APROVECHAMIENTO DE SOLUCIONES DE SOFTWARE LIBRE EN EL MONTAJE Y PUESTA EN MARCHA DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA ORGANIZACIONES COLOMBIANAS

Alejandro Bernal Castiblanco

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

APROVECHAMIENTO DE SOLUCIONES DE SOFTWARE LIBRE EN EL MONTAJE Y PUESTA EN MARCHA DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA ORGANIZACIONES COLOMBIANAS

Alejandro Bernal Castiblanco

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
Mg. Fernando Zambrano Hernández

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

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a Dios, Quien me suministró la salud y sabiduría para el desarrollo del presente trabajo, a mi esposa por su amor, comprensión, motivación y apoyo incondicional; a mis hijos que han fomentado en mí el deseo de superación académico y profesional en pro de una mejor calidad de vida para mi familia, a mi madre y padre que con su acompañamiento y apoyo incondicional me motivaron para desarrollarlo.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, es especial, a los docentes Luis Fernando Zambrano Hernández y Hernando José Peña Hidalgo por su acompañamiento, contribución y ayuda en la construcción de este documento, gestionando los laboratorios para realizar las pruebas pertinentes para el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA FIGURAS

Pág.

GLOSARIO

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.[1]

Denegación de servicio: Conjunto de técnicas en el cual su objetivo es sobrecargar un servicio, con el fin que sea inaccesible a los diferentes usuarios.[2]

Disponibilidad: Capacidad de asegurar la consulta y fiabilidad de forma oportuna a datos o servicios por diferentes usuarios.[3]

IDS: Sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusión Detection System) Aplicación que se utiliza para detectar accesos no autorizados a un ordenador o a una red.[4]

Incidente de seguridad: Acción que afecta la confidencialidad, integridad o disponibilidad de los activos de información de una organización.[5]

Inyección SQL: Ataque a un sistema de información mediante sentencias SQL maliciosas directamente a las bases de datos.[6]

IPS: Siglas de Intrusion Prevention System (sistema de prevención de intrusiones). Aplicación que se encarga de monitorear actividades a niveles de capa 3 red y capa 7 aplicación, con el fin de identificar comportamientos maliciosos.[7]

Pentest: Pruebas en ataques a diferentes entornos o sistemas de información, con l fin de identificar fallos o errores en el sistema.[8]

Phishing: Técnica de ataque mediante engaño que utilizan los ciberdelincuentes con el fin de obtener información personal a través e sitios web falsos.[9]

---

[1]INSTITUTO NACIONAL DE CIBER SEGURIDAD. Glosario de términos de ciber seguridad: una guía de aproximación para el empresario. [En Línea]. INCIBE. 2017. p. 6. Disponible en: (https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf).

[2] Ibid. p. 20

[3] Ibid. p. 21

[4] Ibid. p. 24

[5] Ibid. p. 24

[6] Ibid. p. 25

[7] Ibid. p. 25

[8] Ibid. p. 25

[9] Ibid. p. 25

Política de seguridad: Toma de decisiones en seguridad que aplica una organización en sus sistemas de información posterior de la evaluación sus activos y los riegos a los que están expuestos.[10]

Ransomware: El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.[11]

Suplantación de identidad: Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling).[12]

[10] Ibid. p. 25
[11] Ibid. p.31
[12] Ibid. p.35

RESUMEN

A través del tiempo la evolución en la administración de la información, adquisición de infraestructura, plataformas y servicios de información, diferentes organizaciones colombianas se han preocupado en implementar políticas, procesos y procedimientos enfocados en mitigar los diferentes ataques de ciberseguridad que se han presentado en el año 2020.[13] De acuerdo con diferentes organizaciones dedicadas a la ciberseguridad y a la situación actual por la emergencia sanitaria COVID-19, la organización FORTINET, multinacional estadounidense, identificó 5.400 millones de intentos de ataque por ciberdelincuentes en el primer semestre del presente año.[14]

Por consiguiente, este proyecto aplicado tiene como objetivo presentar a la comunidad interesada, las estrategias y alternativas de aprovechamiento de herramientas informáticas bajo licencia open source en el establecimiento de las operaciones de un CSIRT (Centro de Respuestas a Incidentes Informáticos), a partir de procesos de identificación, evaluación y análisis para el monitoreo, analítica de datos, explotación de información, detección y defensa de incidentes informáticos que pueden ocasionar grandes pérdidas de información en las diferentes organizaciones.

Palabras clave: cibercrimen, gestión de la información, gobierno electrónico, protección de datos, seguridad.

[13] PÉREZ PÉREZ, Yulis. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA. [En Línea]. Bucaramanga: Universidad Piloto de Colombia. 2014. p. 8. Disponible en: (http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y).

[14] EL ESPECTADOR. Detectan más de 5.400 millones de intentos de ciberataques en Colombia. En: El Espectador. [En Línea]. 21 agosto 2020. Disponible en: (https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/).

ABSTRACT

Through time the evolution in information management, acquisition of infrastructure, platforms and information services, different Colombian organizations have been concerned with implementing policies, processes and procedures focused on mitigating the different cybersecurity attacks that have occurred in the year 2020.

According to different organizations dedicated to cybersecurity and the current situation due to the COVID-19 health emergency, the FORTINET organization, a US multinational, identified 5,400 million attack attempts by cybercriminals in the first half of this year.

Therefore, this research project aims to present to the interested community, the strategies and alternatives for taking advantage of computer tools under open-source license in the establishment of the operations of a CSIRT (Computer Incident Response Center), based on identification, evaluation and analysis processes for monitoring, data analytics, information exploitation, detection and defense of computer incidents that can cause large losses of information in different organizations.

Keywords: cybercrime, information management, electronic government, data protection, security.

INTRODUCCIÓN

En la actualidad, el crecimiento a nivel mundial de las tecnologías de la información se debe a las necesidades de las organizaciones en sus actividades diarias; mediante suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, tramites gubernamentales, servicios de emergencia, suministro de agua y energía, entre otros.

Por consiguiente, las organizaciones están implementando herramientas para automatizar sus procesos y procedimientos, con el fin de brindar la disponibilidad de la información de forma oportuna a sus clientes, usuarios e individuos que interactúen con la lógica del negocio de la organización.

Con la implementación de estas tecnologías, las organizaciones deben desarrollar planes y programas a sus infraestructuras tecnológicas en seguridad, con el fin de identificar vulnerabilidades y amenazas que pueden afectar los servicios de disponibilidad, integridad y confidencialidad de la información de una organización.

Asimismo, mediante la investigación de este trabajo es dar conocer a la comunidad interesada, un documento guía que propone una lista de herramientas open source, como también un análisis, evaluación e integración de herramientas de análisis de datos, análisis de logs, herramientas de escáner de vulnerabilidad para la conformación de un CSIRT (Centro de Respuestas a Incidentes Informáticos) para organizaciones colombianas.

Por consiguiente, estas herramientas articuladas su objetivo es identificar vulnerabilidades y amenazas en las infraestructuras tecnológicas, con el fin de que el equipo de CSIRT pueda detectar, responder, minimizar y desarrollar planes y programas para proteger la disponibilidad, integridad y confidencialidad de la información de las organizaciones.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El crecimiento en Colombia en servicios de TI durante la emergencia sanitaria COVID-2019 ha generado un gran impacto de conectividad en un aumento del 51%, en el año 2021. El promedio de conexiones en el año 2020 era de 180.119 nuevos accesos; en comparación al primer semestre del año en curso que es de un 273.668.[15]

De acuerdo con lo anterior, las organizaciones de los sectores educación, producción, y otras ramas de la economía, han tenido que adaptarse al uso de nuevas herramientas y optar por teletrabajo, educación virtual, para así tener un encuentro sincrónico y asincrónico que les permita continuar brindando los servicios esenciales durante la crisis del COVID-19[16]

En consecuencia, las organizaciones públicas y privadas en diferentes áreas han adquirido nuevas herramientas tecnológicas para el desarrollo de sus actividades como por ejemplo aplicaciones en Big Data, Machine Learning y otras más para enfrentar esta revolución de la información.

La causa de adquisición de estas nuevas tecnologías, en el Estudio de Cibercrimen en Colombia, donde actualmente el 45.5% de las denuncias se hacen por canales virtuales y en el transcurso del 2019, se reportaron 28.827 casos, en el país por incidentes informáticos ocasionados por malware durante lo corrido del año crecieron un 612% donde Colombia se encuentra entre los países que recibió el mayor número de ataques por Ransomware en Latinoamérica con un total de 252 lo que corresponde al 30% después de Brasil y Argentina[17]

De acuerdo con el balance de cibercrimen del 2020 en Colombia, en la figura 1 se realiza un análisis del crecimiento en delitos informáticos en Colombia entre el año 2019 y 2020, en el cual, se identifica un crecimiento en el año 2020, el delito con mayor número de denuncias es el hurto por medios informáticos, los delitos que

---

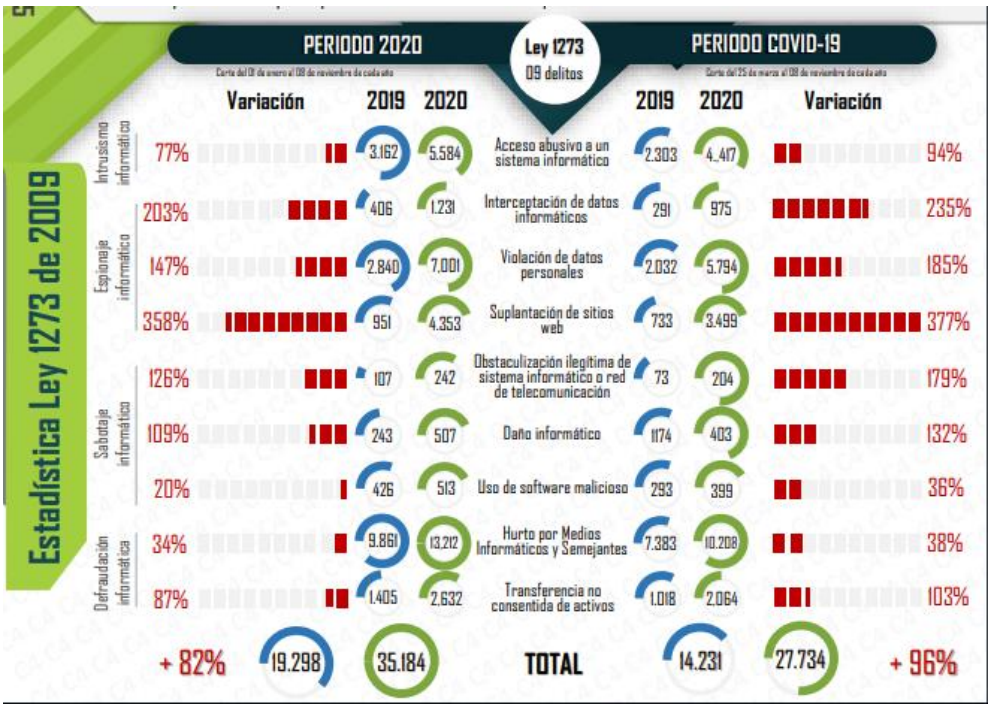
[15] ABUDINEN, Karen. “Colombia superó los 8 millones de accesos fijos a internet en el primer trimestre de 2021”: Karen Abudinen, ministra TIC. MINTIC. [En Línea]. 21 de julio 2021. Disponible en: (https://mintic.gov.co/portal/inicio/Sala-de-prensa/178505:Colombia-supero-los-8-millones-de-accesos-fijos-a-internet-en-el-primer-trimestre-de-2021-Karen-Abudinen-ministra-TIC).

[16] UCLG-CGLU. Tecnologías digitales y la pandemia de COVID-19. [En Línea]. 2022. 17p. Disponible en: (https://www.uclg.org/sites/default/files/eng_briefing_technology_es.pdf).

[17] CCIT. TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA 2019-2020. [En Línea]. PONAL. 2021. p. 20. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

más se incrementaron fueron suplantación de sitios web, violación de datos personales e intercepción de datos informáticos.

Figura 1 Ley 1273 09 delitos 2019-2020



Fuente: Balance de Cibercrimen 2020 – Centro Cibernético Policial – corte del 01 de enero al 8 de noviembre de 2020. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/observatorio/balance_cibercrimen_2020_-_semana_45.pdf

La figura 2 muestra las ciudades más afectadas, entres estas a la cabeza se encuentra la ciudad de Bogotá con un total de 12.081 casos presentados lo cual representa solo el 37% en todo el país, sigue Medellín con un 10%, Cali con un 7% siendo estas las ciudades más grandes de Colombia.

Figura 2 Ciudades con mayor afectación

Fuente: CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. p. 2 Disponible en: (https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf).

En cuanto a modalidades de ataques, en la figura 3 se puede deducir que entre los ataques más comunes se encuentran la estafa por compras electrónicas, phishing, suplantación de identidad, Se puede analizar que el mayor ataque por ciberdelincuentes que se realiza es por comercio electrónico.

Figura 3 Modalidades de ataques

Fuente: CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. p. 2 Disponible en: (https://caivirtual.policia.gov.co/sites/default/files/observatorio/balance_cibercrimen_2020_-_semana_45.pdf).

En consecuencia, a estos ataques el estado ha estado fortaleciendo sus organizaciones una de ellas es el Caí Virtual organización que hace parte del gobierno para combatir el cibercrimen en Colombia, en la figura 4 podemos observar algunos logros obtenidos de parte de esta estrategia nacional.

En la figura 4 se analiza los resultados operacionales en el año 2020, en el Balance de Cibercrimen, se tendieron 11.950 incidentes dentro de los cuales los más significativos fueron los contenidos con material de abuso infantil.

Figura 4 Resultados operacionales

Fuente: CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. p. 2 Disponible en: (https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf).

De acuerdo con estos informes socializados se observa que las organizaciones colombianas no se encontraban preparadas para atender los requerimientos y exigencias de sus clientes comerciales, así como tampoco para mantener entornos digitales de manera segura[18]

Por lo tanto, el uso de todas estas herramientas tecnológicas en teletrabajo, pagos electrónicos conexiones personales y remotas, hizo que aumentaran los ataques por ciberdelincuentes y se presentaron pérdidas de hasta 10.400 millones de dólares para el año 2020[19].

[18]CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. p. 2 Disponible en: (https://caivirtual.policia.gov.co/sites/default/files/observatorio/balance_cibercrimen_2020_-_semana_45.pdf).

[19] CCIT. Tendencias Del Cibercrimen En Colombia 2019-2020. [En Línea]. PONAL. 2021. p. 21. Disponible en: (https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf).

En Colombia las estadísticas por la Fiscalía General de la Nación, informa que las pérdidas en Colombia por ciberseguridad oscilan entre los 120 millones a 5.000 millones de pesos, de acuerdo con la organización.

Estas cifras fueron consolidadas estudio tendencias de cibercrimen en Colombia, liderado por el SAFE (Seguridad Aplicada Al Fortalecimiento Empresarial) TicTac (Tanque de Análisis y Creatividad de las TIC y el CCIT (Cámara Colombiana de Informática y Telecomunicaciones).[20]

Las denuncias por ataques de ciberdelincuentes en el año 2019, el promedio es de 45% el cual fueron reportados 28827 casos de incidentes de ciberseguridad empresarial, los cuales han sido denunciado 17.531 en la Fiscalía en el año 2019.

Del año 2017 a 2019 se han reportado 52.901 denuncias a través de delitos informáticos, hurtos 31.058, robo de identidad 8.037, el cual Bogotá es la ciudad con más ciberataques, Cali y Medellín.[21]

Los ataques por malware ha sido el más utilizado en el año 2020 en Colombia, en un 35% de los incidentes reportados y un 26% en aplicaciones de minería de criptomonedas.

En el segundo trimestre del 2020 se han reportado 561 incidentes de ciberseguridad, el cual aumento el 22% desde el trimestre anterior, ciencia y tecnología es la mayor afectada con el 91%.[22]

Ahora, Las bandas de cibercriminales operan por la Deep web, el cual invitan a consultar diferentes servicios por plataformas, ofreciendo diferentes clases de programas piratas, tarjetas de crédito, armas en más de 50 países del mundo; a los sus clientes les ofrecen anonimato y destrucción de la evidencia, una de las aplicaciones es DISCORD; aprovechan el anonimato, creación de servidores y canales propios.[23]

ASOBANCARIA:

---

[20] Ibid. p.7
[21] Ibid. p.8
[22] SEMANA. Aumentan 605% Ciberamenazas Relacionadas Con La Covid-19. [En Linea]. Semana. 7 de noviembre 2020. Disponible en: https://www.semana.com/tecnologia/articulo/cuanto-subieron-las-ciberamenazas-en-el-segundo-trimestre/305962/.

[23] SEMANA. Así Operan Los Cibercriminales Dentro Y Fuera De La Internet Profunda. [En Línea]. Semana. 6 de agosto 2020. Disponible en: https://www.semana.com/tecnologia/articulo/como-operan-los-cibercriminales-cual-es-la-nueva-estrategia/295042/.

EL CSIRT financiero liderado por Asobancaria es el primer Equipo de Respuesta a Incidentes Cibernéticos del país en establecer un modelo colaborativo y de intercambio de información entre entidades financieras.

PANORAMA DE RIESGOS CIBERNÉTICOS:

Según la evolución de la gestión de Ciber-Riesgos y Seguridad de la Información Deloitte, 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 25 meses con respecto al 2016.

Para el 2017, se han registrado un total de 67 millones de amenazas cibernéticas en América Latina.

Según Cálculos de Asobancaria el fraude a través de canales electrónicos ha crecido cerca de 60.57% de 2015 a 2017.

De acuerdo con el informe Balance del Cibercrimen en Colombia 2017 realizado por el Centro Cibernético Policial, el cibercrimen en el país aumentó 28.3% frente a los resultados obtenidos en 2016.[24]

COLCERT

Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT

Tiene como responsabilidad central la coordinación de la ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional.[25]
CC-CSIRT Policía Nacional

Equipo de respuesta a incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar

[24] CSIRT; ASOBANCARIA. Equipo De Apoyo Para La Respuesta A Incidentes De Ciberseguridad Para El Sector Financiero Colombiano. [En Línea]. CSIRT Financiero. 2022. Disponible en: (https://csirtasobancaria.com/quienes-somos).

[25] Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Resumen de vulnerabilidades para la semana anterior. [En Línea]. COLCERT. 6 de febrero de 2022. Disponible en: (http://www.colcert.gov.co/?q=acerca-de).

el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. [26]

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede diseñar, construir y evaluar un Centro de Respuesta a Incidentes Informáticos para organizaciones colombianas con el uso de herramientas de software libre?

[26] ¿Quiénes Somos? [en línea] cc-csirt-policia.gov. 31 octubre 2020. Disponible en: https://cc-csirt.policia.gov.co/quienes-somos

2. JUSTIFICACIÓN

Actualmente, la revolución de las nuevas Tecnologías de Sistemas de Información y Comunicación (TICS) mediante informe de la Organización Mundial de la Salud, debido a la situación de emergencia sanitaria por el COVID-19; las organizaciones públicas y privadas en diferentes áreas del saber, se están enfrentando a la revolución de la información, de manera que muchas de las entidades se están apoyando en la implementación de nuevas tecnologías[27].

Las organizaciones colombianas por la emergencia sanitaria del presente año están implementando nuevas medidas y alternativas, con el fin de cumplir con sus objetivos misionales; por ejemplo, teletrabajo, e-learning (educación virtual), inteligencia artificial, Machine Learning, análisis de datos, big data, robótica, entre otras.[28]

En el desarrollo de este proyecto aplicado, su objetico principal es la integración de diferentes herramientas de software libre para conformar un CSIRT (Computer Security Incident response Team - Equipo de respuesta ante incidentes de seguridad informática); mediante el cual se utilizaran herramientas opensource; con el fin de lograr la identificación y análisis de vulnerabilidades; para centralizar estos incidentes, realizar toma de decisiones con el fin de mitigar el riesgo a ataques a los sistemas de información y responder de forma oportuna a estos sucesos.

Por consiguiente, estas herramientas de software al ser articuladas ayudan a la priorización de los activos, para detectar, analizar, y responder a ataques informáticos, En el cual estas herramientas ayudan a la planificación e implementación de medidas de seguridad proactivas para prevención mediante planes estratégicos a respuestas a un ciberataque.

---

[27] OPS; OMS. COVID-19 y el rol de los sistemas de información y las tecnologías en el primer nivel de atención. [En Línea]. 23 mayo 2020. Disponible en: (https://iris.paho.org/bitstream/handle/10665.2/52205/OPSEIHISCOVID19200022_spa.pdf?sequence=9).

[28] SEMANA. La tecnología ha sido clave en estos momentos de crisis. En: SEMANA. [En Línea]. 20 abril 2020. ISSN 2745-2794. Disponible en: https://www.dinero.com/tecnologia/articulo/columna-la-tecnologia-ha-sido-clave-en-estos-momentos-de-crisis-por-eliseo-barcas-20-de-abril/284442

3. OBJETIVOS

3.2 OBJETIVO GENERAL

Estructura un documento guía que brinde información de herramienta de software libre que puedan ser usadas en un centro de respuesta a incidentes informáticos para pequeñas y medianas empresas colombianas

3.3 OBJETIVOS ESPECÍFICOS

- Examinar documentación de herramientas de seguridad informática de software libre que puedan ser usadas en las actividades de un centro de respuestas a incidentes informáticos.

- Evaluar la usabilidad de herramientas de software libre que puedan servir como infraestructura tecnológica para respuesta a un evento o incidente informático

- Proponer la integración de herramientas de software libre para soportar las actividades de un centro de respuestas a incidentes informáticos

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Gideon Gartner fundador de la empresa norteamericana Gartner, empresa dedicada a la investigación y consultoría en tecnología de la información, inventa el cuadrante de Gartner para el análisis e investigación de diferentes herramientas tecnológicas, Gartner utiliza los cuadrantes mágicos, el cual clasifica a los proveedores de herramientas de software libre para la integración de un CSIRT, de acuerdo con cuatro categorías: lideres, retadores o aspirantes, visionarios, jugadores de nicho.[29]

De acuerdo con lo anterior, se identifica e investiga las herramientas a evaluar, se definen los criterios de evaluación, se realiza la evaluación de las herramientas seleccionadas de acuerdo con los pro y contras en la implementación, realizar o investigar los diferentes gráficos y realizar un análisis de acuerdo en la posición que se encuentre la herramienta en el eje horizontal y vertical.

Por otra parte, se realiza una lista de términos de referencia que hacen parte del desarrollo de este proyecto:

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes[30].

La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista[31].

La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo[32].

---

[29] ISC ¿Qué es el cuadrante Mágico de Gartner y para qué sirve en transformación digital? [En Línea] ISC Ingeniería, Servicios y Comunicaciones 2023 Disponible en: https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/

[30] KASPERSKY. ¿Qué es la ciberseguridad? [En Línea]. Latam kaspersky. 2022. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[31] Ibid. p. 1

[32] Ibid. p. 1

La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito[33].

La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría[34].

La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos[35].

La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización. Es la práctica de defender las computadoras, los servidores,[36]

Threat Hunting: Se puede definir como el proceso de búsqueda iterativa y Proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.

¿Cómo funciona el Threat Hunting?
Descubre nuevos patrones de ataque mediante la identificación automática de anomalías en el comportamiento de cada usuario, proceso y máquina[37].

---

[33] Ibid. p. 1
[34] Ibid. p. 1

[35] Ibid. p. 1

[36] Ibid. p. 1
[37] PANDA. ¿Qué es Threat Hunting y por qué es necesario? [En Línea]. PANDA SECURITY. 15 noviembre 2018. Disponible en: https://www.pandasecurity.com/es/mediacenter/adaptive-defense/threat-hunting-por-que-necesario/

Cada nuevo patrón se convierte también en un comportamiento de detección de amenazas para detener a futuros hackers, antes de que se produzcan daños, creando así un ciclo de aprendizaje y detección.[38]

Threat Detection and Response (TDR)
Es un servicio de suscripción basado en la nube que se integra con su Firefox para minimizar las consecuencias de las filtraciones y penetraciones de datos a través de la detección temprana y la remediación automatizada de las amenazas de seguridad. TDR recopila y analiza los datos forenses del Firebox y de los extremos de su red para detectar y responder proactivamente a las amenazas de seguridad. Los análisis de ThreatSync permiten a TDR asignar puntuaciones del nivel de amenaza basadas en heurísticas, fuentes de amenazas y un servicio de verificación de malware basado en la nube[39].

Threat Detection and Response solo es compatible con los modelos de dispositivos Firefox y XTMv, y requiere Fireware v11.12 o posterior.
Componentes de TDR

El servicio de suscripción de Threat Detection and Response tiene varios componentes:

Cuenta de Threat Detection and Response
Threat Detection and Response es un servicio basado en la nube alojado por WatchGuard. Su cuenta de Threat Detection and Response en la nube recopila y analiza datos forenses recibidos de los Firebox y Host Sensors en su red. Usted inicia sesión en su cuenta de TDR en el Portal de WatchGuard para configurar los ajustes de la cuenta, la configuración del Host Sensor, y para monitorear y gestionar las amenazas de seguridad[40].

Debido a que sus credenciales de inicio de sesión para TDR son sus credenciales del Portal de WatchGuard, cuando inicia sesión en el Portal de WatchGuard, el inicio de sesión único también le permite iniciar sesión automáticamente en su cuenta de TDR[41].

Dispositivo Firebox o XTMv

---

[38] Ibid. p. 1

[39] Ibid. p. 1

[40] WATCHGUARD. Acerca de Threat Detection and Response. [En Línea]. Disponible en: https://www.watchguard.com/help/docs/help-center/es-419/Content/es-419/Fireware/services/tdr/tdr_about_c.html

[41] Ibid. p. 1

Threat Detection and Response es una suscripción de seguridad que usted activa para su Firebox. En la configuración de Firebox, usted habilita el Firebox para enviar datos a su cuenta TDR, y configura las políticas, los servicios y los ajustes de registro para habilitar el Firebox y el Host Sensor para enviar información a su cuenta de TDR[42].

Host Sensor
Usted instala los Host Sensor en las computadoras de su red. Cada Host Sensor recopila datos forenses del host y los envía a la nube de Threat Detection and Response para su análisis. Los datos forenses incluyen información relacionada con archivos, procesos, conexiones de red y claves de registro en el host. Puede configurar los Host Sensor para simplemente reportar amenazas de seguridad o para tomar medidas para solucionar ciertos tipos de amenazas de seguridad[43].

AD Helper
AD Helper es una aplicación que puede instalar para implementar Host Sensors en su red. AD Helper usa su infraestructura existente de Windows Active Directory para ayudar con la instalación distribuida de Host Sensors en su red.[44]

4.2 MARCO CONCEPTUAL

En un entorno empresarial cada vez más interconectado y digitalizado, la seguridad de la información se ha convertido en un pilar fundamental para las pequeñas y medianas empresas colombianas. La capacidad de identificar, gestionar y responder eficazmente a incidentes informáticos es esencial para proteger los activos digitales y garantizar la continuidad del negocio.

Este documento tiene como objetivo proporcionar una guía integral que, en primer lugar, explora herramientas de software libre adecuadas para establecer un Centro de Respuesta a Incidentes Informáticos (CRII) en el contexto de las pequeñas y medianas empresas en Colombia.

Además, se presentarán conceptos clave relacionados con herramientas para un Centro de Operaciones de Seguridad (SOC), con el fin de brindar una visión completa de cómo fortalecer la ciberseguridad y la capacidad de respuesta en un mundo digital en constante evolución.
SOC: Los Centros de Operaciones de Seguridad, tienen como función, monitorear, rastrear y analizar las diferentes actividades de las redes, servidores,

[42] Ibid. p. 1
[43] Ibid. p. 1

[44] Ibid. p. 1

bases de datos, aplicaciones, mediante los diferentes logs que es la materia prima para analizar cualquier suceso o comportamiento extraño.[45]

Incidente Informático: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información.[46]

Vulnerabilidad: (En Términos de Informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos agujeros pueden tener distintos orígenes, como son los fallos de diseño, errores de configuración o carencias de procedimientos[47].

Amenaza: Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. que podría tener un potencial efecto negativo sobre algún elemento del sistema, que pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). pueden ser internas o externas desde el punto de vista de la organización[48].

Riesgo: Es la probabilidad que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto[49].

Integridad: Asegura que los datos no han sido alterados ni destruidos de modo no autorizado, para mitigar este riesgo; se debe dotar al sistema, mecanismos que prevengan y detecten un fallo de integridad[50].

---

[45] Que es un SOC: Funciones y Objetivos Principales. [En línea]. Nsit. 2022.Disponible en: https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

[46] KASPERSKY. ¿Qué es la ciberseguridad? [En Línea]. latam.kaspersky. 2022. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[47] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [En Línea]. 20 marzo 20217. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[48] Ibid. p.1

[49] Ibid. p.1

[50] Ibid. p.1

Confidencialidad: Esta se encarga de que la información o datos, estén al alcance de los usuarios autorizados[51].

Disponibilidad: Hace relación en que la información esté en el momento oportuno que es requerido por el usuario, asegurando su integridad y confidencialidad. [52]

CSIRT: (Equipos de Respuesta a incidentes de Seguridad) Nacen para mitigar las consecuencias y se pueda restablecer en el menor tiempo posible con un impacto mínimo aceptable en las empresas. Debe controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación, permitiendo determinar su origen y posibles consecuencias, debe coordinar las actividades para una recuperación rápida y eficiente de las actividades que se afectaron, debe también prevenir eventos similares que puedan ocurrir en el futuro, de tal manera que puedan erradicarse las causas raíz del incidente.[53]

4.3 MARCO HISTÓRICO

En noviembre de 1988, Internet era en gran parte desconocido, usado principalmente por gobiernos, organismos gubernamentales, investigadores e instituciones educativas[54].

el 2 de noviembre Robert Tappan Morris, estudiante en la Universidad de Cornell, lanzo el primer gusano informático auto replicante del mundo a través de Internet, Conocido como el "gusano Morris", el código malicioso paralizó 6000 computadoras, o casi el 10% de las que luego se conectaron a Internet. El incidente se resolvió cinco días después, pero requirió la colaboración internacional para resolverlo y resulto en una duplicación masiva de esfuerzos y recursos desperdiciados[55].

---

[51] Ibid. p.1

[52] Ibid. p.1

[53] WELIVESECURITY. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 18 mayo 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/#:~:text=Dado%20este%20escenario%20de%20evoluci%C3%B3n,Computer%20Security%20Incident%20Response%20Team

[54] RETIREMENT. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 23 enero 2018. Disponible en: https://blog.rch1.com/blog/the-crucial-role-of-the-csirt

[55] Ibid. p. 1

A partir del caos causado por el gusano Morris, se formó el Centro de Coordinación / Equipo de Respuesta a Emergencias Informáticas, o CERT / CC. Organizado como un centro de investigación y desarrollo sin fines de lucro financiado con fondos federales, CERT / CC se convirtió en la fuerza impulsora detrás de los CSIRT.[56]

4.4 ANTECEDENTES O ESTADO

- A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019, del total de casos 15948 fueron denunciados como infracciones a la ley 1273 de 2009 por parte de las víctimas, esta cifra corresponde al 57% del total de casos informados[57].

- Según el FBI los ataques BEC (Bussiness Email Compromise) generaron perdidas en organizaciones globales por valor de 12.000 millones de dólares.

- Colombia Recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú (16%), México (14%), Brasil (11%), y Argentina (9%)[58].

- Las pymes fueron el blanco[59]

- El correo electrónico se ha convertido en el medio más utilizado por los ciberdelincuentes para realizar campañas masivas de distribución de Malware a través de la suplantación de entidades oficiales (Fiscalía General de la Nación y La Dirección de Impuestos y Aduanas Nacionales)[60].

- Según datos de la Comisión Federal de Comercio de los EE.UU FTC por sus siglas en inglés (Federal Tarde Comisión), los casos reportados por robo de identidad para la obtención de SIMCARD ante operadores de telefonía celular representan actualmente 9.8% del total de casos reportados en 2018[61].

---

[56] Ibid. p.

[57] CCIT. TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA 2019-2020. [En Línea]. PONAL. 2021. p. 7. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[58] Ibid. p. 13

[59] Ibid. p. 13

[60] Ibid. p. 22

[61] Ibid. p. 25

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

¿QUE ES UN SOC?

Un **SOC** De Siglas en Inglés **Centro de Operaciones de Seguridad** es una unidad centralizada dentro de una organización, dedicada exclusivamente a todos los temas tácticos y operativos asociados con seguridad de la información, también realiza labores orientadas al monitoreo, aseguramiento y defensa de los activos de información por medio de equipos tecnológicos y personal especializado que monitorea en tiempo real los eventos generados por la infraestructura tecnológica de la organización durante las 24 horas del día y los 7 días de la semana[62].
El SOC se basa en las siguientes funciones:

- **Prevención:** Su función principal es minimizar la probabilidad de aparición de incidentes, debe realizar constante vigilancia ante nuevos ataques que comprometen la seguridad, así como implementar medidas preventivas que reduzcan la probabilidad de materialización de amenazas[63].

- **Detección:** Monitoreo constante para detectar amenazas, vulnerabilidades, intrusiones, ataques de seguridad, o cualquier circunstancia donde se implique un incidente de seguridad[64].

- **Análisis:** se estudian los incidentes que surgen en la detección y así poder diferenciar entre amenazas reales o falsos positivos[65].

- **Respuesta:** a todos los planes de acción que se efectúan contra cualquier incidente real de seguridad[66].

También provee servicios de seguridad que deben estar alineados con los objetivos de la organización, quiere decir que dependiendo de las necesidades de la empresa los servicios del SOC pueden variar, existen servicios característicos que hacen parte de este y son:

- **Monitorización Continua de la seguridad:** Se observan constantemente todos los controles de seguridad implementados con el objetivo de detectar posibles

---

[62] MORALES GONZÁLEZ, Carlos; MORENO SÁMCHEZ, Omar y ORTIGOZA PÉREZ, Johanna. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONS DE SEGURIDAD (SOC) PARA FUERZA AÉREA COLOMBIANA. [En Línea]. Bogota D.C.: Universidad Piloto de Colombia. 2014. p. 32 Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1n

[63] Ibid. p. 32

[64] Ibid. p. 32

[65] Ibid. p. 32

[66] Ibid. p. 32

incidentes de seguridad. El SOC debe apoyarse en diferentes herramientas que le proporcionen información completa y en tiempo real del estado en que se encuentra la seguridad de la organización.[67]

- **Detección y Gestión de vulnerabilidades:** Identificar las debilidades que posee la organización es importante para ello se realizan las auditorías que se efectúan en forma automática y periódica dirigidas a diferentes puntos de la infraestructura tecnología de la organización con el fin de identificar debilidades y determinar las acciones correctivas para la eliminación de cada vulnerabilidad.[68]

- **Centralización, tratamiento y custodia de logs:** Para la gestión de la gran cantidad de logs generados por los diversos dispositivos que se manejan, se requiere el uso del sistema SIEM que permite correlacionar los diversos eventos de seguridad para detectar situaciones poco comunes o sospechosas. Estos logs pueden ser almacenados para su posterior consulta y así investigar eventos que ya sucedieron.[69]

- **Respuesta de Resolución:** Ante un incidente de seguridad, el SOC debe desarrollar y activar planes de solución que neutralicen la amenaza teniendo encuentra el nivel de criticidad de los activos comprometidos y el impacto que hay sobre los mismos.[70]

- **Asesoría de Seguridad:** A través de un equipo de profesionales especializados en temas de seguridad de la información apoyan a la dirección en la toma de decisiones de la seguridad de la organización, es por esto que el SOC dispone de personal con conocimiento especializado tales como técnicos en sistemas y comunicaciones, expertos en seguridad física y lógica, juristas especializados, auditores de seguridad y analistas de malware. Lo anterior está sujeto al alcance definido para el SOC.[71]

Programas de prevención: El SOC trabaja por la prevención de incidentes de seguridad a través de la vigilancia constante de nuevas amenazas e implementación de controles preventivos que mitiguen el riesgo de aparición de incidentes de seguridad.[72]

---

[67] Ibid. p. 32
[68] Ibid. p. 32
[69] Ibid. p. 33
[70] Ibid. p. 33
[71] Ibid. p. 33
[72] Ibid. p. 33

4.6 MARCO LEGAL

El uso de sistemas informáticos, software y todo tipo de tecnologías informáticas y de telecomunicaciones está debidamente reglamentada y regulada en Colombia por medio de diferentes decretos y leyes, los cuales fueron creados para garantizar el uso libre y adecuado de estas tecnologías, dentro de las normativas más importantes dentro de las cuales se regula esta investigación las podemos apreciar en la siguiente tabla:

Tabla 1 Lineamientos de Política Para Ciberseguridad y Defensa

Ley- Resolución	Descripción
Ley 527 de 1999 – Comercio Electrónico	**D**efine y Reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.
Ley 599 de 2000	Código Penal. Describe la violación ilícita de comunicaciones, se indican conductas relacionadas indirectamente con el delito informático, como venta o compra de instrumentos que sirvan para interceptar comunicaciones privadas. Menciona el acceso sin autorización a un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.
Ley 1341 de 2009	Define los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrecen servicio de acceso a internet de implementar modelos de seguridad que permitan el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de datos.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Establece los requerimientos mínimos de seguridad y calidad en el manejo de información en medio y canales de distribución de productos y servicios para clientes y usuarios.

MSPI (Modelo de Seguridad y Privacidad de la Información)	Marco integral diseñado para salvaguardar la integridad, confidencialidad y disponibilidad de información en una organización, este tiene una serie de principios y controles que buscan mitigar riesgos y amenazas de seguridad de la información.
Conpes 3854	Políticas y estrategias de seguridad nacional, para que los colombianos y organizaciones identifiquen los riesgos a los que están expuestos en un entorno digital; con el fin de adoptar buenas prácticas a la hora de realizar compras y trámites en línea.
PESI (PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN)	Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias
Decreto 338 de 2022 (Seguridad Digital)	Se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digita, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.
PETI (Plan Estratégico de Tecnología de la Información)	Documento que establece la dirección y los objetivos estratégicos para la gestión de la tecnología de la información (TI) en una organización. Su propósito es alinear la estrategia de TI con los objetivos generales de la organización, garantizando que la tecnología sea un habilitador efectivo para el logro de metas y el desarrollo sostenible.

Fuente: Consejo Nacional De Política Económica Y Social. Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. [En Línea]. Bogotá D.C.: CONPES. 2021. p. 10 – 12. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

4.7 MARCO CONTEXTUAL:

El uso masivo de las tecnologías de la información en todos los ámbitos de la sociedad, así como la convergencia e interconexión de los sistemas ha venido generando nuevos riesgos y vulnerabilidades en todas las organizaciones que se ven presionadas diariamente por el creciente número de amenazas que ponen en peligro sus activos, en algunos casos, realmente críticos para su funcionamiento.

Estas amenazas en el ciberespacio, que en gran medida siguen siendo las mismas que en el mundo físico (fraude, robo, espionaje industrial, terrorismo, sabotaje…) se han visto agravados por la rentabilidad de los ataques automatizados, la acción a distancia y las técnicas de propagación cada día más rápidas y fáciles de emplear.

De igual modo, los ataques han ido ganando en complejidad, sigilo y focalización y especialización en los objetivos, siendo, por tanto, más compleja su resolución (la dificultad en hacer frente a amenazas como rootkits, troyanos, ataques dirigidos, denegaciones de servicios distribuidas -DDoS- o las botnets, es mucho mayor que las amenazas evidentes como el Spam, phishing, virus, gusanos, adware, etc.).

EL panorama descrito obliga a las organizaciones, bien sean públicas, o privadas, a realizar un esfuerzo adicional en preservar la seguridad de sus sistemas y responder a estos nuevos riesgos e incidentes. una preservación que requiere de una política de seguridad integral y, especialmente, del desarrollo de unos servicios y capacidades operativas específicas en materia de operación y respuesta ante incidentes de seguridad.[73]

De este modo, en los últimos años, se han venido desarrollando estructuras orientadas a la operación y gestión de incidentes de seguridad llamados CERT (Computer Emergencia Response Team) o CSIRT (Computer Security Incident Response Team), como solución más adecuada para dar una respuesta eficaz y eficiente a estos nuevos riesgos.[74]

---

[73] CENTRO CRIPTOLOGICO NACIONAL. GUÍA DE SEGURIDAD (CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. España: CONPES. 2011. p. 6. Sin Clasificar. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

[74] Ibid. p. 6

5 DISEÑO METODOLÓGICO

Para lograr los objetivos delineados en el presente documento, se han definido etapas específicas para la integración de herramientas de software libre, con el propósito de consolidar tecnológicamente un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). La finalidad primordial de esta iniciativa es salvaguardar y proporcionar atención eficiente ante cualquier irregularidad informática que pueda impactar los servicios de la organización.

Este proceso de implementación se fundamenta en la adopción de una metodología de investigación aplicada, orientada a la identificación y mitigación proactiva de amenazas y vulnerabilidades. La elección de herramientas de software libre se alinea con la premisa de fomentar la accesibilidad, flexibilidad y transparencia en la gestión de la seguridad de la información.

Las etapas delineadas abarcan desde la evaluación exhaustiva de las necesidades de seguridad específicas de la organización hasta la selección, configuración e integración de las herramientas de software libre pertinentes. Este enfoque sistemático busca no solo fortalecer la infraestructura de seguridad, sino también optimizar la capacidad de respuesta del CSIRT frente a incidentes, garantizando así la continuidad y la integridad de los servicios críticos de la entidad.

Esto se realiza mediante un conjunto de herramientas previamente articuladas, la cual tienen la función de mitigar daños provocados por incidentes informáticos a los sistemas de información; debido a que las amenazas, estrategias y las herramientas que utilizan los ciber atacantes cada vez son mayores y más sofisticadas.

Para este propósito, se requiere un equipo de profesionales especializados en ciberseguridad, cuya función será supervisar y analizar la actividad en la infraestructura de hardware y software de la organización. Este equipo estará encargado de realizar una respuesta oportuna y proporcionar soporte para la recuperación de servicios informáticos, en línea con la RESOLUCIÓN NÚMERO 00500. El objetivo es llevar a cabo actividades preventivas para evitar la ocurrencia de incidentes.

Posteriormente, se investigan las herramientas de código abierto (open source), que son las más preferibles debido a su accesibilidad al público. Estas herramientas permiten la modificación de su código fuente, lo que las hace más económicas, flexibles y duraderas en comparación con las soluciones propietarias. Además, al ser desarrolladas por comunidades, en lugar de depender de una única empresa o

autor, fomentan la colaboración y el establecimiento de estándares compartidos, facilitando así su adopción y evolución continua.[75]

Después de esta fase, se procede con la configuración de un entorno, que en el caso de este proyecto puede ser un entorno de virtualización. En este entorno, se añadirán gradualmente herramientas de detección, gestión de alertas y eventos, y se guardarán los progresos en un repositorio como GitHub u otro similar. También se emplearán herramientas de monitorización, como contenedores Docker, y motores de análisis que ofrecen una amplia gama de analizadores para diferentes amenazas. Además, se aplicarán herramientas de IOC (Indicators of Compromise) para compartir información sobre determinados tipos de malware. Se llevarán a cabo pruebas en un entorno controlado, incluyendo pruebas de penetración, evaluación de vulnerabilidades y verificaciones de compilaciones. Además, se realizará la caza de amenazas de Ciber inteligencia para identificar y mitigar posibles riesgos.[76]

Una vez obtenidos los resultados de la máquina y las herramientas, empezar a generar informes sobre lo que nos arrojaron las herramientas para tomar determinaciones sobre lo que hay que mejorar o eliminar según sea su caso.

---

[75] REDHAT. ¿Qué es el open source?(CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. RedHat. 24 ictubre 2019. Disponible en: https://www.redhat.com/es/topics/open-source/what-is-open-source

[76] CORRAL, Yolanda. Construye y gestiona un SOC con herramientas Open Source. [En Línea]. YolandaCorral. 12 octubre 2020. Disponible en: https://www.yolandacorral.com/construye-y-gestiona-un-soc-con-herramientas-open-source/

6 EXAMINAR DOCUMENTACIÓN DE HERRAMIENTAS DE SEGURIDAD INFORMÁTICA PARA IMPLEMENTAR UN CSIRT

En el contexto de la seguridad informática, la exploración de herramientas de software libre juega un papel fundamental en la identificación y evaluación de soluciones que pueden ser utilizadas en diversas actividades, como la detección de amenazas, la gestión de incidentes y la monitorización de la seguridad.[77]

En base a lo anterior, se abordará la tarea de seleccionar herramientas adecuadas para conformar un CSIRT completo y funcional para diferentes organizaciones. Este proceso implica realizar un análisis y comparar una variedad de herramientas disponibles en el mercado de software libre, teniendo en cuenta diferentes áreas de funcionalidad clave, que incluyen análisis de datos, detección de amenazas, monitorización, gestión de incidentes, automatización de respuestas e intercambio de inteligencia de amenazas.

Para garantizar la efectividad y la eficiencia del CSIRT, es esencial seleccionar herramientas que puedan integrarse de manera cohesiva y complementarse entre sí, permitiendo una colaboración fluida entre los miembros del equipo y una respuesta ágil y eficaz ante incidentes de seguridad cibernética.

A continuación, se explorarán diferentes categorías de herramientas, junto con criterios de evaluación relevantes, con el objetivo de guiar la selección de las herramientas más adecuadas de acuerdo a sus bondades para la integración y conformación de un Centro de Respuestas a Incidentes Informatícos (CSIRT).

En esta exploración, se busca identificar y analizar herramientas de código abierto que sean robustas, flexibles y adecuadas para satisfacer las necesidades específicas de un centro de respuesta a incidentes informáticos (CSIRT, por sus siglas en inglés). Este proceso implica revisar la documentación disponible de algunas herramientas, que puedan ser usadas en las actividades de un centro de respuestas a incidentes informáticos.[78]

En el proceso se examinaron diversas herramientas, entre las cuales destaca la suite ELK (Elasticsearch, Logstash, Kibana). Este análisis permitió evaluar cómo estas herramientas pueden integrarse y ser utilizadas eficazmente para gestionar y responder a incidentes informáticos. A continuación, se presenta una descripción detallada de cada componente de la suite ELK y su relevancia en el contexto de un CSIRT:

---

[77] Elastic. Logstash Reference Documentation. [En Línea]. 2024. Elastic. Disponible en: https://www.elastic.co/guide/en/logstash/current/index.html.
[78] Ibid.

Elasticsearch:

Elasticsearch es una poderosa herramienta de búsqueda y análisis de datos distribuida y de código abierto, construida sobre Apache Lucene. Es diseñada para manejar grandes volúmenes de datos de manera eficiente y proporciona capacidades avanzadas de búsqueda y análisis en tiempo real.[79]

- Es un motor de búsqueda y análisis distribuido basado en Lucene, diseñado para grandes volúmenes de datos y búsqueda en tiempo real.

- Utiliza un modelo de índice invertido para permitir búsquedas rápidas y eficientes en grandes conjuntos de datos.

- Ofrece capacidades avanzadas de análisis de texto, incluyendo análisis de lenguaje natural, tokenización, filtrado y análisis de relevancia.

- Permite la indexación de datos estructurados y no estructurados, como registros de eventos, documentos JSON, datos geoespaciales, etc.[80]

- Proporciona APIs RESTful para interactuar con los datos, realizar consultas y administrar el clúster.[81]

Escalabilidad Horizontal:

La escalabilidad horizontal de Elasticsearch es una de sus características más destacadas. Permite que el sistema maneje eficientemente grandes volúmenes de datos al distribuir la carga de trabajo entre múltiples nodos en un clúster.

Esto significa que a medida que crece el tamaño de los datos o aumenta la carga de trabajo, simplemente se pueden agregar más nodos al clúster para mantener un rendimiento óptimo.

Esta capacidad de escalar horizontalmente garantiza que Elasticsearch pueda manejar conjuntos de datos masivos y seguir siendo altamente disponible incluso en entornos de alto tráfico.[82]

Velocidad y Eficiencia:

---

[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] Ibid.

El motor de búsqueda de Elasticsearch, basado en Lucene, es conocido por su velocidad y eficiencia. Lucene es altamente optimizado y utiliza técnicas avanzadas de indexación y búsqueda para garantizar tiempos de respuesta rápidos incluso en entornos con grandes volúmenes de datos.

Esto significa que Elasticsearch puede realizar búsquedas complejas en grandes conjuntos de datos de manera eficiente, lo que resulta en una experiencia de usuario más rápida y receptiva.

Funcionalidades de Búsqueda Avanzada:

Elasticsearch proporciona una amplia gama de funcionalidades de búsqueda avanzada que van más allá de la simple búsqueda de texto. Además de las búsquedas de texto completo, Elasticsearch admite búsquedas geoespaciales, que permiten buscar datos basados en su ubicación geográfica.

También ofrece búsqueda de facetas, que permite refinar los resultados de búsqueda mediante la aplicación de filtros a los datos. Otras funcionalidades incluyen autocompletado, resaltado de sintaxis y búsqueda fonética, lo que proporciona una experiencia de búsqueda más intuitiva y precisa para los usuarios.

Análisis en Tiempo Real:

La capacidad de Elasticsearch para realizar análisis en tiempo real es fundamental en aplicaciones que requieren monitoreo continuo, detección de anomalías y generación de informes en tiempo real. Elasticsearch puede analizar datos a medida que llegan, lo que permite detectar patrones emergentes, identificar tendencias y alertar sobre eventos importantes en tiempo real.

Esto es especialmente útil en aplicaciones como la monitorización de infraestructuras, la seguridad de la red y el análisis de datos de transacciones financieras.[83]

Ecosistema Extensivo:

El ecosistema de Elasticsearch es rico y diverso, lo que amplía aún más su funcionalidad y flexibilidad. Herramientas como Kibana proporcionan capacidades avanzadas de visualización de datos, permitiendo crear gráficos, tableros y mapas interactivos para analizar y compartir datos. Logstash se utiliza para la ingestión de datos, permitiendo la recopilación, transformación y enriquecimiento de datos antes de ser indexados en Elasticsearch. Beats es una familia de agentes ligeros que se utilizan para enviar datos desde diferentes fuentes a Elasticsearch de manera

[83] Ibid.

eficiente. Este ecosistema extenso y en constante crecimiento hace que Elasticsearch sea una opción atractiva para una variedad de casos de uso y aplicaciones.

En conjunto, estas bondades hacen de Elasticsearch una herramienta versátil y poderosa para el almacenamiento, búsqueda, análisis y visualización de datos a escala. Su capacidad para escalar horizontalmente, su velocidad y eficiencia, sus funcionalidades avanzadas de búsqueda, su análisis en tiempo real y su ecosistema extenso la convierten en una opción popular tanto para empresas como para desarrolladores que buscan una solución robusta para sus necesidades de datos.[84]

Logstash

Esta es una herramienta central en la arquitectura ELK (Elasticsearch, Logstash, Kibana), diseñada para gestionar de forma eficiente la ingestión, transformación y enriquecimiento de datos en entornos empresariales y de TI. Su robusta arquitectura y su conjunto de características avanzadas la convierten en una opción preferida para la recopilación y procesamiento de datos a gran escala.[85]

Escalabilidad y Eficiencia:

Logstash está diseñado para escalar horizontalmente, lo que permite distribuir la carga de trabajo entre múltiples nodos para manejar grandes volúmenes de datos de manera eficiente. Su arquitectura distribuida aprovecha la capacidad de procesamiento y almacenamiento de cada nodo, garantizando un rendimiento óptimo incluso en entornos de alta demanda.

Soporte Integral de Fuentes de Datos:

Logstash ofrece una amplia variedad de conectores y plugins para integrarse con diferentes fuentes de datos. Desde archivos de registro y flujos de eventos hasta bases de datos y servicios web, Logstash es capaz de recopilar datos de prácticamente cualquier fuente y formato, proporcionando una flexibilidad excepcional para adaptarse a los requisitos específicos de cada entorno.[86]

Funcionalidades Avanzadas de Procesamiento:

La flexibilidad de Logstash se extiende a sus capacidades de procesamiento de datos, impulsadas por una extensa biblioteca de plugins. Estos plugins permiten

---

[84] Ibid.
[85] Elastic. Logstash Reference Documentation. [En Línea]. 2024. Elastic. Disponible en: https://www.elastic.co/guide/en/logstash/current/index.html.
[86] Ibid

realizar una variedad de operaciones, como análisis de patrones, filtrado de datos, normalización, enriquecimiento y transformación de datos, garantizando la calidad y coherencia de los datos antes de ser indexados en Elasticsearch.[87]

Integración con el Ecosistema ELK:

Como parte del ecosistema ELK, Logstash se integra estrechamente con Elasticsearch y Kibana para proporcionar una solución completa de análisis de datos. Esta integración permite a los usuarios construir flujos de trabajo completos de ingestión, procesamiento y visualización de datos, simplificando la implementación y la gestión de soluciones de análisis de datos a gran escala.

En resumen, Logstash es una herramienta esencial en la arquitectura ELK, proporcionando capacidades avanzadas de ingestión y procesamiento de datos para entornos empresariales y de TI. Su capacidad de escalar horizontalmente, su amplio soporte de fuentes de datos y sus funcionalidades avanzadas la convierten en una opción robusta y versátil para una variedad de aplicaciones y casos de uso en entornos empresariales y de TI.[88]

Kibana:

Kibana es una plataforma de visualización y análisis de datos diseñada para trabajar en conjunto con Elasticsearch en la arquitectura ELK (Elasticsearch, Logstash, Kibana). Ofrece una amplia gama de herramientas y funcionalidades para explorar, visualizar y analizar datos almacenados en Elasticsearch, proporcionando insights valiosos para la toma de decisiones en entornos empresariales y de TI.[89]

Exploración y Visualización de Datos:

Kibana permite a los usuarios explorar datos de manera intuitiva a través de una interfaz gráfica fácil de usar. Ofrece una variedad de opciones de visualización, incluyendo gráficos, tablas, mapas y diagramas de dispersión, que pueden ser personalizados y configurados según las necesidades específicas del usuario. Esto permite una comprensión rápida y completa de los datos, facilitando la identificación de patrones, tendencias y anomalías.[90]

---

[87] Ibid
[88] Ibid
[89]Elastic. Kibana Reference Documentation. [En Línea]. 2024. Elastic. Disponible en: https://www.elastic.co/guide/en/kibana/current/index.html.
[90] Ibid

Dashboarding y Reporting:

Una de las características más destacadas de Kibana es su capacidad para crear dashboards interactivos y completos, que permiten combinar múltiples visualizaciones en una sola pantalla. Estos dashboards pueden ser compartidos y colaborados entre diferentes usuarios, lo que facilita la comunicación y la toma de decisiones basada en datos dentro de la organización. Además, Kibana ofrece capacidades de reporting para generar informes personalizados y detallados sobre los datos analizados.[91]

Análisis Avanzado de Datos:

Kibana proporciona herramientas avanzadas de análisis de datos que permiten a los usuarios realizar operaciones complejas como agregaciones, filtros, métricas y cálculos de tiempo en sus conjuntos de datos. Esto permite un análisis profundo y detallado de los datos, lo que lleva a insights más significativos y acciones informadas.[92]

Integración con Elasticsearch y Logstash:

Como parte integral del ecosistema ELK, Kibana se integra estrechamente con Elasticsearch y Logstash para proporcionar una solución completa de análisis de datos. Esto permite a los usuarios construir flujos de trabajo completos de ingestión, procesamiento, análisis y visualización de datos, simplificando la implementación y la gestión de soluciones de análisis de datos a gran escala.

En resumen, Kibana es una plataforma potente y versátil para la visualización y análisis de datos, que proporciona herramientas avanzadas para explorar, analizar y comprender datos almacenados en Elasticsearch. Su facilidad de uso, capacidades avanzadas de visualización y análisis, y su integración con el ecosistema ELK la convierten en una opción ideal para una variedad de aplicaciones y casos de uso en entornos empresariales y de TI.[93]

[91] Ibid
[92] Ibid
[93] Ibid

Compatibilidad e Integración:

ELK es altamente compatible con una amplia gama de sistemas y tecnologías, incluyendo sistemas operativos, bases de datos, servidores web, dispositivos de red, etc.[94]

Ofrece integración con herramientas de terceros a través de APIs y conectores específicos, permitiendo la ingestión y análisis de datos desde diferentes fuentes.[95]

Análisis de la Comunidad y Soporte:

ELK cuenta con una comunidad activa de usuarios y desarrolladores que contribuyen con el desarrollo, soporte y mejora continua de las herramientas.[96]

Dispone de foros de discusión, listas de correo, canales de chat y repositorios de código abierto donde los usuarios pueden solicitar ayuda, compartir conocimientos y colaborar en proyectos.[97]

Evaluación de la Seguridad y Fiabilidad:

Elasticsearch, Logstash y Kibana implementan características de seguridad avanzadas, como autenticación, autorización, cifrado de datos y auditoría de acceso.[98]

Se someten regularmente a pruebas de seguridad y se publican actualizaciones y parches para abordar posibles vulnerabilidades y problemas de seguridad.[99]

Licencia:

ELK es de código abierto y está disponible bajo la licencia Apache 2.0, lo que significa que puede ser utilizado, modificado y distribuido libremente sin costo alguno.[100]

---

[94] Elastic. Características del Elastic Stack. [En Línea]. 2024. Elastic. Disponible en: https://www.elastic.co/es/elastic-stack/features
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Elastic. "Seguridad en Elastic Stack". [En línea]. 2023. Elastic. Disponible en: https://www.elastic.co/es/elastic-stack/security.
[99] Ibid.
[100] Elastic. " Presentación de la licencia Elastic v2, simplificada y más permisiva; SSPL sigue siendo una opción". [En línea]. 2024. Elastic. Disponible en: https://www.elastic.co/es/blog/elastic-license-v2

Sin embargo, se ha implementado una nueva licencia, se resume en la migración del código fuente de Elasticsearch y Kibana de la licencia Apache 2.0 a una licencia dual bajo la licencia SSPL 1.0. y la Licencia v2, una versión simplificada y permisiva, que incluye un alto nivel y se aplica a todas las características gratuitas y pagas de Elasticsearch y Kibana.[101]

Sin embargo, es importante considerar los costos asociados con el mantenimiento, la infraestructura y el soporte técnico necesarios para implementar y operar una solución ELK a escala empresarial.[102]

Requisitos técnicos:

Hardware:
Memoria RAM: Recomendado al menos 8 GB para Elasticsearch y Kibana.
Almacenamiento: Disco SSD recomendado para un mejor rendimiento.[103]

Procesador: Depende del volumen de datos y la carga de trabajo, pero se recomienda un procesador multicore.[104]

Sistema Operativo:
Linux: Ubuntu, CentOS, Red Hat Enterprise Linux (RHEL), Debian.
Windows: Server 2012 o posterior.[105]

Java Development Kit (JDK):
Elasticsearch y Kibana requieren Java 8 o superior.
Logstash requiere Java 11 o superior.[106]

Red:
Puertos abiertos: Elasticsearch utiliza el puerto 9200 (HTTP) y 9300 (transporte), Kibana utiliza el puerto 5601 (HTTP), Configuración de firewall para permitir el tráfico en los puertos necesarios.[107]

---

[101] Ibid.
[102] Ibid.
[103]Elastic. "Set up Elasticsearch". [En línea]. 2024. Elastic. Disponible en: https://www.elastic.co/guide/en/elasticsearch/reference/current/setup.html
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Ibid.

De acuerdo con el análisis de la documentación proporcionada por Elasticsearch, Logstash y Kibana (ELK), se lleva a cabo la exploración de las herramientas de software libre para fortalecer el Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT). Este análisis detallado busca identificar la solución e integración óptima que ofrezca capacidades avanzadas de detección de amenazas y monitorización, así como una integración perfecta con el ecosistema ELK, la herramienta Wazuh es una de las candidatas mediante las características técnicas que podemos analizar a continuación:

Evaluación de Bondades y Beneficios de Wazuh:

Wazuh se destaca como una solución de seguridad cibernética de vanguardia que ofrece una amplia gama de capacidades avanzadas para la detección de amenazas y la monitorización de la seguridad. Entre sus bondades más destacadas se encuentran:

Detección de Amenazas Avanzadas:

Wazuh cuenta con un conjunto de reglas de detección avanzadas que permiten identificar una variedad de amenazas cibernéticas, desde malware y intrusiones de red hasta comportamientos sospechosos y vulnerabilidades.[108]

Monitorización Continua en Tiempo Real:

La capacidad de Wazuh para proporcionar una monitorización continua en tiempo real de logs, archivos críticos del sistema y tráfico de red permite una detección proactiva de amenazas y una respuesta rápida ante incidentes de seguridad.[109]

Integración Perfecta con ELK:

Wazuh se integra de forma nativa con Elasticsearch, Logstash y Kibana, lo que facilita la indexación eficiente de datos, el procesamiento enriquecido y la visualización detallada de la información de seguridad. Esta integración proporciona al CSIRT una visión holística y coherente de la postura de seguridad de la organización.[110]

Especificaciones Técnicas de Wazuh:

---

[108] "Detecting Exploitation of xz-utils Vulnerability (CVE-2024-3094) with Wazuh". [En línea]. Wazuh Blog. Disponible en: https://wazuh.com/blog/detecting-exploitation-of-xz-utils-vulnerability-cve-2024-3094-with-wazuh/.
[109] Ibid.
[110] Ibid

Para garantizar una implementación exitosa y un rendimiento óptimo de Wazuh, se deben considerar las siguientes especificaciones técnicas:

Requisitos de Hardware: Se recomienda un servidor con al menos 2 núcleos de CPU y 4 GB de RAM para el servidor principal de Wazuh. Para nodos adicionales, se debe asignar al menos 2 GB de RAM por nodo.

Almacenamiento: Se recomienda un mínimo de 50 GB de espacio disponible en disco para almacenar logs, archivos de configuración y datos procesados.

Conectividad de Red: Se requiere una conexión de red estable y de alta velocidad para permitir la comunicación fluida entre los componentes de Wazuh y otros sistemas de seguridad en la red.

7 ANÁLISIS DE LAS HERRAMIENTAS DE SOFTWARE LIBRE UTILIZADAS EN UN CSIRT

De acuerdo con las funciones del actuar de un CSIRT, como son sus servicios reactivos (Alertas, gestión de incidentes, gestión de vulnerabilidades, gestión de artefactos) otros tipos de servicios son proactivos (Boletines, vigilancia tecnológica, auditorias de seguridad, entre otros).[111]

Para visualizar la información y realizar un análisis de los datos, encontramos diferentes herramientas destacando sus ventajas y desventajas en la siguiente tabla:

Tabla 2 Herramientas Análisis de datos

Herramientas	Ventajas	Desventajas
Splunk	Motor de indexación y búsqueda con arquitectura distribuida que garantiza un rendimiento escalable. Permite la integración de datos de múltiples fuentes en tiempo real.	Costo significativo de licenciamiento, especialmente para implementaciones a gran escala. Requiere una infraestructura robusta para un rendimiento óptimo, lo que puede aumentar los costos operativos.

[111] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES, Servicios CSIRT Gobierno. [En Línea]. COLCERT. 26 julio 2022. Disponible en: https://colcert.gov.co/800/w3-article-208774.html#:~:text=El%20objetivo%20principal%20del%20CSIRT%20Gobierno%2C%20es%20ofrecer,todos%20los%20funcionarios%20y%20encargados%20de%20seguridad%20digital

	Ofrece un lenguaje de consulta flexible para realizar análisis complejos. Soporte para la correlación de eventos y la detección de anomalías en tiempo real. Amigable interfaz de usuario con capacidades avanzadas de visualización.[112]	Consumo de recursos considerable, especialmente en entornos de alto volumen de datos. Curva de aprendizaje pronunciada para aprovechar todas sus capacidades.[113]
Apache Solr	Motor de búsqueda de texto completo basado en Lucene, que ofrece un rendimiento excepcional en búsquedas y consultas complejas. Arquitectura flexible y altamente escalable, adecuada para grandes volúmenes de datos. Extensa API y soporte para la integración con diversas tecnologías y formatos de datos. Capacidad de personalización y extensibilidad mediante complementos y configuraciones avanzadas.[114]	Configuración inicial compleja, especialmente para usuarios sin experiencia en motores de búsqueda o Apache Lucene. Gestión de infraestructura requerida para mantener el rendimiento en entornos de producción a gran escala. Documentación y soporte a veces limitados, dependiendo de la comunidad y el ecosistema de desarrollo.[115]
Sphinx	Motor de búsqueda de texto completo altamente eficiente y de bajo consumo de recursos.	Conjunto de características menos amplio en comparación con algunas soluciones comerciales, especialmente en términos de análisis avanzado.

[112] JAYMON SECURITY. SPLUNK: El SIEM para e control definitivo. [En Línea] 2022. Disponible en: https://jaymonsecurity.com/splunk-un-siem-para-controlarlos-a-todos/
SOLR TUTORIAL. Qué es Solr. [En Línea]. 2022. Disponible en: https://solrtutorial.es/que-es-solr.html
[113] Splunk En Línea] 2022. Disponible en: https://www.splunk.com/
[114] SOLR TUTORIAL. Qué es Solr. [En Línea]. 2022. Disponible en: https://solrtutorial.es/que-es-solr.html
[115] SOLR En Línea] 2022. Disponible en: https://solr.apache.org/

	Rápido tiempo de respuesta incluso con grandes conjuntos de datos, adecuado para aplicaciones con limitaciones de hardware. Soporte para búsqueda en tiempo real y capacidades de indexación distribuida. Integración con varias bases de datos y formatos de datos.[116]	Curva de aprendizaje empinada para usuarios nuevos en motores de búsqueda o Sphinx en particular. Soporte y documentación limitados en comparación con herramientas más populares y bien establecidas.[117]
Elasticsearch	Motor de búsqueda distribuido altamente escalable diseñado para manejar grandes volúmenes de datos en tiempo real. Arquitectura flexible y modular que permite una fácil integración con otras herramientas y tecnologías. Potente lenguaje de consulta para realizar análisis avanzados y búsqueda en tiempo real. Compatibilidad con una amplia gama de lenguajes de programación y bibliotecas de cliente.[118]	Configuración inicial y ajuste requieren conocimientos avanzados de infraestructura y administración de sistemas. La gestión de clústeres y nodos puede ser compleja y requerir una atención cuidadosa para evitar problemas de rendimiento y disponibilidad. Dependencia de herramientas adicionales para ciertas funcionalidades, lo que puede aumentar la complejidad y los costos.[119]
Kibana	Interfaz de usuario intuitiva y atractiva diseñada específicamente para la visualización y análisis de datos.	Dependencia de Elasticsearch como backend, lo que significa que cualquier limitación o problema en Elasticsearch puede afectar la funcionalidad de Kibana.

[116] REPUBLICA. Sphinx, motor de búsqueda de texto Opensource. [En Línea]. 24 JULIO 2007. Disponible en: https://www.republica.com/gizmos/sphinx-motor-de-busqueda-de-texto-opensource-20070724-14061523187/

[117] Sphinx En Línea] 2022. Disponible en: https://sphinxsearch.com/

[118] ELASTIC. El corazón del Elastic Stack, gratuito y abierto. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/elasticsearch/

[119] ELASTIC En Línea] 2022. Disponible en: https://www.elastic.co/es/elasticsearch

	Integración perfecta con Elasticsearch para aprovechar su potencia de búsqueda y análisis. Personalización flexible de paneles y visualizaciones para adaptarse a los requisitos del usuario. Amplia gama de complementos y conectores para integrarse con diversas fuentes de datos.[120]	Requiere conocimientos técnicos para configurar correctamente la integración con Elasticsearch y otras fuentes de datos. No es una solución independiente para análisis de datos, sino que requiere una infraestructura complementaria para funcionar.[121]

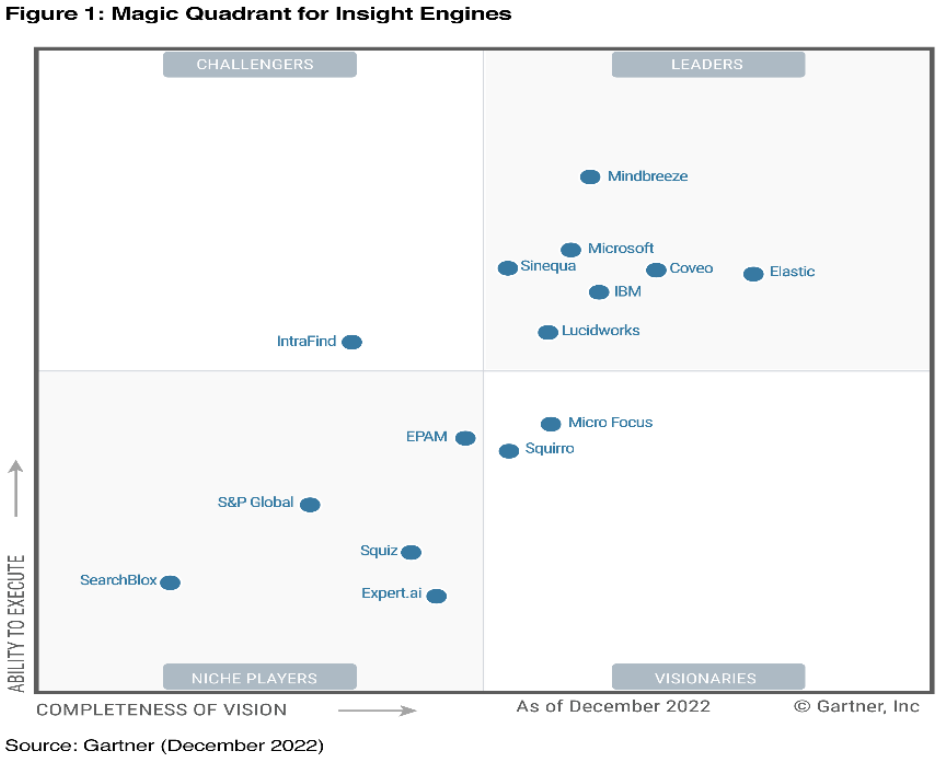
Fuente: ELASTIC. El corazón del Elastic Stack, gratuito y abierto. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/elasticsearch/

La elección de la herramienta adecuada para análisis de logs y búsqueda de texto es fundamental para garantizar la eficacia y eficiencia de las operaciones en entornos empresariales modernos. En este sentido, Elasticsearch emerge como la opción más sólida y versátil debido a una serie de características técnicas y funcionales excepcionales que la distinguen dentro del panorama de herramientas disponibles mediante el siguiente análisis del Cuadrante de Gartner:

[120] ELASTIC. Tu ventana al Elastic Stack. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/kibana/

[121] KIBANA En Línea] 2022. Disponible en: https://www.elastic.co/es/kibana

Figura 5 Cuadrante de Gartner Elasticsearch



Fuente: ELASTIC. Elastic reconocido como Líder en el Magic Quadrant™ de Gartner® 2022 de motores de información. [En Línea]. 2022. Disponible en: (https://www.elastic.co/es/explore/improving-digital-customer-experiences/gartner-magic-quadrant-for-insight-engines-report).

En la Figura 5, se ilustra claramente el posicionamiento de Elastic en el Cuadrante Mágico de Gartner como líder en el ámbito de búsqueda y análisis. Este destacado posicionamiento es el resultado de la conjunción efectiva entre la visión estratégica de Elastic y su excepcional capacidad de ejecución.

La visión estratégica de Elastic, delineada con agudeza, demuestra una comprensión profunda de las dinámicas del mercado y la anticipación proactiva de las tendencias emergentes. Este enfoque estratégico ha permitido a Elastic formular y ejecutar iniciativas que responden de manera precisa a las cambiantes demandas del panorama de búsqueda y análisis.

La capacidad de ejecución de Elastic, destaca su habilidad para implementar de manera precisa y eficiente las estrategias establecidas. Este nivel de ejecución refleja la eficacia operativa de Elastic y su capacidad para ofrecer soluciones avanzadas que cumplen con los más altos estándares del mercado.

Este destacado posicionamiento en el cuadrante de líderes también subraya el compromiso continuo de Elastic con la innovación. Se refleja la introducción exitosa de funcionalidades disruptivas y la adopción proactiva de tecnologías emergentes, impulsando así la excelencia y la relevancia constante de sus soluciones.

De acuerdo con las herramientas indagadas y el ranking en la utilización en gestor de bases de datos la herramienta Elasticsearch y Kibana, son compatibles con expresiones de búsquedas complejas, realiza búsqueda de texto completo, reduce palabras flexionadas, búsqueda distribuida para grandes escalas, es compatible con diferentes lenguajes de programación, la tendencia en su implementación es superior a las herramientas Solr, Splunk, Sphinx, por otra parte; Elasticsearch cuenta con comunidad de contribución por clientes a mejoras de la aplicación.[122]

Mediante la implementación y articulación de Kibana y Elasticsearch nos ayudara a monitorear las redes de comunicación, seguridad perimetral, como son los firewalls, servidores, puestos de trabajos, ERP, bases de datos etc.

Debido a que su frontend es muy amigable para el usuario final o responsable, encargado que supervisa todos los procesos, alertas, anomalías o amenazas que pueden presentarse en las infraestructuras de la organización.

Sin perder su estrategia lo cual es ser proactivo, preventivo, reactivo y correctivo, ya que cualquier ataque, amenaza o incidente de seguridad, después de ser identificado debe ser analizado y corregido, para luego aplicar mejoras para que no se repita el suceso.

- **Herramientas análisis de Logs**

En la conformación del CSIRT, se debe contar con herramientas para el análisis de logs, para la identificación, registro de los eventos y acciones que pueden afectar algún servicio de la organización, a continuación, encontramos Un análisis comparativo realizado mediante la documentación de cada herramienta; en cual se encuentran las diversas ventajas y desventajas entre Loggly, PaperTrail y Logstash

Tabla 3 Ventajas y Desventajas Herramientas Análisis de Logs

Ventajas			
Aspecto	**Loggly**	**PaperTrail**	**Logstash**
Escalabilidad	Alta escalabilidad, capacidad para manejar grandes	Buena capacidad para manejar cargas de trabajo medianas, aunque puede enfrentar	Excelente capacidad de escalabilidad horizontal puede adaptarse a demandas

[122] DB-Engines. Knowledge Base of Relational and NoSQL Database Management Systems. [En Línea] .2022 Disponible en https://db-engines.com/en/ranking/search+engine

	volúmenes de logs con eficiencia.[123]	limitaciones con volúmenes muy altos.[124]	crecientes sin problemas.[125]
Facilidad de Uso	Interfaz intuitiva y fácil de usar, adecuada tanto para usuarios principiantes como avanzados.[126]	Interfaz limpia y simple, aunque no tan avanzada en términos de funcionalidad como otras opciones.[127]	Requiere configuración inicial y conocimiento técnico para aprovechar al máximo todas sus capacidades, pero ofrece un gran potencial una vez configurado correctamente.[128]
Integraciones	Amplia gama de integraciones con herramientas y servicios populares, facilitando la interoperabilidad.[129]	Integraciones limitadas en comparación con otras herramientas, lo que puede requerir soluciones personalizadas para ciertos casos de uso.[130]	Puede integrarse con una variedad de sistemas y servicios mediante plugins, lo que permite una integración más completa y personalizable.
Análisis en tiempo real	Soporta análisis en tiempo real de logs, proporcionando información instantánea sobre el estado del sistema.[131]	Funcionalidad de análisis en tiempo real no tan robusta como otras opciones, lo que puede limitar la capacidad de respuesta ante	La comunidad y la documentación extensa son las principales fuentes de soporte, aunque no hay un soporte dedicado

[123]Loggy. [En Línea]. Disponible en: https://documentation.solarwinds.com/en/success_center/loggly/content/loggly_documentation.htm
[124]PaperTrail. [En Línea]. Disponible en: https://www.papertrail.com/help/papertrail-documentation/
[125] Logstash [En Línea]. Disponible en: https://www.elastic.co/es/kibana
[126] Ibid Loggy
[127] Ibid PaperTrail
[128] Ibid Logstash
[129] Ibid Loggy
[130] Ibid. Paper Trail
[131] Ibib. Loggly

		incidentes críticos.[132]	proporcionado por el proveedor.[133]
Desventajas			
Costo	Los planes de precios pueden resultar costosos para grandes volúmenes de logs, lo que puede ser prohibitivo para algunas organizaciones.[134]	Algunas características avanzadas pueden estar disponibles solo en planes de precios más altos, lo que puede aumentar significativamente los costos.[135]	La implementación y el mantenimiento pueden ser costosos en términos de recursos de infraestructura y tiempo, especialmente a medida que crece la escala de despliegue.[136]
Retención de logs	La retención de logs puede estar limitada en los planes de precios más bajos, lo que puede requerir una inversión adicional para mantener registros históricos.[137]	La retención de logs también puede ser limitada en los planes de precios más bajos, lo que puede dificultar el análisis retrospectivo de eventos.[138]	Dependiendo de la infraestructura subyacente, la retención de logs puede ser un desafío y puede requerir una gestión cuidadosa del almacenamiento.[139]
Flexibilidad	Menos opciones de personalización y configuración avanzada en comparación con otras herramientas, lo que puede limitar su adaptabilidad a casos de uso específicos.[140]	Limitado en cuanto a opciones de personalización y configuración avanzada, lo que puede requerir soluciones alternativas para requisitos específicos.[141]	Altamente flexible y configurable, pero puede requerir habilidades técnicas avanzadas para aprovechar al máximo todas sus capacidades, lo que puede representar una curva de

[132] Ibib. Paper Trail
[133] Ibid Logstash
[134] Ibid. Loggly
[135] Ibib. Paper Trail
[136] Ibid Logstash
[137] Ibid. Loggly
[138] Ibib. Paper Trail
[139] Ibid Logstash
[140] Ibid. Loggly
[141] Ibib. Paper Trail

			aprendizaje pronunciada.[142]
Dependencia de terceros	Dependiente de la infraestructura de terceros, lo que puede introducir vulnerabilidades de disponibilidad si hay interrupciones en esos servicios externos.[143]	Similar a Loggly, su funcionamiento está vinculado a servicios externos, lo que puede generar dependencias críticas para la disponibilidad del sistema.[144]	Algunas características pueden depender de servicios externos, lo que puede introducir puntos únicos de falla y complicar la gestión de la infraestructura.[145]

Fuente: Logstash “Descubre, itera y resuelve con ES|QL en Kibana” [En Línea]. 2023 Disponible en: https://www.elastic.co/es/logstash

De acuerdo con el cuadro anterior, se selecciona la herramienta Logstash como componente central en la conformación de un CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática) se fundamenta en su capacidad excepcional para recopilar, transformar y enviar datos de logs de manera eficiente y escalable. La integración de Logstash con Elasticsearch, como motor de búsqueda y análisis distribuido, fortalece aún más las capacidades del CSIRT al proporcionar una solución completa para la gestión y análisis de incidentes de seguridad.

Logstash, conocido por su flexibilidad y potencia en la manipulación de datos de logs, permite a los equipos de seguridad recopilar registros de múltiples fuentes, como sistemas, aplicaciones y dispositivos de red, y normalizarlos en un formato uniforme para su análisis. Su capacidad para procesar logs en tiempo real garantiza una detección rápida y precisa de eventos sospechosos o maliciosos, lo que es fundamental para la eficacia del CSIRT en la detección y respuesta ante amenazas cibernéticas.

Al integrar Logstash con Elasticsearch, se establece una solución integral para el CSIRT que abarca desde la recopilación y normalización de logs hasta su indexación y análisis avanzado. Elasticsearch, como un motor de búsqueda y análisis distribuido altamente escalable, proporciona capacidades avanzadas para indexar y buscar datos de logs de manera eficiente, permitiendo búsquedas rápidas y análisis profundos de eventos de seguridad.

[142] Ibid Logstash
[143] Ibid Loggly
[144] Ibib. Paper Trail
[145] Ibid Logstash

La combinación de Logstash y Elasticsearch en la conformación de un CSIRT ofrece una serie de beneficios clave. Por un lado, la integración simplifica el flujo de datos de logs al proporcionar una solución completa y coherente para su gestión y análisis. Además, la escalabilidad y flexibilidad de ambas herramientas garantizan que el CSIRT pueda adaptarse dinámicamente a las necesidades cambiantes del entorno de seguridad.

En resumen, la selección de Logstash integrado con Elasticsearch para conformar un CSIRT representa una decisión estratégica que maximiza las capacidades de detección y respuesta ante incidentes de seguridad. La combinación de recopilación de logs en tiempo real, transformación y análisis avanzado de datos de logs proporciona al CSIRT las herramientas necesarias para identificar y mitigar eficazmente las amenazas cibernéticas, fortaleciendo la seguridad de las organizaciones.

- **Escáner de Vulnerabilidad**

Las vulnerabilidades de un sistema son la puerta de entrada de un atacante, es por ello por lo que es importante las herramientas de vulnerabilidad, para identificar el tipo de filtrado de servicios, tráfico de red entre otros, de acuerdo con lo anterior encontramos un análisis detallado mediante un cuadro comparativo de cuatro destacados escáneres de vulnerabilidades: OpenVas, Vega, HIDS y Nmap. Esta comparación proporciona una visión técnica de las fortalezas y debilidades de cada herramienta, ayudando a los profesionales de seguridad a tomar decisiones en la integración de herramientas para conformar un CSIRT:

Tabla 4 Ventajas y Desventajas Escáner de Vulnerabilidad

Aspecto	OpenVAS	Vega	HIDS	Nmap
Escaneo de Red	Realiza un escaneo exhaustivo de la red para detectar vulnerabilidades conocidas y configuraciones erróneas.[146]	Capacidad para realizar escaneos de aplicaciones web en busca de vulnerabilidades comunes mediante	Monitorea continuamente el sistema en busca de comportamientos anómalos y signos de intrusión, ofreciendo una	Realiza un escaneo rápido y flexible de redes y sistemas para identificar puertos abiertos, servicios en ejecución y posibles

[146] Greenbone Networks GmbH. (s.f.). OpenVAS. [En Línea]. Disponible en: https://www.greenbone.net/en/openvas/

		ataques controlados.[147]	defensa activa.[148]	vulnerabilidades.[149]
Base de datos de vulnerabilidades	Utiliza una extensa base de datos de vulnerabilidades para identificar amenazas potenciales en sistemas y aplicaciones, actualizándose regularmente.	Se basa en bases de datos específicas de vulnerabilidades de aplicaciones web para detectar fallos de seguridad, requiriendo actualizaciones periódicas para mantenerse al día con las últimas amenazas.	Dependiendo de las firmas y comportamientos conocidos, puede detectar actividades maliciosas y anómalas, requiriendo actualizaciones frecuentes para mantenerse al día con las tácticas de los atacantes.	Utiliza una base de datos de vulnerabilidades conocidas para identificar posibles riesgos en sistemas y redes, siendo actualizada con regularidad para incluir nuevas amenazas y parches de seguridad.
Interfaz gráfica	Ofrece una interfaz gráfica de usuario (GUI) que simplifica la configuración y visualización de los resultados del escaneo, facilitando la gestión y el análisis de vulnerabilidades.	Proporciona una GUI intuitiva que permite a los usuarios interactuar visualmente con el escáner y analizar los resultados de los escaneos de aplicaciones web de manera efectiva.	Algunas soluciones HIDS pueden ofrecer interfaces gráficas para configurar y monitorizar sistemas, facilitando la gestión y la identificación de amenazas.	Principalmente una herramienta de línea de comandos, aunque existen interfaces gráficas de usuario de terceros que ofrecen funcionalidades adicionales para simplificar el uso y la interpretación de los resultados.

[147] Subgraph. (s.f.). Vega. En Línea]. Disponible en: https://subgraph.com/vega/index.en.html
[148] Tripwire. (s.f.). Host-Based Intrusion Detection System (HIDS). [En Línea]. Disponible en: https://www.tripwire.com/glossary/what-is-host-based-intrusion-detection-system-hids/
[149] Gordon Lyon. (s.f.). Nmap: The Network Mapper. [En Línea]. Disponible en: https://nmap.org/

Detecta vulnerabilidades conocidas	Capaz de identificar vulnerabilidades conocidas en sistemas y aplicaciones, permitiendo una rápida mitigación de riesgos.	Especializado en la detección de vulnerabilidades específicas de aplicaciones web, como inyecciones SQL y XSS, proporcionando una detección precisa en este ámbito.	Puede detectar comportamientos maliciosos conocidos, como intentos de acceso no autorizado o cambios no autorizados en archivos críticos, contribuyendo a la defensa proactiva del sistema.	Identifica vulnerabilidades conocidas y posibles puntos de entrada para atacantes en la red o sistemas individuales, permitiendo la evaluación exhaustiva de la seguridad de los activos de la red.
Desventajas				
Desventajas	Requiere un despliegue y configuración técnica, así como un conocimiento profundo de los sistemas y redes para una implementación eficaz.[150]	Puede no ser tan efectivo para escanear redes o sistemas enteros en comparación con otras herramientas, especialmente en entornos complejos.[151]	Puede generar falsos positivos o negativos debido a la naturaleza dinámica de las amenazas, necesitando ajustes continuos para mejorar la precisión.[152]	La información obtenida puede ser compleja y abrumadora para los usuarios menos técnicos, requiriendo conocimientos avanzados para su interpretación adecuada y la toma de decisiones.[153]

Fuente: Wireshark. 'El analizador de protocolos de red más popular del mundo'. [En Línea]. 2023. Disponible en: https://www.wireshark.org/

De acuerdo con el cuadro anterior, se selecciona la herramienta OpenVas como elemento central en la construcción de un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) se fundamenta en su capacidad para realizar análisis exhaustivos de vulnerabilidades en sistemas y redes. OpenVas, un escáner de vulnerabilidades de red permite identificar posibles puntos débiles en la infraestructura tecnológica mediante la exploración automatizada de puertos,

[150] Tenable®, Inc. (s.f.). Nessus. [En Línea]. Disponible en: https://www.tenable.com/products/nessus
[151] Acunetix. (s.f.). Acunetix. [En Línea]. Disponible en: https://www.acunetix.com/
[152] OSSEC. (s.f.). OSSEC. [En Línea]. Disponible en: https://www.ossec.net/
[153] Wireshark Foundation. (s.f.). Wireshark. [En Línea]. Disponible en: https://www.wireshark.org/

servicios y aplicaciones. Su enfoque integral en la evaluación de la seguridad proporciona al CSIRT información valiosa para la detección proactiva y la mitigación de riesgos de seguridad.

La integración de OpenVas con Elasticsearch y Logstash añade una capa adicional de funcionalidad y análisis avanzado al CSIRT. Elasticsearch, un motor de búsqueda y análisis distribuido facilita la indexación y búsqueda rápida de datos generados por OpenVas, lo que permite una identificación eficiente de vulnerabilidades y amenazas. Por su parte, Logstash se encarga de la recopilación y normalización de datos de OpenVas, asegurando que la información se ingrese de manera coherente y estandarizada en el sistema.

Esta combinación de herramientas proporciona al CSIRT una solución completa y coherente para la detección, evaluación y gestión de vulnerabilidades y amenazas cibernéticas. Además, permite una detección y respuesta más rápidas y eficientes ante incidentes de seguridad, ayudando a minimizar el impacto de posibles brechas de seguridad y proteger los activos críticos de la organización.

En resumen, la herramienta OpenVas integrada con Elasticsearch y Logstash representa una decisión estratégica que maximiza las capacidades de detección y respuesta ante incidentes de seguridad. Esta combinación de análisis exhaustivos de vulnerabilidades, indexación y búsqueda avanzada de datos, y recopilación y normalización de información proporciona al CSIRT las herramientas necesarias para identificar, evaluar y mitigar eficazmente las amenazas cibernéticas, fortaleciendo así la postura de seguridad de la organización en su conjunto.

Gestión de Incidentes:
Para las organizaciones es importante contar con una aplicación de gestión de incidentes, con el fin de realizar una clasificación, detección y análisis[154] mediante algunas de las siguientes herramientas:

Tabla 5 Herramientas Gestor de Incidentes

Aspecto	**The Hive and Cortex**	**ELK**	**PFSENSE**	**EVEBOX**
Automatización de tareas	Facilita la automatización	Capacidad para	Ofrece una amplia	Permite la visualización y

[154] THEHIVE PROYECT. THEHIVE: A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM. [En Línea]. 2023 THEHIVE. 2022. p. 1. Disponible en: https://thehive-project.org/

	de tareas de respuesta a incidentes mediante integraciones con Cortex, lo que permite ejecutar análisis y respuestas automáticas.[155]	automatizar la detección y respuesta a incidentes mediante la configuración de reglas y scripts personalizados [156]	variedad de herramientas de seguridad y firewall para proteger las redes de ataques externos.[157]	gestión de eventos de seguridad a través de una interfaz web intuitiva, facilitando la identificación y respuesta a incidentes.[158]
Escalabilidad	Escalable horizontalmente para gestionar grandes volúmenes de incidentes y datos de seguridad, con la capacidad de añadir nodos según sea necesario para mantener el rendimiento.	Escalable para manejar grandes volúmenes de logs y datos de seguridad mediante la distribución de carga y la agrupación de nodos en un clúster ELK.	Capacidad para crecer con redes de diferentes tamaños, desde pequeñas empresas hasta grandes corporaciones, adaptándose a las necesidades cambiantes de seguridad.	Capaz de manejar grandes volúmenes de eventos de seguridad de manera eficiente, lo que lo hace adecuado para entornos de red de cualquier tamaño.
Integración	Ofrece integración con una amplia gama de herramientas de seguridad y sistemas de detección de amenazas,	Integra fluidamente datos de múltiples fuentes y sistemas de seguridad, proporcionando una visión	Integra funcionalidades de firewall, VPN, proxy y otras para proporcionar una solución completa de seguridad	Puede integrarse con sistemas de detección de intrusos (IDS) y otras herramientas de seguridad para una

[155] THEHIVE PROYECT. Op. Cit. p1
[156] ELASTIC. ¿Qué es el ELK Stack?. [En Línea]. Disponible en: https://www.elastic.co/es/what-is/elk-stack
[157] PFSENSE: Sitio web oficial de pfSense. [En Línea]. Disponible en: https://www.pfsense.org/
[158] EVEBOX: Repositorio oficial de EVEBOX en GitHub. [En Línea]. Disponible en https://github.com/jasonish/evebox

	proporcionando una respuesta integral a incidentes al reunir datos de múltiples fuentes.[159]	unificada de la postura de seguridad de la organización.	para las redes, facilitando la gestión y la respuesta a incidentes.	respuesta coordinada a incidentes, mejorando la eficacia de la respuesta.
Análisis de datos	Ofrece capacidades avanzadas de análisis de datos para identificar patrones y tendencias en los incidentes de seguridad, ayudando a identificar y mitigar amenazas de manera proactiva.	ELK proporciona poderosas capacidades de análisis de datos para correlacionar eventos y detectar anomalías en tiempo real, lo que mejora la capacidad de detección de amenazas.	Ofrece informes detallados y análisis de tráfico para identificar y mitigar amenazas potenciales, proporcionando información crítica para la toma de decisiones de seguridad.	Facilita el análisis y la investigación de eventos de seguridad mediante herramientas de búsqueda y filtrado avanzadas, permitiendo una respuesta rápida y efectiva a los incidentes.
Desventajas				
Curva de aprendizaje	Puede tener una curva de aprendizaje pronunciada debido a la complejidad de la configuración y las funcionalidades avanzadas, lo que puede requerir tiempo y recursos significativos para dominar.	La configuración inicial y la gestión de un clúster ELK pueden ser complejas y requerir conocimientos técnicos especializados, lo que puede dificultar la adopción y el mantenimiento	La configuración y la gestión de las funcionalidades de seguridad pueden ser complicadas para usuarios sin experiencia en redes, lo que puede resultar en una implementaci	La falta de documentación extensa y soporte puede dificultar la implementación y el mantenimiento para usuarios menos experimentados, lo que puede afectar la eficacia de la respuesta a incidentes.

[159]The Hive and Cortex: Sitio web oficial de The Hive Project. [En Línea]. 2022. Disponible en: https://thehive-project.org/

			ón subóptima y vulnerabilidades potenciales.	
Recursos de hardware	Requiere recursos de hardware significativos, especialmente para implementaciones a gran escala con múltiples nodos y alta disponibilidad, lo que puede aumentar los costos operativos.	Necesita recursos de hardware adecuados para manejar grandes volúmenes de datos, lo que puede requerir inversiones significativas en infraestructura, almacenamiento y procesamiento.	La implementación en hardware físico puede requerir inversiones adicionales en equipos y licencias comerciales, lo que puede aumentar los costos de capital y de mantenimiento.	La gestión de recursos de hardware puede ser un desafío, especialmente en entornos con restricciones de presupuesto y recursos, lo que puede limitar la escalabilidad y el rendimiento

Fuente: THEHIVE PROYECT. THEHIVE: A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM. [En Línea]. 2023 THEHIVE. 2022. p. 1. Disponible en: https://thehive-project.org/

En base al análisis del cuadro comparativo, la selección de The Hive y ELK para conformar un CSIRT se basa en la complementariedad y las fortalezas individuales de cada herramienta. The Hive proporciona una plataforma integral para la gestión y automatización de respuestas a incidentes de seguridad, mientras que ELK (Elasticsearch, Logstash, Kibana) ofrece un conjunto completo de herramientas para la recopilación, almacenamiento, visualización y análisis de datos de logs. Al combinar estas dos herramientas, se crea un sistema robusto que aborda tanto la gestión de incidentes como la detección y análisis de amenazas, proporcionando una solución completa para las necesidades del CSIRT.

La integración y flexibilidad son aspectos clave en la selección de estas herramientas. Ambas son altamente integrables, lo que permite su conexión con otras herramientas de seguridad y sistemas utilizados por el CSIRT. The Hive se conecta fácilmente con herramientas de seguridad y sistemas de gestión de incidentes, mientras que ELK ofrece integraciones con una amplia gama de herramientas de seguridad y sistemas de almacenamiento. Esta interoperabilidad facilita una colaboración efectiva entre diferentes equipos y sistemas de seguridad, asegurando una respuesta coordinada y eficiente ante incidentes de seguridad.

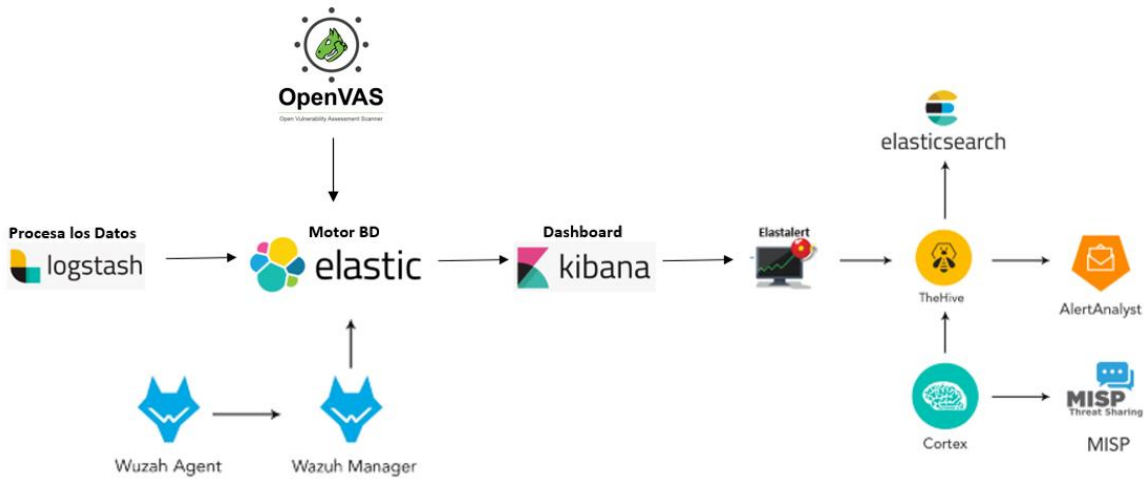
La escalabilidad es otro factor crucial. Tanto The Hive como ELK son altamente escalables, lo que les permite adaptarse a las necesidades cambiantes del CSIRT y gestionar grandes volúmenes de datos de manera eficiente. Esto es esencial para un CSIRT, ya que pueden enfrentarse a una gran cantidad de incidentes de seguridad y datos de logs que requieren procesamiento y análisis en tiempo real.

Finalmente, la combinación de The Hive y ELK proporciona al CSIRT una solución completa y sólida para la detección, gestión y respuesta ante incidentes de seguridad, aprovechando las fortalezas individuales de cada herramienta para garantizar la protección efectiva de los activos de la organización frente a amenazas cibernéticas.

8 INTEGRACIÓN DE HERRAMIENTAS

Luego de analizar las diferentes herramientas de software libre, es importante la integración de estas con el fin de dar respuesta oportuna a un incidente informático, así mismo, se presenta una arquitectura con el objetivo que pueda ser implementada por una organización colombiana de acuerdo con la figura 6:

Figura 6 Integración de Herramientas Opensource



Fuente: modificada Wireshark. 'Qué es un stack de ELK y qué ventajas tiene implementarlo'. [En Línea]. 2023. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-un-stack-de-elk-y-que-ventajas-tiene-implementarlo/

En nuestra estrategia para conformar un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática), integramos una serie de herramientas especializadas ya seleccionadas de acuerdo con el capítulo anterior para detectar, investigar y responder a amenazas cibernéticas de manera efectiva. Cada una de estas herramientas desempeña un papel específico en el proceso, trabajando en conjunto para fortalecer la postura de seguridad de una organización.

El objetivo principal de esta arquitectura es la integración de las herramientas, por una parte, comenzamos con Logstash, Wazuh Agent y OpenVas como los recolectores iniciales de datos. Logstash se encarga de recopilar y procesar los logs y otros datos relevantes de los sistemas y redes, mientras que Wazuh Agent monitorea la actividad en los sistemas locales y envía los logs al Wazuh Manager para su análisis centralizado.

OpenVas por su parte envía la información recopilada los escaneos de vulnerabilidades directamente a Elasticsearch, que es el motor de búsqueda y análisis utilizado en conjunto con Kibana para almacenar, buscar y analizar grandes volúmenes de datos de manera rápida y eficiente. Elasticsearch actuaría como el repositorio central para todos los datos relacionados con la seguridad, incluidos los resultados de los escaneos de OpenVas.

Una vez que los datos son procesados por Logstash, se envían a Elasticsearch, que actúa como el motor de base de datos para almacenar y gestionar los datos de logs. Esta conexión permite una rápida indexación y búsqueda de los datos, lo que es crucial para una detección efectiva de amenazas.

Posteriormente, Kibana se utiliza como interfaz de usuario para visualizar y analizar los datos almacenados en Elasticsearch. Esta integración permite a los analistas de seguridad comprender mejor la información recopilada, identificar patrones de actividad sospechosa y tomar decisiones informadas sobre la respuesta a incidentes.

La herramienta ElastAlert complementa esta configuración al permitir la configuración de reglas de detección de amenazas en los datos indexados en Elasticsearch. Estas reglas flexibles alertan sobre eventos importantes o sospechosos en tiempo real, lo que permite a los analistas detectar y responder rápidamente a posibles amenazas.

Para coordinar y automatizar la respuesta a incidentes, se utilizan The Hive y Cortex. The Hive proporciona un centro de comando para coordinar las investigaciones y acciones de respuesta, mientras que Cortex permite ejecutar análisis y acciones de manera automatizada. Esta integración agiliza el proceso de respuesta a incidentes y garantiza una coordinación efectiva entre los equipos de seguridad.

Por otra parte, MISP se integra para compartir y colaborar en la inteligencia de amenazas, permitiendo el intercambio seguro de información sobre indicadores de compromiso (IOCs) entre organizaciones y comunidades de seguridad. Esta colaboración enriquece la detección de amenazas y mejora la capacidad de respuesta a incidentes al proporcionar información relevante sobre las tácticas, técnicas y procedimientos utilizados por los atacantes.

Finalmente, Alert Analyst se utiliza para analizar y responder a alertas de seguridad de manera colaborativa. Proporciona capacidades de correlación de eventos y análisis de riesgos, lo que permite a los analistas investigar y responder a amenazas cibernéticas de manera efectiva y coordinada.

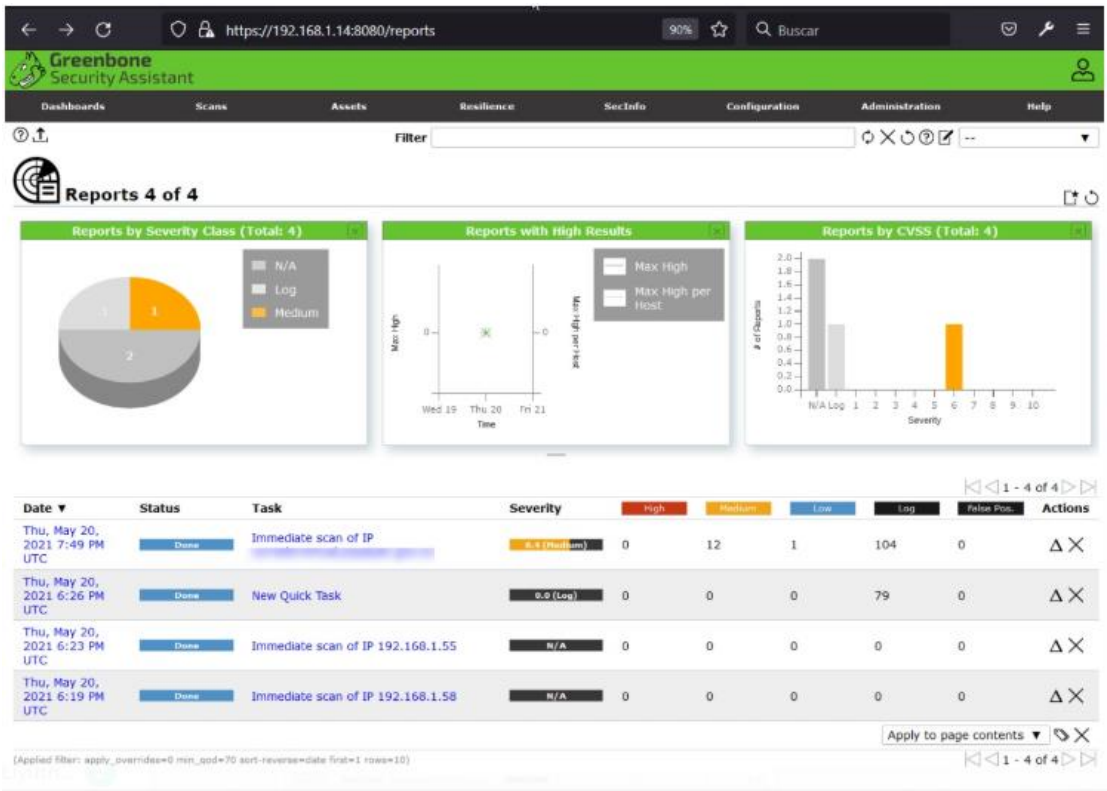
En conjunto, estas herramientas forman una integración completa y robusta del CSIRT, proporcionando capacidades de detección, análisis y respuesta a incidentes

que fortalecen la postura de seguridad de la organización y protegen sus activos contra posibles amenazas cibernéticas.

- **Resultados integración de las herramientas**

De acuerdo con el trabajo realizado, existen herramientas bajo licencia de software libre, que nos permiten adecuar una adecuada gestión a infraestructuras de red; Herramientas GVM OpenVas nos permite realizar la adecuada gestión sobre las vulnerabilidades en sistemas informáticos.

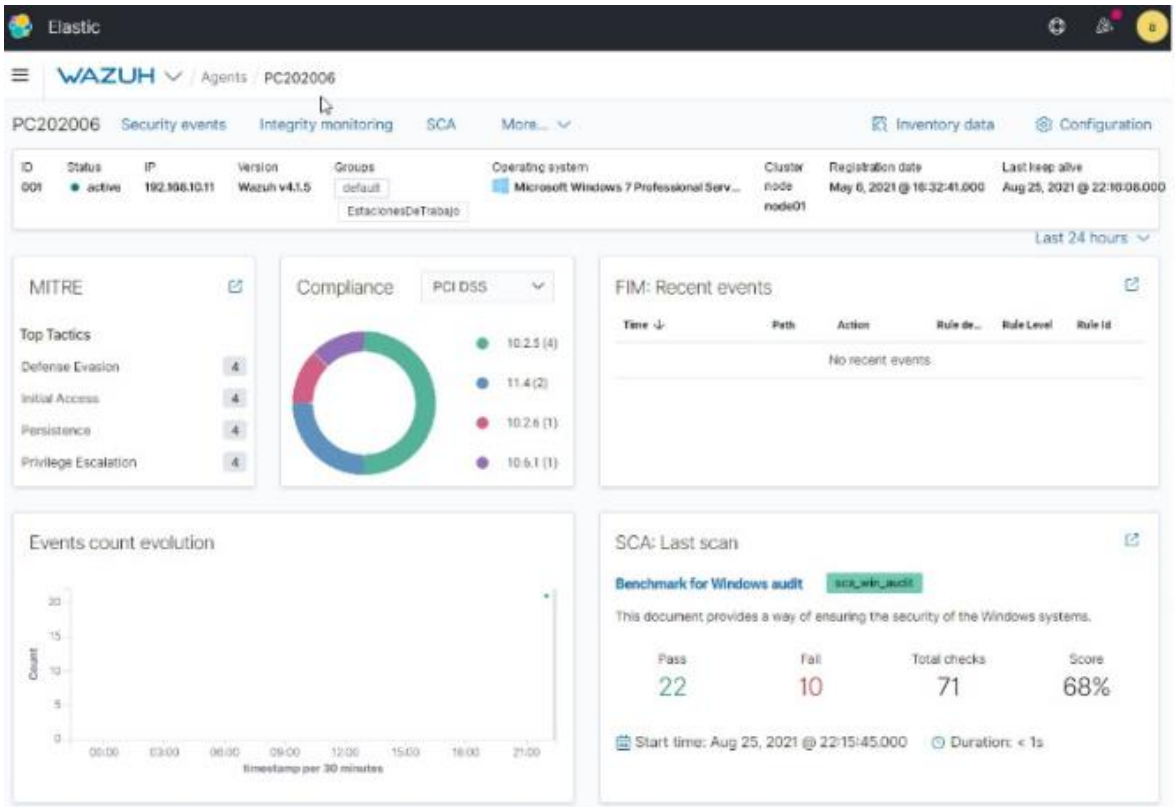
Figura 7 Dashboard OpenVas



Fuente propia

Por otro lado, herramientas como ELK, Wazuh nos permiten hacer una ingesta de datos, que representan el estado de distintas fuentes y orígenes de acuerdo con los parámetros que se establezcan.

Figura 8 Dashboard ELK - Wazuh



Fuente propia

Cabe resaltar que el uso de estas herramientas por ser de tipo de software libre, no cuentan con soporte y cualquier duda o inquietud requiere ir a comunidades en internet.

9 CONCLUSIONES

En Con la implementación de un CSIRT en una organización, las diferentes herramientas articuladas ayudan a recopilar información para un análisis, con el fin de establecer un plan de acción y mitigar los riesgos, para proteger la información de una organización

Por otra parte, se pueden realizar toma de acciones preventivas para mitigar riesgos antes de que se produzca un incidente; como también tomar acciones preventivas para mitigar riesgos antes de que se produzca un incidente.

Proporcionar informes y estadísticas sobre la actividad de seguridad, para aumentar la eficiencia y eficacia de la respuesta a al incidente de seguridad, para una mejora continua en el monitoreo y detección de la amenaza. primer lugar, en el desarrollo de este artículo se logró investigar las diferentes herramientas de software libre para la integración de un CSIRT.

Por otra parte, se realiza un análisis y se seleccionan los componentes para la conformación de un CSIRT.

Finalmente, se realiza la integración de las herramientas aprovechando las bondades de cada herramienta para la puesta en marcha de un CSIRT para las organizaciones colombianas

10 BIBLIOGRAFÍA

ABUDINEN, Karen. “Colombia superó los 8 millones de accesos fijos a internet en el primer trimestre de 2021”: Karen Abudinen, ministra TIC. MINTIC. [En Línea]. 21 de julio 2021. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/178505:Colombia-supero-los-8-millones-de-accesos-fijos-a-internet-en-el-primer-trimestre-de-2021-Karen-Abudinen-ministra-TIC

BEST PRACTICAL. Request Tracker for Incident . [En Línea]. 2022. 1p. Disponible en: https://cyphn.io/

CALDERON, José. ¿QUÉ ES PFSENSE? Y PORQUE ES UN FIREWALL TAN POPULAR. [En Línea]. NETTIX. 20 septiembre 2020. Disponible en: https://www.nettix.com.pe/documentacion/administracion/vpn/que-es-pfsense-y-porque-es-un-firewall-tan-popular/

CAPTERA. Papertrail. [En Línea]. 2022. Disponible en: https://www.capterra.co/software/180057/papertrail

CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. 2p. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CENTRO CRIPTOLOGICO NACIONAL. GUÍA DE SEGURIDAD (CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. España: CONPES. 2011. 60p. Sin Clasificar. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. [En Línea]. Bogota D.C.: CONPES. 2021. 43p. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

CORRAL, Yolanda. Construye y gestiona un SOC con herramientas Open Source. [En Línea]. YolandaCorral. 12 octubre 2020. Disponible en: https://www.yolandacorral.com/construye-y-gestiona-un-soc-con-herramientas-open-source/

CSIRT; ASOBANCARIA. QUIÉNES SOMOS: CSIRT Financiero – Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano. [En Línea]. CSIRT Financiero. 2022. Disponible en: https://csirtasobancaria.com/quienes-somos

CYPHON. FULL STACK DETECTION AND RESPONSE. [En Línea]. 2022. 1p. Disponible en: https://cyphn.io/

DATAMEDIA. ¿Qué es Tableau?. [En Línea]. 2022. Disponible en: https://datademia.es/blog/que-es-tableau

DUPLICATI. Duplicati 2.0: Free backup software to store encrypted backups online For Windows, macOS and Linux. [En Línea]. 2022. Disponible en: https://www.duplicati.com/

EL ESPECTADOR. Detectan más de 5.400 millones de intentos de ciberataques en Colombia. En: El Espectador. [En Línea]. 21 agosto 2020. Disponible en: https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/

ELASTIC. ¿Qué es el ELK Stack?. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/what-is/elk-stack

ELASTIC. El corazón del Elastic Stack, gratuito y abierto. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/elasticsearch/

ELASTIC. Logstash. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/logstash/

ELASTIC. Tu ventana al Elastic Stack. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/kibana/

EveBox. EveBox. [En Línea]. EveBox. 2922. Disponible en: https://www.ibm.com/mx-es/cloud/learn/docker

GARCIA, Hernan. Suricata — IDS/IPS — Introduccion — Parte 1. [En Línea]. 24 octubre 2020. Disponible en: https://hernangarciawolf.medium.com/suricata-ids-ips-introducction-parte-1-486972a3ed22

Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Resumen de vulnerabilidades para la semana anterior. [En Línea]. COLCERT. 6 de febrero de 2022. Disponible en: http://www.colcert.gov.co/?q=acerca-de

IBM. ¿Qué es Docker?. [En Línea]. IBM Cloud Education. 23 junio 2021. Disponible en: https://www.ibm.com/mx-es/cloud/learn/docker

IMAGICLE. Faxes a un clic, no importa la ubicación. [En Línea]. 2022. Disponible en: https://www.imagicle.com/es/products/digital-fax/

INCiBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. [En Línea]. 20 marzo 20217. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INSTITUTO NACIONAL DE CIBER SEGURIDAD. Glosario de términos de ciber seguridad: una guía de aproximación para el empresario. [En Línea]. INCIBE. 2017. 41p. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

KINSTA. ¿Qué Es Apache Web Server? Una Mirada Básica a lo que Es y Cómo Funciona. [En Línea]. 2022. 1p. Disponible en: https://kinsta.com/es/base-de-conocimiento/que-es-apache/

LinkSYS. LinkSYS. [En Línea]. 2022. Disponible en: https://www.linksys.com/hn/p/P-WRT3200ACM/

LINUBE. LOGGLY. [En Línea]. 2022. Disponible en: https://linube.com/blog/loggly-ayuda-registros-en-orden/

MANCOMUN. OSSEC: Sistema de detección de intrusos. [En Línea]. 3 noviembre 2017. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES, . Servicios CSIRT Gobierno. [En Línea]. COLCERT. 26 julio 2022. Disponible en: https://colcert.gov.co/800/w3-article-208774.html#:~:text=El%20objetivo%20principal%20del%20CSIRT%20Gobierno%2C%20es%20ofrecer,todos%20los%20funcionarios%20y%20encargados%20de%20seguridad%20digital

MORALES GONZÁLEZ, Carlos; MORENO SÁMCHEZ, Omar y ORTIGOZA PÉREZ, Johanna. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONS DE SEGURIDAD (SOC) PARA FUERZA AÉREA COLOMBIANA. [En Línea]. Bogota D.C.: Universidad Piloto de Colombia. 2014. 94p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1n

MVWARE. ¿Qué es vSphere Hypervisor?. [En Línea]. 2022. 1p. Disponible en: https://www.vmware.com/co/products/vsphere-hypervisor.html

NAGIOS. Nagios Enterprises. [En Línea]. 2022. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

OPENWEBINARS. Qué es OpenVAS. [En Línea]. 2022. Disponible en: https://openwebinars.net/blog/que-es-openvas/

OPNSENCE. Welcome to OPNsense's documentation!. [En Línea]. 2022. Disponible en: https://docs.opnsense.org/

OPS; OMS. COVID-19 y el rol de los sistemas de información y las tecnologías en el primer nivel de atención. [En Línea]. 23 mayo 2020. Disponible en: https://iris.paho.org/bitstream/handle/10665.2/52205/OPSEIHISCOVID19200022_spa.pdf?sequence=9

PANDA. ¿Qué es Threat Hunting y por qué es necesario. [En Línea]. PANDA SECURITY. 15 noviembre 2018. Disponible en: https://www.pandasecurity.com/es/mediacenter/adaptive-defense/threat-hunting-por-que-necesario/

PANDORA FMS. Pandora FMS: Monitorización como servicio (MaaS). [En Línea]. 2022. Disponible en: https://pandorafms.com/es/#

PÉREZ PÉREZ, Yulis. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA. [En Línea]. Bucaramanga: Universidad Piloto de Colombia. 2014. 9p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

QUILORA VALERAZO, Lisbeth. Análisis de Vulnerabilidades de Seguridad Informática, del Sistema de Gestión Médica SISMEDICALEC, de la empresa Incomsis... [En Línea]. Ambato Ecuador: Universidad Técnica de Ambato. 2019. 135p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31771/alsantillanm.pdf?sequence=1&isAllowed=0079

RAMIREZ NAVIA, Fernando. CACTI: Monitoreo de Red y Reportes Gráfico Opensource. [En Línea]. ITSOFTWARE. 21 septiembre 2017. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

REDCANARY. 2021 Gartner Market Guide for MDR Services: Behind the research. [En Línea]. 10 diciembre 2021. 1p. Disponible en: https://redcanary.com/blog/gartner-2021-market-guide-to-mdr/

REDHAT. ¿Qué es el open source?(CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. RedHat. 24 ictubre 2019. Disponible en: https://www.redhat.com/es/topics/open-source/what-is-open-source

REPUBLICA. Sphinx, motor de búsqueda de texto OpenSource. [En Línea]. 24 JULIO 2007. Disponible en: https://www.republica.com/gizmos/sphinx-motor-de-busqueda-de-texto-opensource-20070724-14061523187/

RETIREMENT. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 23 enero 2018. Disponible en: https://blog.rch1.com/blog/the-crucial-role-of-the-csirt

ROUNDCUBE. About the Roundcube webmail project. [En Línea]. 2022. 1p. Disponible en: https://roundcube.net/about/

SANTILLÁN MOSQUERA, Angela. IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN EMPRESARIAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA JARDINES CRISTO REY LTDA. [En Línea]. PASTO: Universidad Nacional Abierta Y A Distancia. 2019. 140p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31771/alsantillanm.pdf?sequence=1&isAllowed=0079

SAOUT. dm-crypt: a device-mapper crypto target. [En Línea]. 2022. Disponible en: https://www.saout.de/misc/dm-crypt/

SECURITY ONION SOLUTIONS. Security Onion: Visión General. [En Línea]. 2022. Disponible en: https://securityonionsolutions.com/software/

SEMANA. La tecnología ha sido clave en estos momentos de crisis. En: SEMANA. [En Línea]. 20 abril 2020. ISSN 2745-2794. Disponible en: https://www.dinero.com/tecnologia/articulo/columna-la-tecnologia-ha-sido-clave-en-estos-momentos-de-crisis-por-eliseo-barcas-20-de-abril/284442

SERVICIOS DE RED NOONA. Sistema de Monitoreo Zenoss 4.2. [En Línea]. 2022. Disponible en: https://serviciosderednoona.wordpress.com/sistema-de-monitoreo-zenoss-4-2/

SOLR TUTORIAL. Qué es Solr. [En Línea]. 2022. Disponible en: https://solrtutorial.es/que-es-solr.html

SOURSEFORGE. AlienVault OSSIM. [En Línea]. 2022. Disponible en: https://sourceforge.net/projects/os-sim/

SQUID. Squid: Optimising Web Delivery. [En Línea]. 2022. Disponible en: http://www.squid-cache.org/

THEHIVE PROYECT. THEHIVE: A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM. [En Línea]. THEHIVE. 2022. Disponible en: https://thehive-project.org/
UCLG-CGLU. Tecnologías digitales y la pandemia de COVID-19. [En Línea]. 2022. 17p. Disponible en: https://www.uclg.org/sites/default/files/eng_briefing_technology_es.pdf

WELIVESECURITY. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 18 mayo 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/#:~:text=Dado%20este%20escenario%20de%20evoluci%C3%B3n,Computer%20Security%20Incident%20Response%20Team

ZABBIX. Zabbix technical demo video: Explora el resumen técnico rápido de las funciones de Zabbix.. [En Línea]. 2022. Disponible en: https://www.zabbix.com/la/demo