Marco De Trabajo Para El Diseño E Implementación De Un Soc “Security Operation Center” Usando Herramientas De Código Abierto Para Pymes

AUGUSTO GIOVANNI CONDE GIL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

Marco De Trabajo Para El Diseño E Implementación De Un Soc “Security Operation Center” Usando Herramientas De Código Abierto Para Pymes

AUGUSTO GIOVANNI CONDE GIL

Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Manuel Antonio Sierra Rodriguez
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, diciembre de 2023

DEDICATORIA

Dedico este trabajo a mis padres que ya no me acompañan pero que con sus esfuerzos lograron sacar a una familia adelante. Sin su empeño y esfuerzo en los momentos difíciles, sus hijos no podríamos ser las personas de bien que somos hoy en día. Son y serán un ejemplo de superación y lograron demostrar, durante sus años de casado que por más que la vida te genere retos, solo el amor y la unión superar todos los tropiezos que se puedan presentar.

A mi hermana Esperanza que desde el cielo me ve con amor, por todos los momentos felices y por las enseñanzas que me dejo. Gracias a ella soy una mejor persona.

Por último y menos importante, a mi esposa que me ha dado los mejores años de su vida y que me apoya y acompaña siempre en los proyectos que construimos desde el amor.

AGRADECIMIENTOS

Agradezco a cada una de las personas colaboraron con esta monografía ya que sin sus aportes y ayuda este proyecto llegara a buen puerto.

A mis amigos que me dieron sus ideas para poder complementar la información

De la misma forma agradezco a la Universidad Nacional Abierta y a Distancia UNAD a sus directivos y tutores, ya que su invaluable conocimiento aportó no solamente a la construcción de este documento sino también consolidaron el conocimiento en mi carrera profesional.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

Security Operations Center. El centro de operaciones de seguridad hace referencia tanto al equipo responsable de garantizar la seguridad de la información como a la plataforma tecnológica que realiza la supervisión , gestión y administración de los servicios de información y tecnología.

Open Source: Es una expresión que hace referencia al software de código abierto. Es un código diseñado para poder ser modificado, visto y distribuido de la forma en la que el desarrollador considere.

Información y Tecnología: Hace referencia a los activos como Software, Hardware, redes y tecnologías y a los equipos que los gestionan.

Malware. es un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

CSIRT: El Equipo de Respuesta ante Emergencias Informáticas por sus siglas en inglés, es un centro de respuesta a incidentes de seguridad informática. Se encuentra formado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

PYME: Empresa pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y número de trabajadores.

Vulnerabilidad: debilidad que existe en un sistema informático que puede ser empleada por una persona mal intencionada para poder comprometer la seguridad de una organización.

Amenaza: es un evento negativo o una acción que es facilitada por una vulnerabilidad que tiene como objetivo el impacto negativo no deseado sobre un sistema o una aplicación informática.

Ataque informático: es un intento que busca exponer, alterar, destruir eliminar, o acceder a un activo informático dentro de una organización.

Ransomware: es un tipo de malware que restringe el acceso a parte de determinados archivos de un sistema operativo que se encuentra infectado con el fin de pedir un rescate a cambio de quitar esas restricciones.

Infraestructura de TI: corresponde al conjunto de componentes necesarios para que funcione la gestión de servicios empresariales de información y tecnología.

Sistema Operativo: es el conjunto de programas en un sistema informático que permite la gestión de recursos de hardware y que provee servicios a los programas que son llamados aplicaciones de software.

Incidente de IT: es cualquier interrupción que se presenta sobre los servicios de IT una organización que puede llegar a afectar desde un solo usuario hasta toda la empresa.

Marco de referencia: son un conjunto de convenciones que se emplean por un observador para poder comparar con respecto a un escenario en particular.

Firewall: es un sistema que hace de diseño para proteger las redes privadas del acceso no autorizado y que permite al mismo tiempo comunicaciones autorizadas a través de reglas que se implementan.

IDS: Sistema de detección de intrusos por sus siglas en inglés, es un sistema que permite la detección no autorizada a los activos de una organización y que genera una alarma.

IPS: Sistema de protección de intrusos por sus siglas en inglés: es un sistema que toma acciones cuando se generan instrucciones dentro de una red.

SIEM: un sistema de gestión de eventos e información de seguridad es un sistema que permite la centralización y almacenamiento para posteriormente interpretación de los datos relevantes de seguridad de una organización.

Software: son un conjunto de componentes lógicos que se requieren para poder hacer posible la realización de tareas específicas dentro de un sistema operativo.

RED: son un conjunto de equipos y software que se conectan por medio de dispositivos físicos y que envíen y recibe información a través de cualquier medio

de transporte de datos con la finalidad de compartir dicha información y poder ofrecer servicios específicos.

Security Information: son conjunto de medidas preventivas y reactivas que se implementan en las organizaciones y en los sistemas de tecnología para poder resguardar y proteger la información en busca de mantener la confidencialidad disponibilidad e integridad de los datos.

Event Management: son los mecanismos que se emplean para poder establecer y mantener reglas efectivas en los procesos de descarte y correlación de eventos de IT.

Organización: son sistemas administrativos que se crean para poder lograr objetivos corporativos con el apoyo de recursos tecnológicos y talento humano.

Gobernanza TI: es el alineamiento que se genera entre las tecnologías de la información y la comunicación con la estrategia de negocio. Define las metas y la estrategia en todos los departamentos de una empresa y proporciona el mejor uso de la tecnología y de la infraestructura organizativa para poder alcanzarla.

WAF: es un tipo de firewall que supervisa filtra y bloquea tráfico de tipo HTTP desde y hacia una aplicación web. Su diferencia con respecto a un firewall tradicional radica en que puede filtrar el contenido de aplicaciones web que son específicas.

MFA: la autenticación de múltiples factores MFA por sus siglas en inglés es un método de control de acceso informático en el que el usuario se le concede el acceso a un sistema o plataforma a partir de que sean aceptadas dos o más pruebas diferentes de autenticación.

ADC: el controlador de entrega de aplicaciones por sus siglas en inglés es un dispositivo que se encuentra en la red y que permite la gestión de conexiones desde un cliente hacia aplicaciones web que son empresariales y complejas.

PAM: el control de acceso privilegiado es una solución de seguridad que permite proteger a las organizaciones contra las amenazas informáticas ya que supervisa detecta y evita el acceso con privilegios a recursos que son considerados críticos dentro de una organización.

RESUMEN

El Centro de Operaciones de Seguridad, conocido como "SOC," consiste en un grupo de operaciones donde se integran recursos humanos y recursos tecnológicos para poder monitorear y gestionar los incidentes de seguridad informática que un cliente de servicios de TI pueda experimentar. El objetivo de un equipo de SOC es identificar, evaluar y responder a los incidentes de seguridad informática mediante el uso de herramientas tecnológicas y la aplicación de procesos y procedimientos establecidos a través de marcos de referencia. Esto se hace para garantizar la cobertura de las necesidades de seguridad de los sistemas de información de las organizaciones.

Estas herramientas deben permitir la gestión de la seguridad informática, el seguimiento de los incidentes, la detección y prevención de intrusiones, así como la implementación de la inteligencia de amenazas. Por lo tanto, se requieren sistemas como IPS, WAF, MFA, ADC y PAM, entre otras tecnologías, que eviten el acceso y los ataques a la infraestructura de las organizaciones. Sin embargo, debido a los costos asociados con la implementación y puesta en marcha de este tipo de esquemas, las empresas de tipo PYME no pueden costear proyectos de esta naturaleza.

Por lo tanto, una decisión clave que debe tomarse con cuidado es la creación de un equipo de seguridad que puede implementarse reduciendo los costos asociados a las herramientas propias de estos proyectos mediante el uso de plataformas de código abierto.

ABSTRACT

The Security Operations Center, known as "SOC," consists of an operations group where human resources and technological resources are integrated to monitor and manage cybersecurity incidents that a client of IT services may experience. The goal of a SOC team is to identify, assess, and respond to cybersecurity incidents using technological tools and established processes and procedures based on reference frameworks. This is done to ensure coverage of the security needs of organizations' information systems.

These tools should enable the management of cybersecurity, incident tracking, intrusion detection and prevention, as well as the implementation of threat intelligence. Therefore, systems such as IPS, WAF, MFA, ADC, and PAM, among other technologies, are required to prevent access and attacks on the infrastructure of organizations. However, due to the costs associated with implementing and launching such schemes, small and medium-sized enterprises (SMEs) cannot afford projects of this nature.

Hence, a key decision that must be made carefully is the creation of a security team that can be implemented, reducing the costs associated with the tools used in these projects by utilizing open-source platforms.

INTRODUCCIÓN

La seguridad de la información es un aspecto clave para el éxito de cualquier organización en el mundo actual. Sin embargo, las amenazas cibernéticas son cada vez más frecuentes y sofisticadas, lo que requiere una vigilancia y una respuesta constantes.

Para hacer frente a este desafío, muchas organizaciones recurren a los Centros de Operaciones de Seguridad (SOC), que son equipos de profesionales que supervisan y gestionan la seguridad del sistema de información mediante herramientas de recogida, correlación de eventos e intervención remota.

Un SOC permite detectar, analizar y corregir incidentes de ciberseguridad de forma rápida y eficaz, así como mejorar las medidas preventivas y las políticas de seguridad.

Sin embargo, la implementación de un SOC implica una inversión significativa en tecnología y recursos humanos, lo que puede ser un obstáculo para algunas organizaciones.

Una alternativa viable es utilizar software libre para implementar un SOC, lo que ofrece ventajas como la reducción de costes, la flexibilidad, la personalización y la independencia de proveedores.

El software libre es aquel que respeta la libertad de los usuarios y la comunidad, permitiendo su uso, estudio, modificación y distribución sin restricciones.

En este trabajo se presenta una propuesta de implementación de un SOC con software libre para compañías PYME, se describen las principales herramientas disponibles y se analizan los beneficios y los retos que implica esta opción.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En cuanto al diseño e implementación de un SOC (Security Operation Center), no contamos en la actualidad una cantidad adecuada información que defina un marco de referencia y menos aún que incluya el uso de herramientas de código abierto. La información que podemos encontrar con respecto a este tipo de sistemas se encuentra fragmentada y generalizada (Vielberth, Böhm, & Fichtinger, Security Operations Center: A Systematic Study and Open Challenges, 2020)[1]

La información con la que nos podemos encontrar hace referencia a establecer los primeros pasos para la construcción de documentación que defina desde un punto de vista investigativo (Carder, 2022)[2]. Sin embargo, al hablar de la introducción de herramientas de código abierto, la información que se encuentra está limitada, y solo se hace referencia a información comercial que algunos desarrolladores pueden ofertar.

En estos tiempos, las soluciones de seguridad informática tienen un rol importante que jugar en las organizaciones.

Debido a la pandemia del COVID 19, las tareas que se realizan sin contacto físico se volvieron importantes y el trabajo remoto se hizo más valioso.

A la par, los ataques informáticos se han incrementado exponencialmente para compañías en todos los sectores de la economía.

---

[1] VIELBERTH, Manfred, et al. Security operations center: a systematic study and open challenges. En: IEEE Access. 2020. vol. 8, p. 227756-227779.

[2] CARDER, James. How to build a SOC with limited resources. Logrhythm [blog]. (2009). [Consultado el 8, septiembre, 2022]. Disponible en Internet: <https://www.itp.net/public/uk-how-to-build-a-soc-with-limited-resources-white-paper_0.pdf>.

Hay muchas opciones de seguridad que las organizaciones pueden tomar para enfrentarse a esta clase de desafíos que van desde la implementación de un sistema de protección para acceso no autorizados como los firewalls hasta la subcontratación de grandes sistemas de protección de seguridad. Pero, depende de cuánto este la organización dispuesta a invertir en proyectos de seguridad informática.

Sistemas como los firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones son solo algunas de las herramientas que se pueden utilizar para evitar riesgos de seguridad. Sin embargo, la evolución en la sofisticación de estos ataques hace que los procedimientos normales de seguridad sean insuficientes. Para cumplir con los requisitos de seguridad de la información en la actualidad, es necesario que las organizaciones inviertan en el desarrollo de Centros de Operaciones de Seguridad (SOC, por sus siglas en inglés).

En la actualidad, la información disponible sobre el diseño, desarrollo e implementación de un SOC se centra en el establecimiento de objetivos, desafíos, acciones y recursos que podrían ser necesarios. Sin embargo, no se toman en cuenta las herramientas disponibles en el mercado que pueden ser empleadas en el proceso de diseño. Además, no se consideran las herramientas de código abierto como una posible solución para reducir los costos de implementación de un SOC (Bernsmed & Tøndel, 2013)[3].

[3] BERNSMED, Karin y TØNDEL, Inger Anne. Indicators for evaluating information security incident management. En: 2013 Seventh International Conference on IT Security Incident Management and IT Forensics. 2013. p. 3-14.

1.2 FORMULACIÓN DEL PROBLEMA

Actualmente, las soluciones de seguridad informática tienen un rol importante que jugar en las organizaciones, debido a los ataques informáticos que se han incrementado exponencialmente en todos los sectores de la economía.
Otro factor relevante es debido al incremento de la inseguridad por el uso de las TIC en el trabajo remoto, el cual aumento significativamente durante y la post pandemia del Covid-19, por la necesidad de realizar tareas sin contacto físico.
Hay muchas opciones de control de seguridad que las organizaciones toman para enfrentarse a esta clase de desafíos. Como: Sistemas de control lógico y perimetrales como los firewalls, Sistemas de detección de intrusiones y prevención de intrusiones IDS e IPS con equipos dedicados como los UTMs son solo algunas de las herramientas con las que se puede evitar los riesgos de seguridad. Sin embargo, la evolución en la sofisticación de estos ataques hace que los procedimientos normales de seguridad sean inadecuados. Para poder cumplir con los requisitos que tiene ahora, la seguridad de la información se hace necesario que las organizaciones inviertan en el desarrollo de las SOC “System operation Center”.

Otras problemáticas son la carencia de aplicaciones específicas para SOC, aunque se cuenta con herramientas existentes en el mercado. Adicionalmente, no se plantean las herramientas de código abierto como una posible solución en la reducción de los costos de implementación de un SOC.

¿Mediante el uso del SOC con herramientas de código abierto se mitigarán las amenazas de seguridad informática en las organizaciones PYME?

2. JUSTIFICACIÓN

Con esta investigación se pretende identificar las herramientas de código abierto que se pueden proponer y utilizar en el diseño, implementación y operación de SOC "Security Operations Center", teniendo en cuenta que, la documentación existente, hace referencia al diseño desde el punto de vista de los procedimientos que deberían aplicar, alineados con los marcos de referencias en gobernanza TI y no incluyen información acerca de las plataformas que se pueden usar en cada una de las etapas definidas en estos marcos de referencia.

La información recopilada sirve como base para la implementación de un SOC con el uso de herramientas de código abierto para organizaciones que requieran este tipo de plataformas para poder garantizar la seguridad de los activos TI. La literatura que se tiene con respecto al diseño, desarrollo e implementación de un SOC, se enfocan en establecer los objetivos, retos, acciones y recursos que pueden llegar a requerirse. Sin embargo, para esta investigación se profundiza en las herramientas de software libre como opción de seguridad informática fundamental para emplearse en el SOC de organizaciones PYMES.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Proponer un marco de trabajo para el diseño e implementación de un “Security Operation center” SOC, mediante el uso herramientas de código abierto, para las organizaciones PYMES en Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Indagar los principales marcos de referencias, normativas existentes, guías y procedimiento para la implementación de un SOC.

- Analizar las funciones, estructuras, organización y composición de un SOC.

- Determinar las herramientas de software de código abierto para la puesta en marcha de un SOC.

- Establecer el marco de trabajo para la implementación de un SOC con las herramientas de código abierto propuestas para las organizaciones PYME.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Open Source

La expresión open source (o código abierto) hace referencia al software open source (OSS). Este tipo de software es un código que se diseña de manera que pueda ser accesible por el público, siendo todos capaces de ver, modificar y distribuir el código de la forma en que se considere conveniente. (Miller, Voas, & Costello, 2010)[4]

Esta clase de software es desarrollado de forma descentralizada y colaborativa, así que existe una dependencia en la revisión entre los desarrolladores y la producción de la comunidad. Además, puede llegar a ser más económico, flexible y duradero que sus versiones propietarias desarrolladas por las grandes empresas del mercado de software, ya que los encargados de su desarrollo son las comunidades desarrolladoras, la academia y algunas empresas y no un solo autor o una sola empresa. (Schieferdecker, 2012)[5]

4.1.2 ¿Cuál es la diferencia entre el software Propietario y el Open Source?

[4] MILLER, Keith W.; VOAS, Jeffrey y COSTELLO, Tom. Free and open source software. En: IT Professional [en línea]. Noviembre, 2010. vol. 12, no. 6 [consultado el 22, diciembre, 2023], p. 14-16. Disponible en Internet: <https://doi.org/10.1109/mitp.2010.147>. ISSN 1520-9202.

[5] SCHIEFERDECKER, Ina. Trustworthiness of open source, open data, open systems and open standards. En: 2012 IEEE 36th Annual Computer Software and Applications Conference. 2012. p. 82-82.

Según (Xing, 2010)[6], el Software “propietario” o “software de código cerrado”, es aquel cuyo código fuente es propiedad de una persona, un equipo de trabajo o una organización que mantiene el control y uso exclusivo para poder modificarlo.

Solamente los autores originales del software propietario pueden copiar, inspeccionar y modificarlo legalmente. Para poder usar programas propietarios, los usuarios deben aceptar (generalmente al firmar una licencia que se aparece la primera vez que se ejecuta este software) que no harán nada con el software que los autores del software no hayan permitido expresamente.

El software de código abierto es diferente. En este sus creadores ponen su código fuente a disposición de otras personas que deseen ver este código, copiarlo, aprender de él, modificarlo o compartirlo.

Al igual que con el software propietario, los usuarios deben aceptar los términos de una licencia cuando utilizan software de código abierto, pero los términos legales de las licencias de código abierto difieren drásticamente de los de las licencias propietarias.

Según (Gaff & Ploussios, 2012)[7], las licencias de código abierto afectan la forma en que los desarrolladores pueden usar, estudiar, modificar y distribuir software. En general, las licencias de código abierto otorgan a los usuarios de computadoras permiso para usarlo para cualquier propósito que deseen. Algunas licencias se conocen como licencias “copyleft”, que establecen que cualquier persona que publique un programa de código abierto modificado también debe publicar el código fuente de ese programa junto con él. Además, algunas licencias estipulan que

---

[6] XING, Mingqing. Competition between Free Open Source, Commercial Open Source and Proprietary Software. En: Journal of Communications [en línea]. 2013. vol. 8, no. 10 [consultado el 22, diciembre, 2023], p. 665-671. Disponible en Internet: <https://doi.org/10.12720/jcm.8.10.665-671>. ISSN 1796-2021.

[7] GAFF, Brian M. y PLOUSSIOS, Gregory J. Open source software. En: IEEE Computer. 2012. vol. 45, no. 06, p. 9-11. ISSN 1558-0814.

cualquier persona que altere y comparta un programa con otros también debe compartir el código fuente de ese programa sin cobrar una tarifa de licencia por ello.

Por diseño, las licencias de software de código abierto promueven la colaboración y el intercambio, porque permiten que otras personas realicen modificaciones al código fuente e incorporen esos cambios en sus propios proyectos. Animan a los programadores de computadoras a acceder, ver y modificar el software cuando lo deseen, siempre y cuando permitan que otros hagan lo mismo cuando compartan su trabajo.

4.1.3 IDS/IPS

Un sistema de detección de intrusos (IDS) es un sistema que monitorea el tráfico de la red en busca de actividad sospechosa y alerta cuando se descubre dicha actividad.

La detección de intrusos es el proceso en el que se buscan posibles intrusiones como intentos de explotación en incidentes que pueden llegar a ser inminentes en la red, mientras que la prevención de intrusiones realiza la detección de intrusiones luego de tener incidentes detectados eliminando paquetes o terminando sesiones (Alicherry, Muthuprasanna, & Kumar, 2006)[8].

4.1.4 ¿Cuáles son los beneficios de IDS/IPS?

Esos sistemas monitorean el tráfico de red para poder identificar comportamientos maliciosos. Los atacantes intentarán comprometer la red explotando

[8] ALICHERRY, Mansoor; MUTHUPRASANNA, M. y KUMAR, Vijay. High speed pattern matching for network IDS/IPS. En: Proceedings of the 2006 IEEE International Conference on Network Protocols. 2005. p. 187-196.

vulnerabilidades dentro de un sistema o dentro del software. Las plataformas IDS/IPS Identifican estos intentos de explotación bloqueando las que comprometan con éxito cualquier punto dentro de la red. a este tipo de plataformas se deben implementar en los centros de datos y puntos donde se recopila información de red (Abdullah, Lee, Conti, Copeland, & Stasko, 2005)[9]

Estás plataformas funcionan de la siguiente manera:

- Realizan la detección comparando las firmas de los eventos identificados como posibles incidentes de seguridad. Esta es la forma más fácil de detección, ya que compara únicamente la unidad de actividad mediante la comparación de cadenas continuas.
- Detección basada en anomalías: se establecen definiciones de lo que puede considerarse normal, y a partir de aquí se verifican posibles desviaciones significativas. Este es uno de los métodos más importantes cuando se trata de revisar amenazas que son desconocidas.
- Análisis de protocolos: En este método de análisis, se determinan las actividades de protocolo que son normales con cada evento en la red, y se identifican desviaciones.

- Los IPS identifican y controlan las amenazas de forma proactiva en tiempo real, así mismo, genera las alertas para tomar decisiones.

4.1.5 Unified Threat management (UTM)

[9] ABDULLAH, Kulsoom, et al. IDS rainStorm: visualizing IDS alarms. En: IEEE Xplore. 2005. p. 1-10.

(Qi, Yang, Xu, & Li, 2007)[10] comentan que UTM hace referencia a dispositivos de seguridad como una combinación de software, hardware y tecnologías de red, cuya función primordial es el desarrollar múltiples funciones de seguridad.

La definición oficial de UTM es "productos que incluyen múltiples características de seguridad incluidas en una caja". Para poder llegar a ser incluido en esta categoría se requiere que el dispositivo sea capaz de desarrollar funciones firewall de red, funciones de detección/prevención de intrusión IDS/IPS y funciones Gateway antivirus, antimalware, chequeo profundo de paquetes, control de contenidos de navegación, VPNs, Todas estas Funciones en el dispositivo no necesariamente se usarán concurrentemente. Sin embargo, estas deben existir inherentemente.

Algunos de los beneficios de estas plataformas son:

- Efectividad de costo: se reducen el número de dispositivos lo que reduce a su vez el costo tanto de administración como de soporte.
- Fácil de usar: es ideal para empresas que no cuentan personal capacitado y recursos para administración de plataformas complejas.
- Gateway de nivel de aplicación. Adicionalmente la capa de seguridad, este es un dispositivo que provee bloques simples de red para el manejo de ataques antes del ingreso a la red.

Según (Ali, Al Lawati, & Naqvi, 2012)[11] indican que el tipo de soluciones UTM, mejoran el desempeño, la funcionalidad, el precio y la simplicidad. Estos arreglos pueden llegar a incluir funcionalidades como funciones de firewall intrusión y

[10] QI, Yaxuan, et al. Towards system-level optimization for high performance unified threat management. En: International Conference on Networking and Services. 2007. p. 7-7.

[11] ALI, Saqib; AL LAWATI, Maitham H. y NAQVI, Syed J. Unified threat management system approach for securing sme's network infrastructure. En: IEEE Xplore. 2012. p. 170-176.

prevención lo que resulta en un producto que entrega un desempeño mediocre, un conjunto de funciones restringidas y una escalabilidad limitada. Actualmente el desempeño de este tipo de dispositivos depende de la habilitación de las funciones de firewall ya que cuando se habilitan las propiedades de IDS/IPS el desempeño es disminuido, por lo que los fabricantes han trabajado con su equipo de desarrollo para poder implementar soluciones donde el desempeño no se ve menguado.

4.1.6 ¿Qué es un centro de operaciones de seguridad (SOC)?

Un centro de operaciones de seguridad (SOC), por sus siglas en inglés, es un sistema centralizado dentro de una organización, que emplea personal, procesos y tecnología para poder hacer monitoreo y mejorar de forma continua la gestión de seguridad de la organización mientras ejecuta las tareas de prevención, detección, análisis y respuesta a los eventos que afecten la seguridad informática (Bienias, Kołaczek, & Warzyński, 2019)[12].

Citando a (Jarpey & McCoy, 2017)[13] de la Asociación de la industria de tecnología de la computación (Comptia), un SOC se define como “Simply put, a security operations center (SOC – pronounced “sock”) is a team of experts that proactively monitor an organization’s ability to operate securely. Traditionally, a SOC has often been defined as a room where SOC analysts work together.”

Otra definición la podemos encontrar en “A Security Operations Centre (SOC) functions as a team of skilled people operating with defined processes and

---

[12] BIENIAS, Piotr; KOŁACZEK, Grzegorz y WARZYŃSKI, Arkadiusz. Architecture of anomaly detection module for the security operations center. En: 2019 IEEE 28th International Conference on Enabling Technologies. 2019. p. 126-131.

[13] JARPEY, Gregory y MCCOY, Scott. Security operations center guidebook: A practical guide for a successful SOC. [s.l.]: Elsevier Science & Technology Books, 2017. 206 p. ISBN 9780128036822.

supported by integrated security intelligence technologies. The SOC specifically focuses on cyber threat, monitoring, forensic investigation, and incident management and reporting , under the umbrella of an overall security operations environment and clear executive support.", como se puede entender de las definiciones mostradas, el SOC comprende un equipos de personas y recursos tecnológicos que se encuentran alineados con diferentes procesos para poder combatir amenazas cibernéticas, hacer análisis sobre los eventos que ocurren en una red en particular, atender incidencias y generar los reportes respectivos.

4.1.7 Servicios que presta un SOC

Aunque el tamaño del personal de un SOC puede llegar variar dependiendo del tamaño de la organización, En su gran mayoría tiene aproximadamente las mismas funciones y responsabilidades.

Las responsabilidades son las siguientes:

4.1.7.1 Detección y prevención

Cuando se trata de seguridad informática, la prevención tiende a ser siempre más efectiva que la reacción. En lugar de responder a las amenazas a medida que ocurren, un SOC trabaja para monitorear la red las 24 horas del día. Al hacerlo, el equipo SOC puede detectar actividades maliciosas y prevenirlas antes de que puedan causar algún daño sobre los activos de TI de la organización. Cuando el analista de SOC ve algo sospechoso, recopila toda la información que puede para una investigación más profunda.

4.1.7.2 Investigación

En esta etapa de investigación, el analista de SOC analiza la actividad sospechosa para determinar la naturaleza de una amenaza y ver que tanto ha penetrado en la

infraestructura. El analista de seguridad ve la red y las operaciones de la organización desde la perspectiva de un atacante, buscando indicadores clave y áreas de exposición antes de que sean explotados. El analista identifica y realiza una clasificación de los diversos tipos de incidentes de seguridad al comprender cómo se desarrollan los ataques y cómo responder de manera efectiva antes de que se salgan de control. El analista de SOC combina información sobre la red de la organización con la inteligencia de amenazas global más reciente que incluye información específica sobre las herramientas, técnicas y tendencias de los atacantes para realizar una evaluación eficaz (Miloslavskaya, 2016)[14].

4.1.7.3 Respuesta

Después de la investigación, el equipo SOC coordina una respuesta para remediar el problema. Tan pronto como se confirma un incidente, el SOC actúa como el primer equipo de respuesta, realizando acciones como aislar puntos finales, finalizar procesos dañinos, evitar que se ejecuten, eliminar archivos y más. Después de un incidente, el SOC trabaja para restaurar los sistemas y recuperar los datos perdidos o comprometidos. Esto puede incluir borrar y reiniciar puntos finales, reconfigurar sistemas o, en el caso de ataques de ransomware, implementar copias de seguridad viables para eludir el ransomware. Cuando tenga éxito, este paso devolverá la red al estado en el que se encontraba antes del incidente (Miloslavskaya, 2016)[15].

4.1.7.4 Security Information and Event Management.

[14] MILOSLAVSKAYA, Natalia. Security operations centers for information security incident management. En: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud. 2016. p. 131-136.

[15] Ibíd, P 131-136

La gestión de eventos según (Modiri & Sobhanzadeh, 2011)[16], hacen referencia a la recopilación y análisis de los eventos que provienen de todos los elementos de una red dentro de las cuales incluyen IDS, Proxies, Servidores de AD. El objetivo es el recopilar toda la información generada por estos dispositivos de manera que se puedan configurar in formatos específicos. Una vez que el evento se encuentra configurado se le da un formato especial para que pueda ser analizado posteriormente. Una de las ventajas de este tipo de plataformas es la correlación que se genera entre los diferentes eventos usando atributos comunes de forma que se puedan descubrir patrones de ataque que puedan llegar a ser significativos. La información procesada se puede enviar a una base de datos para que sea consultada en futuras búsquedas.

Según (Modiri & Sobhanzadeh, 2011)[17] uno de los enfoques en los cuáles contribuye un equipo de Security Operations Center (SOC), consiste en la creación de reglas que permitan determinar una casuística a los eventos generados en el espacio de tiempo determinado lo cual se puede emplear para generar alertas ante varios eventos del mismo tipo. Si las alertas generadas se consideran falsos positivos se descarta esta alerta y se continúa con el reconocimiento de las siguientes. Por otro lado, si se requiere un análisis más específico el analista decidirá a qué actores involucrar a para el análisis.

4.1.7.5 Ticketing.

Adicionalmente a lo anteriormente mencionado luego de que realiza el proceso de normalización de eventos, la plataforma permite la creación de tickets para poder hacer un seguimiento a los diferentes indicadores de gestión por parte del equipo

[16] MODIRI, Nasser y SOBHANZADEH, Yosef Masoudi. Information security management. En: 2011 International Conference on Computational Intelligence and Communication Networks. 2011. p. 481-484.

[17] Ibíd, P 481-484

de SOC. Dentro de estos indicadores se puede encontrar: tiempo de creación, tiempo de resolución, duración del evento entre otros.

4.1.7.6 AD (Active Directory).

Es un repositorio de información de todos los objetos que se encuentran en una red centralizada. Ese repositorio contiene información como la identidad de los servicios los usuarios los puntos de acceso la autentificación y la autorización. Contiene toda la información de los miembros de un dominio. Con esta información el equipo de SOC puedes verificar quieres atacar recibidos a la infraestructura provienen o no por parte de usuarios o elementos en la red.

5. DESARROLLO DE LOS OBJETIVOS

5.1 NORMATIVAS EXISTENTES Y MARCOS DE REFERENCIAS

La ciberseguridad en Colombia se refiere al conjunto de prácticas, políticas y medidas implementadas para proteger los sistemas informáticos, las redes y los datos de amenazas cibernéticas y garantizar la confidencialidad, integridad y disponibilidad de la información en el entorno digital. En el país, la ciberseguridad está regulada por diversas leyes y regulaciones, entre las cuales destacan la Ley 1273 de 2009, que aborda los delitos informáticos y promueve la protección de sistemas y datos, y la Ley 1581 de 2012, que regula la protección de datos personales y establece medidas para garantizar la privacidad de la información. Además, existen decretos y regulaciones específicas relacionadas con la infraestructura de clave pública y la gestión de incidentes de ciberseguridad. Estas leyes y regulaciones buscan fortalecer la seguridad en línea, promover la confianza en las transacciones digitales y proteger tanto a individuos como a organizaciones de las amenazas cibernéticas.

A continuación, se presentan las leyes, regulaciones y documentos que rigen la ciberseguridad en Colombia

- Ley 527 de 1999 – Comercio Electrónico.
- Ley 603 de 2000 − Control de legalidad de software.
- Decreto 620 de 2005 – Seguridad de la Información
- Ley 1266 de 2008 – Habeas Data.
- Ley 1273 de 2009 − Delitos informáticos.

- Ley 1341 de 2009 – Ley de Tecnologías de la Información y las Comunicaciones.
- Ley 1581 de 2012 − Protección de Datos Personales
- Documento Conpes 3701 de 2011
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009.
- Circular Externa 003 de 2016 de la Superintendencia Financiera de Colombia
- Resolución 1241 de 2018 de la Comisión de Regulación de Comunicaciones (CRC)

5.1.1 Ley 527 de 1999

La (Ley 527 de 1999)[18], conocida como la "Ley de Comercio Electrónico" en Colombia, establece un marco legal para regular las transacciones comerciales realizadas a través de medios electrónicos. Esta ley reconoce la validez jurídica de los contratos y las firmas electrónicos, equiparándolos a los contratos y firmas tradicionales en papel.

Algunos de los puntos clave de esta ley incluyen:

- Reconocimiento de la validez legal: La ley establece que los contratos celebrados electrónicamente son legalmente válidos y vinculantes.

- Firma electrónica: La Ley 527 regula el uso de la firma electrónica como un medio para validar y autenticar documentos electrónicos. Reconoce diferentes tipos de firma electrónica, incluyendo la firma electrónica avanzada, que es la más segura y avanzada.

[18] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 527. (18, agosto, 1999). Ley 527 de 1999.

- Responsabilidad de los intermediarios: La ley establece la responsabilidad de los intermediarios en línea, como proveedores de servicios de internet (ISP), para tomar medidas razonables para prevenir y responder a actividades ilegales en línea.

- Comprobantes electrónicos: La ley permite el uso de comprobantes electrónicos como facturas y recibos electrónicos, lo que simplifica la gestión de documentos en entornos comerciales digitales.

- Protección al consumidor: La Ley 527 incluye disposiciones para proteger a los consumidores en transacciones electrónicas, garantizando la seguridad y la privacidad de los datos personales.

- Autoridades reguladoras: Establece la Superintendencia de Industria y Comercio (SIC) como la entidad encargada de supervisar y regular el cumplimiento de la ley en materia de comercio electrónico y firma electrónica.

5.1.2 Ley 603 de 2000

La (Ley 603 de 2000)[19] en Colombia se refiere a la "Ley sobre la Firma Electrónica y la Infraestructura de Clave Pública (ICP)". Su principal objetivo es establecer un marco legal para regular y promover el uso de la firma electrónica y la infraestructura de clave pública en transacciones y documentos electrónicos. A continuación, se proporciona un resumen de los puntos clave de esta ley:

- Firma Electrónica: La Ley 603 reconoce la validez de la firma electrónica como un medio legalmente válido para firmar contratos y documentos electrónicos, y establece requisitos y estándares para su uso y autenticación.

[19] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 603. (3, agosto, 2000). Ley 603 de 2000.

- Infraestructura de Clave Pública (ICP): La ley establece la creación y regulación de la Infraestructura de Clave Pública, un sistema que permite la emisión y gestión de certificados digitales y claves públicas para garantizar la seguridad y la autenticidad de las transacciones electrónicas.

- Autoridades de Certificación: La ley establece la creación de Autoridades de Certificación, que son responsables de emitir certificados digitales y garantizar la integridad y autenticidad de las firmas electrónicas.

- Validez Jurídica: La ley establece que los documentos electrónicos firmados digitalmente son equivalentes en validez a los documentos en papel y las firmas manuscritas, lo que promueve la adopción de tecnologías digitales en el país.

- Seguridad de la Información: La ley incluye medidas de seguridad para proteger la información y los datos personales en el contexto de la firma electrónica y la ICP.

- Supervisión y Regulación: La Superintendencia de Servicios Públicos Domiciliarios tiene la responsabilidad de supervisar y regular la implementación de la infraestructura de clave pública y la firma electrónica en Colombia.

5.1.3 Decreto 620 de 2005

El (Decreto 620 de 2005)[20] en Colombia establece regulaciones relacionadas con la seguridad de la información y la protección de datos personales en el sector público. Estos son los aspectos resaltantes de este decreto:

[20] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 620. (5, abril, 2005). Decreto 620 de 2005.

- Objetivo: El decreto tiene como objetivo establecer normas y directrices para garantizar la seguridad de la información en las entidades del sector público colombiano y promover la confidencialidad, integridad y disponibilidad de los datos.

- Definición de Datos Sensibles: Define qué se considera como datos sensibles y establece medidas especiales para su tratamiento y protección, reconociendo la importancia de esta categoría de datos.

- Responsabilidad de los responsables y encargados: Establece que las entidades públicas deben designar un responsable de Seguridad de la Información, quien tiene la responsabilidad de implementar y supervisar medidas de seguridad.

- Medidas de Seguridad: El decreto establece las medidas de seguridad que deben ser implementadas para proteger la información, incluyendo aspectos técnicos, organizativos y de recurso humano.

- Registro de Incidentes: Establece la obligación de llevar un registro de incidentes de seguridad, así como la notificación y respuesta a incidentes que puedan afectar la seguridad de la información.

- Transferencia de Datos: Regula la transferencia de datos entre entidades públicas, garantizando que se cumplan las medidas de seguridad y los requisitos legales.

- Auditoría de Seguridad: Establece la realización de auditorías de seguridad de la información para evaluar el cumplimiento de las normas y la eficacia de las medidas de seguridad.

- Sanciones: Advierte sobre las sanciones que pueden imponerse en caso de incumplimiento de las regulaciones de seguridad de la información, incluyendo multas y medidas correctivas.

5.1.4 Ley 1266 de 2008.

La (Ley 1266 de 2008)[21] en Colombia regula la protección de datos personales y establece los principios y normas para su procesamiento adecuado. A continuación, se presenta un resumen de los aspectos principales de esta ley:

- Definición de Datos Personales: La ley define qué se considera como datos personales y regula su uso y tratamiento, reconociendo que son información relativa a personas naturales.

- Principios Rectores: La Ley 1266 establece principios rectores para el tratamiento de datos personales, incluyendo el consentimiento del titular de los datos, la finalidad específica del procesamiento, la calidad de la información, la seguridad de los datos y la confidencialidad.

- Derechos del Titular: La ley reconoce y garantiza los derechos de los titulares de los datos personales, como el acceso a su información, la corrección de datos inexactos, la revocación del consentimiento y la eliminación de datos cuando ya no sean necesarios.

- Responsabilidades de los responsables y Encargados: La ley establece las obligaciones de las entidades que recopilan y procesan datos personales, así como

[21] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266. (25, diciembre, 2008). Ley 1266 de 2008.

de los encargados del tratamiento de datos. Esto incluye la implementación de medidas de seguridad y la notificación de incidentes de seguridad.

- Transferencia Internacional de Datos: Se regulan los procedimientos y requisitos para la transferencia de datos personales a países extranjeros.

- Autoridad Nacional de Protección de Datos (Superintendencia de Industria y Comercio): La ley crea la Autoridad Nacional de Protección de Datos en Colombia, que tiene la responsabilidad de supervisar y hacer cumplir las disposiciones de la ley.

- Sanciones: La ley establece sanciones para quienes incumplan las normas de protección de datos personales, incluyendo multas y la posibilidad de cierre de operaciones.

5.1.5 Ley 1273 de 2009

La (Ley 1273 de 2009)[22] en Colombia es conocida como la "Ley de Delitos Informáticos" y tiene como objetivo principal regular los delitos informáticos y proteger la seguridad de la información en el entorno digital. A continuación, se presenta un resumen de los aspectos clave de esta ley:

- Delitos Informáticos: La ley establece y define una serie de delitos informáticos, incluyendo la interceptación ilegal de datos, la violación de sistemas informáticos, el acceso ilegítimo a sistemas de información, la suplantación de identidad en línea y la difusión de software malicioso, entre otros.

[22] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273. (5, enero, 2010). Ley 1273 de 2009.

- Sanciones: La Ley 1273 establece sanciones penales para quienes cometan delitos informáticos, que pueden incluir multas y penas de prisión, dependiendo de la gravedad del delito.

- Responsabilidad: La ley establece que los individuos, empresas y organizaciones son responsables por garantizar la seguridad de sus sistemas de información y proteger los datos de terceros.

- Protección de Datos Personales: La ley regula la protección de datos personales y prohíbe la divulgación no autorizada de información personal.

- Autoridades Competentes: La Superintendencia de Industria y Comercio de Colombia es la entidad encargada de supervisar y hacer cumplir las disposiciones de la ley.

- Colaboración Internacional: La ley promueve la cooperación internacional para la investigación y persecución de delitos informáticos, incluyendo la extradición de individuos acusados de estos delitos.

- Prevención y Educación: La ley fomenta la concienciación y la educación sobre seguridad informática y ciberseguridad para prevenir delitos informáticos.

5.1.6 Ley 1341 de 2009

La Ley 1341 de 2009[23] en Colombia, también conocida como " Ley de Tecnologías de la Información y las Comunicaciones," es una legislación fundamental que regula

[23] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341. (30, julio, 2009). Ley 1341 de 2009.

el sector de las tecnologías de la información y las comunicaciones en el país. Los aspectos claves de esta ley son:

- Definición de TIC: La ley define las Tecnologías de la Información y las Comunicaciones (TIC) como el conjunto de recursos, herramientas, equipos, programas y aplicaciones que permiten la compilación, procesamiento, almacenamiento, transmisión de información y acceso a servicios de información y comunicación.

- Objetivos: La ley tiene como objetivo promover el acceso universal a las TIC, fomentar la competencia en el sector, garantizar la calidad de los servicios de telecomunicaciones, y promover la investigación y desarrollo en el campo de las TIC.

- Acceso Universal: La ley establece la obligación de garantizar el acceso a los servicios de telecomunicaciones y tecnologías de la información en áreas rurales y urbanas, con un enfoque en la equidad y la inclusión digital.

- Regulación y Competencia: La legislación establece las bases para la regulación y promoción de la competencia en el sector de las TIC, con el fin de evitar prácticas anticompetitivas y garantizar la calidad de los servicios.

- Protección del Consumidor: La ley incluye disposiciones para proteger los derechos de los usuarios de servicios de telecomunicaciones y establece mecanismos de defensa del consumidor.

- Fomento de la Investigación y Desarrollo: La ley promueve la inversión en investigación y desarrollo en el campo de las TIC, así como la transferencia de tecnología y la innovación.

- Autoridades Reguladoras: La ley establece la Comisión de Regulación de Comunicaciones (CRC) como la entidad encargada de la regulación y supervisión del sector de las TIC en Colombia.

5.1.7 La Ley 1581 de 2012

La (Ley 1581 de 2012)[24] en Colombia, también conocida como "Ley de Protección de Datos Personales," establece un marco legal para la protección de la privacidad y los datos personales de los ciudadanos. A continuación, se presenta un resumen de los aspectos clave de esta ley:

- Definición de Datos Personales: La ley define los datos personales como cualquier información vinculada a una persona natural que permita su identificación.

- Derechos de los Titulares: Reconoce y garantiza los derechos de los titulares de datos personales, incluyendo el derecho de acceso a su información, la corrección de datos inexactos, la revocación del consentimiento y la eliminación de datos cuando ya no sean necesarios.

- Principios Rectores: Establece principios fundamentales para el tratamiento de datos personales, como el consentimiento, la finalidad específica, la calidad, la seguridad, la confidencialidad y la transparencia.

- Responsabilidades de los responsables y Encargados: La ley establece las obligaciones de las entidades que recopilan y procesan datos personales, así como de los encargados del tratamiento de datos. Esto incluye la implementación de medidas de seguridad y la notificación de incidentes de seguridad.

---

[24] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581. (17, octubre, 2012). Ley 1581 de 2012.

- Transferencia Internacional de Datos: Regula los procedimientos y requisitos para la transferencia de datos personales a países extranjeros.

- Registro Nacional de Bases de Datos: Establece la creación de un Registro Nacional de Bases de Datos, que debe ser administrado por la Superintendencia de Industria y Comercio.

- Sanciones: La ley establece sanciones para quienes incumplan las normas de protección de datos personales, incluyendo multas y la posibilidad de cierre de operaciones.

- Ámbito de Aplicación: La ley se aplica a todas las entidades públicas y privadas que recopilan, almacenan, procesan o utilizan datos personales en Colombia.

5.1.8 Documento CONPES 3701 de 2011

El Documento (CONPES 3701 de 2011)[25], emitido por el Departamento Nacional de Planeación de Colombia, establece la "Política Nacional de Seguridad y Defensa Cibernética" en el país. A continuación, se presenta un resumen de los aspectos resaltantes de este documento:

- Definición de Ciberseguridad: El CONPES 3701 define la ciberseguridad como el conjunto de políticas, procedimientos, estándares y medidas técnicas y organizativas para proteger la infraestructura de tecnologías de la información y comunicaciones (TIC) y la información digital de amenazas cibernéticas.

[25] DEPARTAMENTO NACIONAL DE PLANEACIÓN DE COLOMBIA. Resolución Conpes 3701 de 2011. (12, mayo, 2011). Política Nacional de Seguridad y Defensa Cibernética.

- Necesidad de una Política Nacional: El documento argumenta la necesidad de establecer una política nacional de ciberseguridad en Colombia debido al aumento de las amenazas cibernéticas y la importancia de garantizar la seguridad de la infraestructura crítica y la información.

- Principios Rectores: Se establecen principios rectores para la ciberseguridad en Colombia, incluyendo la protección de la confidencialidad, integridad y disponibilidad de la información, así como la cooperación y coordinación entre entidades públicas y privadas.

- Gobierno y Coordinación: Se establece un marco de gobierno de la ciberseguridad, que incluye la creación de una Comisión de Coordinación en Ciberseguridad y un Centro Cibernético Nacional para la detección y respuesta a amenazas cibernéticas.

- Protección de la Infraestructura Crítica: Se hace hincapié en la importancia de proteger la infraestructura crítica, como las redes de energía, agua y transporte, ante posibles ataques cibernéticos.

- Capacitación y Concientización: Se promueve la capacitación y la concientización en ciberseguridad tanto en el sector público como en el privado.

- Participación del Sector Privado: Se enfatiza la necesidad de la colaboración entre el gobierno y el sector privado para fortalecer la ciberseguridad en Colombia.

5.1.9 Resolución de la Comisión de Regulación de Comunicaciones (CRC) 2258 de 2009

La Resolución de la Comisión de Regulación de Comunicaciones (CRC) 2258 de 2009[26] en Colombia establece regulaciones relacionadas con la gestión y seguridad de incidentes en las redes y servicios de comunicaciones electrónicas. Estos son los aspectos clave de esta resolución:

- Objetivo: La resolución tiene como objetivo establecer los procedimientos y responsabilidades para la gestión de incidentes de seguridad en las redes y servicios de comunicaciones electrónicas, con el fin de garantizar la integridad y confidencialidad de la información.

- Definición de Incidentes: Define qué se considera un incidente de seguridad en el contexto de las comunicaciones electrónicas, incluyendo eventos que afecten la seguridad de la información y de las redes.

- Reporte de Incidentes: Establece que los operadores de redes y servicios de comunicaciones electrónicas deben notificar a la CRC los incidentes de seguridad que afecten la confidencialidad, integridad o disponibilidad de la información o de los servicios.

- Registros y Documentación: Los operadores deben mantener registros de los incidentes, incluyendo información sobre la naturaleza del incidente, las medidas tomadas y los resultados de la investigación.

[26] COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 2258. (23, diciembre, 2009). Resolución - 2258.

- Cooperación y Colaboración: La resolución promueve la cooperación entre los operadores y la CRC en la gestión de incidentes de seguridad, así como la colaboración con otras entidades y autoridades pertinentes.

- Confidencialidad: Se establece la confidencialidad de la información relacionada con los incidentes de seguridad, salvo cuando se requiera su divulgación por razones legales o de seguridad pública.

- Medidas Correctivas: Los operadores deben tomar medidas correctivas para prevenir la recurrencia de incidentes y mejorar la seguridad de sus redes y servicios.

- Plazos y Reportes: La resolución establece plazos para la notificación de incidentes y la presentación de reportes a la CRC, así como la revisión y seguimiento de las acciones tomadas.

5.1.10 Circular Externa 003 de 2016 de la Superintendencia Financiera de Colombia

La (Circular Externa 003 de 2016)[27] de la Superintendencia Financiera de Colombia establece regulaciones y directrices relacionadas con la ciberseguridad y la gestión de riesgos tecnológicos en las entidades financieras en Colombia. Sus puntos resaltantes son:

- Objetivo: La circular tiene como objetivo establecer lineamientos para la gestión de riesgos tecnológicos y la ciberseguridad en las entidades financieras, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información y sistemas.

[27] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular 003. (1, junio, 2016). Circular Externa 003 de 2016.

- Definición de Riesgos Tecnológicos: Define qué se considera como riesgos tecnológicos y destaca la importancia de su identificación, evaluación y gestión.

- Política de Seguridad de la Información: Exige que las entidades financieras implementen una política de seguridad de la información que incluya aspectos como la asignación de responsabilidades, la concientización de los empleados y la gestión de incidentes.

- Evaluación de Riesgos: Establece la obligación de realizar evaluaciones periódicas de riesgos tecnológicos, identificando posibles amenazas y vulnerabilidades en los sistemas de información.

- Plan de Continuidad del Negocio: Exige la implementación de un plan de continuidad del negocio que permita mantener las operaciones en caso de incidentes tecnológicos, como ciberataques.

- Notificación de Incidentes: Las entidades financieras deben notificar a la Superintendencia Financiera y a otras autoridades competentes en caso de incidentes de ciberseguridad que afecten la operación normal de la entidad.

- Medidas de Seguridad: Señala la importancia de implementar medidas de seguridad tecnológica, incluyendo controles de acceso, cifrado de datos y auditorías de seguridad.

- Gestión de Proveedores: Establece directrices para la gestión de proveedores de servicios tecnológicos, asegurando que cumplan con estándares de seguridad.

- Pruebas de Penetración: Recomienda la realización de pruebas de penetración para evaluar la resistencia de los sistemas ante posibles ataques.

5.1.11 Resolución 1241 de 2018 de la Comisión de Regulación de comunicaciones

La Resolución 1241 de 2018[28] de la Comisión de Regulación de Comunicaciones (CRC) en Colombia establece regulaciones relacionadas con la seguridad de la información y la protección de datos personales en el sector de las tecnologías de la información y las comunicaciones. A continuación, se presenta un resumen de los aspectos clave de esta resolución:

- Objetivo: La resolución tiene como objetivo establecer medidas para la protección de datos personales y la seguridad de la información en el sector de las tecnologías de la información y las comunicaciones (TIC).

- Definición de Datos Personales: Define qué se considera como datos personales y destaca la importancia de su tratamiento adecuado para garantizar la confidencialidad e integridad de la información.

- Consentimiento del Titular: Establece que la recolección y el tratamiento de datos personales deben realizarse con el consentimiento del titular, que debe ser informado y previo.

- Derechos de los Titulares: Reconoce los derechos de los titulares de datos personales, incluyendo el acceso, la rectificación, la actualización, la supresión y la revocación del consentimiento.

[28] COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 1241. (14, mayo, 2009). Resolución 1241 de 2018.

- Seguridad de Datos: Hace hincapié en la importancia de implementar medidas de seguridad para proteger los datos personales y prevenir el acceso no autorizado o la pérdida de información.

- Registro de Bases de Datos: Establece la obligación de las entidades que manejan datos personales de registrar sus bases de datos ante la CRC, proporcionando información detallada sobre su finalidad y uso.

- Transferencia Internacional de Datos: Regula la transferencia de datos personales a países extranjeros, asegurando que se cumplan las medidas de seguridad adecuadas.

- Sanciones: Advierte sobre las sanciones que pueden imponerse en caso de incumplimiento de las regulaciones de protección de datos personales, incluyendo multas y medidas correctivas.

- Notificación de Violaciones de Datos: Establece la obligación de notificar a la CRC y a los titulares en caso de una violación de seguridad que comprometa la confidencialidad de los datos personales.

5.1.12 Marcos de referencia para un SOC

En el momento de realizar este documento, no existe un estándar establecido para el diseño e implementación de un SOC. Adicionalmente, no existe estructuras comunes que definan el funcionamiento de un SOC ni tampoco están definidas las funciones que deben cumplir.

Es por eso por lo que las normas que los regulan son las mismas que se emplean para atender la seguridad informática en una organización.

A continuación, nombraremos las normas que serían aplicables a un modelo de seguridad informática con un SOC

5.1.12.1 ISO/IEC 27001

Es una norma internacional que asegura la confidencialidad y la integridad de los datos y la información, así como los sistemas que intervienen en el procesamiento (ISOTools, 2013)[29].

El estándar ISO 27001, contiene los requisitos del sistema de gestión de seguridad de la información. La norma ISO 27001 es un estándar que se encuentra reconocido de forma internacional, que describe todos los requisitos para construir un marco basado en riesgos para iniciar, implantar, mantener y gestionar la seguridad de la información dentro de la empresa. (Toro, 2016)[30]

En el anexo A se pueden ver enumeradas como resumen los controles que se desarrollan en la norma ISO 27002:2005 que son los que se selecciona para que las organizaciones desarrollen sus SGSI.

Según estándar ISO 27002, se define como una guía de buenas prácticas que fórmula los objetivos de control y controles que se recomiendan para la seguridad de la información. En su actualización más reciente del 15/02/2022 se pueden ver 93 controles, relativos a la organización 37, a las personas 8, a las instalaciones físicas 14 y a la tecnología 34. De acuerdo con esta última revisión es posible que

---

[29] ISO 27001 - sistemas de gestión de seguridad de la información [Anónimo]. Software ISO [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/>.

[30] ¿QUÉ DIFERENCIA existe entre ISO 27001 y SOC 2? [Anónimo]. PMG SSI - ISO 27001 [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.pmg-ssi.com/2016/05/que-diferencia-existe-entre-iso-27001-y-soc-2/>.

cada organización desarrolle los atributos propios para los controles de seguridad para facilitar la integración de la norma ISO 27001, con otros marcos de gobernanza TI y gestión, además de posibilitar la orientación en la implantación de controles sectores industriales o a sectores específicos para las actividades propias de cada organización.

5.1.12.2 NIST CSF

NIST es instituto nacional de estándares y tecnología el departamento de comercio de los estados unidos. El objetivo del marco seguridad cibernética del NIST consiste en ayudar a las empresas y todos los tamaños, en la comprensión administración y reducción de los riesgos seguridad informática y en la protección de las redes y datos.

Este marco integra los estándares de la industria y las mejores prácticas para colaborar con las organizaciones en la administración de los riesgos de ciberseguridad. Procura establecer un lenguaje común que ayuda al personal en todos los niveles de una organización y en todos los niveles de la cadena de suministro a entender y comprender los riesgos de ciberseguridad. El NIST Integra tanto expertos del gobierno como expertos del sector privado.

Este marco no solo ayuda a las organizaciones con la comprensión de los riesgos de ciberseguridad, sino que también ayuda a la reducción de estos a través de la implementación de medidas personalizadas. De igual forma, también apoya la respuesta y recuperación de los incidentes de ciberseguridad.

Un SOC puede emplear este marco como guía, para evaluar, mejorar y entregar métricas que son clave en el establecimiento de un enfoque para la protección en

una organización. Es un punto de partida con la cual se puede construir una estrategia de ciberseguridad organizacional. (Devo.com, 2022)[31]

Las 5 Funciones en las que se compone el marco NIST son:

- Identificación: ayuda a la organización en la comprensión y administración de los riesgos de seguridad informática que pueden afectar los sistemas, activos datos y capacidades. Con esto se busca crear funciones críticas dentro de un contexto de recursos de para poder escalar las amenazas a apropiadas como rapidez.

Se busca obtener una comprensión completa de los recursos como personas, activos físicos y digitales, riesgos, vulnerabilidades y sistema defensa

- Protección: se procura implementar salvaguardas para poder garantizar que los servicios relacionados con infraestructura crítica permanezcan operativos y en caso de algún impacto se podrá limitar. Se debe establecer un enfoque diverso y por capas para poder proteger los recursos de una organización y al mismo tiempo se debe estar listo para poder responder ante cualquier evento.
- Detección: la organización deberá describir las acciones adecuadas que se deban implementar cuando ocurren incidentes decir seguridad. Con el establecimiento de una estrategia eficaz se puede garantizar que el SOC detecte amenazas potenciales de forma rápida y eviten que se conviertan en infracciones significativas.

Se deben a implementar tecnologías y prácticas para detección temprana de eventos que afecten los datos de seguridad.

- Respuesta: esta función establece las actividades apropiadas que el equipo del SOC debe llevar a cabo luego de que se detecta un incidente. Se toma las acciones necesarias para reaccionar adecuadamente ante un incidente de ciberseguridad y se evita que se convierta en incumplimiento grave.

[31] RESOURCE CENTER [Anónimo]. Devo.com [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.devo.com/guide-to-the-future-soc/soc-frameworks>.

- Recuperación: la recuperación usted la identificación de las medidas necesarias para la restauración de las capacidades o los servicios afectados durante la ocurrencia de un evento de ciberseguridad. el objeto es hacer la restauración a condiciones normales en el menor tiempo posible.

Devuelve los activos de la organización al estado original mediante la implantación de resiliencia y la implementación de nuevas medidas preventivas para evitar un ataque repetitivo.

5.1.12.3 Cyber Kill Chain

La "Cyber Kill Chain" (Cadena de Ataque Cibernético) es un concepto y un modelo desarrollado por Lockheed Martin, una empresa de defensa y seguridad, para describir las fases o etapas que suelen seguir los ciberdelincuentes o atacantes en un ciberataque (Lockheed, 2022)[32]. El objetivo de este modelo es ayudar a las organizaciones a comprender cómo operan los atacantes y a desarrollar estrategias efectivas para prevenir, detectar y responder a los ataques cibernéticos. La cadena de ataque se compone generalmente de las siguientes fases: La cadena consta de 7 pasos distintos[33]:

- Reconocimiento (Reconnaissance): En esta fase, los atacantes recopilan información sobre el objetivo. Esto puede incluir la identificación de objetivos potenciales, la búsqueda de vulnerabilidades conocidas y la recopilación de datos sobre la organización, como direcciones de correo electrónico, nombres de empleados y otros detalles que les ayuden a diseñar un ataque efectivo.

---

[32] CYBER KILL chain® [Anónimo]. Lockheed Martin [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

[33] Ibíd,

- Arma (Weaponization): En esta etapa, los atacantes crean o adquieren las herramientas necesarias para llevar a cabo el ataque, como malware personalizado, exploits o payloads que serán entregados al sistema objetivo.

- Entrega (Delivery): Aquí, los atacantes eligen un método para entregar el malware o la carga útil al sistema o red objetivo. Esto puede implicar el envío de correos electrónicos de phishing con archivos adjuntos maliciosos, la creación de sitios web comprometidos o la explotación de vulnerabilidades en el software para ingresar al sistema.

- Explotación (Exploitation): En esta fase, los atacantes aprovechan las vulnerabilidades en el sistema objetivo para ganar acceso. Pueden explotar debilidades en el software, fallos de configuración o incluso ingeniería social para lograr su cometido.

- Instalación (Installation): Una vez que han obtenido acceso, los atacantes instalan el malware o la carga útil en el sistema comprometido. Esto les permite mantener acceso y control continuo sobre la víctima.

- Comando y Control (Command and Control): Los atacantes establecen una conexión y control sobre el sistema comprometido. Utilizan esta conexión para supervisar y administrar el ataque de forma remota, lo que les permite realizar cambios, recopilar datos y expandir el ataque si es necesario.

- Movimiento Lateral (Lateral Movement): Con el acceso a un sistema, los atacantes buscan expandirse dentro de la red objetivo. Pueden buscar otros sistemas y recursos, moverse a través de la red y escalar privilegios para aumentar su control.

- Ejecución de Objetivos (Execution): En esta etapa, los atacantes llevan a cabo sus objetivos reales. Esto puede incluir actividades como robo de datos, manipulación de sistemas, instalación de backdoors o cualquier otro acto malicioso que hayan planificado.

- Persistencia (Persistence): Para mantener el acceso, los atacantes buscan maneras de persistir en la red. Pueden establecer mecanismos de acceso encubiertos, crear cuentas de usuario adicionales o realizar otras acciones para asegurarse de que puedan regresar en el futuro.

- Exfiltración (Exfiltration): En esta última etapa, los atacantes roban y transfieren datos o información confidencial fuera de la organización. Esto puede ser información financiera, datos de clientes, propiedad intelectual u otro tipo de datos valiosos.

5.1.12.4 MITRE ATT&CK Framework

El marco de referencia MITRE ATT&CK, se define como una base de conocimiento global basada en tácticas y técnicas de adversario.

MITRE Corporation, es una organización sin ánimo de lucro cuyo objetivo es la investigación y que se encarga de la administración del centro de desarrollo e investigación financiados por el gobierno de Estados Unidos. En el año 2013, MITRE, creo ATT&CK para investigar datos de telemetría y análisis que están relacionados con la detección posterior a eventos de ciberseguridad. Su objetivo inicial era la documentación de tácticas, técnicas y procedimientos comunes realizadas por ciber delincuentes.

Este marco de referencia aborda cuatro casos de uso clave: inteligencia amenazas, detección y análisis, emulación adversaria y evaluación e ingeniería.

Este marco emplea la evidencia de ataques anteriores como base de referencia para establecer las tácticas adecuadas y poder establecer los posibles pasos de respuesta y las fuentes de datos útiles para un análisis en profundidad de los ataques.

El marco ATT&CK tiene como objetivo ayudar a las organizaciones a comprender y enfrentar las amenazas cibernéticas al proporcionar un conjunto detallado de tácticas, técnicas y procedimientos utilizados por adversarios en ciberataques.

Las principales características y componentes del MITRE ATT&CK Framework son:

- Tácticas: El marco define una serie de tácticas que representan objetivos de alto nivel que los atacantes intentan lograr. Estas tácticas incluyen cosas como el acceso inicial, la persistencia, la ejecución, la evasión de la detección y la exfiltración de datos, entre otras.
- Técnicas: Dentro de cada táctica, se detallan las técnicas específicas que los adversarios utilizan para llevar a cabo los objetivos. Por ejemplo, dentro de la táctica de "Acceso Inicial", puede haber técnicas como "Phishing" o "Explotación de vulnerabilidades".
- Matriz: El MITRE ATT&CK Framework se presenta en forma de una matriz que muestra las tácticas en un eje y las técnicas en el otro. Cada celda de la matriz representa la relación entre una táctica y una técnica específica, indicando cómo los atacantes emplean técnicas para lograr sus objetivos.
- Grupo de adversarios: El marco también identifica grupos de adversarios conocidos y les asigna tácticas y técnicas específicas que han utilizado en ataques documentados.
- Referencias y enlaces: Se proporcionan referencias y enlaces a información adicional para ayudar a los profesionales de la ciberseguridad a aprender más sobre cada técnica y táctica.

5.1.12.5 ISA/IEC 62443:

La serie de normas ISA/IEC 62443 (ISA/IEC, 2017)[34], desarrollada por el comité ISA99 y adoptada por la Comisión Electrotécnica Internacional (IEC), proporciona

[34] ISA/IEC. Industrial communication networks. Network and system security. 63443. [s.l.]: el autor, 2017. 3 p.

un marco flexible para abordar y mitigar las vulnerabilidades de seguridad actuales y futuras en los sistemas de control y automatización industrial (IACS). El comité se basa en los aportes y el conocimiento de los expertos en seguridad de IACS de todo el mundo para desarrollar estándares de consenso que sean aplicables a todos los sectores de la industria e infraestructura crítica.

ISA/IEC 62443 es una serie de normas desarrollada en colaboración entre la Sociedad Internacional de Automatización (ISA) y la Comisión Electrotécnica Internacional (IEC) con el propósito de establecer un marco de ciberseguridad específico para sistemas de control industrial.

El estándar ISA/IEC 62443 se divide en varias partes, cada una de las cuales aborda aspectos específicos de la ciberseguridad en sistemas de control industrial. Estas partes incluyen:

- Parte 1: Definiciones y conceptos clave: Esta sección establece los términos y definiciones fundamentales relacionados con la ciberseguridad en sistemas de control industrial.
- Parte 2: Establecimiento de un programa de ciberseguridad: Ofrece pautas para la creación y gestión de programas de ciberseguridad adaptados a sistemas de control industrial.
- Parte 3: Sistema de gestión de ciberseguridad: Se centra en la implementación de un sistema de gestión de ciberseguridad que abarque políticas, procedimientos y prácticas recomendadas.
- Parte 4: Requisitos específicos de ciberseguridad para productos de seguridad industrial: Define los requisitos para el diseño y la evaluación de productos de seguridad industrial, como firewalls y dispositivos de detección de intrusiones.
- Parte 5: Proveedores de sistemas de control industrial: Establece directrices para que los proveedores de sistemas de control industrial integren la ciberseguridad en sus productos y servicios.

- Parte 6: Requisitos de seguridad funcionales: Aborda la evaluación y el diseño de sistemas de control industrial desde una perspectiva de seguridad funcional.
- Parte 7: Roles y responsabilidades: Define los roles y responsabilidades de las partes involucradas en la ciberseguridad de sistemas de control industrial, como propietarios, operadores y proveedores.
- Parte 8: Evaluación de la seguridad y certificación de productos: Describe los procesos de evaluación de seguridad y certificación de productos relacionados con la ciberseguridad en sistemas de control industrial.

5.1.12.6 NIST SP 800

Las publicaciones de la serie Special Publication (SP) 800 del NIST (Nist.gov, 2023)[35] presentan información de interés para la comunidad de seguridad informática. La serie comprende pautas, recomendaciones, especificaciones técnicas e informes anuales de las actividades de ciberseguridad del NIST.

Las publicaciones SP 800 se desarrollan para abordar y respaldar las necesidades de seguridad y privacidad de la información y los sistemas de información del gobierno federal de los EE. UU. El NIST desarrolla publicaciones de la serie SP 800 de acuerdo con sus responsabilidades legales en virtud de la Ley Federal de Modernización de la Seguridad de la Información y la Ley Pública.

Creada en 1990, la serie informa sobre la investigación, las pautas y los esfuerzos de divulgación del Laboratorio de Tecnología de la Información en seguridad

[35] SP 800-94, guide to intrusion detection and prevention systems (IDPS) | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://csrc.nist.gov/pubs/sp/800/94/final>.

informática, y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas.

La serie NIST SP 800 es un conjunto de documentos de orientación y estándares desarrollados por el NIST para ayudar a las organizaciones a fortalecer la seguridad de la información y proteger sus sistemas contra amenazas cibernéticas. Estos documentos cubren una amplia gama de temas relacionados con la seguridad de la información y se utilizan ampliamente en el ámbito gubernamental y en la industria.

Algunos de los temas clave que abarca la serie NIST SP 800 incluyen:

Gestión de riesgos de seguridad: Los documentos de esta serie proporcionan orientación sobre cómo identificar, evaluar y gestionar los riesgos de seguridad de la información en una organización.

- Ciberseguridad y prácticas de seguridad: Ofrecen recomendaciones para establecer y mantener prácticas de seguridad efectivas, incluyendo la gestión de contraseñas, la autenticación, la autorización y el monitoreo de seguridad.

- Seguridad en sistemas y redes: Los estándares NIST SP 800 abordan la seguridad de sistemas operativos, bases de datos, redes y dispositivos, y proporcionan directrices para su configuración y mantenimiento seguros.

- Criptografía y protección de datos: Los documentos de la serie NIST SP 800 se utilizan para definir estándares de criptografía y protección de datos, incluyendo algoritmos criptográficos y directrices para el cifrado de datos.

- Seguridad en la nube: Se abordan cuestiones de seguridad específicas para la computación en la nube, incluyendo recomendaciones para la evaluación de proveedores de servicios en la nube y la protección de datos en entornos de nube.

- Seguridad de aplicaciones y desarrollo seguro: Se proporciona orientación sobre cómo diseñar, desarrollar y mantener aplicaciones seguras, así como prácticas recomendadas para pruebas de seguridad de aplicaciones.

- Incidentes de seguridad y respuesta a incidentes: La serie NIST SP 800 incluye pautas para la detección, notificación y respuesta a incidentes de seguridad.

5.1.12.7 RFC 2196.

Es una guía para el desarrollo de buenas prácticas políticas y procedimientos de seguridad informática para los tienen sistemas en internet. el objetivo de esta guía es brindar orientación acerca de las prácticas a los administradores para la protección de la información y de los servicios asociados.

los temas que se incluyen son contenidos información de políticas temas técnicos de seguridad de sistemas y redes y respuesta a incidentes de seguridad informática.

Aunque existen en la actualidad muchos marcos de referencia y normas que están atadas a la seguridad informática no existe ninguna que hable directamente de la implementación de un SOC.

El RFC 2196, titulado "Site Security Handbook" (Fraser, 1997)[36], es un documento informativo publicado por la Internet Engineering Task Force (IETF) en septiembre de 1997. Este RFC proporciona orientación y mejores prácticas en materia de seguridad informática para las organizaciones que gestionan sitios y redes en Internet. A continuación, se presenta un resumen de los puntos clave de RFC 2196:

- Importancia de la seguridad: El RFC enfatiza la importancia de la seguridad en la gestión de sitios y redes en Internet. Subraya que la seguridad debe ser una prioridad en todos los aspectos de la operación en línea.

[36] RFC 2196: site security handbook [Anónimo]. IETF Datatracker [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://tools.ietf.org/html/rfc2196>.

- Concienciación y políticas: El documento recomienda que las organizaciones desarrollen una cultura de seguridad, fomentando la concienciación sobre las amenazas y estableciendo políticas de seguridad claras y efectivas.
- Evaluación de riesgos: Se destaca la necesidad de llevar a cabo evaluaciones de riesgos periódicas para identificar las amenazas potenciales y los puntos débiles en la infraestructura de seguridad.
- Seguridad física: El RFC aborda la seguridad física de los activos de red y sugiere medidas para proteger los equipos y los centros de datos.
- Seguridad en la red: Se proporcionan recomendaciones sobre cómo proteger las redes, incluyendo el filtrado de tráfico, la autenticación y el control de acceso.
- Seguridad en sistemas y aplicaciones: El documento hace hincapié en la importancia de mantener sistemas y aplicaciones actualizados y seguros, y ofrece consejos para la gestión de contraseñas, el monitoreo de sistemas y la gestión de incidentes.
- Seguridad en el acceso remoto: El RFC discute la seguridad en el acceso remoto y cómo proteger las conexiones desde ubicaciones externas.
- Educación y entrenamiento: Se recomienda que las organizaciones proporcionen capacitación en seguridad para su personal y usuarios, con el fin de crear una cultura de seguridad sólida.
- Gestión de incidentes: El documento sugiere que las organizaciones desarrollen planes de respuesta a incidentes para abordar de manera eficaz cualquier problema de seguridad que pueda surgir.

5.2 ESTRUCTURA DE UN SOC.

De acuerdo con (Jarpey & McCoy, 2017)[37], se definen las responsabilidades fundamentales que debe tener un SOC, las cuales son:

- Recolección de datos y análisis.
- Gestión de las vulnerabilidades.
- Inteligencias de amenazas
- Cumplimiento
- Gestión de casos y Ticketing
- Colaboración

5.2.1 Recolección de datos y análisis.

Se debe considerar los métodos para la captura de la información que existe en una organización para poder realizar el análisis sobre ésta y determinar las acciones necesarias requeridas. Las fuentes de información pueden varias dependiendo de las fuentes, sin embargo, estas pueden ser las recopiladas a partir de los logs de eventos de los equipos, los paquetes de información que cruzan la red y el flujo de información por elementos de red.

La complejidad de las arquitecturas que una organización puede tener y la cantidad de servicios y sistemas asociados a estos hacen que la operación de captura de información sea compleja. Sin embargo, según propone (Jarpey & McCoy, 2017)[38] se deben realizar preguntas que son comunes para todas las organizaciones, incluyendo las PYMES que son el foco de este documento

[37] op. cit

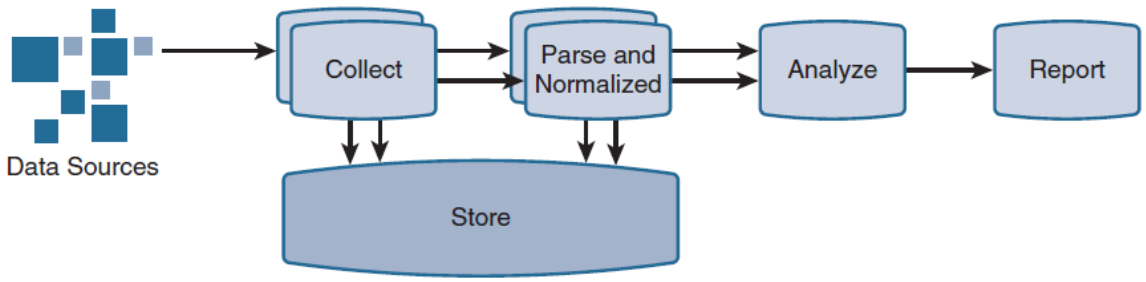
[38] op. cit

Las preguntas a consideras son:

- ¿Cuáles elementos se deben monitorear?
- ¿Qué datos se deben recoger y en que formato?
- ¿Qué nivel de Logging se debe habilitar en cada elemento de red?
- ¿Qué protocolos se deben habilitar en cada elemento para hacer la captura de información?
- ¿Qué capacidad que requiere para el almacenamiento de información y durante cuánto tiempo se debe almacenar?
- ¿Qué datos se deben analizar?
- ¿Qué tanto overhead suma al tráfico de red la recolección de datos introduce?
- ¿Cómo se debe asociar los requerimientos de recolección de datos con la gestión de la capacidad?

El tipo de datos adquiridos debe determinar los mecanismos de captura que se desarrollarán. Para comprender el proceso de captura de datos, se identifican los pasos requeridos, como se muestra en la siguiente figura.

Figura 1 Proceso de Captura de Datos



Fuente Jarpey, G., & McCoy, R. S. (2017). What is a Security Operations Center? In Security Operations Center Guidebook (pp. 3–10). Elsevie

5.2.2 Gestión de vulnerabilidades.

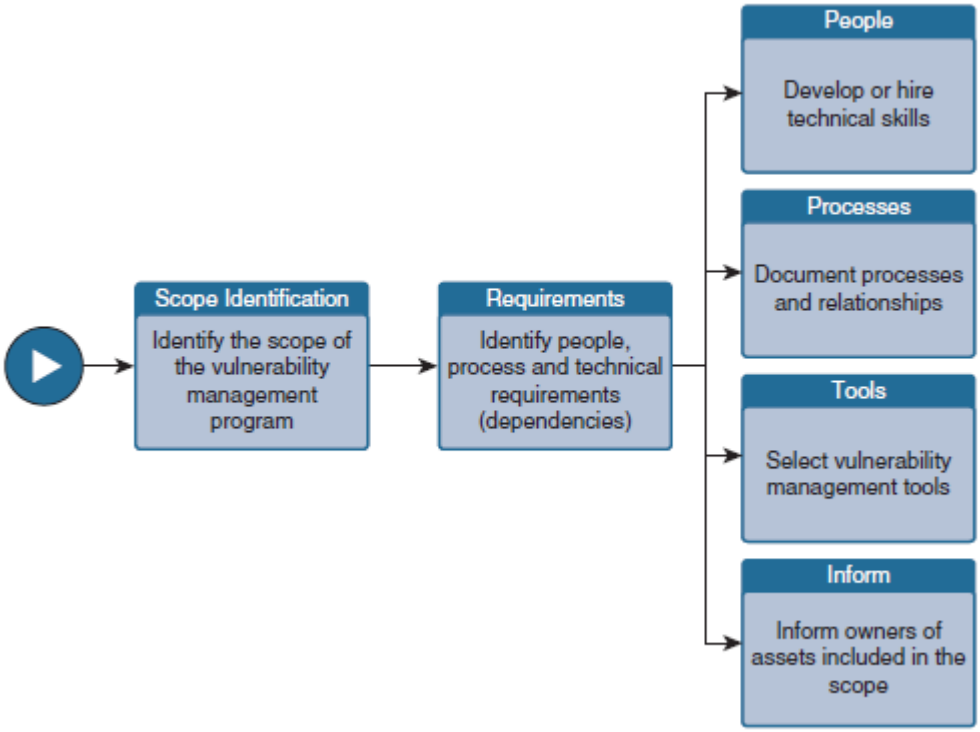
Este proceso consiste en: descubrir, confirmar, clasificar, priorizar, asignar, remediar, y hacer seguimiento a las vulnerabilidades. Es un proceso que se realiza de forma continua y proactiva que se hace de forma automatizada para mantener los sistemas informáticos, redes y aplicaciones libres de ciberataques.

El objetivo de la gestión de vulnerabilidades consiste en reducir la exposición de los activos de una organización a los riesgos a los que está expuesto y se mitigan las vulnerabilidades tanto como sea posible. Esta es una tarea en la que se debe generar un esfuerzo continuo, dada la naturaleza de las amenazas que son cambiantes.

Las vulnerabilidades se pueden percibir como debilidades en las personas procesos y tecnologías. En el contexto en que hace referencia al SOC estas debilidades son de naturaleza técnicas cuando hablamos tanto software como firmware.

Para poder cumplir con la gestión de vulnerabilidades es necesario seguir una serie de pasos para poder identificar, evaluar y corregir todos los riesgos que son asociados con dichas vulnerabilidades. En la siguiente figura podemos ver un modelo de referencia para el manejo de análisis definido por la SysAdmin, Audit, Network, Security, “SANS”

Figura 2 Gestión de vulnerabilidades.



Fuente Jarpey, G., & McCoy, R. S. (2017). What is a Security Operations Center? In Security Operations Center Guidebook (pp. 3–10).

5.2.3 Inteligencia de Amenazas

Según comentan (Muniz, McIntyre, & AlFardan, 2022)[39], consiste en el conocimiento basado en evidencia que incluye el contexto, los mecanismos, los indicadores, los dispositivos accionables, acerca de una amenaza emergente o existente por el daño

[39] SECURITY OPERATIONS center: building, operating, and maintaining your SOC | cisco press [Anónimo]. Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052014>.

a los activos que permite tomar decisiones de acuerdo con esta respuesta a la amenaza.

Es un proceso en el cual se identifican y se analizan las ciber amenazas, lo que implica la reunión de información y datos acerca de una potencial amenaza y al proceso de recopilación procesamiento y análisis de estos datos para comprender mejor dichas amenazas. La inteligencia de amenazas se centra más en temas globales como el examen de los datos y el contexto en el cual se elabora y soporta la información para la toma de decisiones.

Según comentan (Muniz, McIntyre, & AlFardan, 2022)[40] se define en un ciclo de 5 pasos para poder hacer la inteligencia de amenazas: planificación, dirección recopilación procesamiento análisis producción y diseminación las cuales podemos ver a continuación

Figura 3 Threat Intelligence.

Fuente Muniz, J., McIntyre, G., & AlFardan, N. (n.d.). Security operations center: Building operating, and maintaining your SOC. Ciscopress.com

[40] Ibid, P 56-72

5.2.4 Cumplimiento.

El cumplimiento consiste en realizar un monitoreo de todos los activos de la organización contra configuraciones estándar o plantillas, lo que ayuda a detectar cambios en las configuraciones existentes. Esto puede ayudar a una organización a identificar posibles brechas. Este tipo de inconvenientes tradicionalmente no se pueden descubrir a través de los métodos convencionales, como los escáneres de vulnerabilidades, a menos que el problema ya se haya desarrollado. La operación de un SOC debería ser capaz de determinar, a partir de este tipo de análisis, problemas y amenazas que puedan afectar la infraestructura de una organización, aplicando la metodología existente en los sistemas disponibles para llevar a cabo este tipo de análisis

5.2.5 Gestión de Casos y Ticketing.

El equipo del SOC debe poder hacer seguimiento a los incidentes potenciales reportados por los usuarios finales. Se debe poder crear, asignar y dar seguimiento hasta el cierre para asegurar la gestión adecuada del incidente.

El equipo del SOC debe contar con las herramientas adecuadas para poder hacer este tipo de seguimiento, ya que a partir de esta información se pueden crear reportes. Estos reportes sirven para realizar análisis posteriores y extraer estadísticas que puedan ser concluyentes cuando se trata de revisar las incidencias generadas en un período de tiempo.

De acuerdo con (Muniz, McIntyre, & AlFardan, 2022)[41], se deben asignar responsabilidades para que puedan ser supervisadas por una autoridad propietaria. Esto conllevaría a una gestión exitosa en el manejo del caso. Según los autores, se

[41] Ibid

debe aplicar la matriz RACI (R = Responsible, A = Accountable, C = Consult, e I = Inform) para poder identificar los roles y responsabilidades en el proceso de cambios.

Figura 4 Matriz RACI en la gestión de casos.

Function	Project Sponsor	Business Analyst	Project Manager	Software Developer
Initiate project	C		AR	
Establish project plan	I	C	AR	C
Gather user requirements	I	R	A	I
Develop technical requirements	I	R	A	I
Develop software tools	I	C	A	R
Test software	I	R	A	C
Deploy software	C	R	A	C

Fuente Muniz, J., McIntyre, G., & AlFardan, N. (n.d.). Security operations center: Building operating, and maintaining your SOC. Ciscopress.com

5.2.6 Colaboración

El equipo de SOC debe contar con las herramientas y plataformas de colaboración que permitan centralizar la información, gestionarla y acceder a ella de forma que esté disponible tanto para los miembros del equipo como para los auditores externos en caso de que se requiera.

Además de lo anterior, es fundamental considerar que los medios de comunicación juegan un papel esencial y son recursos críticos en el momento de operar. Muchas de estas herramientas ya están disponibles en cualquier organización, como el

correo electrónico, la intranet, las plataformas propias de la organización, entre otros.

La centralización de la información y la colaboración eficiente no solo mejoran la eficacia y la capacidad de respuesta del equipo de SOC, sino que también facilitan la rendición de cuentas y la auditoría externa. El acceso rápido y seguro a los datos es esencial para la toma de decisiones informadas y la identificación oportuna de amenazas y vulnerabilidades. La integración de estas herramientas y recursos dentro de la estrategia del equipo de SOC es esencial para garantizar la seguridad y el éxito operativo en el entorno empresarial.

5.2.7 Arquitectura

Según (Jarpey & McCoy, 2017)[42]., la arquitectura de un SOC puede ser centralizada o distribuida. En el caso de un SOC con una arquitectura centralizada, se sigue un enfoque en el que todos los datos son enviados desde diferentes ubicaciones geográficas u oficinas remotas a un SOC central para su posterior procesamiento.

Por otro lado, en un enfoque distribuido, se utiliza un único sistema operativo que abarca todas las subsidiarias. Desde la perspectiva de los usuarios finales, parece como si estuvieran tratando con una única entidad. Además, este tipo de sistema distribuido permite que todas las entidades reciban, procesen, combinen y proporcionen información de seguridad y servicios a las otras entidades, lo que distribuye la carga de trabajo entre las diferentes entidades.

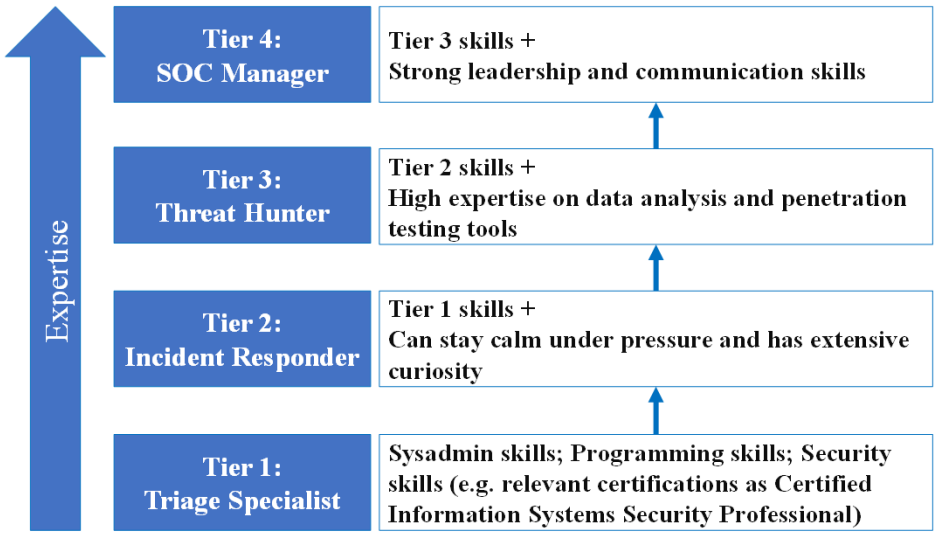
[42] op. cit

Por último, existe una arquitectura descentralizada, que es esencialmente una combinación de los dos sistemas mencionados anteriormente. En este caso, se tienen pequeños grupos de SOC con la posibilidad limitada de informar a uno o varios SOC centrales.

5.2.8 Personal en un SOC

En un Security Operations Center (SOC) según (Vielberth, Böhm, & Fichtinger, Security Operations Center: A Systematic Study and Open Challenges, 2020)[43] se asignan roles importantes que corresponden a diferentes niveles de analistas y gerentes especializados. Estos roles se pueden clasificar de la siguiente manera:

Figura 5 Personal que compone un SOC



Fuente M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges,"

[43] Op, Cit

5.2.8.1 Nivel 1 (Especialista de Clasificación)

- Recopilan datos en bruto y revisan alarmas y alertas.
- Confirman, determinan o ajustan la criticidad de las alertas según su relevancia.
- Identifican riesgos potenciales y diferencian entre fallas genuinas y falsos positivos.
- Realizan el monitoreo de eventos generados por registros de equipos y reportan eventos anómalos.
- Realizan seguimiento a los cambios y generan informes relacionados con la gestión de vulnerabilidades.

5.2.8.2 Nivel 2 (Respuesta a Incidentes)

- Revisan las incidencias críticas escaladas por el Nivel 1, realizando pruebas más detalladas con herramientas apropiadas.
- Buscan comprender el alcance de los ataques y la infraestructura afectada.
- Diseñan estrategias para contener y recuperar la información después de un incidente.
- En caso de que el incidente no se resuelva en este nivel, se escala al Nivel 3.
- Monitorean herramientas de gestión y plataformas de seguridad para identificar problemas.
- Gestionan la configuración y generan informes sobre la calificación de proveedores.
- Analizan estadísticas de incidencias generadas desde el Nivel 1 y entregan informes para su evaluación.

5.2.8.3 Nivel 3 (Gestión de Amenazas)

- El grupo de analistas con mayor experiencia en el SOC.
- Manejan las incidencias escaladas desde los niveles inferiores.
- Realizan pruebas de vulnerabilidad y penetración para identificar posibles vectores de ataque.
- Su responsabilidad principal es identificar amenazas, brechas de seguridad y vulnerabilidades desconocidas.
- Evalúan la operación del SOC en conjunto con el gerente para identificar áreas de mejora.
- Establecen procedimientos para la inteligencia de amenazas y coordinan la resolución de incidentes críticos.

5.2.8.4 Gerente del SOC

- Supervisan las operaciones del equipo y evalúan su desempeño a través del análisis de estadísticas.
- Brindan orientación técnica según sea necesario.
- Administran los recursos del equipo, incluyendo contratación, entrenamiento y evaluación del personal, y diseñan procesos.
- Entregan informes de operación a la junta directiva de la organización.
- Realizan solicitudes para adquirir activos necesarios para la operación del SOC.
- Informan a la organización sobre eventos de seguridad que podrían comprometer la infraestructura tecnológica, permitiendo tomar decisiones internas.

La operación de un Centro de Operaciones de Seguridad (SOC) es un componente crítico en la estrategia de ciberseguridad de cualquier organización. Se destaca su

complejidad y la necesidad de una gestión efectiva para mantener la seguridad de la infraestructura tecnológica.

Uno de los puntos clave es la importancia de la recolección de datos y análisis. Se enfatiza la necesidad de definir qué elementos se deben supervisar, qué datos se deben recopilar y cómo se deben almacenar. Esto es crucial para tomar decisiones informadas y garantizar la seguridad de una organización PYME. La gestión de vulnerabilidades también se destaca como un proceso continuo y proactivo que busca identificar, evaluar y corregir debilidades en sistemas, redes y aplicaciones. La naturaleza cambiante de las amenazas subraya la necesidad de un esfuerzo constante en esta área.

En cuanto a la arquitectura, se describen tres enfoques: centralizada, distribuida y descentralizada. La elección de la arquitectura depende de las necesidades específicas de la organización y su infraestructura.

Por último, el personal en un SOC desempeña roles específicos, desde la recopilación y clasificación de datos hasta la gestión de amenazas y la supervisión a nivel gerencial. Cada nivel tiene responsabilidades específicas en la gestión de seguridad y la respuesta a incidentes, lo que resalta la importancia de contar con un equipo capacitado y bien organizado para hacer frente a los desafíos de seguridad.

En resumen, la operación de un SOC es un proceso complejo y esencial para garantizar la seguridad en el entorno empresarial actual. La gestión de datos, la colaboración, la gestión de vulnerabilidades y la respuesta a incidentes son elementos fundamentales que requieren un enfoque constante y una estrategia sólida. El personal del SOC desempeña un papel crucial en este proceso, asegurando que la organización esté preparada para enfrentar amenazas cambiantes y mantener su infraestructura tecnológica segura.

5.2.9 ¿Es un Security Operations Center Efectivo?

Hasta el momento, hemos explorado cómo funciona y opera un Security Operations Center (SOC) a partir de la información recopilada. Sin embargo, debemos analizar si la información presentada es aplicable a las empresas que forman parte de la entidad organizativa denominada Pyme y si su implementación es viable.

Según (McKee & Kim, 2022)[44], es fundamental establecer una definición clara de lo que es un SOC, ya que muchas organizaciones podrían afirmar que tienen uno. La pregunta relevante es cuántas de estas organizaciones tienen un SOC efectivo, capaz de proteger la disponibilidad, confidencialidad e integridad de sus activos.

(Vielberth, Böhm, Fichtinger, & Pernul, Security Operations Center: A Systematic Study and Open Challenges, 2020)[45], en su estudio sobre los desafíos de los SOC, enfatiza la importancia de identificar las necesidades específicas de la organización para implementar una estructura de seguridad compleja que fortalezca la postura de seguridad.

(Korff, 2023)[46] destaca la influencia de la tecnología en la eficacia de un SOC y la necesidad de que sea fácil de usar. Además, menciona que los SOC sin la

---

[44] THE DEFINITION of soc-cess? SANS 2018 security operations center survey | SANS institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.sans.org/white-papers/definition-soc-cess-sans-2018-security-operations-center-survey/>.

[45] op. cit

[46] HOW MUCH does it cost to build a 24x7 SOC? | Expel [Anónimo]. Expel [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://expel.com/blog/how-much-does-it-cost-to-build-a-24x7-soc>.

tecnología adecuada para la investigación pueden resultar ineficaces y que las inversiones tecnológicas aumentan a medida que crece una organización.

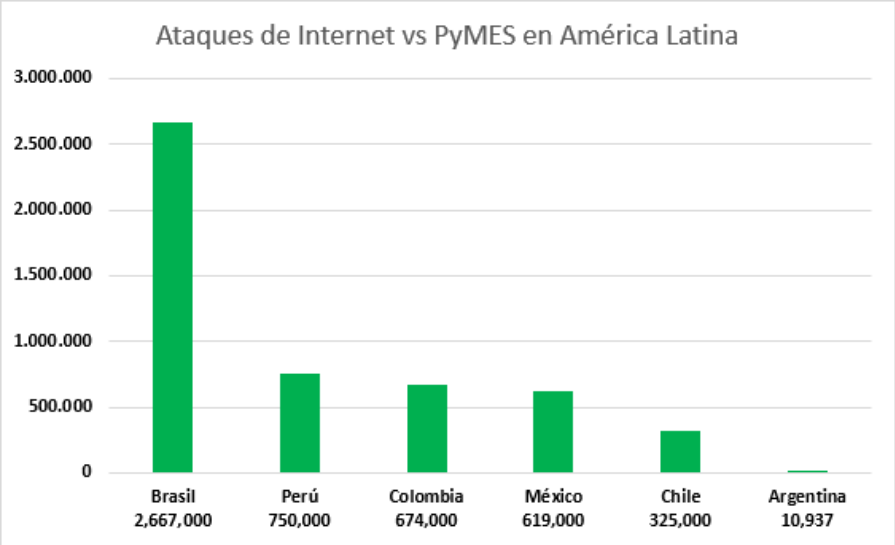
Según Intenz, Colombia es el tercer país que ha experimentado más ataques a las pymes en 2022, con un total de 674.000 ataques, precedido por Brasil con 2.667.000 y Perú con 750.000.

Los autores mencionados hasta el momento hacen referencia a la implementación security Operation center desde el punto de vista técnico y conceptual, Sin embargo, se debe tener en cuenta, la implementación de este tipo de servicio desde el punto de vista del negocio. Es decir, se requiere revisar sí los costos de implementación pueden llegar a ser mucho más grandes de lo que se puede llegar a cubrir a través del ingreso de una organización en cuanto a los indicadores de utilidad.

Según (Korff, 2023)[47]., la implementación de un SOC puede tener costos anuales que varían entre 1.42 millones y 6.25 millones, teniendo en cuenta tanto los costos de personal como las herramientas utilizadas.

[47] op. cit

Figura 6 Ataques de Internet Vs Pymes.



Fuente https://intenz.co/2022/06/16/las-pymes-de-america-latina-enfrentan-un-creciente-numero-de-ciberataques/

La creación de un Security Operations Center (SOC) para una pequeña o mediana empresa (PYME) es un proceso que involucra varios factores críticos para su éxito. Algunos de los factores determinantes en la creación de un SOC para PYME son:

- Necesidades de Seguridad Específicas: El primer paso es comprender las necesidades de seguridad únicas de la PYME. Esto implica identificar los activos críticos, las amenazas relevantes y los riesgos asociados.

- Presupuesto: El presupuesto es un factor crítico, ya que las PYMEs suelen tener recursos limitados. Es esencial establecer un presupuesto realista que cubra los costos de personal, tecnología y capacitación.

- Recursos Humanos: Contratar o capacitar al personal adecuado es esencial. Esto incluye expertos en seguridad cibernética, analistas de seguridad y personal de TI calificado.

- Tecnología: La selección de las herramientas y tecnologías de seguridad adecuadas es crucial. Esto puede incluir software de detección de intrusiones, firewalls, herramientas de monitoreo, entre otros.

- Políticas y Procedimientos de Seguridad: Establecer políticas de seguridad y procedimientos claros es fundamental para guiar las operaciones del SOC y garantizar la coherencia en la respuesta a incidentes.

- Evaluación de Riesgos: Realizar evaluaciones de riesgos periódicas es necesario para identificar nuevas amenazas y evaluar la eficacia de las medidas de seguridad existentes.

- Cumplimiento Normativo: Las PYMEs deben cumplir con regulaciones específicas relacionadas con la seguridad de la información. Asegurarse de que el SOC esté en línea con estos requisitos es fundamental.

- Estrategia de Escalabilidad: Considerar la capacidad de escalabilidad del SOC a medida que la empresa crece. Esto implica que el SOC pueda manejar un mayor volumen de tráfico y activos a medida que la empresa se expande.

- Tercerización de Servicios: En algunos casos, las PYMEs pueden optar por tercerizar ciertos servicios de seguridad cibernética si no tienen los recursos internos necesarios.

- Cultura de Seguridad: Fomentar una cultura de seguridad cibernética en toda la organización es crucial. Todos los empleados deben ser conscientes de las mejores prácticas de seguridad.

Figura 7 Tipos de Security Operations Center

	Basic SOC	Intermediate SOC	Advanced SOC	Learning SOC
General time estimate	months	months+	quarters	1 to 4 years
Annual cost of tools ($millions)				
Log mgmt/correlation	0.25	0.25	0.30	0.50
Detection	negligible	negligible	0.10	0.20
Investigation and response	-	0.10	0.40	0.50
Intel feeds	-	negligible	0.10	0.20
Workflow/orchestration	-	-	0.20	0.30
Intel management	-	-	-	0.20
Annual cost of personnel ($ millions fully loaded at 1.3x, Washington, DC metro area)				
Core 12-person 24x7 SOC	1.17	1.17	1.17	1.17
Senior/escalation support		0.86	0.86	0.86
Hunt team + manager			0.86	0.86
Intel analysts + manager			0.60	0.60
SOC plumbers			0.31	0.31
Dedicated engineering				0.55
Annual total ($M)	**1.42**	**2.38**	**4.90**	**6.25**
One-Time cost of implementation ($ million)				
Approximate costs ($M)	**0.10**	**0.25**	**0.40**	**0.75**

Fuente: https://expel.com/blog/how-much-does-it-cost-to-build-a-24x7-soc/

Hoy solamente al aspecto técnico y financiero se deben tener en cuenta otras consideraciones organizacionales como:

- Las personas: Se pueden considerar el activo más valioso de una organización. Sin embargo, para este tipo de esquema es necesario tener contratados a expertos en seguridad informática los cuales no son comunes de encontrar en el mercado laboral. Las personas son las que se encargan de tomar

los datos que se presentan en las plataformas y tomar las decisiones tanto a largo como a corto plazo sobre esta información

- Infraestructura: como se venía comentando para la implementación de este tipo de servicio es necesario tener las herramientas adecuadas para que se puedan maximizar las capacidades es por esto que cuando se hace este tipo de implementación se debe garantizar que la organización pueda llegar a cumplir con este tópico en su totalidad.
- Tiempo: en condiciones ideales la implementación de este tipo de plataforma puede llevar hasta años, dado que se parte del hecho que se empiece la implementación desde el día cero donde no se cuenta con el personal contratado ni la infraestructura tecnológica instalada.

5.3 HERRAMIENTAS OPEN SOURCE PARA LA OPERACIÓN DE UN SOC

En el entorno siempre cambiante de la seguridad cibernética, la efectividad de un Centro de Operaciones de Seguridad (SOC) es intrínsecamente dependiente de las herramientas y tecnologías que utiliza. Con la evolución constante de amenazas cibernéticas y la complejidad de los sistemas de información, los SOC enfrentan un desafío constante para detectar, analizar y responder a incidentes de seguridad de manera ágil y precisa.

Las herramientas de código abierto, también conocidas como Open Source, han surgido como un pilar fundamental en la operación de un SOC. Estas soluciones ofrecen a los profesionales de seguridad cibernética la capacidad de personalizar y adaptar sus herramientas a las necesidades específicas de sus organizaciones. Además, proporcionan una transparencia esencial en el funcionamiento de las herramientas, lo que es crucial para comprender y mejorar la postura de seguridad.

Se explorará en profundidad una variedad de herramientas Open Source que se han convertido en pilares fundamentales en la operación de un SOC.

Descubriremos cómo estas soluciones técnicas contribuyen a fortalecer la infraestructura de seguridad de las organizaciones y a abordar los desafíos cada vez más complejos que plantean las amenazas cibernéticas en constante evolución.

5.3.1 Definición de activos.

En una organización, podemos encontrar innumerables dispositivos y sistemas, como impresoras, teléfonos, portátiles y PC de escritorio. Sin embargo, es fundamental identificar aquellos en los que la existencia de una amenaza podría afectar la operación de alguna área de la organización o incluso la organización en su totalidad. Esta identificación es esencial para optimizar la priorización de amenazas que afectan a estos activos.

La priorización del esfuerzo en los activos críticos permite a la organización tomar las acciones necesarias y dirigir los recursos, tanto físicos como humanos, de manera eficiente.

El primer paso necesario para la operación de un SOC implica establecer los activos importantes para la organización. Teniendo esto en cuenta, se debe definir:

- Cuáles son los sistemas o activos esenciales para la continuidad del negocio.
- La dependencia existente entre los sistemas.
- La ubicación de la información sensible de la organización.
- Los sistemas clasificados como críticos dentro de la organización.

5.3.2 Descubrimiento de activos.

A partir de la información existente, se debe construir un inventario de los activos de la organización. Esta información debe ser resguardada en un repositorio que estará a cargo de la gerencia del SOC. Por otra parte, teniendo en cuenta la

dinámica de las organizaciones, se puede afirmar que la información nunca estará al 100% actualizada debido a los cambios que pueden surgir a diario, tanto en software como en hardware. Por este motivo, es necesario contar con una herramienta que permita mantener este tipo de inventario actualizado de forma automática.

Según (Vermeer, 2021)[48], para llevar a cabo el proceso de reconocimiento de activos de forma automática, se pueden establecer tres procedimientos. Cada uno de estos tres enfoques requiere recursos y plataformas tecnológicas diferentes, lo que ayuda a obtener un inventario de activos mucho más amplio y específico. Estas tres formas son la monitorización pasiva de la red, el escaneo activo de la red y el inventario de software basado en el host.

5.3.3 Monitoreo pasivo de la red.

El monitoreo pasivo de la red consiste en la identificación de los diferentes hosts a través de la captura de tráfico. Esto implica observar los paquetes que se transmiten a través de la red de una organización en particular. Este proceso se realiza utilizando herramientas capaces de capturar paquetes, como los "sniffers" de red. Sin embargo, es importante tener en cuenta que, para obtener un inventario completo de todos los hosts de la red, es necesario que exista un tráfico activo entre los dispositivos. De lo contrario, la identificación no será posible para aquellos dispositivos que no estén generando tráfico activo.

5.3.3.1 Ejemplo de Sniffers.

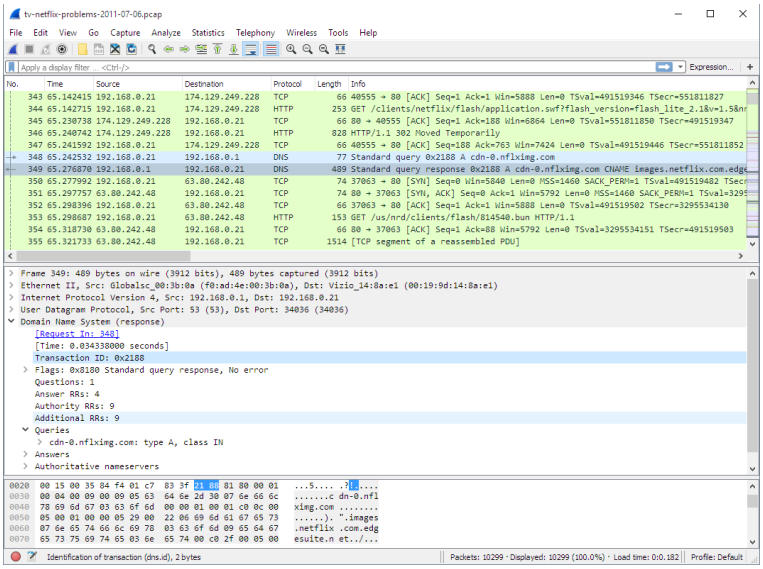
- Wireshark

[48] VERMEER, Mathew, et al. SoK: a framework for asset discovery: systematizing advances in network measurements for protecting organizations. En: 2021 IEEE European Symposium on Security and Privacy (EuroS&P). 2021. p. 440-456.

Es básicamente un analizador de protocolos que permite hacer análisis y solución de problemas de redes de comunicación para datos paquetes y protocolos. Hacer captura de tráfico en la red en tiempo real y la muestra a través de una interfaz gráfica con opciones de organización y filtrado.

Permite hacer examen de datos desde un archivo capturado o capturar tráfico en tiempo real para luego exportarlo. Wireshark se escribió como software libre y se puede distribuir en la mayoría de los sistemas operativos existentes los que incluyen: Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android, y macOS, así como en Microsoft Windows.

Figura 8 Sniffer de red



Fuente https://www.wireshark.org/

5.3.3.2 Monitoreo activo de la red.

Este método de monitorización de la red implica que los hosts respondan a solicitudes desde un servidor específico. A partir de estas respuestas, es posible identificar el tipo de software instalado, el tipo de máquina y los puertos activos. Esto ayuda a mantener un inventario de los hosts, servidores y otros dispositivos en la red de forma automática y actualizada. Sin embargo, debido a la generación de tráfico, puede ocasionar sobrecarga y ruido en la red. Por otra parte, es posible que existan elementos en la red que no respondan debido a las configuraciones de seguridad implementadas.

5.3.3.3 Ejemplo de Network Monitor System.

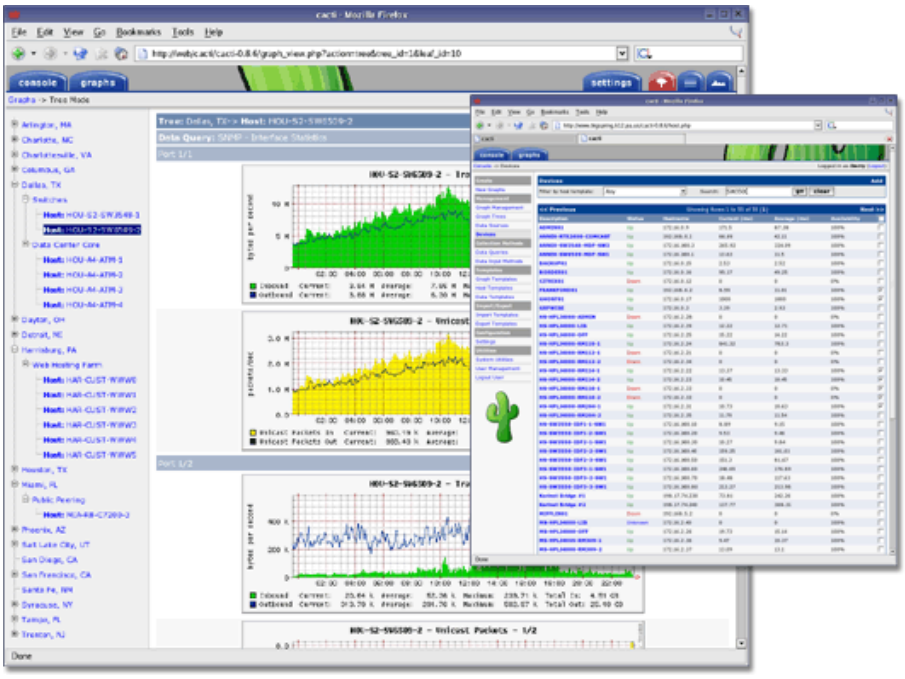
- CACTI

Esta es una herramienta de monitoreo de red de código abierto basada en el sistema de gráficos y el registro de datos de RRDtool. Es una herramienta que se utiliza para sondear redes y recopilar datos de dispositivos en redes de cualquier tamaño. Una de sus ventajas es la capacidad de generar scripts personalizados que permiten llevar a cabo tareas específicas de recopilación de información. Además, es compatible con el protocolo de sondeo SNMP (Simple Network Management Protocol), lo que amplía su versatilidad en la recopilación de datos.

Cacti permite recopilar y organizar información de manera eficiente y ofrece una interfaz gráfica que facilita la visualización de los datos recopilados. Esta herramienta es especialmente útil para administradores de red, ya que les proporciona una visión detallada y organizada de la actividad de la red, lo que les permite tomar decisiones informadas y realizar un seguimiento de la salud y el rendimiento de los dispositivos y servicios en la red.

En resumen, Cacti es una herramienta de monitoreo de red de código abierto que se destaca por su capacidad de recopilación de datos, personalización a través de scripts y compatibilidad con SNMP, lo que la convierte en una herramienta esencial para administrar y optimizar redes de cualquier tamaño.

Figura 9 Herramienta de monitoreo de red Cacti.



Fuente https://es.wikipedia.org/wiki/Cacti

5.3.3.4 Sondeo Basado en el host

En este método para generar inventarios, se puede instalar un agente en los hosts. Este agente permite recopilar información acerca del software instalado en el dispositivo, no solo del que trafica a través de la red o de los puertos activos, sino también de lo que está localmente instalado en el host. A través de esta

herramienta, es posible obtener información mucho más precisa y detallada acerca de los dispositivos que forman parte de la red. Esta información puede incluir modificaciones en los equipos, archivos borrados y registros que hayan sido alterado

Este enfoque es útil para obtener un inventario completo y preciso de los activos de una red, así como para identificar cambios y modificaciones en los dispositivos. Además, permite un monitoreo más detallado de la seguridad y la integridad de los hosts. Un ejemplo de herramienta que utiliza este método es Kibana, que se integra con Elasticsearch y se utiliza para visualizar, analizar y buscar datos en hosts y otros dispositivos en una red. El escaneo basado en el host es valioso para mantener la seguridad y la gestión efectiva de una red.

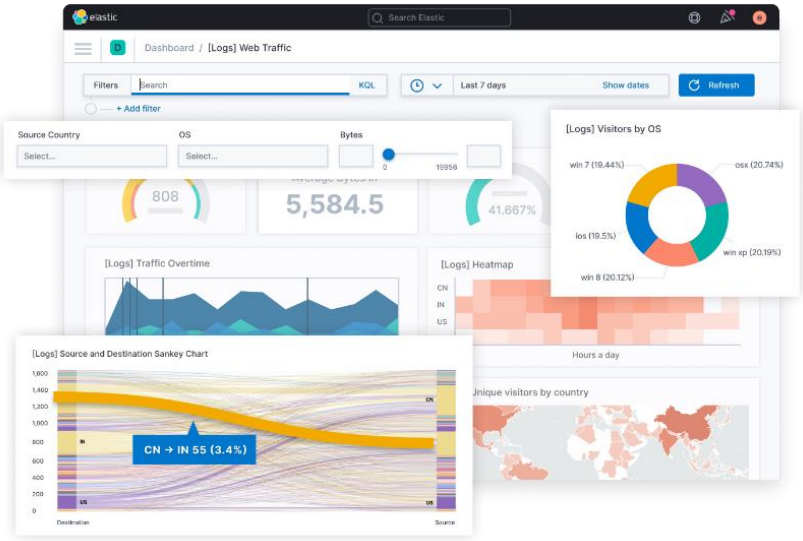
5.3.3.5 Ejemplo de Sondeo Basado en el Host

- Kibana

Kibana es una herramienta gratuita y de código abierto que está integrada en el stack Elastic, proporcionando capacidades para visualizar datos e información interesante almacenada en Elasticsearch. Se utiliza como interfaz de usuario para monitorear, administrar y asegurar clústeres y herramientas relacionadas.

Kibana es especialmente útil para la visualización y análisis de datos y registros almacenados en Elasticsearch, lo que la convierte en una herramienta esencial para quienes desean explorar y comprender los datos en su entorno. Además, ofrece capacidades de búsqueda y filtrado que facilitan la identificación de información relevante. Kibana es ampliamente utilizado en entornos de monitoreo y análisis de logs, lo que permite a los usuarios aprovechar al máximo los datos almacenados en Elasticsearch para tomar decisiones informadas y mantener la seguridad de la red.

Figura 10 Sondeo Basado en el host.



Fuente https://www.elastic.co/es/kibana/

5.3.4 Escaneo de vulnerabilidades

El escaneo de vulnerabilidades de acuerdo con (Scarfone & Mell, 2007)[49] es un proceso fundamental en la ciberseguridad que se utiliza para identificar debilidades y agujeros de seguridad en sistemas informáticos, redes y aplicaciones. Consiste en utilizar herramientas de escaneo y exploración de software para buscar vulnerabilidades conocidas o potenciales que podrían ser explotadas por atacantes. Estas vulnerabilidades pueden incluir errores de programación, configuraciones incorrectas, falta de actualizaciones de seguridad y otros puntos débiles que podrían comprometer la seguridad de un sistema.

[49] SP 800-94, guide to intrusion detection and prevention systems (IDPS) | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://csrc.nist.gov/pubs/sp/800/94/final>.

Durante el proceso de escaneo, se recopila información sobre las vulnerabilidades detectadas, como su gravedad y cómo podrían ser aprovechadas por atacantes. Estos hallazgos se utilizan para generar informes detallados que ayudan a los equipos de seguridad a comprender y priorizar las acciones necesarias para abordar las vulnerabilidades. La corrección de estas debilidades generalmente implica la aplicación de parches, actualizaciones de software, ajustes de configuración o la implementación de medidas de seguridad específicas.

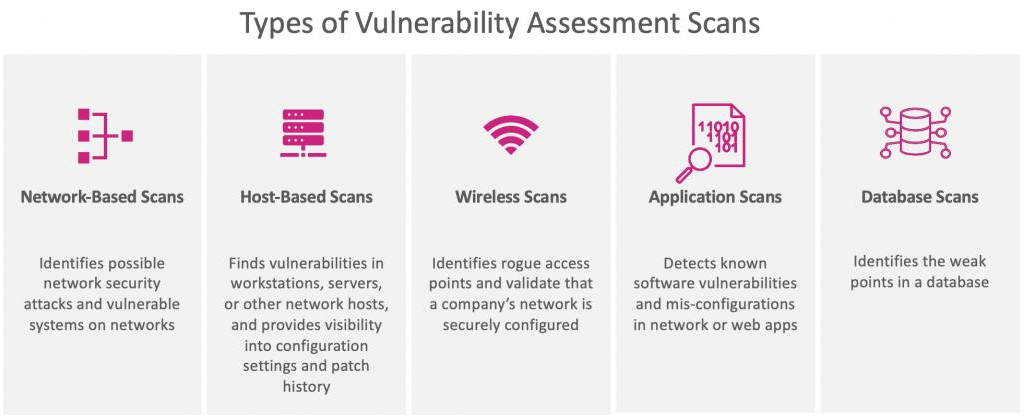
El escaneo de vulnerabilidades es una práctica crítica para garantizar la seguridad de los sistemas y la protección de datos en un entorno cada vez más vulnerable a amenazas cibernéticas. Al realizar escaneos regulares y mantener actualizada la detección de vulnerabilidades, las organizaciones pueden reducir el riesgo de brechas de seguridad y estar preparadas para abordar posibles amenazas antes de que sean explotadas.

Los escáneres de vulnerabilidades son herramientas que permite realizar análisis de los servicios y equipos instalados en una red con el fin de detectar amenazas conocidas. En el análisis de vulnerabilidades, se busca identificar sistemas o equipos en la red que puedan tener vulnerabilidades documentadas en bases de datos, como exploits conocidos, problemas de control de acceso a la red que puedan considerarse inseguros, errores en la programación de paquetes de software, entre otros.

(Balbix, 2019)[50] indica, existen un total de 5 tipos de escáneres de vulnerabilidades:

[50] VULNERABILITY SCANNERS and scanning tools: what to know | balbix [Anónimo]. Balbix [página web]. [Consultado el 21, diciembre, 2023]. Disponible en Internet: <https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/>.

Figura 11 Tipos de escáneres de vulnerabilidades.



Fuente https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/

5.3.4.1 Escáneres Basados en la red.

Los escáneres basados en red son herramientas esenciales en el ámbito de la ciberseguridad y la administración de redes. Su principal función es examinar minuciosamente una red de computadoras en busca de vulnerabilidades, configuraciones incorrectas o posibles amenazas de seguridad que podrían ser aprovechadas por atacantes. Estas herramientas son fundamentales para mantener la integridad y la protección de una red.

Una de las funciones clave de los escáneres de red es la detección de dispositivos activos. Realizan un análisis exhaustivo de la red para identificar los dispositivos que están en línea y accesibles, lo que incluye servidores, computadoras, enrutadores, impresoras, cámaras IP y otros dispositivos de red. Esto proporciona una visión clara de la infraestructura de la red y sus componentes activos.

Además, los escáneres de red también buscan activamente vulnerabilidades conocidas en los dispositivos escaneados. Comparan las características y configuraciones de los dispositivos con una base de datos de vulnerabilidades conocidas para determinar si existen debilidades que podrían ser explotadas por atacantes. Esta identificación temprana de vulnerabilidades es crucial para tomar medidas proactivas y proteger la red contra amenazas potenciales.

5.3.4.2 Escáneres basados en host

Los escáneres basados en host son herramientas esenciales en el campo de la ciberseguridad y la gestión de sistemas informáticos. Su propósito principal radica en la realización de un minucioso análisis de un host o dispositivo individual, como una computadora, servidor o equipo de red, con el fin de identificar vulnerabilidades, configuraciones incorrectas y posibles amenazas a la seguridad. Estas herramientas se utilizan para evaluar y reforzar la seguridad de los sistemas informáticos.

Una de las características distintivas de los escáneres basados en host es su capacidad para detectar vulnerabilidades específicas en el software y las configuraciones de un host en particular. Operan comparando las características y ajustes del host con una base de datos que contiene información sobre vulnerabilidades conocidas. Este proceso permite identificar posibles debilidades que podrían ser explotadas por individuos malintencionados. Como resultado, los administradores de sistemas pueden tomar medidas preventivas para abordar y mitigar estas vulnerabilidades antes de que se conviertan en objetivos de ataques.

Adicionalmente, los escáneres basados en host ofrecen información detallada acerca del software instalado en el host, los puertos que se encuentran abiertos y otros aspectos relacionados con la configuración del sistema. Esta información

resulta fundamental para mantener un inventario preciso de los activos de la red y garantizar que los dispositivos estén configurados de manera segura y en cumplimiento con las políticas de seguridad de la organización. En síntesis, los escáneres basados en host desempeñan un papel crucial en la identificación y mitigación de riesgos en sistemas individuales, contribuyendo a fortalecer la seguridad informática en su conjunto.

5.3.4.3 Escáneres inalámbricos

Los escáneres inalámbricos son herramientas utilizadas en ciberseguridad y administración de redes para identificar y evaluar redes inalámbricas, como las redes Wi-Fi, en busca de vulnerabilidades y posibles amenazas. Estas herramientas permiten a los administradores de redes y expertos en seguridad realizar análisis exhaustivos de las redes inalámbricas, identificar posibles puntos de acceso no autorizados o configuraciones inseguras, y tomar medidas para fortalecer la seguridad de la red.

Los escáneres inalámbricos funcionan capturando datos de las redes inalámbricas dentro de su alcance y analizando esta información en busca de señales de advertencia, como redes abiertas o débilmente protegidas, dispositivos desconocidos o intentos de acceso no autorizado. También pueden identificar problemas de rendimiento en la red inalámbrica y ayudar en la optimización de la configuración de las redes para mejorar la velocidad y la confiabilidad.

Estas herramientas son especialmente útiles en entornos empresariales donde la seguridad de las redes inalámbricas es crítica y puede ser un objetivo para posibles ataques. Los escáneres inalámbricos proporcionan información valiosa que ayuda a proteger la integridad de las redes y garantizan que las comunicaciones inalámbricas se realicen de manera segura y eficiente.

5.3.4.4 Escáneres de aplicaciones.

Los escáneres de aplicaciones son herramientas de seguridad informática diseñadas para identificar vulnerabilidades y debilidades en aplicaciones de software, incluyendo aplicaciones web, móviles y de escritorio. Estas herramientas analizan el código fuente, la configuración y el comportamiento de las aplicaciones en busca de posibles fallos de seguridad que podrían ser explotados por atacantes maliciosos. El objetivo principal de los escáneres de aplicaciones es mejorar la seguridad y proteger la integridad de las aplicaciones, así como los datos y sistemas que interactúan con ellas.

Los escáneres de aplicaciones utilizan diversas técnicas de análisis, como el escaneo estático y dinámico, para identificar vulnerabilidades comunes, como inyección de SQL, cross-site scripting (XSS), y autenticación débil, entre otras. También pueden evaluar la exposición a amenazas conocidas y evaluar si las aplicaciones cumplen con las mejores prácticas de seguridad. Además, los escáneres de aplicaciones pueden ayudar a los desarrolladores a detectar errores de programación y configuración que podrían dar lugar a vulnerabilidades.

Estas herramientas son esenciales en la gestión de la seguridad de las aplicaciones y son ampliamente utilizadas en organizaciones que desarrollan o utilizan software para garantizar que sus aplicaciones sean resistentes a ataques y cumplan con los estándares de seguridad. El uso de escáneres de aplicaciones es una parte fundamental de las prácticas de seguridad de aplicaciones (AppSec) y ayuda a prevenir brechas de seguridad y proteger la información confidencial.

5.3.4.5 Escáneres de bases de datos

Los escáneres de base de datos son herramientas de seguridad informática diseñadas para evaluar y auditar la seguridad de sistemas de gestión de bases de datos (DBMS, por sus siglas en inglés) y las bases de datos almacenadas en ellos. Estas herramientas identifican vulnerabilidades, debilidades y configuraciones incorrectas en los sistemas de gestión de bases de datos que podrían ser explotadas por atacantes maliciosos. El objetivo principal de los escáneres de base de datos es garantizar la integridad y seguridad de los datos almacenados en las bases de datos, así como proteger los sistemas que dependen de ellas.

Los escáneres de base de datos pueden llevar a cabo una variedad de pruebas y análisis, como la identificación de vulnerabilidades de seguridad comunes en las bases de datos, la evaluación de configuraciones inseguras, la detección de contraseñas débiles o predeterminadas, y la evaluación del cumplimiento con las políticas de seguridad y regulaciones. Estas herramientas pueden ser útiles tanto para administradores de bases de datos como para auditores de seguridad, ya que permiten identificar y corregir problemas de seguridad antes de que sean explotados por terceros no autorizados.

En resumen, los escáneres de base de datos son esenciales para garantizar la seguridad de las bases de datos y la información que contienen. Ayudan a prevenir brechas de seguridad, proteger datos confidenciales y mantener la integridad de los sistemas que dependen de estas bases de datos, lo que es fundamental en entornos empresariales y organizaciones que gestionan grandes volúmenes de datos.
Software para Análisis de Vulnerabilidades de Código Abierto

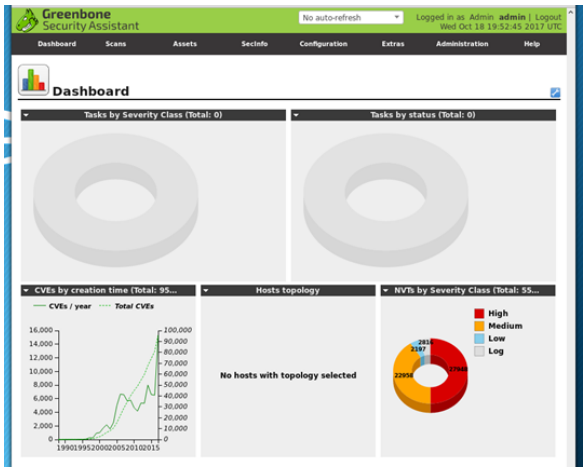
5.3.4.6 Ejemplo de Escáneres de Vulnerabilidades

- OpenVas

OpenVAS (Open Vulnerability Assessment System) es una plataforma de escaneo de vulnerabilidades de código abierto que se utiliza para identificar y evaluar las debilidades de seguridad en sistemas y redes. Es una herramienta esencial en la gestión de la seguridad de la información y se utiliza para detectar posibles amenazas y riesgos en una infraestructura de TI.

OpenVAS realiza un análisis automatizado de sistemas y aplicaciones en busca de vulnerabilidades conocidas. Funciona escaneando activamente dispositivos y redes en busca de problemas de seguridad, como puertos abiertos, configuraciones incorrectas y software desactualizado. La herramienta utiliza una base de datos de vulnerabilidades conocidas y exploits para comparar los hallazgos y generar informes detallados que ayudan a los administradores de sistemas a tomar medidas correctivas.

Figura 12 Openvas.



Fuente http://www.openvas.org/

- OpenSCAP

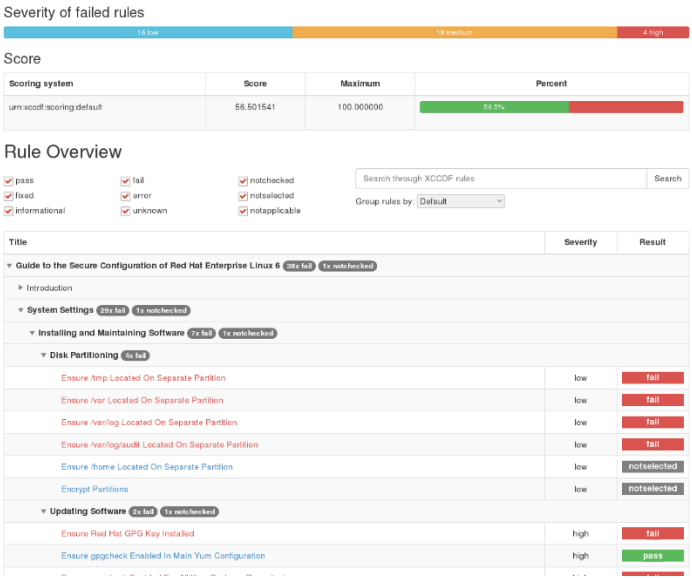
OpenSCAP es una herramienta que automatiza la evaluación y el monitoreo de la seguridad de sistemas y aplicaciones, permitiendo a las organizaciones identificar y corregir vulnerabilidades, configuraciones incorrectas y otros riesgos de seguridad.

Utiliza estándares y perfiles de seguridad reconocidos, como el estándar SCAP (Security Content Automation Protocol), para medir el cumplimiento con políticas de seguridad y regulaciones, como CIS Benchmarks, STIGs, y otros.

OpenSCAP puede escanear sistemas en busca de vulnerabilidades conocidas, verificar configuraciones de seguridad, auditar políticas de acceso, y generar informes detallados sobre el estado de la seguridad.

Es una herramienta valiosa para administradores de sistemas y profesionales de seguridad que desean mantener la seguridad de sus sistemas, garantizar el cumplimiento normativo y mejorar la postura de seguridad de cualquier organización.

Figura 13 Openscap



Fuente https://www.open-scap.org/getting-started/

- Nmap

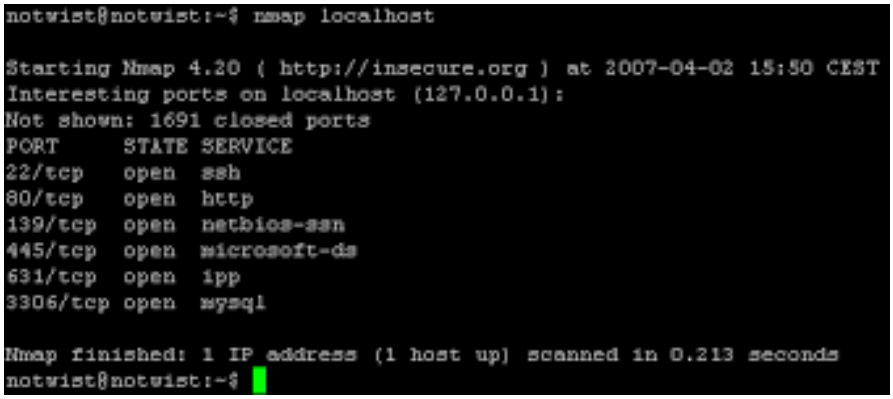
Nmap es una herramienta de línea de comandos que se utiliza para explorar y mapear redes. Su capacidad principal es escanear hosts en una red para determinar su disponibilidad y descubrir puertos abiertos en esos hosts.

Esta herramienta es ampliamente utilizada en seguridad informática para evaluar la seguridad de una red. Puede identificar servicios y sistemas operativos que se ejecutan en los puertos escaneados, lo que es esencial para detectar vulnerabilidades y configuraciones incorrectas.

Nmap ofrece diversas opciones de escaneo, desde escaneos simples de puertos hasta escaneos más avanzados que incluyen detección de sistemas operativos, detección de versiones de servicios y escaneo de vulnerabilidades.

Es una herramienta de código abierto ampliamente reconocida y respaldada por una comunidad activa de usuarios y desarrolladores.

Figura 14 NMAP



Fuente. https://en.wikipedia.org/wiki/Nmap

- Wireshark

Wireshark es una herramienta de análisis de protocolos de red ampliamente utilizada en la seguridad informática para la detección y evaluación de vulnerabilidades. Su función principal es capturar y analizar el tráfico de red en tiempo real o a partir de archivos de captura.

Wireshark se utiliza para analizar el tráfico de red en busca de vulnerabilidades y amenazas de seguridad. Esto implica la identificación de posibles debilidades en protocolos, servicios y aplicaciones que pueden ser explotadas por atacantes.

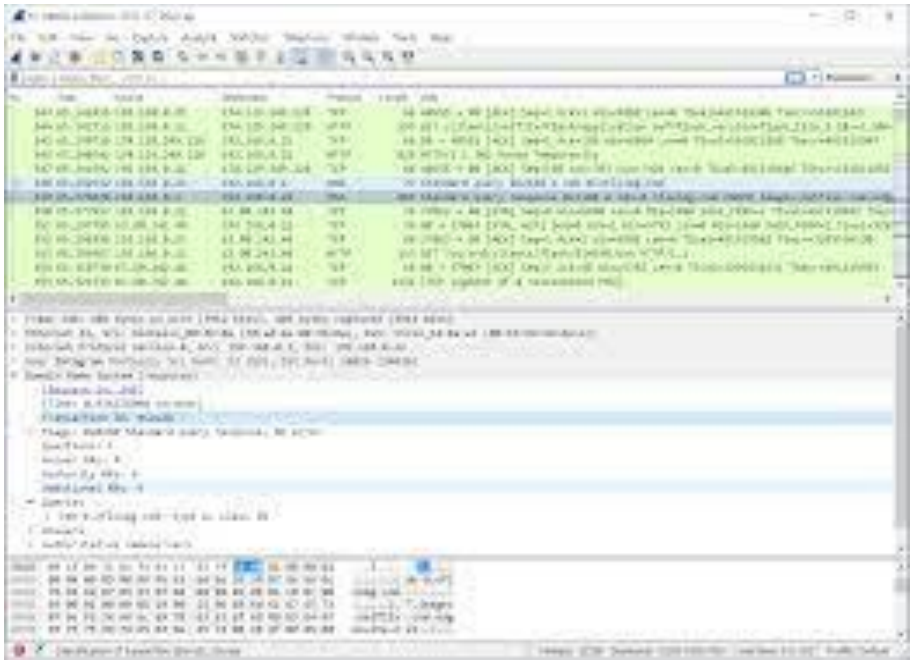
La herramienta puede capturar paquetes de datos que fluyen a través de una red y proporciona una vista detallada de cada paquete. Los analistas de seguridad

pueden examinar los datos para detectar posibles problemas, como contraseñas en texto claro, ataques de fuerza bruta, inyección de comandos, y otras amenazas.

Wireshark es útil para analizar ataques de red en tiempo real, lo que permite a los profesionales de seguridad detectar y responder a amenazas de manera efectiva.

Además de la detección de vulnerabilidades, Wireshark también se utiliza para identificar configuraciones incorrectas y problemas de seguridad en la red. Puede ayudar a identificar dispositivos mal configurados, servidores vulnerables y otros riesgos potenciales.

Figura 15 Wireshark



Fuente https://www.wireshark.org/

5.3.5 Detección de Intrusiones.

De acuerdo con (Raghunath & Mahadeo, 2008)[51], los sistemas de detección de intrusiones son herramientas empleadas para detectar accesos no autorizados a una red o sistema, generando alarmas a través de archivos o registros que luego son analizados por el equipo del SOC. Nuestra plataforma genera una alarma cuando se detecta algún tipo de acceso no autorizado a estos sistemas, pero no realiza acciones correctivas ante tales accesos. Por otro lado, existen las Intrusion Prevention Systems (IPS), que también se utilizan para detectar accesos no autorizados, pero con la capacidad de prevenirlos o incluso mitigarlos.

Los IDS se basan en el uso de reglas para analizar el tráfico en una red. Cuando un evento cumple con alguna de las reglas configuradas, se genera una alarma o aviso que el analista del SOC debe analizar para determinar las acciones correctivas necesarias con el fin de prevenir incidentes críticos en la red.

5.3.5.1 Network Intrusion Detection System (NIDS)

Los Network Intrusion Systems (NIDS) (Raghunath & Mahadeo, 2008)[52] son sistemas diseñados para detectar intrusiones en tiempo real al analizar el tráfico de red en busca de anomalías que podrían representar un riesgo para los activos críticos e infraestructura de una organización. Como se mencionó anteriormente, estos sistemas se basan en la definición de reglas, las cuales pueden ser personalizadas y ajustadas según las necesidades del personal del SOC. Además,

---

[51] RAGHUNATH, Bane Raman y MAHADEO, Shivsharan Nitin. Network intrusion detection system (NIDS). En: 2008 First International Conference on Emerging Trends in Engineering and Technology. 2008. p. 1272-1277.

[52] Ibid

existen repositorios de reglas que son generados por la comunidad y que pueden ser utilizados en caso de ser necesarios. Algunas empresas también crean sus propios repositorios de reglas, diseñados específicamente para su uso interno y sin ser compartidos fuera de la organización. Cuando se detectan eventos que cumplen con estas reglas, el sistema genera alarmas para alertar al personal del SOC y tomar las medidas necesarias.

Estos sistemas son esenciales para salvaguardar la seguridad de una red, ya que permiten una respuesta más rápida y efectiva ante posibles amenazas. Además, su capacidad de personalización garantiza que se adapten a las necesidades específicas de cada organización. También es importante destacar que la comunidad de seguridad informática contribuye al desarrollo de reglas y firmas para NIDS, lo que amplía el conjunto de herramientas disponibles y fortalece la ciberseguridad a nivel global.

5.3.5.2 Host Intrusion Detection System (HIDS)

El Host Intrusion Detection System (HIDS) es un sistema de detección que opera mediante la instalación de un agente directamente en el host o dispositivo que se busca proteger. A través de este análisis, se pueden identificar host comprometidos por ataques o intentos de ataques, y se pueden activar respuestas automáticas para corregir o mitigar dichos ataques. Este enfoque tiene ventajas significativas, ya que permite la recolección de datos y registros de eventos con alta precisión. Además, supervisa la integridad de archivos y claves de registro, genera un inventario detallado de procesos en ejecución y aplicaciones instaladas, monitorea puertos, detecta artefactos de malware, evalúa la configuración y supervisa las políticas activas.

Una de las ventajas más notables de los HIDS es su versatilidad, ya que los agentes pueden ser instalados en diversos sistemas operativos, lo que amplía su aplicabilidad. Además, estos sistemas se pueden configurar a través de una interfaz de gestión que está disponible para los responsables del SOC. Esto facilita su adaptación a las necesidades y características específicas de cada organización y permite una administración centralizada de la seguridad en los hosts. Estos sistemas son cruciales para proteger activos críticos y garantizar la integridad y seguridad de los dispositivos en una red.

5.3.5.3 Intrusion Prevention System.

Un Sistema de Prevención de Intrusiones (IPS) es una plataforma de seguridad que tiene la capacidad de monitorear de manera constante una red en busca de actividades maliciosas y tomar medidas para prevenirlas. Los IPS son una evolución más avanzada en comparación con los Sistemas de Detección de Intrusiones (IDS), ya que, a diferencia de los IDS que solo generan alertas cuando se detecta actividad sospechosa, los IPS pueden prevenir o tomar acciones correctivas cuando se detecta actividad maliciosa. En muchos casos, estos sistemas están integrados en firewalls de próxima generación (NGFW) o en sistemas unificados de amenazas (UTM). La implementación de un IPS se realiza en función del volumen de tráfico y de la cantidad de activos vulnerables presentes en la red.

Los IPS monitorean el flujo de tráfico de red entre el origen y el destino, generalmente ubicados detrás de un firewall. Utilizan diferentes métodos de prevención de intrusiones, que incluyen:

- Basados en firmas: Este enfoque busca coincidencias entre el tráfico y firmas de amenazas conocidas. Si se detecta una coincidencia, se toma una acción para bloquear o prevenir la amenaza. Sin embargo, este método no puede identificar ataques nuevos que no estén registrados en las firmas de amenazas.

- Basados en anomalías: Este método supervisa el tráfico en busca de comportamientos anormales en comparación con el comportamiento estándar de la red. Se basa en muestras aleatorias de actividad y utiliza tecnología de inteligencia artificial y aprendizaje automático para identificar amenazas. Aunque es más robusto que el enfoque basado en firmas puede generar falsos positivos.
- Basados en políticas: Este enfoque se basa en las políticas definidas por la empresa y bloquea cualquier actividad que viole esas políticas. Aunque es menos común que los otros dos métodos, es útil para aplicar restricciones específicas a la actividad de la red según las políticas de seguridad de la organización.

5.3.5.4 Software para la Detección y Prevención de Intrusiones de Código Abierto.

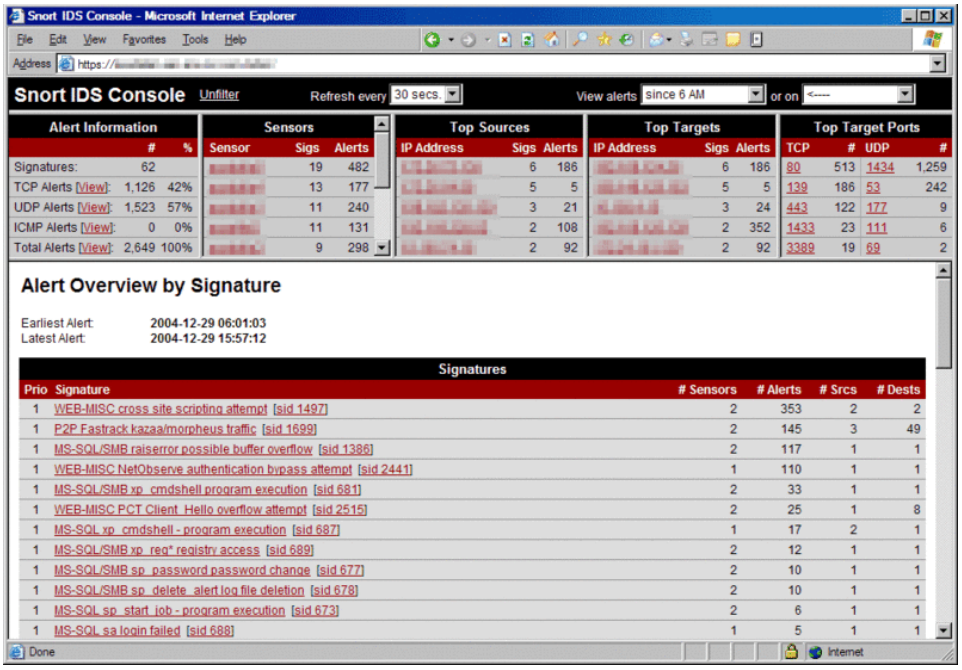
- Snort.

Este es un sistema de detección de intrusos y prevención de ingreso pasado en red. Snort es un sistema de detección de intrusiones de código abierto creado por Martin Roesch en 1998. Este software es ampliamente utilizado en el ámbito de la seguridad informática y se emplea para detectar actividades maliciosas en redes de computadoras. Snort opera analizando el tráfico de red en tiempo real y se basa en reglas personalizables para identificar patrones y comportamientos sospechosos que puedan indicar intrusiones o amenazas de seguridad.

Las funcionalidades clave de Snort incluyen la detección de intrusiones en tiempo real, la capacidad de analizar paquetes de datos en busca de amenazas, la generación de alertas cuando se detecta actividad maliciosa y la capacidad de adaptarse a las necesidades específicas de seguridad de una organización mediante reglas personalizadas. Snort puede operar como un Sistema de Detección de Intrusiones en Red (NIDS) para monitorear y alertar sobre amenazas, o como un Sistema de Prevención de Intrusiones (IPS) para bloquear o prevenir actividades maliciosas.

En resumen, Snort es una herramienta esencial en el campo de la seguridad informática que fue desarrollada por Martin Roesch. Opera mediante la detección de patrones y comportamientos sospechosos en el tráfico de red en tiempo real y ofrece una amplia gama de funcionalidades para fortalecer la seguridad de redes y sistemas.

Figura 16 Plataforma SNORT



Fuente https://es.wikipedia.org/wiki/Snort

La implementación de Snort puede presentar desafíos, como la complejidad de configuración, la posibilidad de falsos positivos y falsos negativos, el impacto en el rendimiento del sistema y la red, la necesidad de actualizaciones constantes, costos asociados, protección limitada y la necesidad de un aprendizaje continuo. A pesar

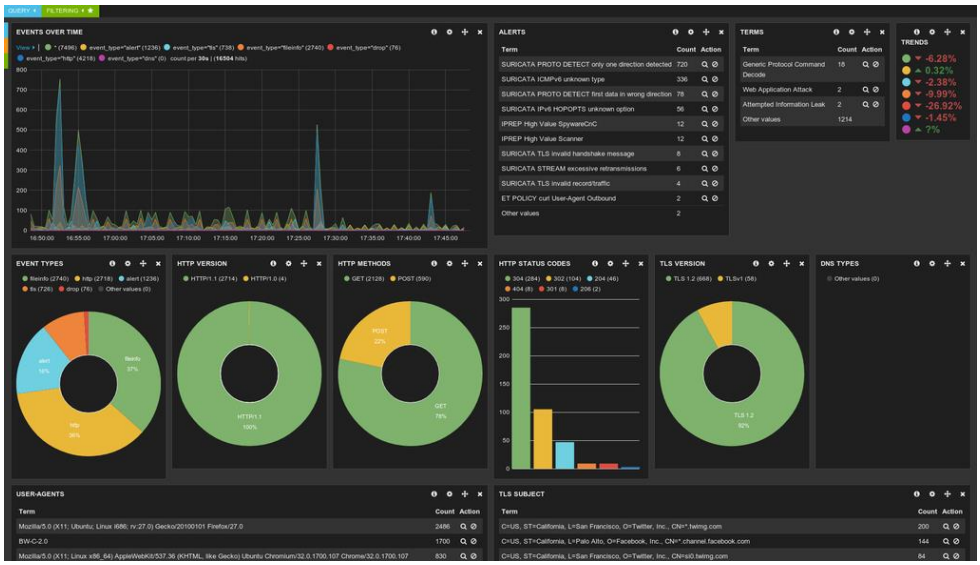
de estos desafíos, Snort sigue siendo valioso para la seguridad cibernética cuando se administra correctamente.

- Suricata

Suricata es una herramienta de prevención y detección de intrusiones de código abierto y alta velocidad diseñada para garantizar la seguridad de las redes y sistemas de información. Fue desarrollada como una bifurcación de Snort y proporciona un conjunto de características más avanzadas. Suricata es altamente versátil y se ejecuta en varios sistemas operativos, incluyendo Linux, Windows y FreeBSD. Ofrece funciones como detección de amenazas en tiempo real, análisis de tráfico de red, registro de eventos, capacidad de inspección profunda de paquetes, soporte para reglas personalizadas y el uso de una variedad de protocolos.

Suricata está optimizada para un alto rendimiento y es capaz de analizar el tráfico de red a alta velocidad. Puede integrarse con otros sistemas de seguridad y herramientas de administración, lo que lo convierte en una herramienta valiosa para la protección de redes empresariales y sistemas críticos. Además, Suricata es conocida por su capacidad de inspección de aplicaciones en capas superiores y la detección precisa de amenazas, lo que la convierte en una opción popular para garantizar la seguridad de la red en entornos empresariales y de datos sensibles.

Figura 17 Plataforma Suricata.



Fuente https://en.wikipedia.org/wiki/Suricata_%28software%29

- Zeek.

Zeek, anteriormente conocido como Bro, es un sistema de monitorización y análisis de red de código abierto que opera en sistemas basados en Unix, como Linux y macOS. Funciona pasivamente observando el tráfico de red y registrando eventos y metadatos relacionados con esa actividad. Zeek emplea una variedad de módulos y scripts para analizar el tráfico y extraer información relevante de los paquetes de datos.

Las capacidades de Zeek son diversas y poderosas. Puede detectar y registrar eventos de red, como conexiones TCP/UDP, solicitudes HTTP, DNS y mucho más. También tiene la capacidad de analizar el contenido de los paquetes, lo que lo hace eficaz en la detección de amenazas cibernéticas y actividades maliciosas. Zeek es

altamente personalizable a través de scripts y reglas, lo que permite a los administradores adaptarlo a las necesidades específicas de su red y organización.

Zeek es ampliamente utilizado en entornos de seguridad cibernética y permite la generación de registros detallados para el análisis posterior. Su capacidad para proporcionar visibilidad y detectar intrusiones en la red lo convierte en una herramienta valiosa para la monitorización de seguridad y la investigación de incidentes. Funciona en tiempo real y es especialmente útil para identificar comportamientos anómalos en la red y posibles amenazas cibernéticas.

Figura 18 Plataforma Zeek.

Fuente https://www.criticalpathsecurity.com/services/managed-zeek-ids/zeek-ids-use-cases/

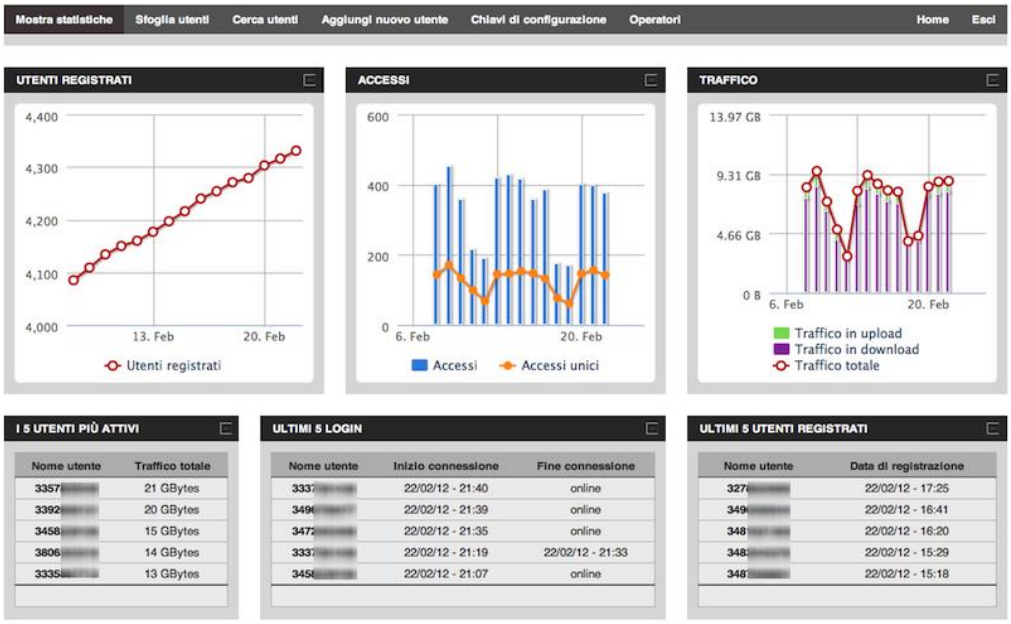
- OpenWIPS-ng.

OpenWIPS-ng es un sistema de prevención de intrusiones inalámbricas de código abierto diseñado para proteger las redes Wi-Fi contra amenazas y ataques. Su funcionamiento se basa en la monitorización continua del tráfico de red inalámbrica para detectar comportamientos y patrones anómalos que puedan indicar intrusiones o actividades maliciosas.

Este sistema es altamente personalizable y adaptable, lo que lo hace adecuado para una amplia variedad de entornos y necesidades de seguridad. OpenWIPS-ng se ejecuta en sistemas basados en Unix y es compatible con la mayoría de las tarjetas inalámbricas y adaptadores Wi-Fi. Puede detectar una amplia gama de amenazas, como ataques de denegación de servicio (DoS), ataques de hombre en el medio (MitM), intentos de intrusión y escaneos no autorizados de la red inalámbrica.

OpenWIPS-ng ofrece una solución efectiva para proteger las redes inalámbricas y garantizar la integridad y la seguridad de los datos transmitidos a través de ellas. Su capacidad para detectar y responder proactivamente a las amenazas lo convierte en una herramienta valiosa para garantizar la seguridad de las redes Wi-Fi en entornos empresariales, institucionales y domésticos.

Figura 19 Plataforma Openwisp.



Fuente https://openwisp.org/legacy.html

- Sguil.

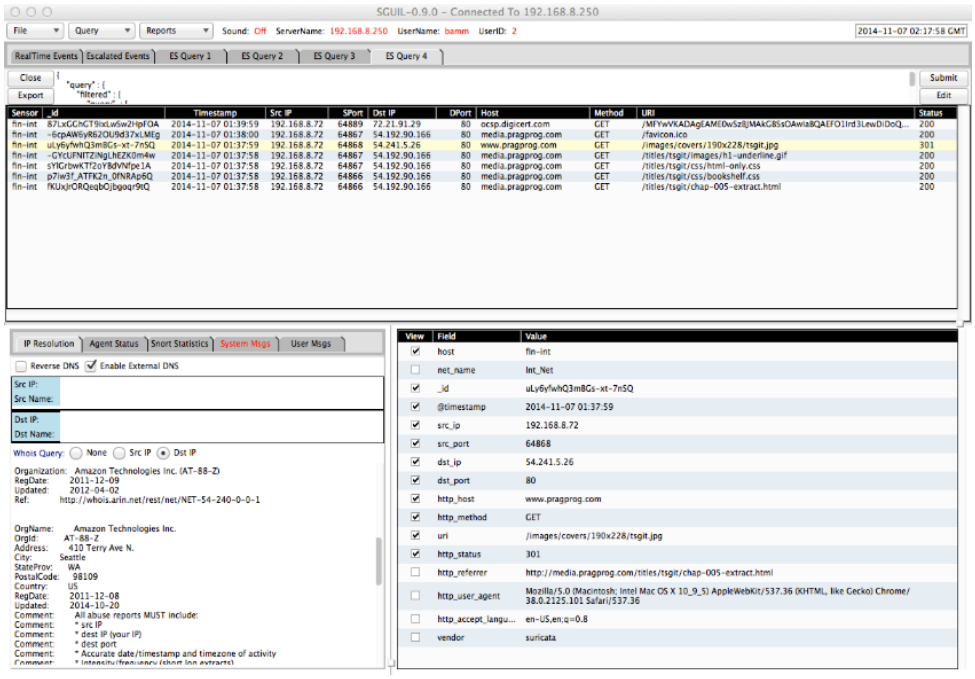
Sguil es una plataforma de gestión de seguridad de red de código abierto que se utiliza para monitorear, analizar y responder a amenazas y eventos de seguridad en una red. Diseñada para la detección y respuesta de intrusiones, Sguil integra varias herramientas y componentes de seguridad en un único entorno para proporcionar una visión centralizada de la seguridad de la red.

Funciona recopilando y correlacionando datos de múltiples fuentes, como sensores de IDS (Sistemas de Detección de Intrusiones) y registros de firewall, y los presenta en una interfaz unificada para su análisis por parte de los analistas de seguridad. Sguil también facilita la colaboración y la comunicación entre los miembros del

equipo de seguridad, lo que permite una respuesta más rápida y efectiva a incidentes.

Sguil es altamente personalizable y se puede adaptar a las necesidades específicas de una organización. Ofrece una variedad de características que ayudan a los equipos de seguridad a identificar amenazas, investigar incidentes y tomar medidas correctivas.

Figura 20 Plataforma Squil



Fuente https://bammv.github.io/sguil/

5.4 MARCO DE TRABAJO

Un marco de referencia para un SOC define la arquitectura de los componentes que entregan la funcionalidad del SOC y cómo se interrelacionan.

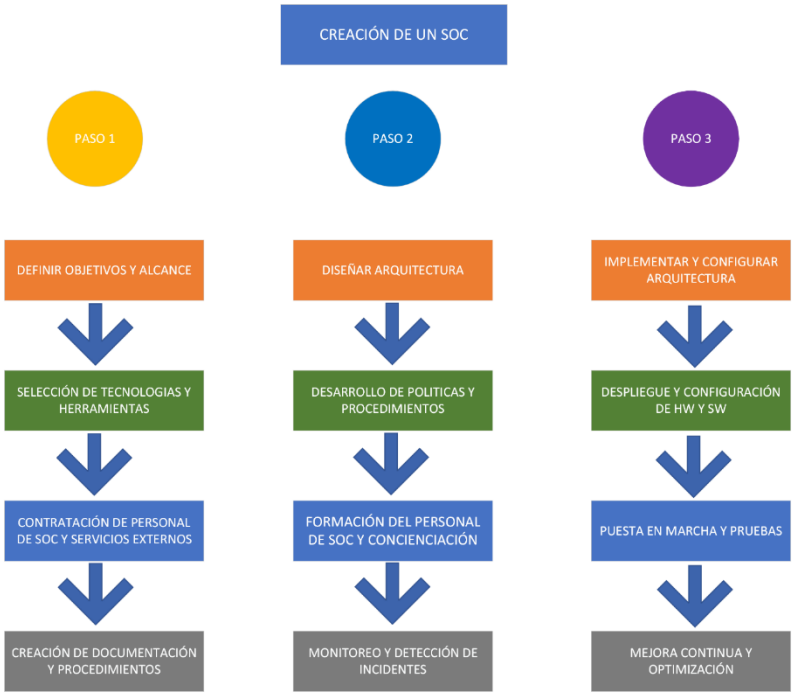
- Definir los objetivos y alcance del SOC: Antes de comenzar, es importante tener claridad sobre los objetivos del SOC y qué áreas de seguridad cubrirá. Esto puede incluir la detección de amenazas, la respuesta a incidentes, la monitorización de la red y otros aspectos.

- Establecer un equipo de seguridad: Reunir un equipo dedicado que estará a cargo de operar y mantener el SOC. Este equipo puede incluir analistas de seguridad, investigadores de incidentes, especialistas en respuesta a incidentes, administradores de sistemas y otros profesionales.

- Definir los procesos y procedimientos: Documentar los procesos y procedimientos para la detección, análisis y respuesta a incidentes. Esto puede incluir la gestión de alertas, el escalamiento de incidentes, la clasificación de incidentes, la comunicación con las partes interesadas, entre otros.

- Seleccionar y configurar las herramientas de seguridad informática: Investigar y seleccionar las herramientas de código abierto adecuadas para el SOC. Algunas herramientas populares incluyen Snort, Suricata, OSSEC, ELK Stack, TheHive y MISP. Estas herramientas deben configurarse y personalizarse de acuerdo con las necesidades específicas.

Figura 21 Marco de Trabajo



Fuente: Propia

- Configurar la monitorización de eventos y registros: Establecer la recopilación y monitorización de eventos y registros de seguridad de la infraestructura de red. Esto implica la configuración de registros de sistemas operativos, sistemas de información, control lógico, aplicaciones, firewalls, IDS/IPS y otros dispositivos de red.

- Implementar los procesos de correlación y análisis de eventos: Utilizar las herramientas seleccionadas para correlacionar y analizar los eventos y registros recopilados. Esto ayudará a identificar y gestionar amenazas y patrones de comportamientos maliciosos.

- Establecer un proceso de gestión de incidentes: Definir un proceso que incluya la clasificación, respuesta, contención y recuperación de la información en caso

de incidentes. Herramientas como TheHive son útiles para la colaboración y el seguimiento de incidentes.

- Implementar un proceso de inteligencia de amenazas: Configurar herramientas para la identificación de fuentes de amenazas y compartir indicadores de compromiso y datos relevantes sobre amenazas.

- Realizar revisiones periódicas: Es fundamental realizar revisiones regulares de las buenas prácticas en el uso de herramientas de seguridad, procesos y procedimientos para garantizar su eficacia y realizar mejoras continuas.

- Capacitar y sensibilizar al personal: Proporcionar capacitación continua a los empleados y el personal del SOC para mantenerse actualizados sobre las amenazas y técnicas de prevención de seguridad informática.

5.4.1 Procesos y procedimientos para crear un SOC

En cuanto a los procesos y procedimientos para la creación de un SOC, se deben implementar una serie de prácticas para garantizar la eficacia y eficiencia de las operaciones de seguridad. Esto incluye definir los objetivos, el alcance, las funciones y las responsabilidades del SOC, así como los indicadores de rendimiento (KPI) y los niveles de servicio (SLA) esperados.

También se debe establecer una metodología de gestión de incidentes que abarque las fases de detección, análisis, priorización, respuesta, contención, erradicación, recuperación e investigación forense.

La arquitectura de red debe ser diseñada e implementada para permitir la captura y el análisis del tráfico de red y los eventos de seguridad generados por diferentes sistemas y dispositivos.

Se debe determinar, instalar y configurar las herramientas de seguridad informática de código abierto que se utilizarán en el SOC. La integración de estas herramientas, junto con la configuración y el mantenimiento según las mejores prácticas, es esencial.

La monitorización constante de eventos y registros de seguridad es crucial para la detección temprana de amenazas. Los procesos de correlación y análisis ayudarán a identificar patrones de comportamientos maliciosos.

La gestión de incidentes debe abordar la clasificación, respuesta, contención y recuperación de incidentes, utilizando herramientas de colaboración y seguimiento.

Un proceso de inteligencia de amenazas debe configurarse para identificar fuentes de amenazas y compartir indicadores de compromiso y otra información relevante.

Por último, se deben realizar pruebas periódicas para garantizar el funcionamiento efectivo de las herramientas y los procedimientos, así como la documentación y revisión continua de los incidentes y lecciones aprendidas.

5.4.2 Desafíos en la creación de un SOC

Crear un SOC con herramientas de código abierto implica desafíos que se deben tener en cuenta:

- La integración y la compatibilidad de las diferentes herramientas entre sí, con otros sistemas de información o servicios pueden ser complejos y requieren de alto nivel de conocimiento técnico.

- La calidad y la fiabilidad de las herramientas de código abierto pueden variar según el nivel de desarrollo, mantenimiento y soporte que tengan por parte de la comunidad o los desarrolladores.

- La seguridad y la privacidad de las herramientas de código abierto pueden verse comprometidas al no aplicar las medidas adecuadas y pertinentes, como verificar la autenticidad y la integridad del código fuente, revisar las licencias y los permisos de uso, o cifrar y proteger los datos sensibles.

- La escalabilidad y el rendimiento de las herramientas de código abierto pueden ser limitados al no disponer de los recursos o la infraestructura necesarios para soportar el volumen y la velocidad de procesamiento de los datos y eventos de seguridad que se generan en el SOC.

5.4.3 Ventajas en el uso de herramientas de código abierto

- Usar herramientas de código abierto para un SOC tiene algunas ventajas que se deben considerar. Algunas de estas ventajas son:

- La flexibilidad y la personalización de las herramientas de código abierto, que permiten adaptarlas a las necesidades y los requisitos específicos de cada SOC y cada organización.

- La innovación y la colaboración de las herramientas de código abierto, que se benefician del aporte y la retroalimentación de una amplia comunidad de usuarios y desarrolladores que contribuyen a mejorar y actualizar las herramientas constantemente.

- La transparencia y la auditoría de las herramientas de código abierto, que facilitan el acceso y la revisión del código fuente y los procesos internos de las herramientas, lo que puede aumentar la confianza y la seguridad en su uso.

- El ahorro y la accesibilidad de las herramientas de código abierto, que suelen tener un costo menor o nulo en comparación con las herramientas comerciales o propietarias reduciendo el presupuesto y los recursos necesarios para implementar y mantener el SOC.

5.4.4 Desventajas en el uso de herramientas de código abierto

- La seguridad de los datos puede verse comprometida por la apertura del código y la ausencia de un sistema de protección. Esto significa que el software puede ser vulnerable a ataques externos o internos, o que se pueda acceder a información confidencial o sensible sin autorización. Además, al no contar con un proveedor responsable, la responsabilidad de la seguridad recae en el usuario final.

- Puede generar costos a largo plazo al requerir de soporte, capacitación o resolución de fallas. Esto significa que el software puede presentar errores, incompatibilidades o limitaciones que requieran de asistencia técnica especializada, que puede ser difícil de encontrar o tener un costo elevado. También puede implicar una inversión en tiempo y recursos para capacitar al personal o para adaptar el software a las necesidades específicas, aunque estos costos son menores en comparación con el software privativo.

- En algunos casos puede faltar soporte técnico específico o garantías por parte de los creadores. Esto significa que el software puede no tener un respaldo oficial o una documentación adecuada que facilite su uso o su mejora. También significa que el usuario no tiene a quién reclamar o exigir en caso de que el software falle o no cumpla con sus expectativas. Teniendo en cuenta las mejores prácticas

se recomienda realizar la revisión previa para mitigar riesgos de seguridad con el uso de dichas herramientas.

6. CONCLUSIONES

El marco de trabajo para implementar un SOC utilizando herramientas de código abierto comprende los procesos y herramientas esenciales para establecer este tipo de sistema en una organización. Se basa en el conocimiento que se tiene sobre la implementación de SOC, utilizando estándares y marcos de referencia ya conocidos por los responsables de TI en la organización.

En este documento, hacemos referencia a los marcos de trabajo de SOC que ayudan a alinear un equipo SOC con los procesos descritos en estos marcos. Estos marcos están respaldados por normas como ISO 27001, NIST CSF y Cyber Kill Chain. Sin embargo, el que mejor se adapta al funcionamiento de un SOC es el NIST CSF.

Por otro lado, se definió las funciones, roles, organización y composición. Para lograr esto, es necesario tener un conocimiento tanto global como detallado de los activos e infraestructura de la organización, así como un análisis preciso para identificar todos los activos que son vulnerables y críticos para los procesos en la organización. Posteriormente, procedemos a realizar el monitoreo. En estos primeros pasos, podemos utilizar herramientas de código abierto. Es fundamental tener en cuenta que, según la cantidad de activos, infraestructura y redes de una organización, se deben emplear plataformas sólidas en las que se instalen herramientas de seguridad informática para analizar estos activos e infraestructura.

Una vez identificados los activos críticos de la organización, se lleva a cabo el proceso de monitoreo en el que se revisan los patrones de comportamiento en la red para identificar posibles anomalías que puedan representar un riesgo de seguridad para los activos de la organización. Es importante determinar la herramienta que brinde la información más relevante, eficacia y eficiencia para facilitar la toma de decisiones adecuadas cuando se presente un evento en la red.

Durante el análisis de estos eventos, se deben considerar las brechas y vulnerabilidades en la seguridad informática de la organización. Cada organización

tiene sus propias debilidades y amenazas, y es responsabilidad de las organizaciones llevar a cabo acciones correctivas y de gestión.

Se recomienda contar con un repositorio de información y herramientas que permitan el análisis de los eventos y los datos de la red, y faciliten la implementación de tecnologías como la inteligencia de negocios, la inteligencia artificial, la minería de datos, la ciencia de datos y la analítica de negocios.

El enfoque de este trabajo se centra en la implementación mediante el uso de herramientas de seguridad informática de código abierto. Es esencial seleccionar personal especializado para llevar a cabo esta implementación, profesionales con el conocimiento necesario en plataformas basadas en código abierto. Dado que no se dispone del soporte que se encuentra en las herramientas propietarias, el conocimiento de estos profesionales servirá como base para proteger la información en la implementación de este tipo de proyecto

7. RECOMENDACIONES

Se recomienda que la organización establezca una estrategia alineando los objetivos comerciales, los de la junta directiva y los de TI. La primera etapa es evaluar la infraestructura y los activos de TI de la empresa, seguido por la creación de un inventario de los recursos existentes. Luego, se debe llevar a cabo un análisis de riesgos para evaluar el impacto de estos activos de TI en la organización y, de esta manera, identificar brechas y vulnerabilidades que podrían materializarse en riesgos explotables por atacantes externos. Esta información deberá actualizarse cada vez que se incorporen nuevos activos de TI, siguiendo las políticas de la organización.

Además, es esencial planificar estratégicamente el desarrollo de procesos y procedimientos que guiarán al equipo del SOC en las operaciones de monitoreo, detección de eventos, respuesta a incidentes, generación de informes y seguimiento de casos.

La organización y su gobierno de TI deben revisar y actualizar regularmente las estrategias, procesos y procedimientos establecidos para mantenerse al día frente a las amenazas y vulnerabilidades internas y externas. La implementación de controles y la capacitación del personal son igualmente importantes.

El equipo del SOC debe mantener un inventario actualizado de los activos de la organización, que incluye redes de datos, bases de datos, dispositivos host, servidores y demás infraestructura. También debe considerar los servicios prestados por terceros que interactúan con los activos de la organización y que pueden representar amenazas a la seguridad.

El SOC está compuesto por un grupo de expertos en seguridad informática, cualificados y con experiencia en procesos de la información, infraestructura

tecnológica y normatividad. Su función principal es ayudar a la organización a defenderse de los delincuentes informáticos y fortalecer la seguridad de la información.

Cuando se implementan herramientas de seguridad informática de código abierto, es fundamental asegurarse de que los profesionales contratados estén cualificados y tengan un conocimiento técnico sólido en las plataformas basadas en código abierto utilizadas en los procesos, desde el inventario de activos hasta el análisis de riesgos. Dado que estas herramientas no cuentan con soporte garantizado al no ser propietarias, la capacidad del personal es esencial.

Se recomienda establecer un repositorio para la gestión de la información de seguridad informática vinculado a un conjunto de herramientas de código abierto. Esto facilitará análisis posteriores que fortalecerán las políticas de seguridad basadas en la información recopilada

8. BIBLIOGRAFIA

ABDULLAH, Kulsoom, et al. IDS rainStorm: visualizing IDS alarms. En: IEEE Xplore. 2005. p. 1-10.

ALI, Saqib; AL LAWATI, Maitham H. y NAQVI, Syed J. Unified threat management system approach for securing sme's network infrastructure. En: IEEE Xplore. 2012. p. 170-176.

ALICHERRY, Mansoor; MUTHUPRASANNA, M. y KUMAR, Vijay. High speed pattern matching for network IDS/IPS. En: Proceedings of the 2006 IEEE International Conference on Network Protocols. 2005. p. 187-196.

BERNSMED, Karin y TØNDEL, Inger Anne. Indicators for evaluating information security incident management. En: 2013 Seventh International Conference on IT Security Incident Management and IT Forensics. 2013. p. 3-14.

BIENIAS, Piotr; KOŁACZEK, Grzegorz y WARZYŃSKI, Arkadiusz. Architecture of anomaly detection module for the security operations center. En: 2019 IEEE 28th International Conference on Enabling Technologies. 2019. p. 126-131.

CARDER, James. How to build a SOC with limited resources. Logrhythm [blog]. (2009). [Consultado el 8, septiembre, 2022]. Disponible en Internet: <https://www.itp.net/public/uk-how-to-build-a-soc-with-limited-resources-white-paper_0.pdf>.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 2258. (23, diciembre, 2009). Resolución - 2258.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 1241. (14, mayo, 2009). Resolución 1241 de 2018.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581. (17, octubre, 2012). Ley 1581 de 2012.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273. (5, enero, 2010). Ley 1273 de 2009.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341. (30, julio, 2009). Ley 1341 de 2009.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266. (25, diciembre, 2008). Ley 1266 de 2008.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 603. (3, agosto, 2000). Ley 603 de 2000.

DEPARTAMENTO NACIONAL DE PLANEACIÓN DE COLOMBIA. Resolución Conpes 3701 de 2011. (12, mayo, 2011). Política Nacional de Seguridad y Defensa Cibernética.

GAFF, Brian M. y PLOUSSIOS, Gregory J. Open source software. En: IEEE Computer. 2012. vol. 45, no. 06, p. 9-11. ISSN 1558-0814.

RESOURCE CENTER [Anónimo]. Devo.com [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.devo.com/guide-to-the-future-soc/soc-frameworks>.

RFC 2196: site security handbook [Anónimo]. IETF Datatracker [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://tools.ietf.org/html/rfc2196>.

VULNERABILITY SCANNERS and scanning tools: what to know | balbix [Anónimo]. Balbix [página web]. [Consultado el 21, diciembre, 2023]. Disponible en Internet: <https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/>.

CYBER KILL chain® [Anónimo]. Lockheed Martin [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

HOW MUCH does it cost to build a 24x7 SOC? | Expel [Anónimo]. Expel [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://expel.com/blog/how-much-does-it-cost-to-build-a-24x7-soc>.

ISA/IEC. Industrial communication networks. Network and system security. 63443. [s.l.]: el autor, 2017. 3 p.

ISO 27001 - sistemas de gestión de seguridad de la información [Anónimo]. Software ISO [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/>.

JARPEY, Gregory y MCCOY, Scott. Security operations center guidebook: A practical guide for a successful SOC. [s.l.]: Elsevier Science & Technology Books, 2017. 206 p. ISBN 9780128036822.

MILLER, Keith W.; VOAS, Jeffrey y COSTELLO, Tom. Free and open source software. En: IT Professional [en línea]. Noviembre, 2010. vol. 12, no. 6 [consultado

el 22, diciembre, 2023], p. 14-16. Disponible en Internet: <https://doi.org/10.1109/mitp.2010.147>. ISSN 1520-9202.

MODIRI, Nasser y SOBHANZADEH, Yosef Masoudi. Information security management. En: 2011 International Conference on Computational Intelligence and Communication Networks. 2011. p. 481-484.

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 620. (5, abril, 2005). Decreto 620 de 2005.

QI, Yaxuan, et al. Towards system-level optimization for high performance unified threat management. En: International Conference on Networking and Services. 2007. p. 7-7.

¿QUÉ DIFERENCIA existe entre ISO 27001 y SOC 2? [Anónimo]. PMG SSI - ISO 27001 [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.pmg-ssi.com/2016/05/que-diferencia-existe-entre-iso-27001-y-soc-2/>.

RAGHUNATH, Bane Raman y MAHADEO, Shivsharan Nitin. Network intrusion detection system (NIDS). En: 2008 First International Conference on Emerging Trends in Engineering and Technology. 2008. p. 1272-1277.

SCHIEFERDECKER, Ina. Trustworthiness of open source, open data, open systems and open standards. En: 2012 IEEE 36th Annual Computer Software and Applications Conference. 2012. p. 82-82.

SEARCH | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://csrc.nist.gov/publications/sp800>.

SECURITY OPERATIONS center: building, operating, and maintaining your SOC | cisco press [Anónimo]. Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052014>.

SP 800-94, guide to intrusion detection and prevention systems (IDPS) | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://csrc.nist.gov/pubs/sp/800/94/final>.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular 003. (1, junio, 2016). Circular Externa 003 de 2016.

THE DEFINITION of soc-cess? SANS 2018 security operations center survey | SANS institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. [Consultado el 22, diciembre, 2023]. Disponible en Internet: <https://www.sans.org/white-papers/definition-soc-cess-sans-2018-security-operations-center-survey/>.

VERMEER, Mathew, et al. SoK: a framework for asset discovery: systematizing advances in network measurements for protecting organizations. En: 2021 IEEE European Symposium on Security and Privacy (EuroS&P). 2021. p. 440-456.

VIELBERTH, Manfred, et al. Security operations center: a systematic study and open challenges. En: IEEE Access. 2020. vol. 8, p. 227756-227779.

XING, Mingqing. Competition between Free Open Source, Commercial Open Source and Proprietary Software. En: Journal of Communications [en línea]. 2013.

vol. 8, no. 10 [consultado el 22, diciembre, 2023], p. 665-671. Disponible en Internet: <https://doi.org/10.12720/jcm.8.10.665-671>. ISSN 1796-2021.