



PROCESO DIRECCIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUÍA DE APRENDIZAJE

- Denominación del Programa de Formación: Tecnólogo en Gestión de Redes de Datos
- Código del Programa de Formación: 228183
- Nombre del Proyecto: Implementación y Gestión de una Red Convergente Segura basada en Estándares Internacionales
- Fase: Evaluación
- Actividad del proyecto: Realizar la validación del plan de seguridad de la red de datos, mediante el uso de herramientas de software que permitan determinar los riesgos y vulnerabilidades informáticas
- Competencia: Administrar hardware y software de seguridad en la red a partir de normas internacionales
- Resultados de Aprendizaje Alcanzar:
 - ✓ Verificar eventos en la infraestructura de red, mediante herramientas y técnicas de análisis de datos que permitan determinar incidentes de seguridad.
- Duración de la Guía: 110 horas

2. PRESENTACIÓN



Figura 1 <https://acortar.link/RjPel4>

En la última década con la evolución del Internet y los dispositivos con los cuales nos podemos conectar, tenemos la posibilidad de realizar operaciones en línea, las cuales anteriormente debían realizarse de manera presencial. Este es un avance significativo, pero implica que nuestros datos e información están expuestos en la red. De igual manera, a nivel corporativo, los niveles de información que se manejan son muy altos, y los modelos de negocio y los desarrollos tecnológicos pueden sufrir ataques de todo tipo, desde el robo de información, hasta la denegación de servicios básicos de la organización. Los intrusos pueden obtener acceso a la red a través de vulnerabilidades del software, ataques al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona.



Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

El aprendiz a través del desarrollo de esta actividad adquiere la capacidad de configurar software y hardware aplicando políticas de seguridad que le permitirá monitorear la red de datos que administra y aplicar técnicas básicas de informática forense para determinar el nivel de seguridad con que cuenta la información.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

Identificar la importancia de la elaboración de documentación y monitoreo de la seguridad en una red de datos.

De manera individual, los aprendices reflexionarán respecto a las dos preguntas que se presentan a continuación:

- ¿Qué importancia tiene el documentar los procedimientos de una actividad?
- ¿Qué beneficio trae el monitoreo constante de los eventos en una red?
- ¿Cómo puede la empresa proteger sus activos de red?
- ¿Mencione 2 buenas practicas que deben tener empresas referte a la protección de activos?

Los aprendices se dividirán en grupos de cuatro (4) personas y realizarán la reflexión de cuál es el impacto que tiene en las organizaciones no contar con una adecuada política de seguridad.

Duración de la actividad: 1 hora

Modalidad de trabajo: Individual y grupal

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Computadores, Internet, Video Beam.

3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.)

Identificar los conceptos básicos del monitoreo de la red que permitan llevar a cabo una gestión eficiente de los recursos.

De acuerdo a su experiencia de aprendizaje cada aprendiz debe responder los interrogantes planteados, ingresando al siguiente formulario:



<https://forms.gle/dM2MQeJwGkAcY81R8>

Después en sesión (o formación) el instructor socializará las conclusiones de los interrogantes planteados en el formulario

Duración de la actividad: 1 hora

Modalidad de trabajo: Individual

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Computadores, Internet, Video Beam

3.3 Actividades de apropiación del conocimiento (Conceptualización y Teorización).

3.3.1. Reconocer los conceptos fundamentales del análisis forense digital para definir la metodología a seguir en una investigación.



Tomado de: [Metodología de Análisis Forense | Ninjas de la Web](#)

Los aprendices conformarán equipos de trabajo de máximo cuatro (4) personas, en donde se revisarán algunos conceptos utilizados en el análisis forense digital.



En una actividad de exposición cada grupo presentará en plenaria el tema asignado por el instructor. Para ello desarrollará una presentación en la plantilla SENA, en donde incluirá al final una actividad de pregunta-respuesta para el auditorio. Durante y después de cada una de las presentaciones, el instructor profundizará en los temas en cuestión, a la vez que servirá de apoyo en la aclaración de dudas que los aprendices expositores no puedan resolver.

- Etapas de un análisis forense.
- Cadena de custodia de las evidencias digitales.
- Sistemas de ficheros y recuperación de archivos borrados.
- Los metadatos de los archivos.
- Tipos de evidencias y orden de volatilidad.
- Adquisición de las evidencias en caliente y en frío.
- Imagen forense versus clonado forense, adquisición física y lógica.
- Crear imagen forense con FTK Imager.
- Crear un caso forense con autopsy

En sesión el instructor intervendrá para solucionar y aclarar las dudas que se tengan frente al tema.

Duración de la actividad: 30 Horas

Modalidad de trabajo: Grupal

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Equipos de Cómputo, Software ofimático

Evidencia: presentaciones power point

3.3.2. Recolectar datos de una muestra forense aplicando técnicas de peritaje





Tomado de <https://acortar.link/BiGn1P>

Los aprendices deberán trabajar de forma individual la muestra forense entregada por el instructor aplicando técnicas de investigación acorde a lineamientos y procedimientos establecidos, durante el desarrollo de la sesión el instructor supervisa y orienta el desarrollo de la actividad.

Finalmente, el aprendiz deberá entregar un informe forense donde detalle cada uno de los hallazgos encontrados soportando evidencias del proceso realizado

Duración de la actividad: 10 Horas

Modalidad de trabajo: Grupal

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Equipos de Cómputo, Software ofimático

Evidencia: presentaciones power point

3.3.3. Determinar los requerimientos mínimos para la implementación de técnicas de monitoreo sobre una red de datos.



Tomado de <https://acortar.link/tvg3Oy>

Los aprendices conformarán equipos de trabajo de máximo cuatro (4) personas, en donde se revisarán algunas técnicas utilizadas para efectuar el monitoreo de una red y la documentación de la seguridad de la red de datos de la organización.

En una actividad de exposición cada grupo presentará en plenaria el tema asignado por el instructor. Para ello desarrollará una presentación en la plantilla SENA, en donde incluirá al final una actividad de pregunta-respuesta para el auditorio. Como apoyo a la presentación, los aprendices deberán preparar una práctica en la cual implementen una solución utilizando el tema asignado. Durante y después de cada una de las



presentaciones, el instructor profundizará en los temas en cuestión, a la vez que servirá de apoyo en la aclaración de dudas que los aprendices expositores no puedan resolver.

- Monitoreo de registros con el Visor de Eventos.
- Monitoreo y análisis de eventos con Servidor Syslog.
- Monitoreo de puertos e IP con Nmap.
- Monitoreo de tráfico con Wireshark.
- Monitoreo de redes inalámbricas con Aircrack.
- Monitoreo de vulnerabilidades Nessus.
- Monitoreo de vulnerabilidades web for pent test.
- Explotación con Metasploit tipo bind y reverse.
- Ataque de fuerza bruta y diccionarios con hydra

Con la guía del instructor, el aprendiz realizará de forma individual la implementación sobre una máquina virtual de cada una de las técnicas presentadas por los expositores.

En sesión el instructor intervendrá para solucionar y aclarar las dudas que se tengan frente al tema.

Duración de la actividad: 40 Horas

Modalidad de trabajo: Grupal

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Equipos de Cómputo, Software ofimático

Evidencia: formato servicio técnico

3.3.4. Identificar técnicas de ingeniería aplicas por ciberdelincuentes según mapa conceptual



Tomado de: <https://acortar.link/qnsQlr>



Una de las técnicas mas comunes empeladas en la auditoria de la norma ISO 27000 consiste en generar una cultura de control y prevención de incidentes de seguridad que puedan afectar los activos de información, mediante engaño a personas con el fin de obtener datos y credenciales que permitan la suplantación de identidad en un sistema de información.

Los aprendice realizaran lectura previa del material de apoyo disponible, posteriormente el instructor realiza la exposición de las diferentes técnicas de ingeniería social y citara algunos ejemplos. Al finalizar el aprendiz deberá resolver el taller de identificación de técnicas de ingeniería social

Duración de la actividad: 5 horas

Tipo de actividad: Grupal

Evidencia de aprendizaje: informe de tipos de ingeniería social

Ambiente Requerido: Ambiente de aprendizaje virtual

Materiales: Equipos de cómputo, internet, software ofimático

3.4 Actividades de transferencia del conocimiento.

Realizar una auditoria forense a un sistema operativo involucrado en un incidente de seguridad para detectar intentos de acceso errados o no autorizados en los datos.

Los aprendices trabajarán en parejas y realizarán el análisis del caso propuesto por el instructor, donde deben recopilar los eventos del sistema. Para la actividad será necesario contar con una máquina virtual con un sistema operativo cliente Windows, en el cual cada deberán identificar cuantos usuarios están creados, zona hora, últimos archivos accedidos, historial de navegación, impresiones y correos sin leer, posteriormente, almacenarán el archivo de eventos EVT siguiendo la guía indicada en el documento Obtención de registros, y finalmente con esta información montar un caso forense en el software autopsy que le permita acceder a la información puntual de los archivos encontrados en el paso anterior, identificando los metadatos y demás características que le permitan seguir la cadena de custodia y así encontrar hallazgos que permitan resolver el caso propuesto por el instructor.

Duración de la actividad: 23 Horas

Modalidad de trabajo: Grupal

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Equipos de Cómputo, Software ofimático

Evidencia: Reporte de hallazgos encontrados en un informe forense



4. ACTIVIDADES DE EVALUACIÓN

En mesa redonda se realizará un diálogo entre aprendiz e instructor acerca de la identificación de fortalezas y debilidades con respecto a las actividades de aprendizaje de desarrollo en la guía.

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento: Evaluaciones Digitales Evidencias de Desempeño: Asistencia y participación en clase. Evidencias de Producto: Procesador de Texto (Actividad de Reflexión). Presentación de técnicas de monitoreo. Presentación conceptos análisis forense digital. Práctica análisis de registros de eventos en Windows. Práctica análisis del historial de navegación web. Práctica recuperación de archivos borrados con software forense.	Apropia los estándares de seguridad, líneas base de configuración de dispositivos y servicios, procedimientos y políticas de seguridad para la entidad. Implementa los componentes de hardware y software, según políticas y procedimientos técnicos para la organización. Instala software de protección de redes como antimalware, antispam y de seguridad perimetral según requerimientos del plan de seguridad. Documenta los hallazgos del análisis de vulnerabilidades y amenazas, identificando el nivel de impacto sobre los activos críticos para la organización según las metodologías vigentes.	Técnica: Formulación de preguntas Instrumento: Cuestionario • Listas de chequeo. • Rúbrica. • Cuestionario. Técnica: Observación sistémica. Lluvia de ideas. Técnicas: • Exposición. • Debate. • Demostraciones. Técnica: Infografía Instrumento: lista de chequeo

5. GLOSARIO DE TÉRMINOS



- **Adware:** Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.
- **Amenaza:** Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).
- **Amenazas polimorfas:** Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.
- **Antispam:** Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.
- **Antivirus:** Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- **•Aplicaciones engañosas:** Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.
- **•Ataques multi-etapas:** Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.
- **Ataques Web:** Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
- **Blacklisting o Lista Negra:** La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.
- **Bot:** Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (bot net).
- **Botnet:** Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.



- **Caballo de Troya:** Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.
- **Canal de control y comando:** Un canal de mando y control es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.
- **Carga destructiva:** Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.
- **Crimeware:** Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.
- **Ciberdelito:** El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.
- **Definiciones de virus:** Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.
- **Descarga inadvertida:** Una descarga inadvertida es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa.
- **Encriptación:** La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.
- **Exploits o Programas intrusos:** Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.
- **Firewall:** Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- **Firma antivirus:** Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los



virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

- Greylisting o Lista Gris: La lista gris es un método de defensa para proteger a los usuarios de correo electrónico contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un remitente que no es reconocido por el agente de transferencia de correos. Si el correo es legítimo, el servidor de origen tratará de nuevo y se aceptará el correo electrónico. Si el correo es de un remitente de spam, probablemente no se reintentará su envío y por lo tanto, no logrará pasar el agente de transferencia de correos.
- Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.
- Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.
- Lista blanca o Whitelisting: La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.
- Keystroke Logger o Programa de captura de teclado (Keylogger): Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.
- Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.
- Negación de servicio (DoS): La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.
- Pharming: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer pharming cambiando el archivo de los equipos anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS.



- Phishing: A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- Protección heurística (Heuristics-Based Protection): Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica. Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles
- Rootkits: Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, interceptación de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.
- Seguridad basada en la reputación: La seguridad basada en la reputación es una estrategia de identificación de amenazas que clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son probablemente malignas o benignas. Estos atributos pueden incluir diversos aspectos como la edad de los archivos, la fuente de descarga de los archivos y la prevalencia de firmas y archivos digitales. Luego, se combinan los atributos para determinar la reputación de seguridad de un archivo. Las calificaciones de reputación son utilizadas después por los usuarios informáticos para determinar mejor lo que es seguro y permitirlo en sus sistemas. La seguridad basada en la reputación debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- Sistema de detección de intrusos: Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.



- Sistema de prevención de intrusos: Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- Software de seguridad fraudulento (rogue): Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.
- Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing
- Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.
- Toolkit: Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.
- Variantes: Las variantes son nuevas cepas de malware que piden prestado códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.
- Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa. Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.
- Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas.



6. REFERENTES BIBLIOGRÁFICOS:

<http://biblioteca.sena.edu.co/paginas/bases.html> ingresar con el número de documento
Libros Biblioteca SENA.

- Lázaro Dominguez, F. (2013). Informática forense: Introducción. Bogotá: Ediciones de la U.
 - Baca Urbina, G. (2016). Introducción a la seguridad informática. Distrito Federal: Grupo Editorial Patria.
 - Cano, J. J. (2015). Computación forense: Descubriendo los rastros informáticos. México: Alfaomega.
- Bases de datos SENA.
- Gómez López, J. (2014). Administración de sistemas operativos. Recuperado de: <https://ebookcentral-proquest-com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3228996>
 - Raya Cabrera, J. (2014). Sistemas operativos en red. Recuperado de: <https://ebookcentral-proquest-com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3229158>

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Juan Pablo Agredo castaño	Instructores	CEAI	10-07-2023

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio