**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| **PROGRAMA DE FORMACIÓN** | Tecnólogo en implementación y operación de la ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | **220501111 -** Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | **RESULTADOS DE APRENDIZAJE** | **220501111-02.** Realizar el monitoreo de la seguridad digital de acuerdo con los indicadores y métricas establecidos. |

|  |  |
| --- | --- |
| **NÚMERO DEL COMPONENTE FORMATIVO** | 08 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | 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. |
| **PALABRAS CLAVE** | Amenazas, controles, *logs*, SIEM, vulnerabilidades |

|  |  |
| --- | --- |
| **ÁREA OCUPACIONAL** | Servicios |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Monitoreo y análisis de *logs***

1.1 Tipos de *logs*

1.2 Características del monitoreo y análisis de *logs*

**2. Fundamentos de SIEM**

**3. Fundamentos de SOC *- Security Operation Center***

3.1 Objetivos de los SOC

3.2 Alcance

**4. Técnicas de recopilación de información**

4.1 Tipos de *Information Gathering*

4.2 Características

4.3 Aplicación de *Information Gathering*

**5. Análisis de vulnerabilidades técnicas**

**6. Gestión de incidentes de seguridad digital**

6.1 Estándares y *Frameworks*

6.2 Características de la gestión de incidentes de seguridad

6.3 Aplicación de la gestión de incidentes de seguridad

1. **DESARROLLO DE CONTENIDOS**

**Introducción**

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

OKEst\_CF08\_0\_Introduccion\_formato\_4\_video\_DI\_2023

**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:

OKEst\_CF08\_1\_Monitoreo\_y\_Analisis\_de\_Logs\_formato\_2\_infografia\_interactiva\_puntocaliente\_DI\_2023

**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:

OKEst\_CF08\_1.1\_TiposDeLogs\_formato\_2\_infografia\_interactiva\_puntocaliente\_DI\_2023

**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:

OKEst\_CF08\_1.2\_CaracteristicasDelMonitoreoYAnalisis\_formato\_9\_acordeon\_DI\_2023

**2. Fundamentos de SIEM**

UnSIEM (*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).

Entérese, en profundidad, de los fundamentos en SIEM, requeridos para avanzar en este componente formativo, estudiando conscientemente el **Anexo\_1\_FundamentosDeSIEM**.

**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).

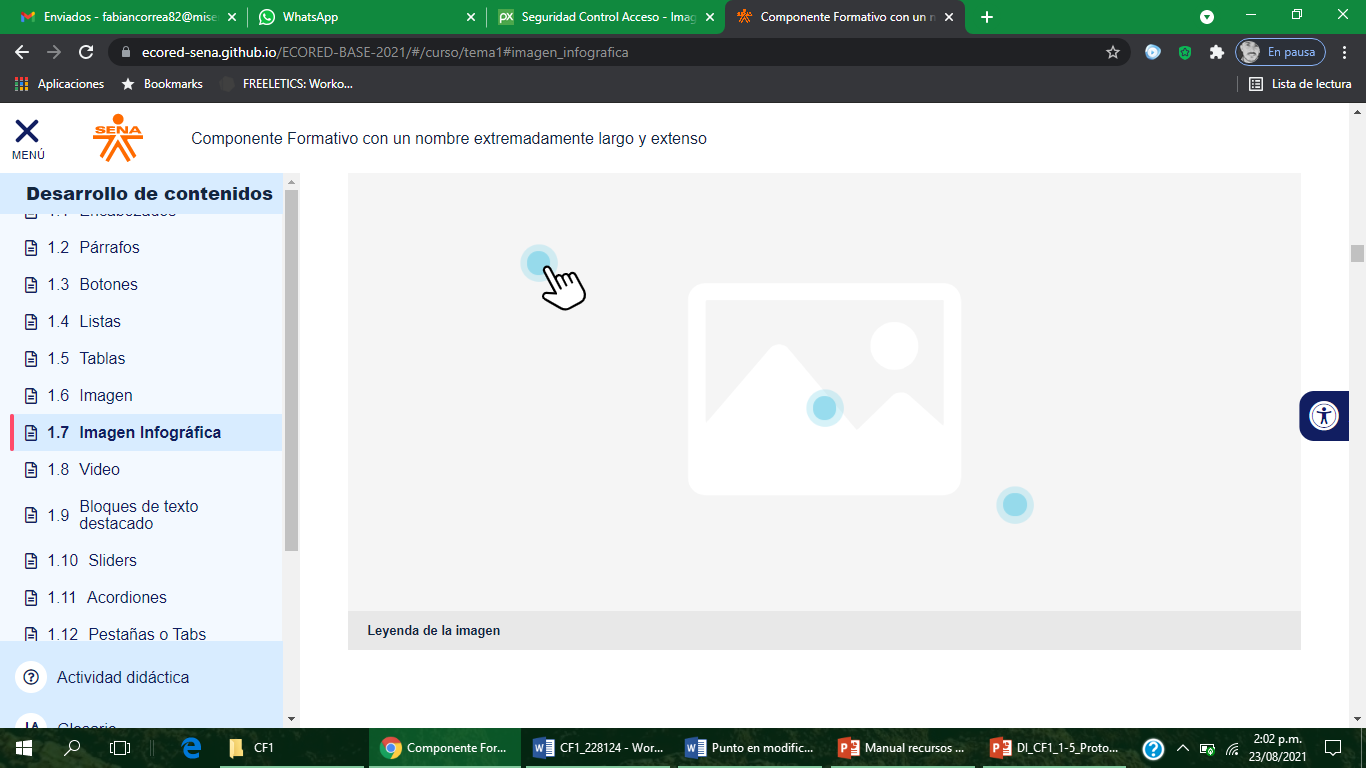
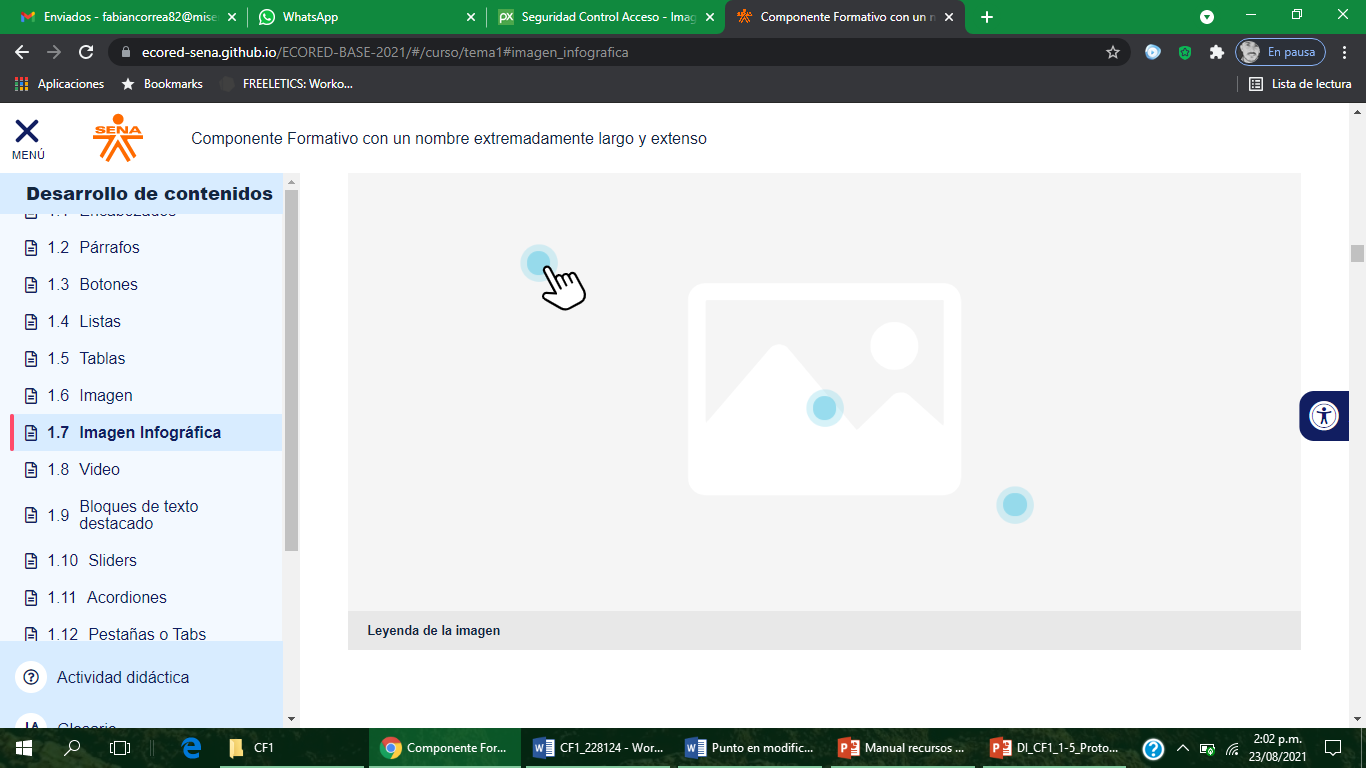
A continuación, se detallan algunos conceptos y elementos generales de las etapas de operación de un SOC, que favorecen un correcto funcionamiento:

OKEst\_CF08\_3\_Fundamentos\_de\_SOC\_formato\_12\_rutas\_DI\_2023

**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!**

**¡Importante!**

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:

OKEst\_CF08\_3.2\_Alcance\_de\_un\_SOC\_formato\_10\_tabs\_verticales(pasos)\_DI\_2023

**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 informaciónse 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 arma 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.

OKEst\_CF08\_4\_TecnicasRecopilacionInformacion\_formato\_9\_acordeon\_DI\_2023

**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 infografía:

OKEst\_CF08\_4.1\_TiposDeInformationGathering\_formato\_2\_infografia\_interactiva\_modales\_DI\_2023

**4.2 Características**

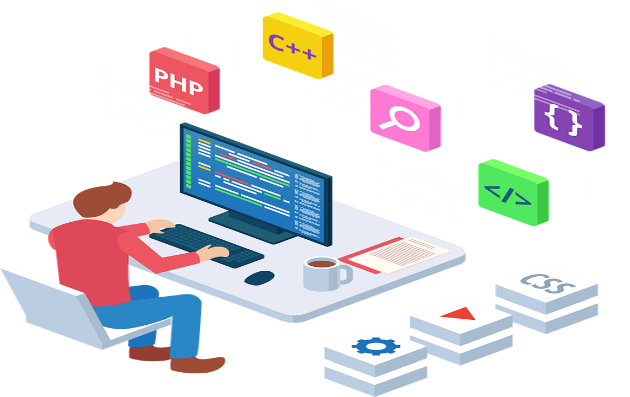
Las características de las técnicas de recolección son muy particulares ya que, gracias a ellas justamente, es que se facilita violentar los sistemas de una organización o de las personas y la sociedad.

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

OKEst\_CF08\_4.2\_Característicasde\_las\_técnicas\_de\_recopilación\_de información\_formato\_13\_tarjetas\_DI\_2023

**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*

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

**https://tools.kali.org/tools-listing**

**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.*

Profundice en los elementos del análisis de vulnerabilidades técnicas, necesarios para el estudio de este componente formativo. Visite el **Anexo\_2\_AnalisisVulnerabilidadesTecnicas**. Procure llevar registro en su libreta personal de apuntes. ¡**Adelante**!

**6. Gestión de incidentes de seguridad digital**

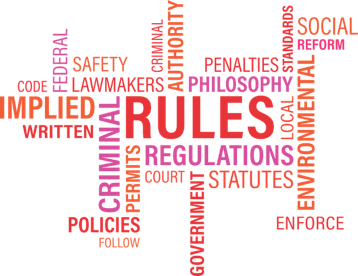
La gestión de incidentes de seguridad digital consiste en un proceso continuo con una serie de actividades para el manejo adecuado de incidentes de seguridad digital; dichas actividades se enfocan en identificar y responder ante vulnerabilidades, eventos e incidentes de seguridad digital que se presenten 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, visualizando el recurso que se presenta a continuación.

OKEst\_CF08\_6\_GestionIncidentesSeguridadDigital\_formato\_6\_slide\_diapositivas\_simple\_DI\_2023

**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.

Para profundizar en el conocimiento, asimilación e importancia de tales estándares, para la gestión de incidentes de seguridad, haga atento estudio del **Anexo\_3\_EstandaresYFrameworks**.

**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:

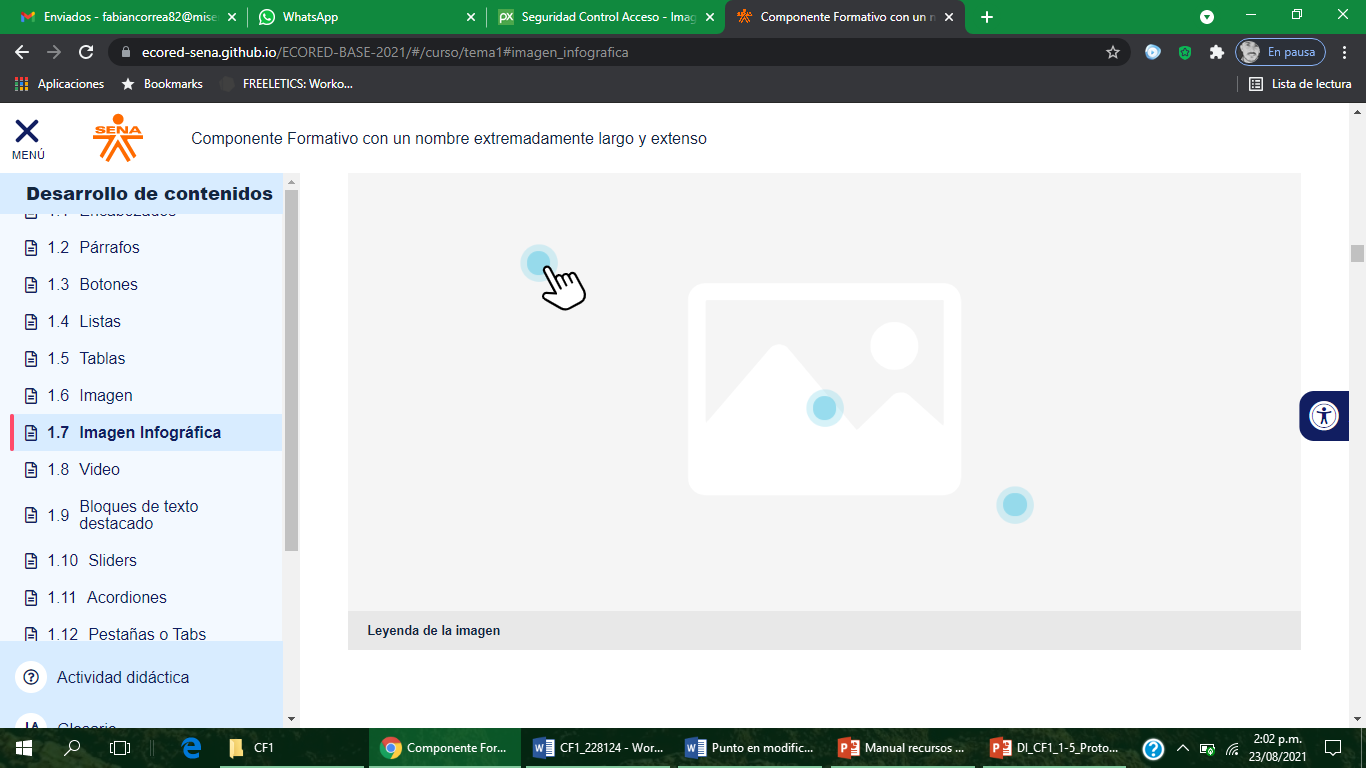
OKEst\_CF08\_6.2\_CaracteristicasGesionIncidentes\_formato\_6\_slide\_diapositivas\_titulos\_DI\_2023

**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:

OKEst\_CF08\_6.3\_AplicacionGetionIncidentes\_formato\_1\_infografia\_estatica\_DI\_2023



**¡Muy importante!**

1. **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.

Diagrama

Descripción generada automáticamente

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| Nombre de la Actividad | Conceptualizando la Seguridad Digital: monitoreo y respuesta de incidentes. |
| Objetivo de la actividad | Establecer un marco conceptual para comprender y aplicar los fundamentos del monitoreo y la respuesta de incidentes en seguridad digital. |
| Tipo de actividad sugerida | **Interfaz de usuario gráfica  Descripción generada automáticamente** |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexos/ CF08\_Formato\_5\_actividad\_didactica\_relacionar\_terminos\_DI\_2023 |

1. **MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, artículo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| **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. <https://reunir.unir.net/bitstream/handle/123456789/3618/ALONSO-ALEGRE%20DIEZ%2C%20MARIA%20BEGO%C3%91A.pdf?sequence=1&isAllowed=y> | 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.* <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> | Guía metodológica. Documento en línea | <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> |
| **2. Fundamentos de SIEM** | AT&T Cybersecurity. (2021). *Deployment guide.* <https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf> | 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).* <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72567/6/jlopezfernanTFG0118memoria.pdf> | 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.* <https://owasp.org/www-pdf-archive/Hacking_Etico_Cacer%C3%ADa_de_Vulnerabilidades.pdf> | 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.* <https://www.offensive-security.com/metasploit-unleashed/information-gathering/> | 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. <https://tools.kali.org/tools-listing> | Web | <https://tools.kali.org/tools-listing> |
| **5. Análisis de vulnerabilidades técnicas** | Owasp Foundation. (2017). *Los diez riesgos más críticos en aplicaciones web.* Owasp. <https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf> | 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.* <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf> | 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.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf> | 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.<https://owasp.org/www-community/Vulnerability_Scanning_Tools> | Página Web | <https://owasp.org/www-community/Vulnerability_Scanning_Tools> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| **TÉRMINO** | **SIGNIFICADO** |
| **Amenaza** | toda aquella acción o serie de acciones que aprovechan las vulnerabilidades para romper la seguridad de los sistemas. |
| **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. |
| **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. |
| **Escáner de vulnerabilidades** | herramienta *software* que busca y analiza las debilidades o fallas de los elementos o dispositivos que componen una red. |
| **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. |
| **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. |

1. **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>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| **Autor (es)** | Joaquín Patiño Cerón | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial. | Septiembre 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro agropecuario La Granja, | Septiembre 2021 |
| Ana Catalina Córdoba Sus | Revisora Metodológica y Pedagógica | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Septiembre 2021 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital - Centro para la Industria de la Comunicación Gráfica. | Octubre del 2021. |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** | Gloria Lida Alzate Suarez | Adecuador Instruccional | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
| Alix Cecilia Chinchilla Rueda | Metodología para la formación virtual | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de acuerdo con la directriz de Dirección General. |
| Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Centro de gestión de mercados, Logística y Tecnologías de la información- Regional Distrito Capital | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |