Monitoreo y respuesta de incidentes de seguridad digital

Breve descripción:

Con el estudio de este componente, el aprendiz fortalecerá su capacidad de asimilar y aplicar conceptos para la realización de actividades de monitoreo y respuesta de incidentes de la seguridad digital; igualmente, afianzará su capacidad de comprender los conceptos de análisis de “logs”, vulnerabilidades e incidentes.

Noviembre 2023

Tabla de contenido

Introducción

Estimado aprendiz, a través del siguiente video, podrá conocer los aspectos relevantes sobre el monitoreo y respuesta de incidentes de seguridad digital:

Video 1. Monitoreo y respuesta de incidentes de seguridad digital

Comentado [AF1]: No hay miniatura.

Enlace de reproducción del video

Comentado [AF2]: No hay video

Síntesis del video: Monitoreo y respuesta de incidentes de seguridad digital
En las organizaciones se presentan diversos riesgos de ciberseguridad, por esta razón se ven en la necesidad de implementar diversos controles de seguridad digital. Estos controles son fundamentales para mitigar riesgos, pero es esencial revisarlos y mantenerlos regularmente para garantizar la seguridad a largo plazo.

La rápida evolución tecnológica abre la puerta a nuevas vulnerabilidades, así mismo, las amenazas evolucionan adquiriendo capacidades para violentar sistemas que anteriormente no podían.

Por lo anterior, es necesario realizar monitoreo de la seguridad digital de acuerdo con los indicadores y métricas establecidos o planificados para obtener información técnica de los controles de seguridad digital, partiendo de registros e información técnica de diversos dispositivos.

En este componente formativo, se detallarán los conceptos necesarios para llevar a cabo actividades de monitoreo y acciones de respuesta a incidentes en el ámbito de la seguridad digital.

Se explorarán elementos de análisis de "logs", vulnerabilidades e incidentes. Recuerde:

- ✓ Explorar todos los recursos didácticos que el componente tiene para usted.
- ✓ Llevar un registro de los elementos teóricos, conceptuales y prácticos que vaya asimilando en el recorrido del componente.
- ✓ Tener a la mano una herramienta de registro: computadora, libreta de notas o cualquier otra que le permita llevar apuntes.
- ✓ Seleccionar un buen momento y un espacio oportuno para el estudio de este componente.
- ✓ Repasar cada punto del componente que usted considere que debe reforzar.

1. Monitoreo y análisis de “logs”

Consiste en realizar una revisión periódica de los controles de seguridad digital y de los sistemas informáticos, con base en los registros de eventos de los mismos. Dicho análisis, puede ser aplicado según se requiera de manera manual o automatizada.

Los monitoreos pueden automatizarse por medio de herramientas de “software” facilitando el análisis y toma de decisión.

Para comprender mejor la actividad de monitoreo y análisis de “logs”, le presentamos a continuación, una descripción de conceptos y detalles importantes:

A. **“Log” o registro:** consiste en un archivo plano de texto o base de datos en el cual se encuentran, cronológicamente, los eventos, sucesos y cambios que han ocurrido en un sistema informático, tales como aplicaciones, servidores, servicios de red, entre otros.
B. **Dónde se encuentra:** en archivos planos de texto o en bases de datos de los sistemas. Pueden ser leídos manual o automáticamente por administradores y/o auditores de sistemas, mediante herramientas especializadas como los correlacionadores, que leen “logs” de diversos dispositivos; también pueden relacionarlos y generar alarmas con base en las bases de conocimiento y parámetros de configuraciones previas.
C. **Huella o rastro:** un “log” o registro, en cierto modo, es una huella o rastro que deja el usuario al interactuar con un sistema, elemento de red, servicio o aplicación. De tal forma que los “logs” son vitales como evidencia digital en el desarrollo de investigaciones dentro de una organización.
D. **Análisis de “logs”:** es la recolección de datos de “logs” o registros, contrastarlos con bases de conocimiento (lógicas, experiencias,

referencias, etc.), logrando generar salidas de datos para realizar análisis, monitorización e informes.

E. **Monitoreo de "logs":** consiste en la sistematización de la información de los "logs" de diversos dispositivos de una red, sujetos de monitoreo; de tal manera que se puedan correlacionar, analizar y entender los eventos que se están presentando en tiempo real, ayudando a la toma de acciones de respuesta o mitigación de fallos y amenazas.

1.1. Tipos de "logs"

Existen diversos tipos de "logs" y estos son sujetos de monitoreo y análisis, por tanto, es de suma importancia lograr un entendimiento suficiente de los mismos. Los tipos de "logs" más frecuentes son, por un lado, los "logs" de sistemas operativo y red y, por otro, los "logs" de servicios y aplicaciones.

A continuación, se presentan elementos de suma importancia sobre los tipos de "logs", que se deben conocer:

Tipos de "logs"

A. **De sistemas operativos y red**: "logs" de "hosts", sistemas operativos Windows, GNU/Linux y "Routers"

- ✓ **"Host":** son puntos de conexión final en una red, tales como computadores, tabletas y dispositivos móviles, los mismos generan diversos "logs" que se describen a continuación.
  "Logs" de consola, "logs" de sistemas ("Syslog"), "job log", "operlog", "hard-copy log".

- ✓ **Windows:** la información sobre registros en Windows se presenta en los registros de eventos, que son sucesos que se almacenan en un registro de eventos en el equipo y se pueden observar en el visor de eventos de Windows. Incluyen eventos relacionados con el sistema, aplicaciones, seguridad y configuración. Errores, advertencias e información.
- ✓ **GNU/Linux:** es un sistema operativo "Open Source", que puede recopilar "logs" de acuerdo con el acceso de los usuarios, características del sistema, fallo en los intentos de conexión y utilización de recursos. Esto suministra ventajas de seguridad, porque puede descubrir usos indebidos rápidamente en sus registros, pero su desventaja es su gran volumen de registros complicando la gestión de información de los "logs". El nombre y localización del fichero puede variar de acuerdo con variantes y versiones de GNU/Linux.
- ✓ **"Routers":** los "routers" y "switches" registran eventos relacionados con la conectividad y acceso a redes. Estos registros, principalmente para seguridad, contienen detalles como direcciones IP, servicios, nombres de "hosts" y fechas de conexión, priorizando seguridad sobre funciones de red. Este tipo de detalles de estos "logs", son relevantes para la correlación de eventos dentro de un sistema SIEM.

B. **De servicios o aplicaciones:** serie de servicios y aplicaciones. Se deben conocer los servicios que prestan y los ficheros que aportan información de seguridad.

- ✓ **De seguridad:** son datos importantes que se deben investigar y cruzar entre ellos para obtener la mayor información posible, como el tráfico de red, y evitar vulnerabilidades y amenazas.
  - Next Generation Firewall.
  - "Antimalware".
  - Sistema de detección de intrusiones (IDS).
  - "Proxies".
- ✓ **Servicio de correo:** los "logs" que se presentan en los servicios de correo aportan información sobre el origen y destino de los mensajes, como: dirección del remitente y destinatario, IP del remitente y destinatario, fecha e ID del mensaje. Esta es información que se utiliza para el filtrado y/o reporte de "Spam" o correos maliciosos.
- ✓ **Servidores de aplicaciones:** son servidores que soportan herramientas "software" y proporcionan servicios y aplicaciones en la red pública (en Internet) o privada (dentro de la empresa). Los mismos generan una serie de "logs" basados en su sistema operativo. Según servicios y aplicaciones que proporciona, dichos "logs" son muy útiles para un SIEM y, especialmente, para los procesos de auditoría de sistemas.
- ✓ **Sistemas de monitorización:** es un programa que tiene como finalidad la comprobación del correcto estado, funcionamiento y

disponibilidad de los sistemas, redes y servicios. Nagios, Patrol y Tivoli son los sistemas más conocidos.

- ✓ **Otros servicios:** servicios que deben ser considerados en el momento de la recopilación y análisis de "log", lo que dependerá de los sistemas de información de cada empresa.
  - Servidores web.
  - Base de datos.
  - Servidor de archivos.
  - Servidor FTP.

1.2. Características del monitoreo y análisis de "logs"

El monitoreo y análisis de "logs" puede darse de manera automatizada o manual. Actualmente, se automatizan en la mayoría de casos para facilitar el análisis y la toma de acciones ante eventos, logrando de manera rápida el control de eventos, amenazas, vulnerabilidades e incidentes adversos.

Las siguientes son las características del monitoreo y análisis de "logs", en relación con la recopilación, correlación y almacenamiento de información:

A. **Manual:** este tipo de monitoreo y análisis de "logs" se realiza especialmente en actividades de auditoría de sistemas y análisis forenses.
B. **Automatizada:** es comúnmente utilizado en procesos de monitoreo de seguridad digital en tiempo real, desarrollando actividades de recolección, correlación y almacenamiento de "logs", dando como resultado

información rápida para el análisis, reportes e informes que ayuden a identificar fallas, amenazas y demás eventos adversos de manera rápida.

C. **"Logs" de conexiones de origen y destino:** son los registros de conexiones de origen y destino en la red, donde se detalla el nombre del "host", IP, puertos, protocolos, tiempos y fecha de conexión.
D. "**Logs**" **de acceso:** son los registros de acceso en sistemas, servicios y aplicaciones, en los cuales se describe el nombre de usuario, IP de origen, fecha y hora de acceso, intentos de accesos válidos y fallidos.
E. **"Logs" de cambios:** son los registros de cambios en sistemas, servicios y aplicaciones, además del nombre de usuario, cambios en la configuración (incluidos roles y contraseñas de accesos), archivos modificados, fecha y hora del cambio.

2. Fundamentos de SIEM

Un **SIEM** (Security Information and Event Management en inglés), es una definición utilizada para aplicaciones que involucran **SEM** (Security Event Management - Gestión de Eventos de Seguridad) que recoge, agrega y actúa sobre los eventos de seguridad y **SIM** (Security Information Management - Gestión de Información de Seguridad) que correlaciona, normaliza e informa sobre los datos de eventos de seguridad recogidos. Las herramientas SIEM ofrecen un análisis en tiempo real para eventos de seguridad generados en gran medida por la infraestructura de los sistemas de información (Avella, Calderón y Mateus, 2015).

Fundamentos de SIEM, "Security Information and Event Management". Ver documento anexo **"Security Information and Event Management"**, ubicado en la carpeta de anexos, con la finalidad de ampliar los conocimientos en el tema.

3. Fundamentos de SOC – Security Operation Center

Un centro de operaciones de seguridad o SOC, se puede entender como la conformación de un equipo de técnicos, profesionales y especialistas con habilidades en seguridad digital e infraestructura tecnológica que se apoyan en el uso de herramientas "hardware" y "software" para lograr cumplir con la responsabilidad de detectar, analizar y responder ante eventos, vulnerabilidades e incidentes de ciberseguridad.

El Centro de Operaciones de Seguridad, SOC, se refiere al equipo responsable de garantizar la seguridad de la información. El SOC es una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota. El SIEM (Security Information Event Management) es la principal herramienta del SOC, ya que permite gestionar los eventos de un sistema de información (Oracle.com, 2021).

A continuación, se detallan algunos conceptos y elementos generales de las etapas de operación de un SOC, que favorecen un correcto funcionamiento:

A. **Prevención:** con base en la experiencia y adopción de buenas prácticas de ciberseguridad, el SOC debe apropiar medidas de prevención a nivel técnico y de conciencia en la organización. Entre las soluciones preventivas se pueden considerar aplicación de controles de seguridad ("Firewalls",

"AntiMalware", etc.), el monitoreo continuo de la seguridad, el análisis y gestión de las vulnerabilidades técnicas.

B. **Detección:** consiste en el monitoreo constante de los eventos para detectar amenazas, vulnerabilidades, intrusiones y fallos de seguridad, para responder de manera rápida y eficaz. La principal herramienta que apoya esta etapa son las SIEM.
C. **Análisis:** en esta etapa se deben analizar los eventos detectados para determinar si corresponden a amenazas reales o si son falsas alertas. Los sistemas SIEM ayudan en el proceso de análisis con su base de datos de conocimientos y experiencias anómalas, registradas previamente, así como en la configuración de las reglas de cumplimiento.
D. **Respuesta:** consiste en las acciones que se toman para responder frente a un evento o incidentes de ciberseguridad; las mismas deben estar planificadas de manera que se apliquen las medidas o controles de forma eficaz.

3.1. Objetivos de los SOC

El objetivo de un SOC es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques diferentes. Estos supervisan y analizan la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas, en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad o un compromiso (Oracle.com, 2021).

El SOC debe garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen adecuadamente. Los SOC están

generalmente compuestos por analistas e ingenieros de seguridad, así como por gerentes que supervisan las operaciones de seguridad (Oracle.com, 2021).

¡Atención! Las capacidades adicionales de algunas SOC pueden incluir el análisis avanzado, el criptoanálisis y la ingeniería inversa del "malware" para analizar los incidentes.

¡Importante! Los equipos de SSC trabajan en estrecha colaboración con los equipos de respuesta para garantizar que el problema de seguridad se aborde adecuadamente una vez que se ha descubierto.

Los objetivos de un centro de operaciones de seguridad (SOC), deben enfocarse en:

- ✓ Reducir riesgos y tiempo de indisponibilidad de aplicaciones y servicios.
- ✓ Control y prevención de amenazas.
- ✓ Disminuir la carga de trabajo administrativa del personal de seguridad.
- ✓ Establecer al personal de seguridad y definición responsabilidades.
- ✓ Indicar los tiempos de soporte y escalamiento de eventos.
- ✓ Definir los procesos de auditoría y soportes de cumplimiento.
- ✓ Responder a incidentes y recuperación.

3.2. Alcance

El alcance de un SOC puede ser establecido según los requisitos del negocio, y se deben determinar los servicios y aplicaciones a proteger, así como las redes y otros activos de información que se consideren.

A continuación, se describen los aspectos necesarios para definir el alcance de un SOC:

A. **Requisitos del negocio:** en el marco de cumplimientos legales, contractuales y de las estrategias operacionales que la compañía haya establecido.
B. **Activos necesarios a proteger:** se deben considerar los sistemas, servicios y aplicaciones, como los servidores de bases de datos y aplicaciones, que actuarán como fuentes de eventos para el SIEM.
C. **Equipo y responsabilidades:** es esencial considerar las capacidades del personal disponible y definir responsabilidades alcanzables dentro del contexto, asegurando una asignación adecuada y realista de tareas.
D. **Presupuesto, recursos y herramientas:** de acuerdo con el presupuesto, recursos y herramientas de ciberseguridad que se destinen para la implementación y operación del SOC se establece el alcance y objetivos que se permitan cumplir.

4. Técnicas de recopilación de información

Dentro del proceso de Ethical Hacking - EH, la primera etapa consiste en recopilar la mayor cantidad de información posible para preparar las pruebas de análisis de vulnerabilidades y Pentest (Pruebas de Penetración a Sistemas). Esta etapa de recopilación de información se denomina Information Gathering, este concepto se sustenta en que es un paso previo que un ciberdelincuente utiliza para recoger la mayor

cantidad de datos posibles para preparar con mayor eficacia un ataque a una organización u objetivo.

El atacante recolecta los datos de su objetivo por medio de fuentes públicas, tales como internet, buscadores, redes sociales y plataformas de acceso público; con la información que va recolectando armar posibles vectores de ataque, para los cuales utilizará las herramientas técnicas que mejor le faciliten el lograr sus objetivos.

Ahora, se sugiere estudiar algunos conceptos y elementos clave de las técnicas de recopilación de información, así como identificar los aspectos más importantes y llevar un registro en la libreta personal de apuntes.

A. **Conducta ética en ciberseguridad**

   Afianzamiento ético y moral de las personas para promover el buen comportamiento y cumplimiento de los principios de seguridad de la información. Así, si una persona que se desenvuelve en el sector de las tecnologías de la información y la ciberseguridad debe mantener una conducta ética para la preservación de la seguridad en los sistemas y el entorno, gestionando de manera adecuada vulnerabilidades y amenazas y todo riesgo de ciberseguridad.

B. **Ethical Hacking**

   Proceso de seguridad digital donde personas o equipos de personas, expertos técnicos o profesionales, realizan pruebas de seguridad digital, simulando ataques controlados y previamente planificados a los sistemas y/o activos. Este proceso busca descubrir vulnerabilidades y malas configuraciones en los sistemas y/o tecnologías utilizadas en una empresa, para aplicar correcciones, actualizaciones y controles de seguridad digital.

C. Pasos del Ethical Hacking

- ✓ Establecimiento de objetivos y alcance.
- ✓ Recopilación o Information Gathering, "Footprinting", escaneo y enumeración.
- ✓ Ejecución, obtención de accesos y logro de objetivos planteados con evidencias.
- ✓ Análisis.
- ✓ Documentación o informe técnico completo y detallado.
- ✓ Presentación o resumen ejecutivo.

D. Vector de ataque, de red y adyacente

Son los medios o canales de explotación de vulnerabilidades por parte del atacante. Facilita determinar facilidades para penetrar sistemas y determinar métodos posibles de ataque, sin intervención humana por parte de la víctima. A las vulnerabilidades se les asocia el vector de ataque, los cuales se agrupan en:

- ✓ **Vector de red:** un ataque puede explotar una vulnerabilidad de manera remota por medio de servicios basados en Internet.
- ✓ **Vector adyacente:** el ataque se puede realizar a la vulnerabilidad desde la misma red adyacente, en una misma red local.

E. Vector local y vector físico

- ✓ **Vector local:** una vulnerabilidad puede ser explotada según las capacidades de lectura, escritura y ejecución en el sistema, se suele requerir de interacción de ingeniería social para engañar al usuario del sistema para que realice acciones maliciosas como abrir un archivo infectado.

- ✓ **Vector físico:** el atacante requiere realizar manipulación física para lograr vulnerar un sistema o componente.

F. Delito cibernético

Forma emergente de delincuencia transnacional de rápido crecimiento. Al crecimiento y expansión del internet los delincuentes han logrado sacarle provecho. Con unos dos mil millones de usuarios mundialmente, el ciberespacio es el lugar ideal para los delincuentes, quienes pueden permanecer anónimos y acceder a todo tipo de información personal que se guarda en línea (Naciones Unidas, 2021).

4.1. Tipos de Information Gathering

Los tipos de recolección de información hacen referencia a las distintas técnicas y variados métodos para dicha actividad; tales técnicas y métodos son de suma importancia y requieren ser comprendidas y asimiladas suficientemente con miras a su aplicación.

Ahora, se presenta una serie de tipos de técnicas de recopilación de información, se invita a estudiarlas a conciencia a través de la siguiente información:

A. "Footprinting" (huella): procedimiento que reúne gran cantidad de información de la víctima u objetivo. El "footprinting" es activo cuando se crea en el momento que los datos personales son divulgados de manera consciente y deliberada o cuando hay contacto con el propietario. Es huella pasiva o seudónima cuando se recolecta información sin el propietario, con lo anterior se puede exponer la seguridad del objetivo.

B. **Proceso de "footprinting":**
   - ✓ Se recolecta información de la organización o de personas (motores de búsqueda, redes sociales, información pública).
   - ✓ Se recolecta información de la red ("hosts" e IP, puertos, "software" y aplicaciones en red).
   - ✓ Se recolecta información de servidores de Internet (DNS, direcciones IP públicas, servicios o puertos públicos, "software"/aplicaciones públicas).

C. **"Scanning" o exploración:** técnicas que se utilizan para reconocer "host2, puertos y servicios que se encuentran dentro de una red, con el fin de obtener la mayor cantidad de datos que se utilizan en la creación de una visión general de la organización para preparar un ataque a la misma.

D. **Proceso de "scanning":** en el proceso de escaneo o de exploración se realiza escaneo de "hosts", escaneo de puertos (servicios de red), escaneo de vulnerabilidades.

E. **"Enumeration" o enumeración:** consiste en enumerar e identificar los nombres de hosts, usuarios, recursos compartidos, servicios, entre otra información que pueda ser relevante. Esta actividad puede ser realizada paralelamente con el "scanning" o exploración.

F. **¡Atención!** Las técnicas de recopilación de información deben ser utilizadas de manera responsable, teniendo en cuenta que tiene características particulares para violentar los sistemas de una organización e incluso de las personas y la sociedad en general.

4.2. Características

Las características de las técnicas de recolección son muy particulares ya que, gracias a ellas justamente, es que se facilita violentar los sistemas de una organización o de las personas y la sociedad.

Las características principales de las técnicas de recopilación de información se describen a continuación:

A. **Uso de fuentes abiertas o públicas:** obtiene la mayor cantidad de información de fuentes públicas, internet, redes sociales, plataformas, etc., que permiten conocer a una organización o a las personas.
B. **Exploración:** realiza procesos de escaneos técnicos no intrusivos para obtener datos técnicos de "hosts", puertos, servicios y vulnerabilidades para una mejor preparación de las pruebas de intrusión.
C. **Perfilamiento:** aplica un perfilamiento del objetivo con la información obtenida que permite aplicar habilidades de ingeniería social para obtener más información relevante.
D. **Mejora planificación de pruebas de intrusión:** con la información obtenida, se logra una comprensión más clara del objetivo, permitiendo una planificación más efectiva para incrementar las probabilidades de éxito en las pruebas de penetración o en la toma de control de acceso del objetivo.

4.3. Aplicación de Information Gathering

La aplicación de las técnicas de recolección de información o Information Gathering, pueden ser desarrolladas de manera planificada dentro de un proceso de Ethical Hacking, siguiendo los principios éticos, profesionales y legales.

"La base para cualquier prueba de penetración exitosa es un reconocimiento sólido. Si no realiza una recopilación de información adecuada, tendrá que agitarse al azar, atacando máquinas que no son vulnerables y omitiendo otras que sí lo son" (Offensive Security, 2021).

Para la aplicación de las técnicas de recolección de información se pueden utilizar diversas herramientas técnicas, las cuales se listan a continuación:

- ✓ FOCA
- ✓ Goofile
- ✓ Maltego
- ✓ Nessus Essentials
- ✓ Nmap / ZenMap
- ✓ NSLookup
- ✓ NTop
- ✓ OpenVas
- ✓ SET Toolkit
- ✓ SPARTA
- ✓ Wireshark
- ✓ Whois Lookup

“Kali Tools / Tool Documentation”

Conozca más herramientas y sus descripciones en kali.org Kali Linux Tools Listing.

Enlace de la página web

5. Análisis de vulnerabilidades técnicas

El análisis o escaneo de vulnerabilidades consiste en el descubrimiento de debilidades o vulnerabilidades de seguridad, en los elementos de una red. El mismo, puede ser realizado con diversas herramientas existentes, y es un proceso que es necesario realizar previamente a una prueba de intrusión, o bien puede ser realizado como parte de un proceso de endurecimiento o “hardening”.

Análisis de vulnerabilidades técnicas. Ver documento anexo **Análisis de vulnerabilidades técnicas**, ubicado en la carpeta de anexos, con la finalidad de ampliar los conocimientos en el tema.

6. Gestión de incidentes de seguridad digital

La gestión de incidentes de seguridad digital consiste en un proceso continuo con una serie de actividades para el manejo adecuado de incidentes de seguridad digital; dichas actividades se enfocan en identificar y responder ante vulnerabilidades, eventos e incidentes de seguridad digital que se presenten en el desarrollo de operaciones tecnológicas y actividades de los usuarios en el uso de los sistemas de información.

Este proceso abarca preparación, detección, análisis y recuperación, garantizando la confidencialidad, integridad y disponibilidad de los servicios tecnológicos en situaciones de seguridad.

Se invita a conocer los conceptos y elementos clave de la gestión de incidentes de seguridad, a continuación.

A. **Equipo de respuesta a incidentes:** equipo con miembros debidamente capacitados y confiables que se encarga de manejar, apropiadamente, los incidentes durante su ciclo de vida. Se conocen como **equipo de respuesta a incidentes de seguridad de la información ISIRT**, del inglés Information Security Incident Response Team. Su función básica está orientada a detectar y responder frente a incidentes de seguridad de la información o seguridad digital, para proteger y recuperar los sistemas de información; aplicaciones, programas en red, servidores, entre otras.
B. **Usuarios:** son las personas, procesos de una organización u organizaciones que hacen uso de servicios tecnológicos supervisados y monitoreados por un equipo de respuestas a incidentes.
C. **Evento de seguridad digital:** suceso que indica una posible violación de la seguridad digital o falla de los controles, lo que supone un potencial incidente de seguridad digital. Los eventos de seguridad digital, detectados y tratados a tiempo, minimizan el riesgo de impacto adverso en las organizaciones.
D. **Incidente de seguridad digital:** son uno o una serie de eventos de seguridad digital relacionados e identificados, que pueden afectar los

componentes y servicios tecnológicos de una organización, impactando de manera adversa las operaciones de negocio.

E. **Reporte de incidentes de seguridad digital:** actividades de notificación de sucesos que representan posibilidad de ocurrencia de vulnerabilidades o incidentes, presentes o futuros, que pueden ser realizadas por los usuarios de los sistemas de información en una organización. Generalmente, los reportes de incidentes de seguridad los realizan los usuarios a los puntos de contacto o equipos de seguridad, según como se haya estructurado en la organización.

F. **Manejo de incidentes:** actividades para informar, evaluar, responder y tratar incidentes de seguridad y aprender de ellos. El manejo de incidentes depende de la capacidad del equipo de respuestas, las herramientas de seguridad como los SIEM y los demás recursos que se tengan disponibles en la organización.

G. **Respuesta a incidentes:** acciones que se aplican para mitigar o resolver un incidente de seguridad; pueden enfocarse en **proteger** para evitar impactos adversos mayores, y en **restaurar** para recuperar elementos impactados y lograr volver a las operaciones normales de un sistema de información, incluyendo sus datos e información.

H. **Punto de contacto – PoC:** es un rol, dentro de una organización, que actúa como referente para la gestión de incidentes; desempeña actividades de comunicación entre los usuarios de los sistemas de información y los equipos de respuesta a incidentes, para las gestiones adecuadas de los mismos. El PoC puede ser parte de un equipo de respuestas a incidentes (ISIRT).

I. **Investigación de seguridad digital:** desarrollo de actividades de revisión, examen e indagación para el análisis e interpretación de uno o una serie de sucesos para ayudar a comprender un incidente de seguridad digital.

6.1. Estándares y "frameworks"

Los estándares y marcos de referencia ("frameworks") de gestión de incidentes de seguridad son las referencias base para adoptar, estructurar, modelar y documentar un proceso adecuado de gestión de incidentes de seguridad digital.

Estándares y "frameworks" para la gestión de incidentes de seguridad digital. Ver documento anexo **Estándares y "frameworks" para la gestión de incidentes de seguridad digital**, ubicado en la carpeta de anexos, con la finalidad de ampliar los conocimientos en el tema.

6.2. Características de la gestión de incidentes de seguridad

La gestión de incidentes de seguridad digital tiene particularidades o características que la convierten en un aspecto clave dentro de la ciberseguridad.

La preparación, monitoreo de las funcionalidades tecnológicas y controles de ciberseguridad, comunicación, análisis y respuesta ante incidentes, hacen que la gestión de incidentes de seguridad digital sea necesaria de incorporar en los modelos de seguridad de la información, sistemas de gestión de la seguridad de la información y en la aplicación y operación de la ciberseguridad.

Las siguientes características de la gestión de incidentes de seguridad digital, aportan gran valor a la ciberseguridad:

A. **Preparación:** permite que la planificación de implementación, de controles de seguridad y no se enfoque únicamente, en la protección simplificada, sino también en la prevención de incidentes de seguridad, de tal forma que se incorporen soluciones de seguridad o configuraciones especiales que permitan el monitoreo y control de la ciberseguridad.
B. **Monitoreo:** aporta una visión constante de los eventos en los dispositivos, servicios y demás elementos de la red, logrando una monitorización constante de los sucesos anómalos, favoreciendo una mejor respuesta y control de los incidentes de ciberseguridad.
C. **Comunicación:** incorpora la comunicación como estrategia para las actividades de alertas y respuestas tempranas ante incidentes, de tal manera que los usuarios de los sistemas, servicios y elementos de la red puedan reportar y ser informados sobre el estado de la ciberseguridad.
D. **Análisis:** se adquiere una capacidad analítica sobre los eventos, incidentes y vulnerabilidades de ciberseguridad, que sirve para entender el comportamiento de amenazas y los riesgos generados, con lo cual los equipos dan respuesta a incidentes y pueden tomar acciones para el aislamiento y contención de amenazas, lograr la protección de los activos de información.
E. **Respuesta:** logra que los equipos den respuesta a incidentes, adquieran un lineamiento sistémico para responder ante eventos, incidentes y

vulnerabilidades de ciberseguridad y contrarrestar (contener y erradicar) las amenazas.

F. **Conocimiento:** aporta a la ciberseguridad una base de conocimiento de las lecciones aprendidas de los sucesos adversos, logrando así mejorar los conocimientos y habilidades en relación con los eventos, incidentes y vulnerabilidades para una mejor gestión de incidentes de seguridad digital.

6.3. Aplicación de la gestión de incidentes de seguridad

La gestión de incidentes de seguridad digital puede ser aplicada en varios contextos, entendiendo que la misma puede ser parte interiorizada de un área tecnológica en una organización, o bien un servicio ofrecido por una empresa dedicada a la ciberseguridad. Puede aplicarse la gestión de incidentes de seguridad digital, como los servicios propios dentro la organización o como un servicio para terceros (clientes).

La gestión de incidentes de seguridad digital puede ser aplicada, principalmente, en algunos de los siguientes escenarios, ya sea como servicios propios o para terceros:

A. **Departamentos de sistemas:** áreas de tecnología responsables de la ciberseguridad de los sistemas, servicios y elementos de la red.
B. **"Data Center":** centros de datos conformados por equipos de infraestructura tecnológica y responsables de la ciberseguridad de los sistemas, servicios y elementos de la red.
C. **NOC, Network Operation Center:** centros de operación de redes de datos encargados de la ciberseguridad de los sistemas, servicios y elementos de la red.

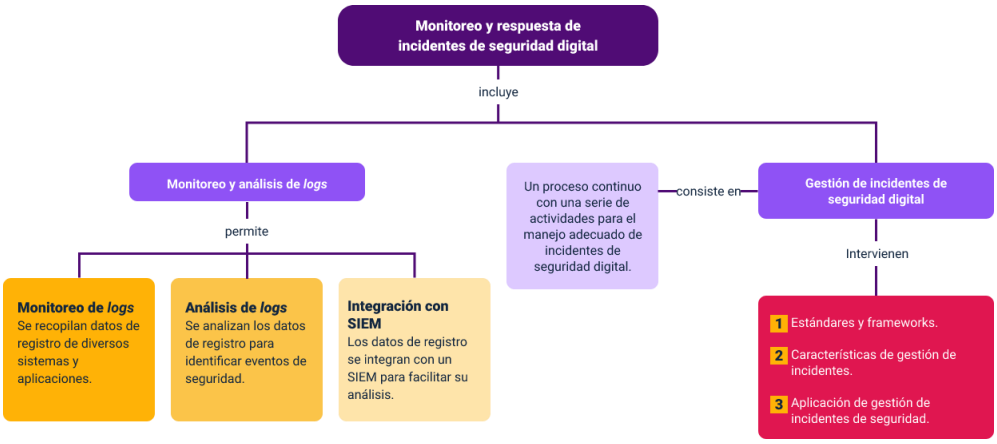
D. **SOC, Security Operation Center:** centros de operación de seguridad que son responsables de la ciberseguridad de los sistemas, servicios y elementos de la red.

¡Muy importante!

La aplicación de las buenas prácticas de la gestión de incidentes de seguridad digital debe estar enfocada en detectar, informar, evaluar, responder, tratar, aprender y concientizar sobre los eventos, incidentes y vulnerabilidades de seguridad digital, para tener mayor comprensión sobre las amenazas y riesgos de ciberseguridad de las partes interesadas de una organización.

Síntesis

En el proceso de Monitoreo y respuesta de incidentes de seguridad digital, se inició con la exploración de registros en "Monitoreo y Análisis de Logs". Estos datos se integran en "Fundamentos de SIEM", mientras el "Security Operation Center (SOC)" establece objetivos claros y alcance definido. Se aplicaron "Técnicas de Recopilación de Información" para análisis detallado y, a través del "Análisis de Vulnerabilidades Técnicas", se identifican debilidades potenciales. Finalmente, la "Gestión de Incidentes de Seguridad Digital", respaldada por estándares y “frameworks”, gestionan los incidentes en tiempo real para garantizar una seguridad digital integral. A continuación, se presenta un mapa conceptual que resume la información de este proceso.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Monitoreo y análisis de "logs"	Alonso, M. (2016). *Gestión de logs. [Trabajo fin de máster, Universidad Internacional de La Rioja, Logroño*]. Repositorio Institucional UNIR.	Trabajo de grado para máster	https://reunir.unir.net/bitstream/handle/123456789/3618/ALONSO-ALEGRE%20DIEZ%2C%20MARIA%20BEGO%C3%91A.pdf?sequence=1&isAllowed=y
2. Fundamentos de SIEM	Avella, J., Calderón, L., y Mateus, C. (2015). *Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM*.	Guía metodológica. Documento en línea	https://repository.ucatolica.edu.co/server/api/core/bitstreams/f233d3b4-04cb-4ba5-a9cd-26412e0f2b87/content
2. Fundamentos de SIEM	AT&T Cybersecurity. (2021). *Deployment guide*.	Guía de implementación. Documento en línea	https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf
2. Fundamentos de SIEM	López, J. (2017). *Análisis y gestión de vulnerabilidades de sistemas informáticos con software libre (AGVISL).*	Documento en línea	http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72567/6/jlopezfernanTFG0118memoria.pdf
4. Técnicas de recopilación de información	García, J. (2015). *Hacking ético: cacería de vulnerabilidades*.	Documento en línea	https://owasp.org/www-pdf-archive/Hacking_Etico_Cacer%C3%ADa_de_Vulnerabilidades.pdf
4. Técnicas de recopilación de información	Offensive Security. (2021). *Recopilación de información en Metasploit*.	Documento en línea	https://www.offensive-security.com/metasploit-unleashed/information-gathering/

4. Técnicas de recopilación de información	Kali Tools. (2021). *Listado de herramientas de Kali Linux. Kali.*	Web	https://www.kali.org/tools/
5. Análisis de vulnerabilidades técnicas	Owasp Foundation. (2017). *Los diez riesgos más críticos en aplicaciones web*. Owasp.	Otro	https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
5. Análisis de vulnerabilidades técnicas	Scarfone, K., Souppaya, M., Cody, A., y Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment*.	Documento en línea	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
5. Análisis de vulnerabilidades técnicas	Ministerio de Tecnologías de la Información y Comunicaciones. (2016). *Guía metodológica de pruebas de efectividad.*	Documento en línea	https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf
5. Análisis de vulnerabilidades técnicas	Owasp Foundation. (2021). *Vulnerability scanning tools. Owasp*.	Página Web	https://owasp.org/www-community/Vulnerability_Scanning_Tools

Glosario

Activo de información: elemento que tiene valor para un individuo, organizaciones o gobiernos. Es un componente el cual almacena, trata, muestra o transporta datos e información, pudiendo ser físicos o digitales, por ejemplo, una base de datos, "software", sistemas de información, papel, discos duros, personas, procesos, etc.

Amenaza: se define como toda aquella acción o serie de acciones que aprovechan las vulnerabilidades para romper la seguridad de los sistemas.

Equipo de respuesta a incidentes: equipo de una organización con miembros debidamente capacitados y confiables que se encarga de darle el manejo apropiado a los incidentes durante su ciclo de vida. Los equipos de respuesta a incidentes se conocen como equipo de respuesta a incidentes de seguridad de la información ISIRT, del inglés Information Security Incident Response Team. Su función básica está orientada a detectar y responder frente a incidentes de seguridad de la información o seguridad digital, con el propósito de proteger y recuperar los sistemas de información; aplicaciones, programas en red, servidores, etc.

Escáner de vulnerabilidades: herramienta "software" que busca y analiza las debilidades o fallas de los elementos o dispositivos que componen una red.

Evento de seguridad digital: suceso que indica una posible violación de la seguridad digital o falla de los controles, lo cual suponen un potencial incidente de seguridad digital.

Incidente de seguridad digital: uno o una serie de eventos de seguridad digital relacionados e identificados que pueden afectar los componentes y servicios tecnológicos de una organización, impactando de manera adversa con las operaciones de negocio.

Investigación de seguridad digital: desarrollo de actividades de revisión, examen e indagación para el análisis e interpretación de uno o serie de sucesos para ayudar a comprender un incidente de seguridad digital.

“Log”: en español registro, consiste en un archivo plano de texto en el cual se encuentran cronológicamente los eventos, sucesos y cambios que han ocurrido en un sistema informático, tales como aplicaciones, servidores, servicios de red, etc.

Usuarios: personas, procesos de una organización u organizaciones que hacen uso de servicios tecnológicos que son supervisados y monitoreados por un equipo de respuesta a incidentes.

Vulnerabilidad: en informática, se define como una debilidad o fallo de seguridad que se presenta en un sistema de información, que puede estar compuesto por “software”, “hardware” y otros componentes y servicios tecnológicos, generando riesgos de seguridad de la información.

Referencias bibliográficas

Avella, J., Calderón, L., y Mateus, C. (2015). *Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM*. https://repository.ucatolica.edu.co/bitstream/10983/2847/1/GU%C3%8DA%20METODOL%C3%93GICA%20PARA%20LA%20GESTI%C3%93N%20CENTRALIZADA%20DE%20REGISTROS%20DE%20SEGURIDAD%20A%20TRAV%C3%89S%20DE%20UN%20SIEM.pdf

Offensive Security. (2021). *Recopilación de información en Metasploit*. https://www.offensive-security.com/metasploit-unleashed/information-gathering/

Oracle (2021). *¿Qué es un SOC? Oracle*. https://www.oracle.com/es/database/security/que-es-un-soc.html.

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal Gutiérrez	Responsable del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Joaquín Patiño Cerón	Experto temático	Regional Cauca - Centro de Teleinformática y Producción Industrial
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Regional Tolima - Centro agropecuario La Granja
Ana Catalina Córdoba Sus	Revisora Metodológica y Pedagógica	Regional Distrito Capital - Centro para la Industria de la Comunicación Gráfica
Rafael Neftalí Lizcano Reyes	Asesor pedagógico	Regional Santander - Centro Industrial del Diseño y la Manufactura
José Gabriel Ortiz Abella	Corrector de estilo	Regional Distrito Capital - Centro para la Industria de la Comunicación Gráfica
Gloria Lida Alzate Suarez	Adecuador Instruccional	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Alix Cecilia Chinchilla Rueda	Metodología para la formación virtual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Yuly Andrea Rey Quiñonez	Diseñador web	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información

Comentado [AF3]: Cuando actualicen los créditos hacerlo acá.

Nombre	Cargo	Regional y Centro de Formación
Diego Fernando Velasco Güiza	Desarrollador Fullstack	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Nombre_responsable	Animador y Producción audiovisual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Leyson Fabián Castaño Pérez	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información