DISEÑO DOCUMENTAL DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) QUE ESTABLEZCA LAS HERRAMIENTAS TECNOLOGICAS PARA EL DESARROLLO DEL CSIRT DE LA ORGANIZACIÓN PLATINO SISTEMAS

DIEGO ANDRES POVEDA BERNAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2025

DISEÑO DOCUMENTAL DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) QUE ESTABLEZCA LAS HERRAMIENTAS TECNOLOGICAS PARA EL DESARROLLO DEL CSIRT DE LA ORGANIZACIÓN PLATINO SISTEMAS

DIEGO ANDRES POVEDA BERNAL

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

Yenny Stella Nuñez
Directora de Curso – Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2025

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 05 de mayo de 2025

DEDICATORIA

Con amor dedico este trabajo primero que todo a Dios que es mi apoyo fundamental para cumplir mis metas, a mis hijos y mi esposa, que han sido mi inspiración en todo momento, muchos de mis logros incluido este se los debo a ustedes, también lo dedico a mis padres que, con su apoyo, me formaron con reglas y me motivaron constantemente a alcanzar mis logros.

AGRADECIMIENTOS

Primeramente, quiero agradecer a la Universidad Nacional Abierta y a Distancia UNAD por la oportunidad que me brindó de poderme formar como profesional, así como a los docentes que me acompañaron durante este proceso que gracias a su conocimiento y enseñanzas me apoyaron para seguir luchando por mi carrera día a día.

Agradezco a la Ing. Yenny Stella Nuñez quien gracias a su apoyo, capacidad y conocimiento me ha guiado en el desarrollo de esta tesis.

CONTENIDO

pág.

GLOSARIO

Centro de Operaciones de Seguridad (SOC): Un centro dedicado a monitorear y gestionar la seguridad de la información de una organización, detectar y responder a amenazas cibernéticas.

CSIRT (Computer Security Incident Response Team): Equipo encargado de la gestión de incidentes de seguridad informática, incluyendo la detección, respuesta y recuperación.

Herramientas Tecnológicas: Software, hardware y soluciones específicas utilizadas en el SOC y CSIRT para llevar a cabo tareas de seguridad, como sistemas de detección de intrusiones, análisis de registros y software de respuesta a incidentes.

Seguridad de la Información: Conjunto de prácticas y medidas para proteger la confidencialidad, integridad y disponibilidad de los datos de la organización.

Vulnerabilidad: Debilidad o fallo en un sistema que puede ser explotado por una amenaza para comprometer la seguridad.

Análisis de Vulnerabilidades: Proceso de identificar y evaluar posibles debilidades en sistemas y aplicaciones que podrían ser explotadas por atacantes.

Detección de Intrusiones: Tecnología y procedimientos utilizados para identificar actividades maliciosas o no autorizadas en una red o sistema.

Gestión de Eventos de Seguridad (SIEM): Plataforma que permite la recopilación, correlación y análisis de eventos de seguridad de múltiples fuentes.

Firewall: Dispositivo o software que controla el tráfico de red y aplica reglas de seguridad para proteger la red de ataques.

Honeypot: Sistema diseñado para atraer a atacantes y recolectar información sobre sus tácticas y técnicas.

Respuesta a Incidentes: Proceso que implica la identificación, contención, erradicación y recuperación después de un incidente de seguridad.

Políticas de Seguridad: Documentos que establecen las reglas y procedimientos de seguridad que deben seguirse en una organización.

Plan de Continuidad del Negocio (BCP): Estrategia y procedimientos para mantener la operación de la organización en caso de incidentes graves.

Evaluación de Riesgos: Proceso de identificación y análisis de los riesgos de seguridad informática para priorizar acciones de mitigación.

Ciberseguridad: Prácticas y medidas de seguridad específicas para proteger sistemas y datos en entornos digitales.

Autenticación: Proceso de verificar la identidad de un usuario o sistema antes de permitir el acceso a recursos protegidos.

Autenticación Multifactor (MFA): Método que requiere más de una forma de autenticación para verificar la identidad de un usuario, como contraseña y verificación por SMS.

Cifrado de Datos: Proceso de transformación de datos en un formato ilegible para proteger su confidencialidad durante la transmisión o almacenamiento.

Auditoría de Seguridad: Revisión y análisis de los controles de seguridad y políticas para garantizar su efectividad.

Trazabilidad de Incidentes: Capacidad para rastrear y documentar todas las acciones tomadas en respuesta a un incidente de seguridad.

Gestión de Identidad y Acceso (IAM): Conjunto de políticas y tecnologías para gestionar y controlar el acceso de usuarios a recursos digitales.

Incidente de Seguridad: Evento no deseado que compromete la seguridad de la información, como un ataque exitoso o una brecha de datos.

Informe de Incidentes: Documento que registra detalles de un incidente de seguridad, incluyendo su impacto y acciones tomadas para resolverlo.

Seguridad Informática: Protección de sistemas, redes y datos contra amenazas y riesgos, garantizando la confidencialidad, integridad y disponibilidad de la información.

Amenaza Informática: Cualquier evento o acción que tenga el potencial de dañar sistemas, redes o datos.

Ataque Informático: Acción intencionada para explotar una debilidad en la seguridad de un sistema y comprometer la confidencialidad, integridad o disponibilidad de la información.

Malware: Software malicioso diseñado para dañar o comprometer sistemas y datos, incluyendo virus, gusanos, troyanos y ransomware.

Phishing: Técnica de engaño que involucra el uso de correos electrónicos, sitios web u otros medios para obtener información confidencial de forma fraudulenta.

Autorización: Concesión de permisos específicos a usuarios o sistemas para acceder a recursos o realizar acciones determinadas.

Biometría: Método de autenticación basado en características físicas o comportamentales únicas de un individuo, como huellas dactilares o reconocimiento facial.

Seguridad de la Red: Conjunto de medidas y políticas diseñadas para proteger la integridad y confidencialidad de las comunicaciones en una red.

Intrusión: Acceso no autorizado a un sistema o red por parte de un atacante.

Registro de Eventos (Log): Registro de actividades y eventos en un sistema o red que puede ser utilizado para la detección de amenazas y la investigación de incidentes.

Hacker Ético: Profesional de la seguridad informática que utiliza sus habilidades para identificar vulnerabilidades y mejorar la seguridad de sistemas de manera legal y ética.

Parche de Seguridad: Actualización de software diseñada para corregir vulnerabilidades conocidas y mejorar la seguridad.

Seguridad en la Nube: Prácticas y medidas de seguridad para proteger los datos y sistemas alojados en servicios de nube.

RESUMEN

El alcance de esta tesis abarca cada uno de los requerimientos necesarios para el desarrollo de un modelo del centro de operaciones de seguridad SOC y el hardware y software que se va a utilizar para el desarrollo de las actividades del CSIRT que se proyecta crear como una de las metas principales en la organización Platino Sistemas.

Con esta propuesta se le da a conocer a la organización que con este modelo se puede ofrecer un mejor servicio a cada uno de sus clientes, implementando niveles de servicio y gestionando de una manera eficiente los incidentes de seguridad que se puedan presentar y así identificar, notificar y supervisar actividad sospechosa que amenace la integridad de la información obteniendo resultados de calidad y cumpliendo con los requerimientos de cada cliente.

El objetivo principal es la gestión a vulnerabilidades e incidentes cibernéticos que se puedan llegar a presentar en empresas donde su activo más preciado es la información, estableciendo medidas, políticas y procedimientos adaptables a su infraestructura en relación con la seguridad informática de cada una de ellas.

Como resultado a lo anterior es la reacción inmediata frente a ataques e incidentes, dando inicio desde una supervisión pasiva obteniendo información hasta el reporte del evento, sin embargo, antes de que pueda ocurrir un ataque se debe determinar la manera más apropiada de cómo va a ser la reacción frente a este hecho, recurriendo a los procedimientos establecidos y si es el caso revisar el sistema de gestión de seguridad de la información implementado en dicha empresa.

ABSTRACT

The scope of this thesis covers each of the requirements for the development of a model of the SOC security operations center and the hardware and software that will be used for the development of the activities of the CSIRT that is planned to be created as one of the the main goals in the Platino Sistemas organization.

With this proposal, the organization is made aware that with this model it can offer a better service to each of its clients, implementing service levels and efficiently managing security incidents that may arise and thus identify, notify and monitor suspicious activity that threatens the integrity of the information, obtaining quality results and complying with the requirements of each client.

The main objective is to manage vulnerabilities and cyber incidents that may occur in companies where their most valuable asset is information, establishing measures, policies and procedures adaptable to their infrastructure in relation to the computer security of each of them.

As a result of the above is the immediate reaction to attacks and incidents, starting from a passive supervision obtaining information until the event report, however, before an attack can occur, the most appropriate way of how it is going to occur must be determined. be the reaction to this fact, resorting to established procedures and, if necessary, review the information security management system implemented in said company.

INTRODUCCIÓN

Para las organizaciones en la actualidad su información es el activo más preciado pero a su vez es lo que más preocupa debido al incremento de procedimientos que atentan contra su confidencialidad, integridad y disponibilidad, así que optan por tomar controles y medidas para gestionar de forma proactiva las vulnerabilidades, amenazas e incidentes con el fin de moderar y controlar el impacto que puede ocasionar y afecte el normal funcionamiento de las operaciones de cada uno de los clientes de la organización.

Ahora las organizaciones dependen bastante de su infraestructura tecnológica así que deben garantizar la disponibilidad de los sistemas informáticos instalando herramientas de seguridad que garanticen una mayor protección ante continuos ataques cibernéticos, así que se hace necesario la implementación de un Centro de Operaciones de Seguridad (SOC) para que se encargue del control de amenazas y de respuestas eficientes frente a los incidentes y así proteger la información, dependiendo del costo hay empresas que optan por contratar los servicios de un SOC externo y así siempre tener protegida la información.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Hoy en día el mayor activo de una empresa, organización o negocio es la información, esta principalmente se almacena en servidores o en estaciones de cómputo estando expuesta a ataques cibernéticos donde los más comunes son malware, phishing, Social Engineering y Denial of Services, esto se puede dar por error humano, virus, robo de archivos, uso inadecuado de internet, a través del correo electrónico y todo esto puede traer consecuencias graves para la empresa y hasta el cierre total de ella, según estudios el 60% de las empresas que pierden información cierran dentro de los seis meses siguiente a lo ocurrido y el 93% que pierden información por más de 10 días se declaran en quiebra un año después[1].

Debido a esto surge la necesidad de estar supervisando constantemente la infraestructura y así detectar vulnerabilidades y amenazas con ayuda de herramientas especializadas para tener una reacción inmediata y hacer frente a estos ataques, y así proteger la confidencialidad e integridad de la información, de todas formas la organización debe tomar conciencia que el riesgo siempre va a estar presente a pesar de todas las medidas que se puedan adoptar ya sea para mitigar o corregir cualquier daño que se pueda presentar, por eso se debe involucrar a todo el personal y los procesos que la integran para crear una cultura de seguridad informática y ser eficientes ante las amenazas cibernéticas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede garantizar que la organización Platino Sistemas de respuesta efectiva a incidentes cibernéticos para proteger la información de sus clientes?

[1] ACIS. La pérdida de datos les cuesta a las empresas más de 4 millones de dólares al año [en línea]. Bogotá [Consulta: 14 de marzo 2021]. Disponible en: https://acis.org.co/portal/content/la-p%C3%A9rdida-de-datos-les-cuesta-las-empresas-m%C3%A1s-de-4-millones-de-d%C3%B3lares-al-a%C3%B1o

2 JUSTIFICACIÓN

La necesidad y alto grado de dependencia de las Tecnologías de la Información y Comunicaciones TICs lleva a las empresas a estar analizando toda la información crítica que viaja a través de la red y tomar acciones respecto a la prevención y protección frente a posibles ataques que pueda comprometer la información de valor.

En la actualidad las empresas invierten en equipos robustos e infraestructura tecnológica, pero esto no es suficiente, así que hay la necesidad de complementarlo con el diseño de un Centro de Operaciones de Seguridad (SOC) ya que por medio de este se puede prevenir de que haya incidentes y se puedan materializar las amenazas a la información, seguido de la detección donde se supervisa constantemente para detectar cualquier amenaza y ataques a la seguridad, y si llega haber algún incidente este se analiza y se da una respuesta de acuerdo a lo ocurrido.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Elaborar el diseño documental de un Centro de Operaciones de Seguridad (SOC) que establezca las herramientas tecnológicas para el desarrollo de las actividades del Equipo de Respuesta a Incidentes de Seguridad (CSIRT) de la organización Platino Sistemas.

3.2 OBJETIVOS ESPECÍFICOS

- Diseñar la estructura tecnológica del Centro de Operaciones de Seguridad SOC para su óptimo funcionamiento.

- Establecer los procedimientos y las políticas de respuesta a incidentes de seguridad para dar soporte dependiendo del servicio contratado.

- Estructurar cada uno de los roles y entrenamiento requeridos para conformar el equipo de trabajo del Centro de Operaciones de Seguridad.

- Establecer las herramientas de hardware, software y el laboratorio de pruebas para el desarrollo de las actividades del Equipo de Respuesta a Incidentes de Seguridad (CSIRT).

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La información es el activo más preciado de las empresas por eso se hace necesario tomar medidas que reduzcan las posibilidades de ataques cibernéticos, contemplando sistemas de control para mantener la confidencialidad, integridad y que la información esté siempre disponible.

Hay distintas herramientas de seguridad que se implementan en las empresas, pero todo esto se puede centralizar implementando un Centro de Operaciones de Seguridad (SOC) que debe contar con personal calificado que está en la capacidad de reaccionar frente a los ataques de seguridad, a continuación, se describen algunos términos de seguridad informática.

4.1.1 Ataque informático

Es un intento de acceso a un sistema informático para causar daños, robar información confidencial o alterar el funcionamiento, esto a través de virus o malware que pone en riesgo la seguridad informática, estos ataques son causados por personas llamadas “piratas informáticos” mediante el envío de virus o malware diseñados de tal forma que pueden burlar la seguridad de nuestra red[2].

4.1.2 Firewall

Elemento informático también llamado contrafuego, es el que previene y protege una red privada de ataques bloqueando el acceso a usuarios no autorizados, solo permite el tráfico que cumpla con las reglas previamente especificadas examinando todo lo que entra y sale de la red[3].

4.1.3 Seguridad informática

Es el proceso que impide la ejecución de operaciones no autorizadas de un sistema informático protegiendo la integridad y privacidad de la información, a través de

[2] ECURED. Ataque informático [en línea]. Cuba [Consulta: 14 de marzo 2021]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

[3] ID GRUP. Qué es un Firewall y cómo funciona [en línea]. Barcelona [Consulta: 14 de marzo 2021]. Disponible en: https://idgrup.com/firewall-que-es-y-como-funciona/

antivirus, firewall y diferentes medidas que se puedan tomar ya que lo más vulnerable es el software, hardware y los datos[4].

4.1.4 IDS e IPS

Los Sistemas de Detección de Intrusos (IDS) y los Sistema de Prevención de Intrusos (IPS) son sistemas que aumentan la seguridad en nuestras redes y se encargan de supervisar el tráfico examinando la red y los puertos, donde se analizan paquetes de datos para detectar actividad sospechosa.

Los IDS tienen una base extensa actualizada de firmas de ataques conocidas que al momento de monitorizar el tráfico lo compara con la información que dispone y si hay una actividad sospechosa emite una alerta para que los responsables del área de TI tomen las respectivas acciones[5].

4.1.5 Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es un conjunto de políticas de administración de la información, este término es utilizado por la ISO 27001:2005 donde se encuentran los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) a través del ciclo PHVA (Planear, Hacer, Verificar, Actuar), que busca asegurar la confidencialidad, integridad y disponibilidad de la información minimizando los riesgos de seguridad[6].

4.1.6 Centro de Operaciones de Seguridad (SOC)

Es un centro de trabajo que se encarga de gestionar la seguridad de la información y el responsable de garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente.

Para ello debe contar con un equipo de profesionales especialistas encargado de contener, analizar y hacer seguimiento a la actividad en redes, servidores, bases de datos, sitios web entre otros, buscando comportamientos anormales que pueden ser un incidente y puedan comprometer la seguridad de la información.

---

[4] NETEC. ¿Qué es seguridad informática? [en línea]. Bogotá [Consulta: 16 de marzo 2021]. Disponible en: https://www.netec.com/que-es-seguridad-informatica

[5] PUNT INFORMATIC. Sistemas de detección y prevención IDS e IPS: ¿Para qué sirven? [en línea]. Barcelona [Consulta: 16 de marzo 2021]. Disponible en: https://puntinformatic.com/sistemas-de-deteccion-y-prevencion-ids-e-ips/#:~:text=Tanto%20los%20Sistemas%20de%20Detecci%C3%B3n,datos%2C%20para%20detectar%20patrones%20sospechosos

[6] FIRMA-e. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? [en línea]. Murcia España [Consulta: 16 de marzo 2021]. Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

5 DISEÑO METODOLÓGICO

La principal técnica de recolección de datos que se va a usar es la encuesta y el análisis documental, y el tipo de investigación es aplicada.

Si es pertinente se va a utilizar herramientas de análisis como Kali Linux que es un software libre que tiene bastantes herramientas para realizar ataques y hacking ético, también con máquinas virtuales para realizar simulacros de ataques informáticos.

6 DESARROLLO DE LOS OBJETIVOS

6.1 ESTRUCTURA TECNOLÓGICA DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El SOC o Centro de Operaciones de Seguridad, es un centro de trabajo que se encarga de monitorear y analizar cada una de las actividades en las redes de datos, aplicaciones web, servidores, bases de datos, etc... con el fin de identificar comportamientos anormales y así dar respuesta a incidentes o vulnerabilidades de seguridad a través de equipos tecnológicos y personal especializado que permita entregar un soporte efectivo para asegurar la protección de la información de los clientes.

Para el funcionamiento óptimo del SOC se debe desplegar tecnología que será utilizada por el personal especializado para realizar sus actividades de análisis y entregar soluciones, se puede implementar en:

- Redes de datos.
- Seguridad de red.
- Sistemas.
- Plataformas de seguridad.
- Sistemas de control de acceso a la red.
- Sistemas de descifrado.
- Sistemas de detección de vulnerabilidades.
- Servidores.

Las siguientes son herramientas tecnológicas que se pueden implementar:

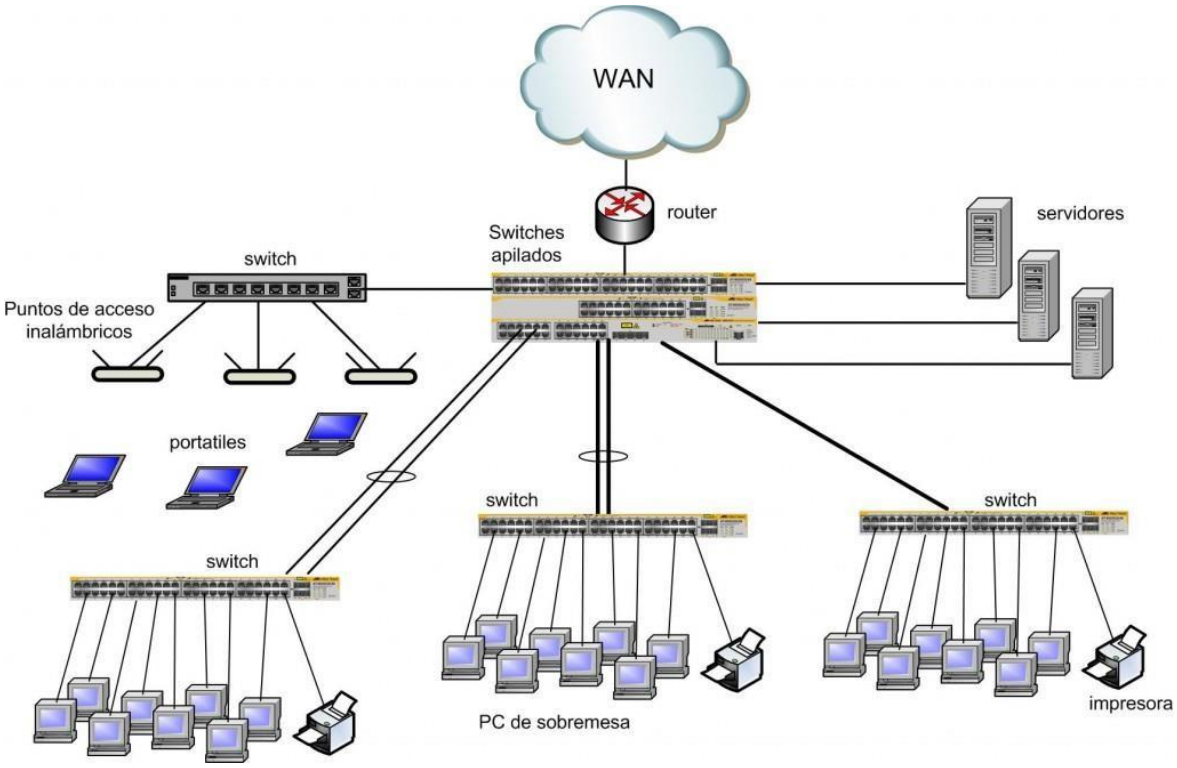
- SIEM.
- Firewall.
- Sistemas de detección de intrusos (IDS).
- Sistema de prevención de intrusos (IPS).
- DMZ

6.1.1 Redes de datos

Una de las principales necesidades de los centros de operaciones de seguridad son las redes de datos, ya que sin esta condición no se puede implementar un SOC.

Las redes de datos se pueden dividir de distintos tipos como por ejemplo red de área local (LAN), red de área metropolitana (MAN), red de área ampliada (WAN) entre otras, partiendo de aquí se encuentra la red interna, la red externa y en medio de estas dos una muy importante que es la DMZ o zona desmilitarizada.

Figura 1. Redes LAN



Fuente: Redes telemáticas, http://redestelematicas.com/los-tipos-de-redes-de-datos-ejemplos/

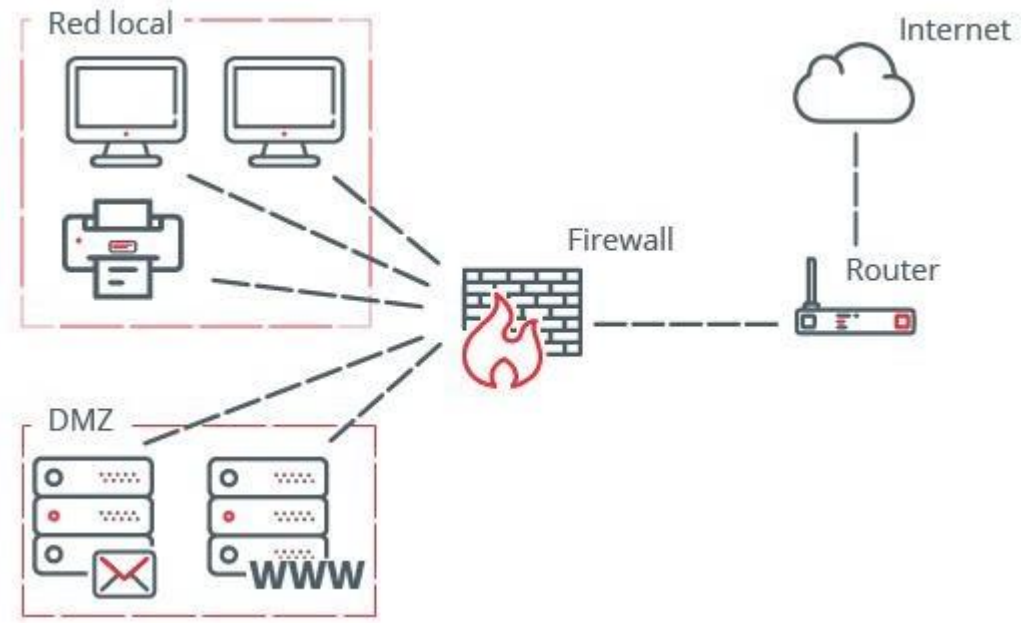
6.1.2 DMZ

Una DMZ o zona desmilitarizada es una red que está presente en medio de la red interna de la organización y la red externa que generalmente es el internet.

La DMZ tiene como objetivo que las conexiones desde la red interna y la red externa hacia la DMZ estén permitidas, así que los equipos conectados a la DMZ no se pueden conectar directamente con la red interna, pero si pueden dar servicio a la red externa, actuando como un filtro entre la conexión a internet y la red interna verificando que las conexiones entre las dos sean permitidas.

Generalmente se ubican los servidores que se acceden desde afuera como el servicio de acceso a la página WEB o el de correo electrónico y crean tráfico entre la DMZ y la red interna, casi siempre dentro de las opciones del firewall es donde se crea una DMZ.

Figura 2. Red local con una DMZ



Fuente: incibe, https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

6.1.3 Plataformas de seguridad

En el SOC se encuentran tecnologías para operar la seguridad de las organizaciones como:

Sistemas de Detección de Intrusiones (IDS) y Sistemas de Prevención de Intrusiones (IPS):

- **Snort:** Un sistema de detección de intrusiones de código abierto.
- **Suricata:** Similar a Snort, pero con soporte para IPS y un alto rendimiento.

Sistemas de Información y Eventos de Seguridad (SIEM):

- **Splunk:** Plataforma de análisis de registros y SIEM que permite la correlación y búsqueda avanzada.
- **QRadar (IBM Security QRadar):** Ofrece detección avanzada, análisis de registros y respuesta a amenazas.
- **LogRhythm:** Un SIEM que combina análisis de registros, detección de amenazas y automatización de respuesta.

Herramientas de Automatización y Orquestación de Seguridad:

- **Demisto (Ahora parte de Palo Alto Networks):** Ayuda a automatizar flujos de trabajo de seguridad y orquestar respuestas.

- **Phantom (Ahora parte de Splunk):** Proporciona automatización y orquestación de seguridad para acelerar la respuesta a incidentes.

Firewalls de Próxima Generación (NGFW):

- **Palo Alto Networks:** Ofrece capacidades de firewall avanzadas y detección de amenazas en tiempo real.

- **Cisco Firepower:** Combina firewall, IPS, control de aplicaciones y detección de amenazas en una sola plataforma.

Soluciones de EndPoint Detection and Response (EDR):

- **CrowdStrike:** Proporciona visibilidad y respuesta a amenazas en tiempo real en dispositivos finales.

- **Carbon Black (Ahora parte de VMware):** EDR con capacidades de detección y respuesta en el endpoint.

Honeypots y Honeynets:

- **Kippo:** Un honeypot SSH de código abierto para atraer y registrar intentos de intrusión.

- **Modern Honey Network (MHN):** Una solución para desplegar y gestionar múltiples honeypots.

Gestión de Identidad y Acceso (IAM):

- **Okta:** Ofrece gestión de acceso y autenticación de usuarios de forma segura.

- **OneLogin:** Proporciona autenticación centralizada y gestión de identidades.

Herramientas de Análisis de Malware:

- **Cuckoo:** Una plataforma de análisis de malware de código abierto.

- **VirusTotal:** Un servicio en línea que permite cargar y analizar archivos sospechosos.

Gestión de Registros y Eventos de Seguridad (SIEM):

- **ELK Stack (Elasticsearch, Logstash, Kibana):** Una pila de código abierto para análisis de registros y visualización.

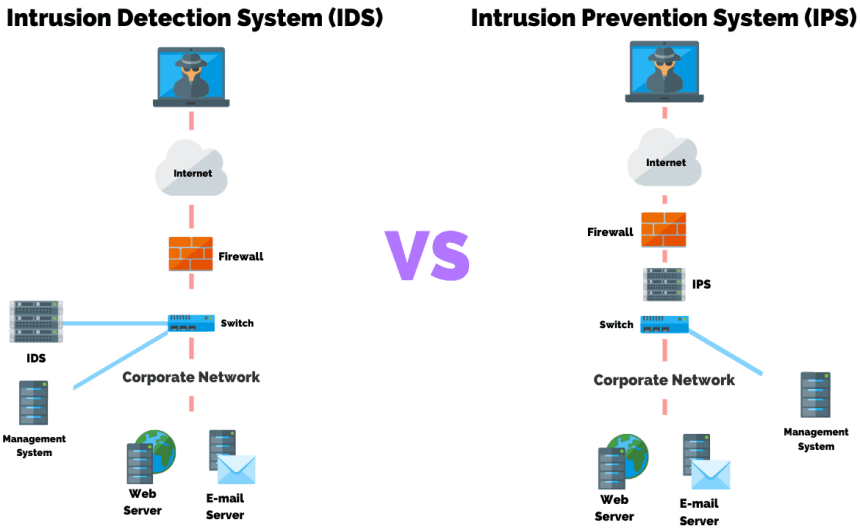
- **Graylog:** Plataforma de registro y análisis de registros de código abierto.

Estas herramientas SIEM efectúan el análisis de eventos sospechosos y así responder con precisión ante amenazas en tiempo real, agregando un gran valor a las tareas que se llevan a cabo por los encargados de la seguridad permitiendo efectuar ciertos análisis que no sería posible sin esta tecnología.

Los sistemas de control de acceso a la red son los que permiten implementar las políticas de seguridad y así conseguir información sobre los accesos e inicios de sesión a la red, son útiles para poder tomar medidas preventivas sobre los usuarios y dispositivos de la red, un ejemplo claro sería inhabilitar un usuario para que no pueda volver a ingresar a la red luego de detectarse un comportamiento irregular.

Sistemas de detección de intrusos y sistemas de prevención de intrusos, son sistemas que controlan el acceso a una red para protegerlos de ataques, y monitorean cada evento ocurrido en la red para analizarlos y así encontrar posibles incidentes y que pueden ser amenazas a las políticas de seguridad implementadas en la organización.

Figura 3. IDS vs IPS



Fuente: HUAWEI, https://forum.huawei.com/enterprise/en/differences-between-ids-and-ips/thread/484497-867

6.2 POLÍTICAS Y PROCEDIMIENTOS DE RESPUESTA A INCIDENTES

La política de seguridad es la encargada de describir todo lo que se desea proteger e indica el compromiso que tiene la organización para dar respuesta a incidentes de seguridad, tiene como objetivo reducir los riesgos, garantizar la confidencialidad, integridad y disponibilidad de la información, así como cumplir con cada una de las reglas vigentes.
Para esto se debe identificar los activos de los clientes que se deben proteger que puede ser:

- Software.
- Hardware.
- Bases de datos.
- El personal.
- Riesgos.
- Asignación de responsabilidades.

Estas políticas son esenciales para establecer un marco de trabajo sólido para la gestión de incidentes y la operación de SOC y CSIRT en una organización. Cada política proporciona directrices y reglas claras para abordar aspectos clave de la seguridad de la información y la respuesta a incidentes.

Política de Detección de Eventos:

Esta política establece los criterios y procesos para detectar eventos de seguridad en los sistemas y redes de la organización. Describe las tecnologías y herramientas utilizadas para la detección de amenazas y establece las directrices para la configuración y administración de estas soluciones.

Política de Registro de Eventos:

Esta política define los requisitos y procedimientos para registrar eventos de seguridad y actividad en los sistemas y redes de la organización. Establece la retención de registros, formatos de registro y las responsabilidades de los administradores y operadores para mantener registros precisos.

Política de Recolección de Información:

Esta política especifica cómo se recopila, almacena y protege la información relacionada con la seguridad de la organización. Define los tipos de datos que deben recopilarse, los métodos de recolección y los protocolos para garantizar la integridad y confidencialidad de la información.

Política de Evaluación de Eventos o Incidentes según Severidad y Prioridad:

Esta política establece criterios para evaluar la gravedad y prioridad de los eventos de seguridad o incidentes. Define los umbrales y parámetros que se utilizan para determinar la importancia de un evento, lo que permite asignar recursos y acciones apropiadas según la severidad y prioridad.

Política de Reunión de Comité de Seguridad:

Esta política describe la estructura, frecuencia y objetivos de las reuniones del comité de seguridad de la organización. Especifica quiénes son los miembros del comité, sus roles y responsabilidades, y cómo se deben abordar y resolver los asuntos de seguridad.

Política de Asignación de Incidentes:

Esta política establece el proceso y los criterios para asignar incidentes a los miembros del CSIRT o al equipo de operaciones de SOC. Define cómo se priorizan y distribuyen los incidentes, considerando la gravedad, el impacto y la disponibilidad de recursos.

Política de Ejecución de Contención de Incidentes:

Esta política describe los pasos y procedimientos que deben seguirse para contener y mitigar incidentes de seguridad. Detalla las acciones específicas que el equipo del CSIRT y el personal de SOC deben tomar para minimizar el daño y restaurar la normalidad operativa de manera segura.

Proceso de Resolución y Gestión de Incidentes:

Este proceso describe las actividades y pasos que se deben seguir para identificar, evaluar, contener, mitigar y resolver incidentes de seguridad. Incluye la notificación, el análisis de causas raíz, la documentación de hallazgos y la restauración de servicios afectados. El objetivo principal es minimizar el impacto de los incidentes y evitar su recurrencia.

Proceso de Priorización y Clasificación de Eventos:

Este proceso se enfoca en la evaluación y clasificación de eventos de seguridad detectados por herramientas de monitoreo y detección. Define criterios y métodos para determinar la gravedad y prioridad de cada evento, lo que ayuda a asignar recursos y atención adecuada según la importancia de cada situación.

Proceso de Mitigación:

Este proceso se centra en la implementación de medidas y acciones para reducir o eliminar los riesgos y amenazas detectadas. Incluye la aplicación de soluciones técnicas, cambios en políticas o procedimientos, y la ejecución de contramedidas específicas para proteger la infraestructura y los activos de la organización.

Procesos de Post-Incidentes:

Estos procesos se llevan a cabo después de que se ha resuelto un incidente de seguridad. Incluyen la revisión y análisis de la respuesta al incidente, la documentación de lecciones aprendidas y la implementación de mejoras en políticas y procedimientos. El objetivo es fortalecer la preparación y la capacidad de respuesta futura.

Proceso de Administración de Recursos de Red y de Sistemas de Información Propios del SOC:

Este proceso describe cómo se gestionan y mantienen los recursos tecnológicos específicos utilizados en el SOC, como herramientas de monitoreo, hardware, software y sistemas de registro. Incluye la configuración, actualización, parcheo y gestión de activos para garantizar su disponibilidad y eficacia en la detección y respuesta a amenazas.

A continuación, se nombran algunas amenazas que llevan a crear las políticas.

6.2.1 Divulgación accidental

Puede ser información sensible que accidentalmente un empleado permite que otras personas vean, o que envía a través de un correo, el simple hecho de tener, por ejemplo, las contraseñas de ahí pegadas en la pantalla del computador, todos eso, son malas prácticas y son temas que hacen parte también de esa divulgación accidental de información sensible.

6.2.2 Empleado curioso, manejo indebido de equipos de trabajo, ingeniería social

Esto tiene que ver mucho con todo el tema que por simple curiosidad se da clic a algo entrando a lugares que no son sitios oficiales o se realiza alguna descarga en algún sitio donde la mayoría de las veces se presta para que se pueda descargar malware a nuestros equipos, el tema de ingeniería social que es esa información que muchas veces nos solicitan y nosotros proporcionamos, puede ser en un formulario, o a través de algo atractivo sin tener en cuenta los riesgos que esto conlleva.

6.2.3 Violación de la privacidad de los datos por un externo con intrusión física

Todo esto tiene que ver con el tema de violación de la privacidad de los datos que son vulnerables que muchas veces se tienen en los sitios y por medio de las cuales los atacantes aprovechan este tipo de vulnerabilidades para infectar o propagar malware en los equipos.

6.2.4 Propagación de Malware y Ransomware

En este tiempo es común escuchar hablar de Malware que es una amenaza bastante conocida, talvez el Ransomware como tal no sea tan familiar, sin embargo, es un tipo de malware que secuestra la información de un equipo y la cifra para poder pedir rescate por ella siendo así uno de los ataques más comunes que se vienen presentando donde muchas veces aparece el mensajito que su información ha sido cifrada y si quiere rescatarla tiene que pagar cierta cantidad de dinero en bitcoin o en criptomonedas que en la actualidad se está moviendo bastante.

6.2.5 Percepciones de los empleados o empleadores

Concientizar a empleados y a la alta dirección que podemos ser un blanco de ataque, a veces está el pensamientos que eso pasa en otra entidad pero quizá a nosotros no, porque tal vez ellos si tienen información importante que puedan querer hurtar o que puedan afectarlos realmente, pero no, esta es una de las percepciones, que debemos empezar dejar a un lado porque todos en el entorno digital podemos ser un blanco de ataques, esto digamos que puede ir desde un ataque informático hasta el robo de información para acceder a nuestras cuentas bancarias, información sensible que podamos manejar o información que publicamos muchas veces en las redes sociales y que pueden servir para que se produzca un ciberataque.

En los usuarios también está la percepción que los ataques son sólo externos, eso es que muchas veces se ve que atacaron cierta entidad o sucedió algún ataque en otro país como España, Estados Unidos y vemos que estamos tan interconectados actualmente que en algún determinado momento alguno de esos ataques que pudo haberse visto en cierto país nos pueden llegar a afectar, entonces es importante entender esto, que no son solo ataques externos, sino que también pueden afectarnos tanto personalmente como a las entidades o empresas.

Se debe tener mucho cuidado cuando llega al correo un mensaje desconocido y se le da clic porque de pronto parece que es real o se ve verdadero, pero puede ser que sea un ataque porque la mayoría de estos necesitan la interacción del usuario final para poder desencadenar la amenaza como tal y afectar la información y los equipos, hay bastantes casos en las entidades que cuando se le da clic a alguno de estos adjuntos o links que ubican en estos correos se empiezan a enviar correos masivos a los contactos que están asociados a esa cuenta, así que hay tener

cuidado porque con solo un clic puede hacer que otros también sean infectados y se propague una infección en toda una entidad o en una red de equipos.

6.2.6 Política de respuesta a incidentes

Esta política de respuesta a incidentes ofrecerá al SOC el alcance y los objetivos que le permita a cada integrante del equipo conocer y trabajar por un mismo propósito. Para el establecimiento de la política es necesario tener en cuenta los siguientes elementos:

6.2.7 Objetivos y propósitos de la política

Es donde se declaran los objetivos y los propósitos de la política para dar cumplimiento de esta, allí debemos identificar los peligros, las amenazas internas y externas, evaluar y valorar los riesgos para poder establecer los controles que sean necesarios.

6.2.8 Alcance de la política

Se debe identificar claramente que abarca esta política, a quien le aplica y los requisitos que de cumplir.

Figura 3. IDS vs IPS

Fuente: Normas ISO, https://www.normas-iso.com/iso-27001/

6.2.9 Actualizar el Sistema Operativo y las aplicaciones

Una de las políticas principales que se debe tener en cuenta es actualizar el sistema operativo y las aplicaciones, es de suma importancia que se pueda llevar a cabo actualizaciones de todos y cada uno de los sistemas operativos y de las aplicaciones debido a que este es una de las brechas o vulnerabilidades mayormente identificadas, por eso hay que tener la última versión estable más reciente y que es la que recomienda el fabricante, un ejemplo de esto es Windows 7 ya está sin soporte, entonces es importante que se tenga en cuenta que cuando un equipo está sin soporte ya no va a recibir actualizaciones de seguridad.

6.2.10 Identificar el Phishing

Los correos que llegan, es importante antes de abrirlo, validar el remitente, la información que se proporciona, el tipo de información que están solicitando, el adjunto que está llegando, hay campañas de malware en este tiempo que tienen que ver con entes de control o entes gubernamentales de control como por ejemplo un correo del Runt, de la DIAN y de entidades bancarias, donde se solicita que se descargue un archivo o de clic aquí porque tiene un comparendo, entonces es muy importante que se aprenda a identificar todos estos correos y antes de dar clic o descargar un adjunto, ser muy cuidadosos en la revisión de esto y dado el caso que no se tenga la certeza de la veracidad de este correo, remitirse al personal que pueda brindar un apoyo y una validación a esta primera revisión que como usuario final se le hace.

6.2.11 Software licenciado

Esto es clave poder tener el software licenciado y evitar todo el tema de crack o el serial de estos de páginas no oficiales porque en la mayoría de los casos, estas mismas páginas permiten que haya descarga de malware y así infectar nuestros equipos o dispositivos, porque ya no es solamente el PC, sino que también el tema del celular que es algo que se usa recurrentemente, en el cual también muchas veces se descarga este tipo de virus.

6.2.12 Políticas para medios extraíbles

Hace parte de esas políticas donde se bloquea o se permite el acceso a ciertos dispositivos como USB, SD o CDs.

6.2.13 Uso de claves seguras

Esto es sumamente importante, es un tema de establecer mucha conciencia porque en algún momento por facilidad o por rapidez, se tiende a colocar contraseñas fáciles como el mes de nacimiento o el primer nombre y el año de nacimiento y

pueden ser fácilmente identificadas mediante las técnicas que usan los ciberatacantes para descifrar este tipo de contraseñas, entonces es muy importante que se haga uso de contraseñas mucho más robustas que pueden ser alfanuméricas que varían en una letra mayúscula, una minúscula caracteres especiales como un asterisco o un porcentaje, incluso hay herramientas que nos permiten crear contraseñas más seguras.

6.2.14 No divulgar información de la entidad a terceros

No copiar información que puede ser sensible a algún correo externo, tratar en lo posible de no tener esta práctica, sino que más bien hacer uso de repositorios que tenga autorizado la entidad como por ejemplo el OneDrive.

6.2.15 Concepto de mínimo privilegio

Esto tiene que ver con dar los permisos a lo que sea necesario para ciertos usuarios, por ejemplo, si un empleado sólo necesita acceder mediante la VPN a consumir “X” o “Y” servicio solamente va a tener permisos para acceder a “X” o “Y” servicios que no permita entrar a cualquier otro servicio solo lo que el usuario necesita consumir.

6.2.16 Múltiples factores de autenticación

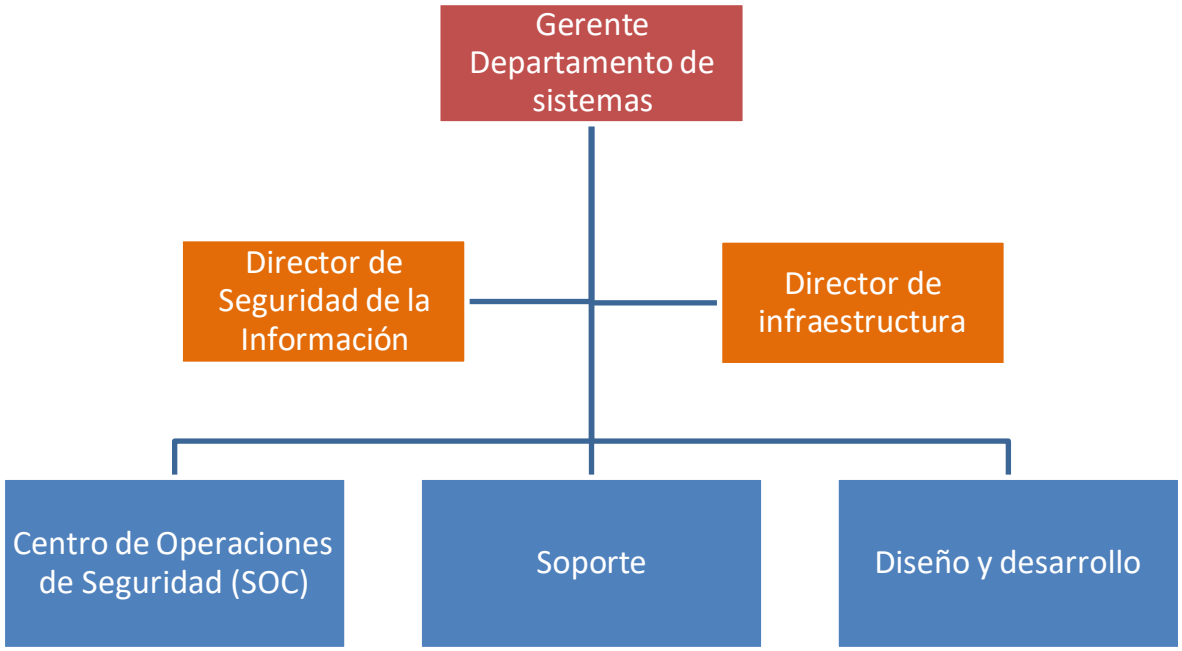
Debe ser recomendado para los empleados en cada una de sus cuentas de usuario de correo, en las redes sociales y en la mensajería instantánea debe estar la opción de utilizar el múltiple factor de autentificación, es cierto que muchas veces es molesto que después de colocar la contraseña se debe colocar un código que llega al celular o por correo dependiendo de la configuración que se haya realizado pero por seguridad es lo mejor, eso es lo que permite que haya una mayor protección en las cuentas de usuario y de los dispositivos, esta es una buena práctica que se debe llevar a cabo.

6.3 ESTRUCTURA DE PERFILES Y ROLES DEL EQUIPO DE TRABAJO DEL SOC

6.3.1 Estructura organizacional

Debido a las diferentes interacciones de los directivos de las diferentes áreas del departamento de sistemas, se realiza el siguiente organigrama que cada uno de los empleados de la empresa Platino Sistemas debe conocer:

Figura 3. Estructura Organizacional



Fuente: El Autor

6.3.2 Perfiles del equipo de trabajo del SOC

Como integrantes de un Centro de Operaciones de Seguridad (SOC), se van a encontrar diferentes perfiles dentro del contexto de la seguridad, ya que los perfiles son amplios así mismo el área de la Seguridad engloba un extenso rango de disciplinas y actividades.

En este sentido, puede ser que el perfil medio de un trabajador que forme parte del SOC es de un analista o especialista en ciberseguridad.

Un SOC se acostumbra a estructurar de distintos niveles principalmente depende del tipo de actividad que se va a realizar y su nivel de especialización que cuenta cada uno de los siguientes recursos:

En un nivel 1 de un SOC, se tienen a los analistas de ciberseguridad, que su principal función es la de vigilar y supervisar cada una de las alertas de seguridad que vienen de las herramientas del SOC. En un primer análisis si es necesario conforme al tipo de alerta o incidencia, debe ser escalado a los técnicos analistas de nivel 2.

En el nivel 2 donde están los analistas senior, se encargan de hacer un primer mapeo del tipo de alarma y afectación de los sistemas que se van a proteger, si por alguna razón hay un impacto, los analistas senior del SOC tienen la capacidad de suministrar una respuesta y formular las acciones correcciones que sean pertinentes al caso.

Por último, tenemos el nivel 3 del SOC, Son lo que se llaman «Navy Seals» del entorno Ciberseguro del SOC. Nivel conformado para dar soporte con profesionales con una mayor capacitación y experiencia en aspectos de ciberseguridad. Este personal experto, tiene la capacidad de realizar o resolver los incidentes de seguridad que les han entregado desde el nivel 2, a demás documentan y realizan procedimientos para dar respuesta a futuras amenazas para ser controladas

Los perfiles especializados en ciberseguridad van a requerir diferentes herramientas para poder realizar sus actividades eficientemente en el Centro de Operaciones de Seguridad (SOC). y así detectar e identificar ataques que puedan comprometer la seguridad de la información de la empresa.

6.3.3 Definición de roles y estructura organizacional

En relación con la anterior estructura los deberes y el entrenamiento requerido para el equipo de trabajo son los siguientes:

6.3.4 Analista de Alertas (primer nivel)

•Deberes: Supervisar continuamente las alertas que se reciben en el SOC y evaluar estas alertas de seguridad y dependiendo lo que defina la política de seguridad se escalan al segundo nivel.

•Entrenamiento requerido: Creación y parametrización de alertas de seguridad, conocimientos mínimos en Networking y manejo de eventos mediante la herramienta SIEM, actualización de nuevas vulnerabilidades e investigación de nuevas herramientas informáticas.

6.3.5 Analista de Respuesta a Incidentes (segundo nivel)

•Deberes: Debe analizar si el sistema o los datos han sido impactados y de ser así recomendaría una respuesta de corrección frente a incidentes de seguridad.

•Entrenamiento requerido: Análisis forense, manejo de herramientas de penetración, hacking y exploits, análisis de malware con ayuda de herramientas de sandboxing.

6.3.6 Profesionales Altamente Capacitados (tercer nivel)

•Deberes: Se encargan de resolver los incidentes e implementan métodos para detección de amenazas, busca posibles incidentes con el objetivo de prevenirlos.

•Entrenamiento requerido: Habilidades en realizar pentesting, análisis de amenazas.

6.3.7 Director del SOC

•Deberes: Es el que planea, coordina y administra los recursos para la correcta operación del SOC, debe garantizar la disponibilidad de los recursos para atención oportuna de los eventos críticos y disponibilidad del personal para que la operación sea continua 24 horas al día los 365 días al año, realiza la revisión de las políticas y objetivos del SOC.

•Entrenamiento requerido: Especialización de dirección de tecnologías.

6.4 HERRAMIENTAS DE HARDWARE Y SOFTWARE PARA LAS ACTIVIDADES DEL CSIRT

Para garantizar el funcionamiento eficiente del CSIRT en la organización Platino Sistemas, es necesario contar con una infraestructura tecnológica adecuada que soporte tanto las operaciones diarias como la gestión de incidentes de seguridad. A continuación, se presentan las herramientas divididas en dos categorías: hardware y software.

6.4.1 Herramientas de Hardware

El equipamiento físico es esencial para soportar la operación continua del CSIRT, permitiendo la recolección, almacenamiento, análisis y recuperación de datos, así como la implementación de medidas de seguridad física y lógica. Entre los principales elementos de hardware se encuentran:

- Servidores dedicados: para el alojamiento de bases de datos, sistemas SIEM, plataformas de gestión de incidentes y servidores de respaldo.

- Firewalls de nueva generación (NGFW): como Cisco Firepower o Palo Alto, que permiten inspección profunda de paquetes, control de aplicaciones y detección de amenazas.

- Switches gestionables y segmentación VLAN: para aislar la red del CSIRT y aplicar políticas de seguridad.

- Dispositivos de almacenamiento NAS o SAN: para copias de seguridad, análisis forense y archivo de logs.
- Unidades de respaldo ininterrumpido (UPS): para asegurar la continuidad operativa ante fallos eléctricos.
- Estaciones de trabajo especializados: con características de alto rendimiento para análisis forense digital y ejecución de laboratorios virtuales.
- Dispositivos de red para monitoreo: como TAPs (Test Access Points) o SPAN ports para la captura de tráfico en tiempo real.

6.4.2 Herramientas de Software

A continuación, se muestran las herramientas de software para el desarrollo de las actividades del CSIRT que permiten automatizar, centralizar y fortalecer la gestión de eventos de seguridad, detección de incidentes, respuesta y análisis posterior:

Función del CSIRT	Herramienta	Descripción	Tipo
Monitoreo y detección de eventos	**Wazuh**	Plataforma SIEM y HIDS con análisis de logs, alertas y correlación	Open source
Análisis de malware	**Cuckoo Sandbox**	Automatiza el análisis de malware en entornos aislados	Open source
Gestión de incidentes	**TheHive**	Plataforma de gestión de incidentes integrada con Cortex y MISP	Open source
Recolección y análisis de evidencia	**Autopsy**	Herramienta forense para análisis de discos y recuperación de evidencia	Open source
Compartición de indicadores de compromiso (IoC)	**MISP (Malware Information Sharing Platform)**	Compartición de IoCs y correlación con amenazas externas	Open source
Gestión de vulnerabilidades	**OpenVAS / Greenbone**	Escáner de vulnerabilidades de red y servicios	Open source
Respuesta y contención	**SOCless (AWS)** o scripts personalizados con **Ansible/PowerShell**	Automatización de respuestas a incidentes	Mixto
Comunicación y coordinación	**Zammad / GLPI**	Mesa de ayuda para canalizar incidentes y tareas	Open source

6.4.3 Pasos para realizar un laboratorio controlado a partir del uso de máquinas virtuales

A continuación, se dan los pasos a seguir para realizar una simulación de un entorno controlado que permita probar las herramientas propuestas para el CSIRT, y así verificar su funcionamiento y documentar evidencias del proceso para la puesta en marcha del Centro de Operaciones de Seguridad (SOC).

1. **Entorno virtualizado**

Como primer paso se deben instalar cada una de las máquinas virtuales en VirtualBox para simular los distintos nodos de trabajo del CSIRT. La topología es la siguiente:

Máquina Virtual	Sistema Operativo	Rol	Herramientas principales
CSIRT-Server	Ubuntu Server 22.04	Gestión de incidentes	TheHive, Cortex, MISP
SIEM-Node	Ubuntu Desktop 22.04	Recolección y análisis	Wazuh
Victim-Win	Windows 11 Pro	Endpoint víctima	Agente Wazuh, vulnerable intentionally
Attacker	Kali Linux	Nodo atacante	Metasploit, Nmap, Wireshark

2. **Escenarios del laboratorio**

Escenario 1: Detección de intrusión con Wazuh

Objetivo: Detectar una exploración de puertos desde Kali Linux a la máquina Windows utilizando Wazuh.

Pasos:

1. Instalar Wazuh Manager en SIEM-Node y configurar el dashboard.
2. Instalar el agente de Wazuh en Victim-Win.
3. Desde Kali Linux ejecutar *nmap -sS 192.168.56.10*.
4. Verificar en el dashboard de Wazuh que se genere la alerta de escaneo.
5. Ver consola de Nmap en Kali ejecutando el escaneo.
6. Ver interfaz de Wazuh mostrando la alerta generada.

Escenario 2: Registro del incidente en TheHive

Objetivo: Documentar un incidente detectado y relacionarlo con los datos capturados por Wazuh.

Pasos:

1. Iniciar sesión en TheHive.
2. Crear un nuevo caso con título: "Escaneo de puertos desde Kali".
3. Adjuntar evidencia: logs del agente Wazuh.
4. Ver formulario de creación de caso en TheHive.
5. Ver caso abierto con evidencias adjuntas.

Escenario 3: Automatización con Cortex

Objetivo: Analizar un archivo sospechoso mediante Cortex desde TheHive.

Pasos:

1. Configurar integración entre TheHive y Cortex.
2. Subir archivo de prueba (simulado o de EICAR) como artefacto.
3. Ejecutar análisis desde Cortex.
4. Ver la ejecución de job en Cortex.
5. Ver el resultado del análisis con clasificación del archivo.

Escenario 4: Compartición en MISP

Objetivo: Compartir un IOC detectado en el incidente.

Pasos:

1. Ingresar a MISP desde CSIRT-Server.
2. Crear un nuevo evento con IP de origen del ataque.
3. Asociar evento con tags y correlaciones.
4. Ver el formulario de nuevo evento.
5. Ver evento creado con IOCs cargados

Escenario 5: Análisis forense

Objetivo: Extraer evidencia de la máquina comprometida (Victim-Win).

Pasos:

1. Utilizar FTK Imager para capturar disco o memoria.
2. Analizar artefactos con Autopsy.
3. Observar la interfaz de FTK capturando imagen.
4. Revisar el reporte en Autopsy con archivos sospechosos encontrados.

Al realizar los pasos mencionados se puede validar la integración de herramientas de software para la operación del CSIRT en un entorno controlado. Las pruebas pueden demostrar la capacidad de detección, gestión y análisis de incidentes, siendo replicables y escalables a producción.

7 CONCLUSIONES

- Se dieron los lineamientos para la operación del SOC y la gestión de incidentes y problemas, las cuales se deben tener en cuenta para ver qué actividades desarrollar cuando se presenten eventos o incidentes identificados.

- Al establecer las políticas para la operación del SOC hay más claridad respecto a cómo se debe actuar para garantizar confidencialidad, integridad y disponibilidad de la información.

- Se definieron los roles y responsabilidades de acuerdo a las exigencias mínimas requerida para poder operar el SOC.

- Se definieron que herramientas tanto de hardware como de software se requieren para poder realizar las actividades propias del Centro de Operaciones de Seguridad (SOC).

8 RECOMENDACIONES

- La cultura de la seguridad digital es una responsabilidad no solamente del área de TI o de la alta dirección, sino responsabilidad de todos y de cada uno de los funcionarios usuarios finales que hacen parte de las entidades o empresas y también todo esto cobija también parte de lo que hacemos en nuestro día a día en nuestros hogares y a todos los servicios que accedemos desde allí.

- Se requiere la evaluación de las herramientas utilizadas para el manejo de los incidentes debido que hay unas que no generan reportes de los incidentes detectados.

- Se recomienda que se evalúe las fortalezas y debilidades relacionada a los incidentes con el fin de que si se vuelven a presentar ya se esté preparado para que no haya una afectación en la continuidad del negocio de cada uno de los clientes de la organización.

9 BIBLIOGRAFÍA

1. ACIS. La pérdida de datos les cuesta a las empresas más de 4 millones de dólares al año [en línea]. Bogotá [Consulta: 14 de marzo 2021]. Disponible en: https://acis.org.co/portal/content/la-p%C3%A9rdida-de-datos-les-cuesta-las-empresas-m%C3%A1s-de-4-millones-de-d%C3%B3lares-al-a%C3%B1o

2. ECURED. Ataque informático [en línea]. Cuba [Consulta: 14 de marzo 2021]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

3. ID GRUP. Qué es un Firewall y cómo funciona [en línea]. Barcelona [Consulta: 14 de marzo 2021]. Disponible en: https://idgrup.com/firewall-que-es-y-como-funciona/

4. NETEC. ¿Qué es seguridad informática? [en línea]. Bogotá [Consulta: 16 de marzo 2021]. Disponible en: https://www.netec.com/que-es-seguridad-informatica

5. PUNT INFORMATIC. Sistemas de detección y prevención IDS e IPS: ¿Para qué sirven? [en línea]. Barcelona [Consulta: 16 de marzo 2021]. Disponible en: https://puntinformatic.com/sistemas-de-deteccion-y-prevencion-ids-e-ips/#:~:text=Tanto%20los%20Sistemas%20de%20Detecci%C3%B3n,datos%2C%20para%20detectar%20patrones%20sospechosos

6. FIRMA-e. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? [en línea]. Murcia, España [Consulta: 16 de marzo 2021]. Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

7. ISO2700.ES. SGSI [sitio web]. España [Consulta: 20 de marzo 2021]. Disponible en: https://www.iso27000.es/sgsi.html

8. EALDE. Ciberseguridad y riesgos digitales [en línea]. Madrid, España [Consulta: 20 de marzo 2021]. Disponible en: https://www.ealde.es/que-es-centro-operaciones-ciberseguridad/

9. HARD2BIT. ¿Qué es un SOC y por qué es importante para tu negocio? [en línea]. Madrid, España [Consulta: 20 de marzo 2021]. Disponible en: https://hard2bit.com/blog/que-es-un-soc-y-por-que-es-importante-para-tu-negocio/

10. IU. ¿Qué es la seguridad informática y cómo puede ayudarme? [en línea]. Bogotá [Consulta: 20 de marzo 2021]. Disponible en: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

11. DELOITTE. Pasos a seguir ante un ataque informático [en línea]. Barcelona, España [Consulta: 20 de marzo 2021]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

12. EITB.EUS. CIBERATAQUES [sitio web]. España [Consulta: 20 de marzo 2021]. Disponible en: https://www.eitb.eus/es/tag/ciberataques/

13. COLCERT. Grupo de respuesta a emergencias cibernéticas de Colombia [sitio web]. Colombia [Consulta: 20 de marzo 2021]. Disponible en: http://www.colcert.gov.co/

14. WELIVESECURITY. Cuál es la diferencia entre virus y malware [en línea]. República Eslovaca [Consulta: 20 de marzo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/08/18/diferencia-entre-virus-malware/

15. DIGICERT. ¿En qué consisten el malware, los virus, el spyware y las cookies? [en línea]. España [Consulta: 20 de marzo 2021]. Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

16. SOTESA. Las 5 causas más habituales de pérdida de datos en tu empresa (y cómo evitarlas) [en línea]. Tenerife, España [Consulta: 20 de marzo 2021]. Disponible en: https://sotesa.com/las-5-causas-mas-habituales-perdida-de-datos-empresa/

17. EMPRESARIAL & LABORAL. La pérdida de datos les cuesta a las empresas más de 4 millones de dólares al año [en línea]. Bogotá [Consulta: 20 de marzo 2021]. Disponible en: https://revistaempresarial.com/tecnologia/seguridad-informatica/perdida-datos-cuesta-empresas-4-millones-dolares-ano/

18. BESERVICES. Pérdida de datos para las empresas ¿Cómo solucionarlo? [en línea]. España [Consulta: 20 de marzo 2021]. Disponible en: https://www.beservices.es/perdida-datos-empresas-n-5356-es

19. IMF. ¿Qué es un SOC y qué actividades realiza? [en línea]. España [Consulta: 20 de marzo 2021]. Disponible en: https://blogs.imf-formacion.com/blog/tecnologia/que-es-soc-actividades-realiza-201903/

20. ODS. Diferencias entre un Centro de Operaciones de Seguridad interno y externo [en línea]. Reino Unido [Consulta: 20 de marzo 2021]. Disponible en: https://opendatasecurity.io/es/soc-que-es-y-por-que-es-interesante-para-tu-empresa/

21. ODS. ¿Qué tipos de empresas necesitan un Centro de Operaciones de Seguridad? [en línea]. Reino Unido [Consulta: 20 de marzo 2021]. Disponible en: https://opendatasecurity.io/es/soc-que-es-y-por-que-es-interesante-para-tu-empresa/

22. SECURE SOFT. ¿Cómo organizar un CSIRT? [en línea]. Bogotá [Consulta: 21 de marzo 2021]. Disponible en: https://securitysummitperu.com/articulos/como-organizar-un-csirt/

23. AIUKEN. Centro de Operaciones de Seguridad (SOC) [en línea]. Madrid, España [Consulta: 21 de marzo 2021]. Disponible en: https://www.aiuken.com/es/services/security-operation-center

24. GMS. ¿Por qué se debe contratar un SOC (Security Operations Center)? [en línea]. Bogotá [Consulta: 21 de marzo 2021]. Disponible en: https://gmsseguridad.com/soluciones/soc/

25. BIT. Ventajas de implantar un Centro de Operaciones de Seguridad [en línea]. Barcelona, España [Consulta: 21 de marzo 2021]. Disponible en: https://www.bit.es/knowledge-center/ventajas-de-implantar-un-soc-o-centro-de-operaciones-de-seguridad/

26. ASOBANCARIA. CSIRT financiero un enfoque colaborativo a la ciberseguridad [en línea]. Bogotá [Consulta: 21 de marzo 2021]. Disponible en: https://www.asobancaria.com/csirt/

27. SECURE & IT. CSIRT [en línea]. Madrid, España [Consulta: 21 de marzo 2021]. Disponible en: https://www.secureit.es/csirt/

28. TECHTARGET. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT) [en línea]. España [Consulta: 21 de marzo 2021]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

29. TECHTARGET. CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia? [en línea]. España [Consulta: 21 de marzo 2021]. Disponible en: https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

30. UNIVERSIDAD DE LOS ANDES. Constitución de un equipo de respuesta a incidentes para el sector financiero en Colombia [en línea]. Bogotá [Consulta: 21 de marzo 2021]. Disponible en: https://sistemas.uniandes.edu.co/maestrias/mesi/proyectos/proyecto.php?id=24

31. PAGEPERSONNEL. Cuáles son los perfiles ideales de un equipo de trabajo eficaz [en línea]. España [Consulta: 22 de marzo 2021]. Disponible en: https://www.pagepersonnel.es/advice/candidatos/desarrollo-profesional/cu%C3%A1les-son-los-perfiles-ideales-de-un-equipo-de-trabajo

32. ORACLE. ¿Qué es un SOC? [en línea]. España [Consulta: 22 de marzo 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

33. ICM. La tecnología SIEM para la seguridad informática [en línea]. Barcelona, España [Consulta: 22 de marzo 2021]. Disponible en: https://www.icm.es/2020/08/18/tecnologia-siem/

34. SOFECOM. SIEM la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran [en línea]. Madrid, España [Consulta: 22 de marzo 2021]. Disponible en: https://sofecom.com/que-es-un-siem/

35. NSIT. Cuáles son las funciones del SOC [en línea]. Bogotá [Consulta: 22 de marzo 2021]. Disponible en: https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

36. GMS. Por qué contratar un SOC [en línea]. Bogotá [Consulta: 23 de marzo 2021]. Disponible en: https://gmsseguridad.com/soluciones/soc/

37. ORACLE. Como funciona un SOC [en línea]. España [Consulta: 23 de marzo 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

38. SCIELO. Política y seguridad de la información [en línea]. La Paz, Bolivia [Consulta: 23 de marzo 2021]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

39. BOGOTA. Políticas de seguridad de la información [en línea]. Bogotá [Consulta: 24 de marzo 2021]. Disponible en: http://www.gobiernobogota.gov.co/transparencia/atencion-ciudadano/pol%C3%ADticas-seguridad-la-informaci%C3%B3n-y-protecci%C3%B3n-datos-pesonales

40. SGC. Políticas de seguridad de la información [en línea]. Bogotá [Consulta: 24 de marzo 2021]. Disponible en: https://www2.sgc.gov.co/AtencionAlCiudadano/Paginas/politica-seguridad-de-la-informacion.aspx