Sitio web]. (5, julio, 2022). [Consultado el 28, octubre, 2022]. Disponible en Internet: <https://sistemas.acis.org.co/index.php/sistemas/article/download/11/8/>.

ASURZA CACERES, Josue David. Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa bafing S.A.C. en 2021. repositorio.cientifica.edu.pe [Sitio web]. (2022). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://repositorio.cientifica.edu.pe/handle/20.500.12805/2414>.

BUSTAMANTE, Antonia Terán; ARAGÓN, Griselda Dávila y CASTAÑÓN IBARRA, Rosario. Gestión de la tecnología e innovación: un modelo de redes bayesianas. www.redalyc.org [Sitio web]. (7, enero, 2019). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://www.redalyc.org/journal/2811/281161618004/movil/>.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Estudio semestral Tendencias del cibercrimen: Ciberseguridad en la era de la movilidad digital. www.ccit.org.co [Sitio web]. (julio, 2022). [Consultado el 12, octubre, 2022]. Disponible en Internet: <https://www.ccit.org.co/estudios/estudio-semestral-tendencias-del-cibercrimen-ciberseguridad-en-la-era-de-la-movilidad-digital/>.

CARDENAS RODRIGUEZ, Diego Alejandro. Diseño de un sistema de seguridad para la protección y prevención de intrusos ids/ips en la red empresarial de puntoqom minimizando el riesgo y asegurando los activos de información de la organización. repository.unad.edu.co [Sitio web]. (2022). [Consultado el 9, diciembre, 2022]. Disponible en Internet: <https://repository.unad.edu.co/bitstream/handle/10596/51475/dacardenasrod.pdf?sequence=1&isAllowed=y>.

Concepto Definición. [Sitio web]. (2023, 23 de febrero). Data center. https://conceptodefinicion.de/. https://conceptodefinicion.de/data-center/

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. colaboracion.dnp.gov.co [Sitio web]. (16, abril, 2016). [Consultado el 2, octubre, 2022]. Disponible en Internet: <https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf>.

COYLA JARITA, Yony. Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral

de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca. repositorio.upeu.edu.pe [Sitio web]. (26, mayo, 2019). [Consultado el 21, octubre, 2022]. Disponible en Internet: <https://repositorio.upeu.edu.pe/handle/20.500.12840/2002>.

DELL TECHNOLOGIES. Data Protection in a Time of Digital Transformation. www.dell.com [Sitio web]. (abril, 2021). [Consultado el 28, octubre, 2022]. Disponible en Internet: <https://www.dell.com/es-es/dt/data-protection/gdpi/index.htm#scroll=off&pdf-overlay=//www.delltechnologies.com/asset/es-es/products/data-protection/briefs-summaries/global-data-protection-index-infographic-global.pdf>.

DE LUZ, S. Configura pfSense para proteger tu hogar o empresa con este firewall [Sitio web].]. (abril, 2021). [Consultado el 22, mayo, 2022]. Disponible en Internet: <https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/>.

ESET SECURITY REPORT. Security Report Latinoamérica 2022. https://www.welivesecurity.com/ [página web]. (2022). [Consultado el 1, junio, 2023]. Disponible en Internet: <https://www.welivesecurity.com/wp-content/uploads/2022/10/ESET-security-report-LATAM2022.pdf>

GONZÁLEZ GÓMEZ, Diego. Sistemas de Detección de Intrusiones. dgonzalez.net [Sitio web]. (julio, 2003). [Consultado el 29, octubre, 2022]. Disponible en Internet: <https://dgonzalez.net/papers/ids/ids_v1.0.pdf>.

GOMEZ, Diego González. Sistema de detección de intrusiones. https://dgonzalez.net/ [página web]. (1, julio, 2007). [Consultado el 5, noviembre, 2023]. Disponible en Internet: <https://dgonzalez.net/papers/ids/ids_v1.0.pdf>.

GOMEZ, V. (s/f). Analizando la seguridad de la red con snorby – DOJOConf Panamá 2022. Dojoconfpa.org.[Consultado el 16, octubre, 2022] <https://dojoconfpa.org/analizando-la-seguridad-de-la-red-con-snorby/>.

GOODMAN, Seymour; DETMAR W. STRAUB y RICHARD BASKERVILLE. Information security : policy, processes, and practices. (2017). [Consultado el 1, noviembre, 2023]. Disponible en Internet: <https://eds-p-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/ebookviewer/ebook/ZTAwMHh3d19fMjc1NTEzX19BTg2?sid=d87ca403-93ad-4b3f-816c-49faf1ffa4e6@redis&vid=2&format=EB&rid=4>.

INCIBE. Glosario de términos de ciberseguridad. www.incibe.es [Libro Digital]. (2020). [Consultado el 16, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf>.

INGALLS, Sam. Best intrusion detection and prevention systems (IDPS) for 2022. www.esecurityplanet.com [Sitio web]. (6, octubre, 2022). [Consultado el 29, octubre, 2022]. Disponible en Internet: <https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/>.

IRWIN, Luke. What is information security management? - IT governance UK blog. IT Governance UK Blog [página web]. (22, febrero, 2022). [Consultado el 12, noviembre, 2023]. Disponible en Internet: <https://www.itgovernance.co.uk/blog/what-is-information-security-management>.

Joel Esler, PulledPork 3 — Actualización de reglas para Snort 3 [Sitio Web]. [Consultado 19, septiembre, 2022]. Disponible En: https://blog.snort.org/2021/06/pulledpork-3-rule-updating-for-snort-3.html

Manuelfrancoblog.wordpress.com, Barnyard2: Unificar alertas de Snort en MySQL [Sitio Web]. [Consultado 19, septiembre, 2022]. Disponible En: https://manuelfrancoblog.wordpress.com/2017/10/23/barnyard2-unificar-alertas-de-snort-en-mysql/

MARTÍNEZ RAMÍREZ, CARLOS ANDRÉS. DOCUMENTACIÓN TÉCNICA Y PROTOCOLO PARA LEVANTAMIENTO DE INFORMACIÓN EN CENTROS DE DATOS. /repositorio.ucp.edu.co [Sitio web]. (2020). [Consultado el 26, noviembre, 2022]. Disponible en Internet: <https://repositorio.ucp.edu.co/bitstream/10785/3027/1/CDPEIST48.pdf>.

MICROSOFT. Report Foreword by Bret Arsenault, Chief Information Security Officer at Microsoft. www.microsoft.com/es-co/security/ [Sitio web]. (junio, 2022). [Consultado el 22, octubre, 2022]. Disponible en Internet: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE58Ymd>.

OSORES, Melisa. Solo 11% de las pymes tiene una solución completa de seguridad IoT. www.computerweekly.com [Sitio web]. (14, octubre, 2022). [Consultado el 25, octubre, 2022]. Disponible en Internet: <https://www.computerweekly.com/es/noticias/252526128/Solo-11-de-las-pymes-tiene-una-solucion-completa-de-seguridad-IoT>.

OSTEC. DS: historia, concepto y terminología. https://ostec.blog/ [página web]. (1, octubre, 2015). [Consultado el 5, noviembre, 2023]. Disponible en Internet: <https://ostec.blog/es/seguridad-perimetral/ids-conceptos/>.

PATHAK, Amrita. 8 herramientas IDS e IPS para una mejor seguridad y conocimiento de la red. geekflare.com [Sitio web]. (16, febrero, 2022). [Consultado el 28, octubre, 2022]. Disponible en Internet: <https://geekflare.com/es/best-ids-and-ips-tools/>.

PÉREZ, Yuli. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA. http://polux.unipiloto.edu.co/ [Sitio web]. (2017). [Consultado el 15, octubre, 2022]. Disponible en Internet: <http://polux.unipiloto.edu.co:8080/00003620.pdf>.

POLICÍA NACIONAL DE COLOMBIA. Normatividad sobre delitos informáticos. www.policia.gov.co [Sitio web]. (30, octubre, 2022). [Consultado el 22, octubre, 2022]. Disponible en Internet: <https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos>.

RAMÍREZ MÁRQUEZ, Jimmy Fernando. Análisis, desarrollo e implementación de un sistema de seguridad para el fortalecimiento de vulnerabilidades e integridad de aplicaciones web académicas. http://dspace.espoch.edu.ec/ [Sitio web]. (12, marzo, 2022). [Consultado el 29, octubre, 2022]. Disponible en Internet: <http://dspace.espoch.edu.ec/handle/123456789/15708>.

SHEYLA LEACOCK, Analizando la seguridad de la red con snorby [Sitio Web]. [Consultado 19, septiembre, 2022]. Disponible En: https://dojoconfpa.org/analizando-la-seguridad-de-la-red-con-snorby/#:~:text=Snorby%20es%20una%20aplicaci%C3%B3n%20web,en%20el%20formato%20binario%20Unified2

SNORT.ORG. Manual de usuario de Snort 3. (22, marzo, 2023). [Consultado el 14, abril, 2023]. Disponible en Internet: < http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>.

TORO, R., & MAURICIO, A. (2022). Diseño de un plan de seguridad informática para el sistema de información de la Alcaldía Municipal de Támesis en base a la política de Gobierno Digital. Medellín - Colombia.

WWW.DNSSTUFF.coM. 7 Best Intrusion Detection Software and Latest IDS Systems. www.dnsstuff.com [Sitio web]. (18, febrero, 2020). [Consultado el 13, octubre, 2022]. Disponible en Internet: <https://www.dnsstuff.com/network-intrusion-detection-software>.

ZAMBRANO, Farias. Diseño de un sistema de detección de intrusos usando SNORT a través del análisis de tráfico en tiempo real y el análisis de protocolos [en línea]. Tesis doctoral. Guayaquil: Universidad de Guayaquil, 2022 [consultado el 13, noviembre, 2022]. Disponible en Internet: <http://repositorio.ug.edu.ec/handle/redug/59777>.

ANEXOS

Anexo A Carta Formal Aprobación de Proyecto 1

V0.1

Bogotá, 26 de octubre de 2022

Señor:
Juan Pablo Luna R.
Gerente Tecnología

Asunto: Autorización para la ejecución del proyecto titulado:
SISTEMA DE PREVENCIÓN Y DETECCIÓN DE ATAQUES PARA CORREDOR EMPRESARIAL S.A.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a COMUNICACIONES EMPRESARIALES DE COLOMBIA S.A.S de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: SISTEMA DE PREVENCIÓN Y DETECCIÓN DE ATAQUES PARA CORREDOR EMPRESARIAL S.A. el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente:

"Identificar incidentes de seguridad y posibles fugas de información en tiempo real en la red interna de la empresa COMUNICACIONES EMPRESARIALES DE COLOMBIA S.A.S "

Anexo B Carta Formal Aprobación de Proyecto 2

V0.1

"Automatizar por medio de estándares de búsqueda identificar amenazas en información enviada a través de la red"

"Ayuda a identificar problemas o posibles errores de seguridad en la red"

para obtener como resultado un alto impacto en la seguridad de la empresa COMUNICACIONES EMPRESARIALES DE COLOMBIA S.A.S

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por COMUNICACIONES EMPRESARIALES DE COLOMBIA S.A.S
- La empresa *COMUNICACIONES EMPRESARIALES DE COLOMBIA S.A.S* deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y

Anexo C Carta Formal Aprobación de Proyecto 3

V0.1

anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bogotá D.C., a los (26) días del mes de (Octubre) de 2022

Cordialmente,

Jimmy Rogelio Soto
Estudiante UNAD.

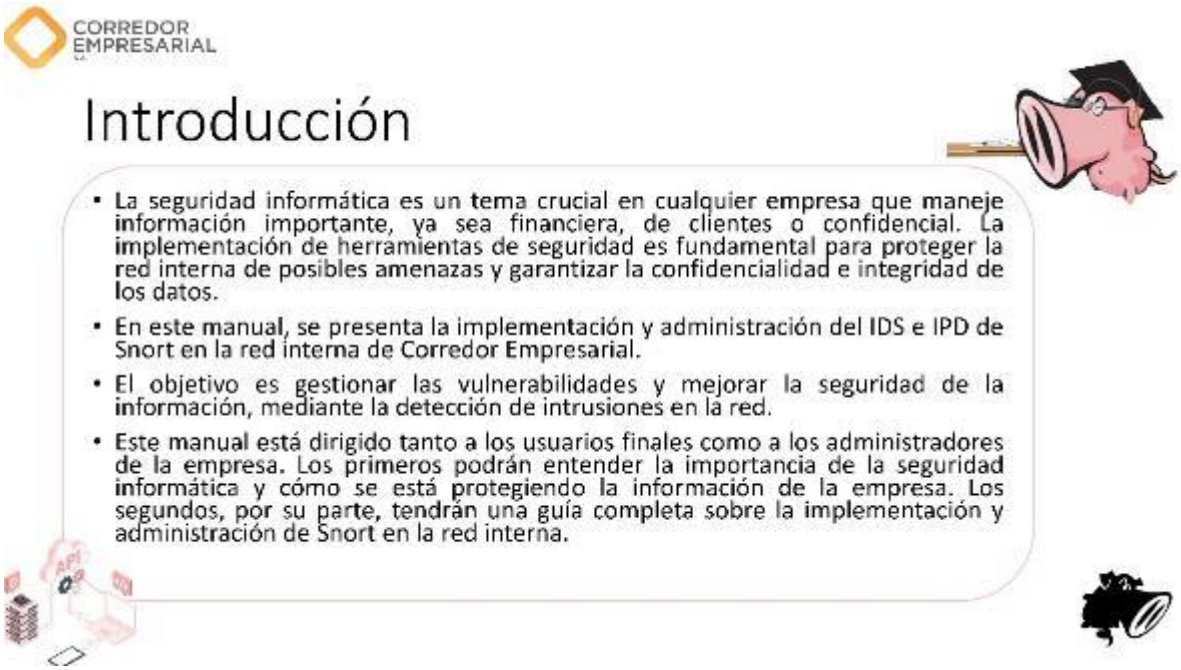
Juan Pablo Luna R.
Representante Legal.

Anexo D Manual Pdf

Figura 40 Manual 1

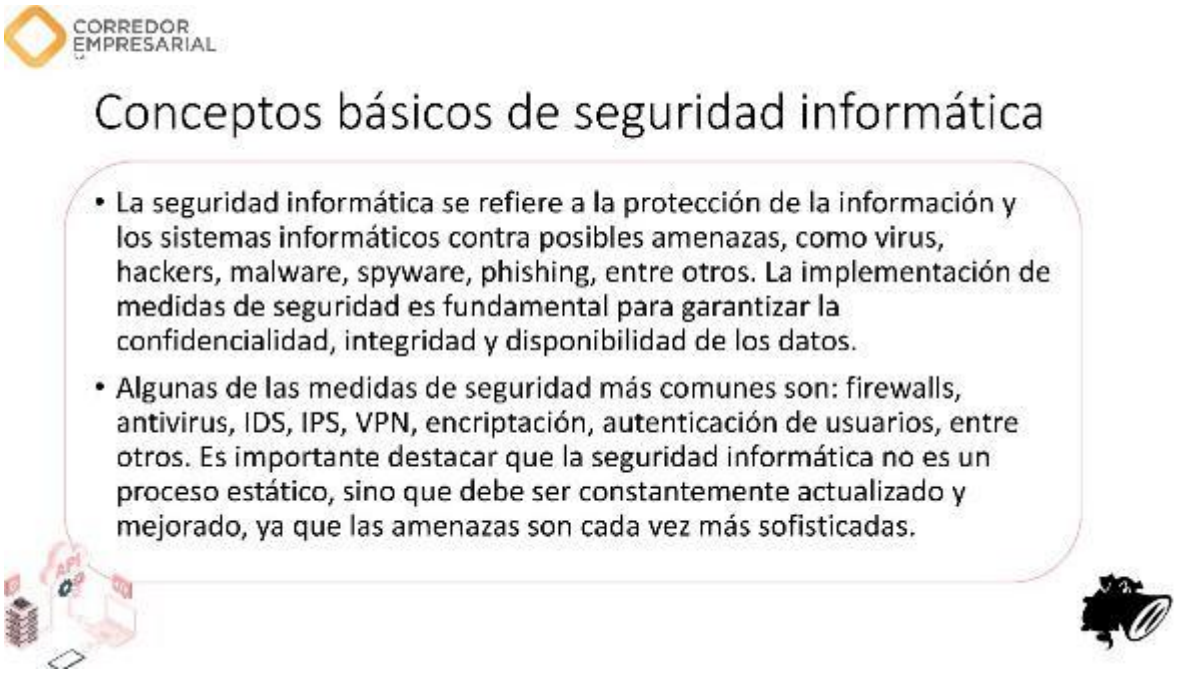
Fuente: propia

Figura 41 Manual 2



Fuente: propia

Figura 42 Manual 3



Fuente: propia

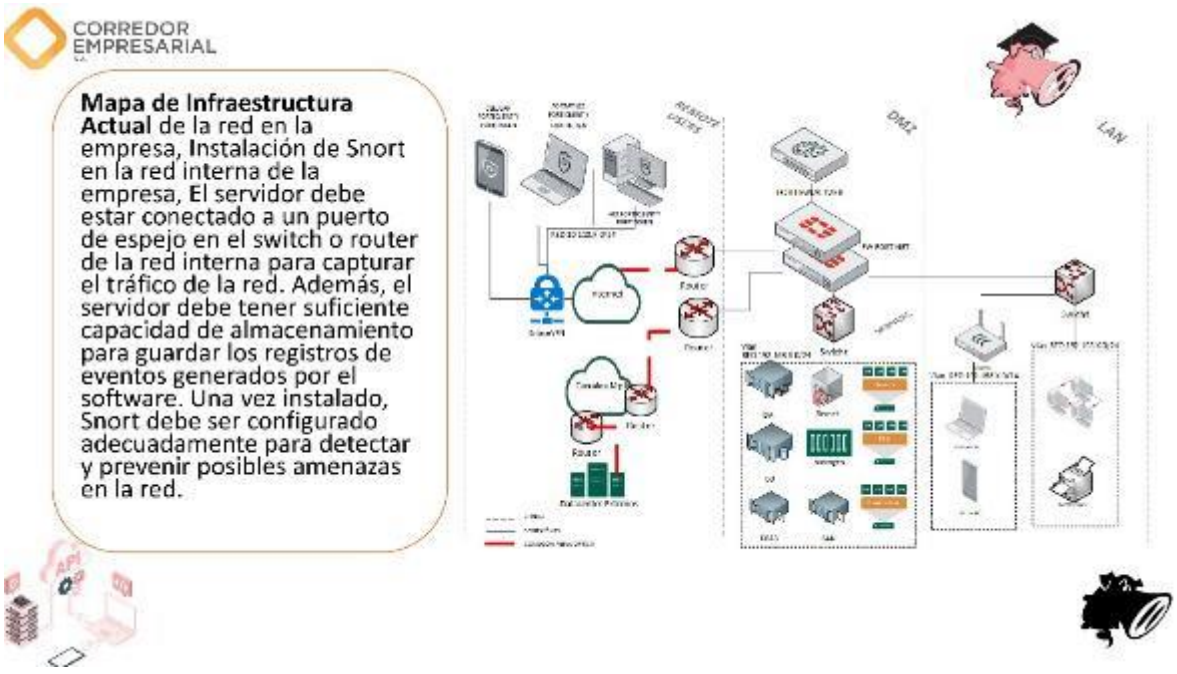
Figura 43 Manual 4

Fuente: propia

Figura 44 Manual 5

Fuente: propia

Figura 45 Manual 6



Fuente: propia

Figura 46 Manual 7

Fuente: propia

Figura 47 Manual 8

Fuente: propia

Figura 48 Manual 9

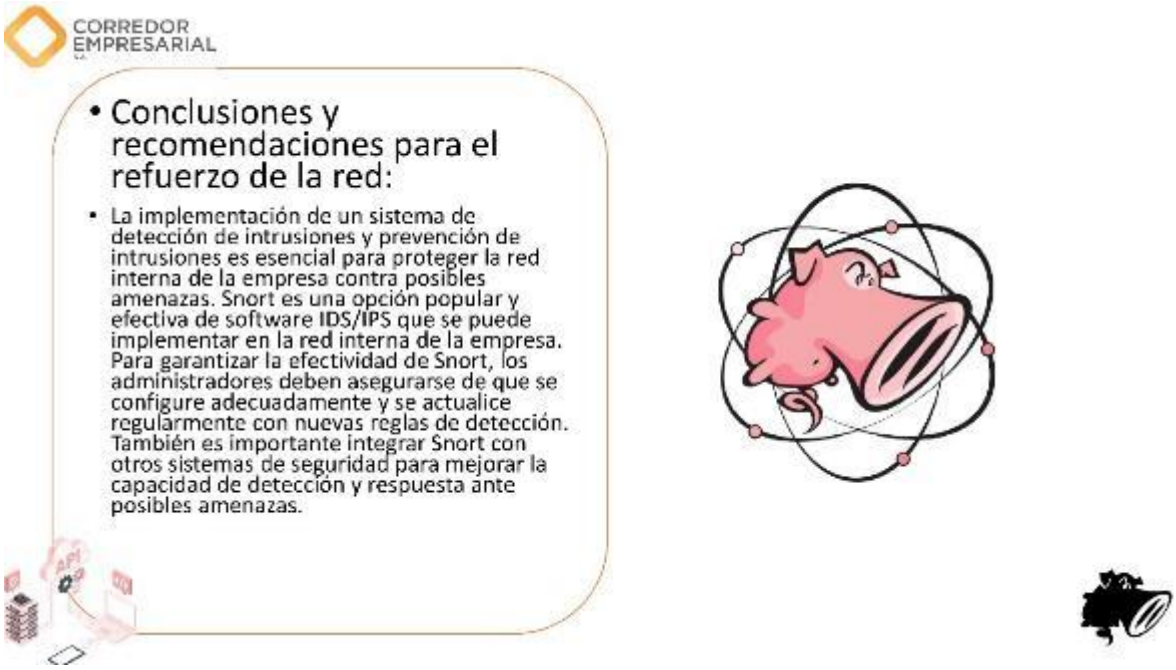
- Análisis de alertas en Snort:
- El análisis de alertas en Snort es crucial para garantizar que las alertas generadas por el software se manejen de manera efectiva. Los administradores deben revisar las alertas y determinar si son reales o falsos positivos. Las alertas reales deben ser investigadas y resueltas de manera oportuna, mientras que las falsas alarmas deben ser desestimadas para evitar una sobrecarga del sistema

Fuente: propia

Figura 49 Manual 10

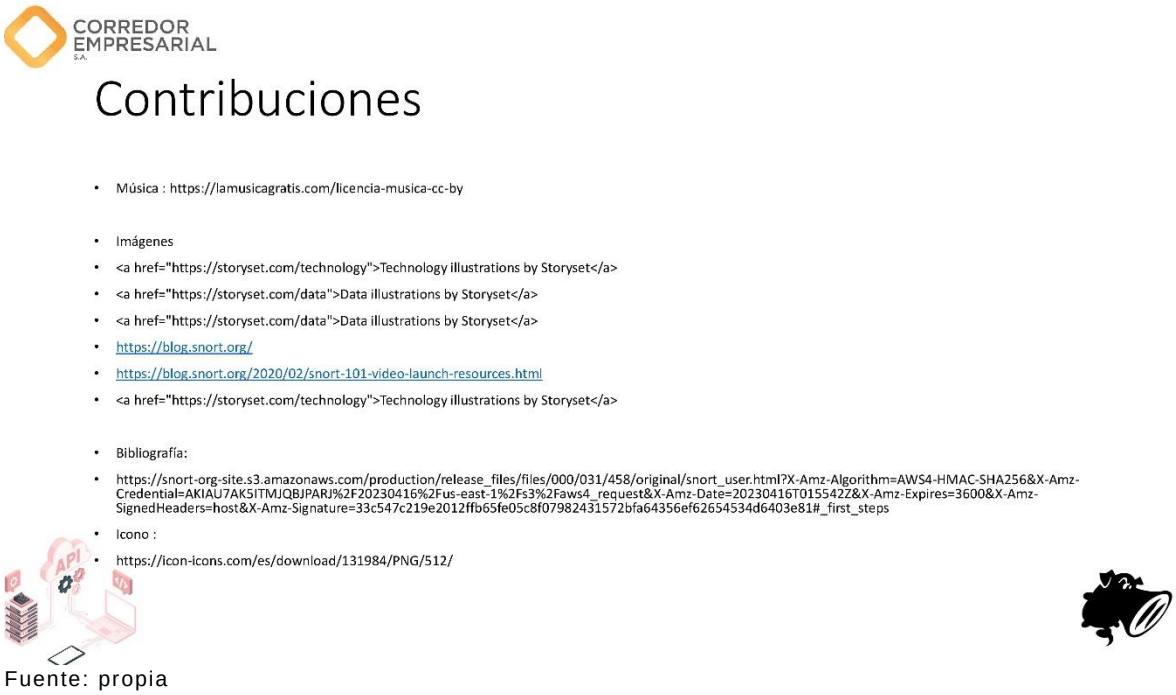
Fuente: propia

Figura 50 Manual 11



Fuente: propia

Figura 51 Manual 12



Fuente: propia

Anexo E Capacitación

Figura 52 Capacitación Usuarios

Pontificia Universidad JAVERIANA Bogotá

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

VICERRECTORÍA DE EXTENSIÓN Y RELACIONES INTERINSTITUCIONALES
EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA
EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Certifica que:

JIMMY ROGELIO SOTO

797

Participó en el Diplomado:

CIBERSEGURIDAD

Realizado del 23 de junio al 13 de octubre de 2022, con una intensidad de 120 horas.
En constancia se expide el presente certificado y se refrenda con las respectivas firmas.

Vicerrectora Extensión y Relaciones Interinstitucionales

Decano
Facultad de Ingeniería

Directora de Economía Digital
Ministerio de Tecnologías de la Información y las Comunicaciones

miércoles 12 de octubre de 2022

Fuente: propia

Anexo F Enlace de Vidéo

https://www.youtube.com/watch?v=vbKpL7cKkEA