**PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL**

**FORMATO GUÍA DE APRENDIZAJE**

## 1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación**: Gestión de Redes de Datos.
- **Código del Programa de Formación: 228183 v2**
- **Nombre del Proyecto**: Implementación y gestión de una red convergente segura basada en estándares internacionales.
- **Fase del Proyecto**: Evaluación.
- **Actividad de 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
- **Competencia**: Administrar hardware y software de seguridad en la red a partir de normas internacionales
- **Resultados de Aprendizaje Alcanzar:**

✓ Implementar el plan de seguridad en la organización aplicando estándares y normas internacionales de seguridad vigentes.

- **Duración de la Guía**: 210 Horas

**PRESENTACIÓN**



*Figura 2.1 Dispositivos de Seguridad Firewalls Cisco*

En la última década con la evolución del Internet y los dispositivos con los cuales nos podemos conectar, tenemos la posibilidad de realizar operaciones on-line, las cuales anteriormente debían realizarse de manera presencial, este paradigma cambio, hoy se pueden realizar transacciones en línea de todo tipo (compras, pagos de servicios públicos, pago de cuentas bancarias, etc.), esto 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.

Es por esto por lo que, se debe diagnosticar el estado actual de la red, aplicando estándares internacionales, que nos permitan revisar los fallos o huecos de seguridad, no solo a nivel informático, sino locativo y de seguridad industrial. Esto con el fin de realizar un diseño correcto de políticas de seguridad que ayuden a evitar pérdida del activo más importante de una empresa, la información.

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 implementar políticas de seguridad que garanticen la disponibilidad y protección de los datos contra amenazas y vulnerabilidades.

## 2. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

### 2.1 Actividades de Reflexión inicial.

### 2.1.1 Identificar las políticas de seguridad y su importancia para las redes de la actualidad mediante la socialización de experiencias previas.

Los aprendices deberán responder las siguientes preguntas y en grupos de 4 personas realizar la reflexión de cuál es el impacto que tiene en las organizaciones una adecuada política de seguridad.

¿Cuál considera que es el principal activo de una empresa en la actualidad?
¿Cuál considera que es el impacto de las políticas de seguridad?
¿Cuál considera que es la importancia de apropiar conocimientos acerca de seguridad?

El instructor al finalizar ayudará a los aprendices aclarando las dudas sobre la importancia de las políticas de seguridad y su importancia para las redes de la actualidad, tomando como base su experiencia y las presentaciones realizadas por ellos.

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad a internet, TV

Material de apoyo: Academia Cisco NETACAD

Duración de la actividad: 1 horas.

## 2.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.

### 2.2.1 Identificar la terminología y conceptos bases necesarios para la implementación de las políticas de seguridad mediante la socialización en grupos colaborativos.

Conformando grupos de trabajo o continuando con el mismo grupo de personas de la Actividad de Reflexión, para esta actividad se deben tener algunos conocimientos básicos en los conceptos de seguridad de equipos activos de interconexión como Routers y Switches. Con base a dichos conocimientos previos respondan el siguiente cuestionario:

| **¿Reconozco esto conceptos?** | **¿Si / No?** | **Mencione por qué necesita saber esto** |
|---|---|---|
| ISO 27000 | | |
| AAA | | |
| ACL | | |
| Seguridad en Switch | | |
| VPN | | |

El instructor será el moderador de la plenaria y de las exposiciones también se encargará resolver dudas al

finalizar cada socialización.



Figura 3.1 Dominios Seguridad ISO 27002

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad a internet, TV

Material de apoyo: Academia Cisco NETACAD

Duración de la actividad: horas.

### 2.3 Actividades de apropiación del conocimiento (Conceptualización y Teorización).

#### 2.3.1 Reconocer los conceptos teórico-prácticos que hacen parte de una red segura, mediante la participación de la socialización de temas por medio de grupos de trabajo colaborativos.

Para el correcto desarrollo de estas actividades, el instructor repartirá la siguiente lista de temas relacionados con el proceso de implementación de las políticas de seguridad en un ambiente corporativo, se conformarán grupos de máximo 4 personas, y entre estos se distribuirán en partes iguales, los temas. Los aprendices deben cumplir con los objetivos teóricos que el instructor plantee y cada uno de ellos plasmarlos en una presentación. La socialización tendrá una duración aproximada de 4 horas por cada subtema, y será acompañado en todo momento del instructor para aclarar cualquier tipo de duda. Además, al finalizar cada sesión, cada grupo deberá disponer de algún método para interactuar con sus compañeros, ya sea quiz, foro o mesa redonda, el cual le permita determinar si los conceptos claves de cada tema han quedado claros en cada aprendiz.

Es obligatorio que las diapositivas se realicen usando la plantilla oficial de la institución para PowerPoint. Este y otros factores acerca del buen uso de las herramientas informáticas serán establecidos y acordados

entre el instructor y los aprendices, previo al desarrollo de los siguientes temas. Se le recomienda al instructor evaluar este tipo de aspectos.

**Lista de temas**

**Seguridad en la LAN**

- STP, RSTP, BPDUguard y Portfast
- VTP y EtherChannel.
- FRRP (HSRP, GLBP, VRRP)
- DHCP Snooping, DAI, DHCP Relay.
- Port Security, Err Disable, SPAN Monitor.
- SSH, AAA, NTP y Syslog

**Seguridad en la WAN**

- Teoria VPN.
- ACL, NAT – PAT.
- Práctica VPN con IKEv1 entre Router.
- Práctica Easy VPN (Acceso Remoto).
- Configuración básica ASA.

La actividad inicia con la conformación de equipos de trabajo colaborativos de máximo 4 personas, los cuales posteriormente realizarán la consulta acerca del tema entregado a cada uno de los grupos. El instructor también se encargará de entregarle el material de apoyo necesario para que tome las bases principales de la consulta.

Una vez recopilada la información, cada grupo realizará una presentación en PowerPoint acerca de lo investigado. Esta presentación deberá realizarse en la plantilla entregada por el instructor y debe tener un buen contenido práctico (Ejemplos, Demostraciones, Gráficos, entre otros), al finalizar la presentación debe tener una serie de preguntas, las cuales permitirán interactuar con los demás compañeros.
Después de tener preparada la presentación se procederá con la socialización del tema investigado: Inicialmente se realizará rápidamente a nivel del equipo colaborativo para finalizar la preparación (10 minutos) y luego se expondrá a todo el grupo completo con el acompañamiento del instructor. La duración mínima de la exposición será de 2 horas y máxima de 5 horas. Al finalizar se realizará una Socialización de Cierre y resolución de dudas por parte del instructor.

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad internet, TV, Packet tracer, Pnetlab, VMware,

SO Windows 10 pro, SO Windows Server 2022 Standard (ISO , Lightshot.

Material de apoyo: Academia Cisco NETACAD, Pendrive, Router, Switches, AP, cables de consola, Patch Cord, cables seriales.

Evidencias de aprendizaje: Presentación de PowerPoint de Conceptos básicos y configuraciones y Servicios implementados, que deberá subirla en plataforma y el portafolio del aprendiz. Evaluación de conocimiento Teórico.

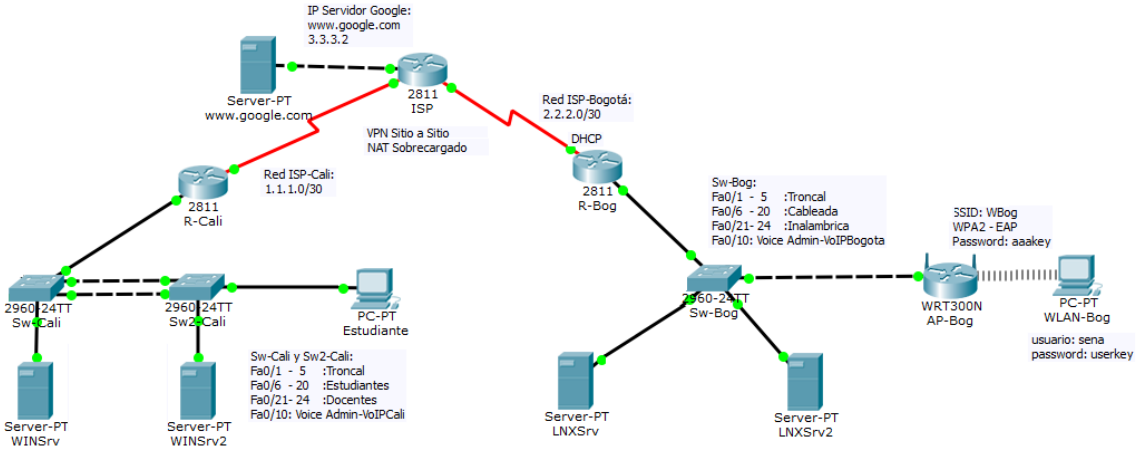
Instrumentos de evaluación: Cuestionario, simulación, Taller

Duración de la actividad: 9 Horas aprox. por Sub-Actividad promedio. (12 actividades: **120 horas**).

## 2.4 Actividades de transferencia del conocimiento.

### 2.4.1 Configurar una Topología de Red de Datos Segura, de acuerdo con los conocimientos obtenidos durante las actividades de apropiación.

De manera individual, en el simulador Packet Tracer, el aprendiz deberá ir implementando la topología presentada en la siguiente imagen, en donde una vez finalizado cada socialización de las actividades de apropiación, deberá ir configurando lo aprendido, hasta finalmente tener la topología totalmente funcional.




***Fuente:*** *Diseño propio generado en el Simulador PKT*

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad internet, TV, Pendrive, SO Windows 10 pro, SO Windows Server 2019 Standard, VMware, Lightshot

Material de apoyo: Academia Cisco NETACAD, Taller de Redes con aire acondicionado, equipado con 12 computadores, con acceso a internet, software para diseño (Packet Tracer, Pnetlab, MS Visio, MS Project,) y Libros Cisco CCNA, SO Windows 10 pro, SO Windows Server 2022 Standard (ISO), VMware,

Lightshot.

Evidencias de aprendizaje: Informe en un documento pdf, que ilustren el paso a paso de las configuraciones de la red y la implementación de todos los servicios, entregar la simulación totalmente funcional en el simulador Packet Tracer, al igual que el bloc de notas de configuración, en el lugar asignado en el portafolio del aprendiz de manera **Individual**.
Instrumento de evaluación: Lista de chequeo.
Duración de la actividad: **88 horas**

## 3. PLANTEAMIENTO DE EVIDENCIAS DE APRENDIZAJE PARA LA EVALUACIÓN EN EL PROCESO FORMATIVO.

Una vez finalizada la socialización, resueltas las dudas y realizado los Talleres prácticos, se realizará el Examen Teórico de cada módulo, el cual entregará la evaluación Final del aprendizaje obtenido en este periodo. La preparación final y presentación de los 2 exámenes prácticos y el examen final teórico tomará un estimado de unas 16 horas aproximadamente.

También se debe tener en cuenta que esta guía se fundamentará no solo en la apropiación de conocimientos nuevos, sino que también tendrá en cuenta la mejora en habilidades tales como el nivel investigativo, autoaprendizaje y participación activa en clase por parte del aprendiz. Es por lo anterior que esta guía evaluará la participación en Clase a partir de la interacción activa en el ambiente de aprendizaje, teniendo en cuenta el horario establecido para este grupo con el instructor encargado de esta guía, en la plataforma de horarios. https://appsceai.com/Saf/.

Después de haber realizado todas las actividades planteadas en esta guía, el aprendiz realizará una autoevaluación de su proceso de aprendizaje, en el cual indicará cuales considera se convirtieron en sus fortalezas, y cuáles son aún las falencias a superar. Además, tendrá el espacio para realizar recomendaciones que crea necesarias para una mejora continua de este proceso de aprendizaje, que incluye contenido y acompañamiento por parte del instructor. Esto se socializará al finalizar todo el contenido de la guía.

**Entrega de Evidencias**: Al finalizar, las actividades usted deberá de haber cumplido y entregado las siguientes Evidencias, recuerde que estas evidencias son las mismas para cada subactividad vista (si aplica):

- ✓ Presentación de PowerPoint – Grupal – Evidencia de Producto y desempeño
- ✓ Socialización – Grupal – Evidencia de Conocimiento y desempeño
- ✓ Actividad Práctica – Individual – Evidencia de Conocimiento y desempeño
- ✓ Examen Teórico – Individual – Evidencia de Conocimiento
- ✓ Exámenes Prácticos – Individual – Evidencia de desempeño
- ✓ Participación en Clase – Individual – Evidencia de desempeño.

| Fase del proyecto formativo | Actividad del proyecto formativo | Actividad de Aprendizaje | Evidencias de Aprendizaje | Criterios de Evaluación | Técnicas e Instrumentos de Evaluación |
|---|---|---|---|---|---|
| **Fase 4-Evaluación** | 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 | Conocer los fundamentos de seguridad que le permita la interpretación del plan de seguridad.<br><br>Identificar las políticas de seguridad y su importancia para las redes de la actualidad mediante la socialización de experiencias previas.<br>Reconocer los conceptos teórico-prácticos que hacen parte de una red segura, mediante la<br><br>participación de la socialización de temas por medio de grupos de trabajo colaborativos. | **Evidencias de Conocimiento:**<br><br>Identifica las políticas de seguridad y su importancia para las redes de la actualidad.<br><br>Identifica la terminología y conceptos bases necesarios para la implementación de las políticas de seguridad<br><br>**Evidencias de Conocimiento y Desempeño**<br><br>Reconoce los conceptos teórico-prácticos que hacen parte de una red segura. | ✓ Implementa las políticas, controles y procedimientos de acuerdo con el plan de seguridad.<br><br>✓ Implementa los componentes de hardware y software, según políticas y procedimientos técnicos para la organización.<br><br>✓ Asegura las comunicaciones entre sedes utilizando estrategias de conexión segura como VPN. | **Técnica de Evaluación:**<br>Formulación de Preguntas.<br><br>**Instrumento de Evaluación:**<br>Cuestionario.<br><br>**Técnica de Evaluación:**<br>Valoración de los Laboratorios.<br><br>**Instrumento de Evaluación:**<br>Lista de Chequeo |

| | | | | | |
|---|---|---|---|---|---|
| | | Identificar la terminología y conceptos bases necesarios para la implementación de las políticas de seguridad mediante la socialización en grupos colaborativos.<br><br>Reconocer los conceptos teórico-prácticos que hacen parte de una red segura, mediante la participación de la socialización de temas por medio de grupos de trabajo colaborativos.<br><br>Configurar una Topología de Red de Datos Segura, de acuerdo con los conocimientos obtenidos | **Evidencias de Producto y Desempeño**<br><br>Configura una Topología de Red de Datos Segura. | ✓ Implementa planes de recuperación de desastres y de continuidad del negocio para los servicios críticos de la organización. | **Técnica de Evaluación:**<br>Observación Directa.<br><br>**Instrumento de Evaluación:**<br>Lista de Chequeo. |

| | | | | | |
|---|---|---|---|---|---|
| | | durante las actividades de apropiación.<br><br>Reconocer los aspectos más importantes de la gestión y monitoreo de una red e implementar la a través de una herramienta centralizada de eventos. | | | |

## 4. GLOSARIO DE TÉRMINOS

**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, intercepción 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.

**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, 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 las 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 principiantes 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 prestados códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguidos del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

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.

## 5. REFERENTES BILBIOGRÁFICOS

Documentos de Principales para el Desarrollo de la guía:


- Cisco Networking Academy. CCNA SRWEv7 Módulos 1 al 16
- Cisco Networking Academy. CCNA ENSAv7 Módulos 1 al 14


Otros documentos de apoyo:


- Bibliografía SENA: Recuerde que las credenciales de ingreso son el documento identidad.
- Cisco Networking Academy. CCNA Routing and Switching Semestre 3. Recuperado el 16 de octubre de 2020 de https://www.netacad.com/es

- Tanenbaum, Andrew S.: Computer Networks, 4th Ed. Prentince-Hall, 2003.
- Dong, J. (2007). Network dictionary. Saratoga, Calif.: Javvin Technologies, Inc.
- Douglas E. Comer. Redes de computadoras e Internet. Recuperado el 16 de octubre de 2020. http://www.ebooks7-24.com.bdigital.sena.edu.co/?il=3262
- Edwards, J., & Bramante, R. (2009). Networking self-teaching guide: OSI, TCP/IP, LANs, MANs, WANs, implementation, management, and maintenance. Wiley Pub.
- Tanenbaum, A. S. (2010). Redes de computadoras. Pearson Educación.
- Guide to Cisco routers configuration. (2017). Springer Berlin Heidelberg.
- Lammle, T. (2016). CCNA routing and switching complete study guide (Second edition). Sybex, a Wiley brand.
- Pedro García, Jesús Esteban Díaz. Transmisión de datos y redes de computadores (2018). Recuperado el 16 de octubre de 2020. http://www.ebooks7-24.com.bdigital.sena.edu.co/?il=4449
- Velte, Toby J., and Anthony T. Velte. Manual de Cisco® (4a. ed.), McGraw-Hill Interamericana, 2008. ProQuest Ebook Central, Recuperado el 16 de octubre de 2020. https://ebookcentralproquestcom.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3192676 .
- Díaz, Gabriel, et al. Seguridad en las comunicaciones y en la información, UNED - Universidad Nacional de Educación a Distancia, 2004. ProQuest Ebook Central, https://ebookcentral-proquest-com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3199002.
- Bellido, Quintero, Enrique. Equipos de interconexión y servicios de red (UF1879), IC Editorial, 2014. ProQuest Ebook Central, https://ebookcentral-proquest-com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=4310541 .


## 6. CONTROL DEL DOCUMENTO

| | Nombre | Cargo | Dependencia | Fecha |
|---|---|---|---|---|
| **Autor (es)** | Gustavo A Díaz | Instructor | CEAI | 30 Enero de 2017. |
| | Gustavo Rodríguez | Instructor | CEAI | |
| | Mario G Castillo | Instructor | CEAI | |
| | Oscar Castillo y | Instructor | CEAI | |
| | Carlos Tapasco | Instructor | CEAI | |

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

| | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
|---|---|---|---|---|---|
| **Autor (es)** | Jeffry Steven Hernández Torres | Instructor | CEAI | 23/07/2018 | Actualización de formato. |
| | Gustavo Adolfo Rodríguez | Instructor | CEAI | 07 de octubre de 2021 | Cambio de formato, adecuaciones al nuevo programa formativo, glosario y bibliografía. |
| | Diego Fernando Rodríguez Mapallo | Instructor | CEAI | 10 de octubre de 2025 | Cambio de formato, adecuaciones al nuevo programa formativo, glosario y bibliografía. |
| | Sandra Patricia Galíndez | Instructora formadora | CEAI | 23/10/2025 | Viable para ejecución. |