Nombre del documento: 2. Evidencia obligación 1. Planeación FPI

Competencia: 280102129 Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica.

Resultado de aprendizaje: RAP02 - Comprobar la conectividad de la red, de acuerdo con normativa de telecomunicaciones y orden de trabajo

Programa de formación: Sistemas Teleinformáticos

1. I.E. Antonia Santos 2 fichas
   Tc. Sistemas Teleinformáticos
   ID: 2961352, 2961365

2. I.E. Santa Bárbara 2 fichas
   ID: 2961426, 2961427

Guía de aprendizaje No. 2

Enlace: **Guía de aprendizaje No. 2**

Evidencia de desempeño: El aprendiz realiza una exposición sobre conceptos relacionados con las subredes utilizando organizadores gráficos.

Evidencia de producto: Informe técnico donde se documente el cálculo de subredes, asignación de direcciones IP, configuración de routers y pantallazos con la prueba de conectividad realizada entre los dispositivos de diferentes subredes validad mediante el comando ping.

Material de apoyo: Material de apoyo

Criterios de evaluación:

- Caracteriza pruebas de fallas en la red según requerimientos técnicos.
- Efectúa pruebas de conectividad de hardware y/o software, operación de servicios y protocolos de infraestructura, disponibilidad, rendimiento y calidad, de acuerdo con normativa de telecomunicaciones, orden de trabajo, aplicando normas de SST y ambientales.
- Valida el estado de la red de acuerdo con la conectividad, el inventario tecnológico y su disponibilidad técnica según normativa.

Instrumentos de evaluación:

1. Lista de chequeo desempeño
2. Lista de chequeo producto

Guía de aprendizaje No. 3

Programa de formación: Sistemas Teleinformáticos

I.E. JAG 2 fichas
Tc. Sistemas Teleinformáticos
ID: 2961287, 2961273

Competencia: 280102129 Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica.

Resultado de aprendizaje: RAP 03 - Documentar las acciones realizadas en la red de acuerdo con la normativa

Enlace: **Guía de aprendizaje No. 3**

Evidencia de desempeño: El aprendiz realiza una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas

Evidencia de producto: Protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.

Material de apoyo: Material de Apoyo

Criterios de evaluación:

- Registra información del estado de la red y su conectividad, de acuerdo con procedimientos y normativa.
- Mantiene al día el inventario tecnológico en los registros establecidos.

Instrumentos de evaluación:

1. Lista de chequeo desempeño
2. Lista de chequeo producto

Programa de formación

Sistemas Teleinformáticos

Guía de aprendizaje número 2

Competencia

Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica

Resultado de aprendizaje

RAP 02 - Comprobar la conectividad de la red, de acuerdo con normativa de telecomunicaciones y orden de trabajo.

PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Sistemas Teleinformáticos
- **Código del Programa de Formación:** 233108 V1
- **Nombre del Proyecto Formativo:** Fortalecimiento de los servicios Teleinformáticos de equipos y redes en las MIPYMES de la región de Boyacá.
- F**ase del Proyecto:** Análisis
- **Actividad de Proyecto Formativo:** Diagnosticar el estado de la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.
- **Competencia:** 280102129 Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica.
- **Resultados de Aprendizaje:** RAP02 - Comprobar la conectividad de la red, de acuerdo con normativa de telecomunicaciones y orden de trabajo
- **Duración de la Guía de Aprendizaje:** 48 horas

2. PRESENTACIÓN

Bienvenidos estimados aprendices a esta experiencia de aprendizaje. La presente guía de aprendizaje ha sido diseñada para proporcionar un enfoque estructurado y detallado sobre los temas fundamentales relacionados con el direccionamiento IP y la planificación de redes. Los contenidos abordarán conceptos clave necesarios para comprender la arquitectura de las redes, cómo se organizan y cómo se gestionan mediante técnicas de subnetting y asignación de direcciones IP.

Fomentaremos el aprendizaje colaborativo y el intercambio de ideas entre los aprendices. Al colaborar en equipo y discutir los conceptos, enriqueceremos la experiencia de todos, promoviendo un ambiente de desarrollo integral. Vincularemos los conocimientos previos con los nuevos temas para garantizar un aprendizaje significativo, creando una experiencia dinámica y enriquecedora para el desarrollo de competencias en redes de datos.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1. Actividades de reflexión inicial

Descripción de la actividad: En esta actividad, los aprendices reflexionarán sobre la importancia del direccionamiento IP en la organización de redes. Se utilizará una combinación de reflexión grupal e individual para que los aprendices comprendan cómo los dispositivos se comunican a través de redes, y cómo las direcciones IP juegan un papel crucial en esta comunicación. A través de ejemplos cotidianos y la discusión en equipos, los aprendices conectarán los conceptos teóricos con aplicaciones prácticas.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

Discusión grupal: Los aprendices trabajarán en equipos de 4 personas para discutir el papel de las direcciones IP y compartir ideas.

Plenaria dirigida: El instructor guiará una discusión final para conectar los conceptos tratados en la reflexión con los temas que se verán en la exposición.

Materiales de formación:

Acceso a internet para que los aprendices investiguen rápidamente ejemplos de cómo las direcciones IP se usan en el día a día.

Material de apoyo:

Duración de la actividad: N/A

Desarrollo de la actividad:

1. Introducción: El instructor da la bienvenida y plantea la pregunta inicial: "¿Cómo crees que los dispositivos que usamos diariamente están conectados y se comunican entre sí en una red?"
2. Reflexión grupal: Los aprendices se organizan en equipos de 4 personas. Discuten cómo creen que funciona el proceso de comunicación en una red y el rol de las direcciones IP. El equipo debe llegar a un consenso y preparar una respuesta breve para compartir con el grupo.

3. Discusión en plenaria El instructor recoge las ideas de los diferentes equipos. Se conecta la discusión con los temas a tratar en la exposición, como las clases de IP, subnetting y planificación de redes empresariales.

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

Descripción de la actividad: Esta actividad busca identificar y activar los saberes previos de los aprendices sobre los temas de direccionamiento IP, clases de redes, subnetting y planificación de redes. A través de una dinámica grupal, los aprendices colaborarán para recordar, compartir y discutir conocimientos previos, lo que permitirá al instructor ajustar la exposición de acuerdo con las necesidades del grupo.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

Técnica del mapa mental colaborativo: Los aprendices trabajarán en grupos pequeños para construir un mapa mental conjunto sobre los conceptos de IP, clases de redes y subnetting.

Discusión guiada: Los equipos presentarán su mapa mental y compartirán sus conocimientos previos con los otros grupos.

Plenaria y retroalimentación: El instructor guiará una plenaria donde se clarificarán conceptos erróneos y se reforzarán los saberes clave.

Materiales de formación:

Software de creación de mapas mentales

Preguntas orientadoras sobre los conceptos de direcciones IP, clases de IP, máscara de subred, y subnetting.

Material de apoyo:

Acceso a internet para realizar investigaciones rápidas durante la dinámica si es necesario.

Software ofimático para el registro de ideas.

Duración de la actividad: N/A

Desarrollo de la actividad:

1. **Introducción:** El instructor presenta el objetivo de la actividad: "Queremos identificar qué sabemos sobre direcciones IP, clases de IP y subnetting antes de comenzar la exposición." Se explican las reglas de trabajo en equipo y la metodología de la actividad.
2. **Formación de equipos:** Los aprendices se dividen en equipos de 4 personas. Cada equipo recibirá una guía con preguntas orientadoras para ayudar a la creación del mapa mental colaborativo.
3. **Construcción del mapa mental:** Cada equipo debe construir un mapa mental sobre los conceptos de direccionamiento IP, clases de IP, máscara de subred, subnetting y planificación de redes. Pueden usar herramientas digitales, deben discutir y colocar en el mapa sus conocimientos previos sobre cada uno de los temas.
4. **Presentación de resultados y discusión:** Cada equipo presenta su mapa mental al resto del grupo. Los equipos explican los conceptos que recuerdan y cómo creen que están relacionados.
5. **Plenaria y retroalimentación:** El instructor toma notas de las presentaciones y aclara conceptos erróneos. Se refuerzan los conocimientos clave en los que todos los equipos coincidieron, y se introducen elementos adicionales que serán desarrollados en la exposición.

3.3. Actividades de apropiación:

Actividad de aprendizaje a desarrollar: Realizar una exposición sobre conceptos relacionados con las subredes utilizando organizadores gráficos.

Descripción de la actividad: El aprendiz investigara y elaborara un cuadro sinóptico que organice y sintetice los conceptos clave sobre subnetting y sus temas relacionados. Posteriormente, realizara una exposición del cuadro sinóptico, explicando los puntos principales ante el grupo.

Temas Para Exponer en el Cuadro Sinóptico:

1. Direcciones IP y Clases de Redes:
    - Definición y estructura de una dirección IP.

- Clasificación de direcciones IP (Clase A, B, C, D, E).
- Usos de cada clase de IP en redes.

2. Máscara de Subred:
    - ¿Qué es una máscara de subred?
    - Cálculo de la máscara de subred y su relación con el número de hosts por subred.
3. Cálculo de Subnetting:
    - Proceso para calcular el número de subredes.
    - Cálculo del número de hosts por subred.
    - Ejemplos prácticos.
4. Direccionamiento IP Privado vs Público (Tabla comparativa):
    - Diferencia entre IP pública y privada.
    - Rango de direcciones IP privadas (Clase A, B, C).
    - Aplicaciones comunes.
5. Broadcast y Direcciones de Red:
    - Definición de dirección de red y de broadcast.
    - Cómo identificarlas en una subred.
6. IP Estática vs Dinámica (DHCP):
    - Diferencia entre IP estática y dinámica.
    - Funcionamiento del protocolo DHCP.
7. Planificación de Subredes en Redes Empresariales:
    - Diseño de subredes en redes empresariales.
    - Asignación de rangos para departamentos.

Estrategias o técnicas didácticas activas:

Exposición y Discusión: Cada aprendiz crea su propio cuadro sinóptico y lo expone ante el grupo, fomentando la participación y la retroalimentación.

Preguntas y Respuestas: Se abrirá un espacio para preguntas y respuestas después de cada exposición.

Discusión final: Reflexión conjunta sobre los conceptos y su utilidad en redes empresariales y cotidianas.

Materiales de formación:

- Computadoras con acceso a internet.

Material de apoyo:

Acceso al recurso digital sobre redes y comunicación CISCO CCNA EXPLORATION V5.

Evidencias de aprendizaje:

Desempeño. El aprendiz realiza una exposición sobre conceptos relacionados con las subredes utilizando organizadores gráficos.

Instrumentos de evaluación: Lista de chequeo

Duración de la actividad: 24 horas

Desarrollo de la actividad:

1. **Introducción a los Temas:** El instructor explica los temas básicos de subnetting y presenta ejemplos de cálculos de subredes.
2. **Creación del Cuadro Sinóptico:** Los aprendices diseñan su propio cuadro sinóptico, organizando los conceptos clave de subnetting y los temas adicionales.
3. **Exposición del Cuadro Sinóptico:** Cada aprendiz presenta su cuadro sinóptico frente al grupo, explicando los temas y respondiendo preguntas de sus compañeros.
4. **Discusión y Conclusión:** El grupo participa en una discusión moderada por el instructor, revisando los conceptos clave y resolviendo cualquier duda.

3.4. Actividades de Transferencia el Conocimiento:

Actividad de aprendizaje a desarrollar: Diseñar y configurar dos (2) subredes, interconectadas mediante un router, utilizando Cisco Packet Tracer asegurando la correcta asignación de direcciones IP y la configuración de la conectividad.

Descripción de la actividad: Los aprendices serán divididos en grupos y cada equipo realizara el análisis para establecer el diseño de subredes con base en una dirección IP dada. Configurarán routers y switches para interconectar las subredes. Al final, cada equipo validará la conectividad mediante pruebas de comunicación (ping) entre los dispositivos de las subredes.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

Aprendizaje basado en problemas: Resolverán un caso práctico con necesidades de segmentación de red.

Trabajo colaborativo: Los equipos colaborarán para diseñar y configurar las subredes.

Exploración guiada: Los aprendices tendrán una guía paso a paso para configurar dispositivos en Packet Tracer.

Materiales de formación:

Ejercicios prácticos para calcular subredes orientados por el instructor.

Software Packet Tracer

Material de apoyo: Acceso al recurso digital sobre redes y comunicación CISCO CCNA EXPLORATION V5.

Software Packet Tracer

Evidencias de aprendizaje:

Producto. Informe técnico donde se documente el diseño y la configuración de dos (2) subredes y pantallazos de las pruebas de conectividad realizada entre los diferentes dispositivos validadas mediante el comando ping.

Instrumentos de evaluación: Lista de chequeo de producto

Duración de la actividad: 24 horas

Desarrollo de la actividad:

1. **Introducción Teórica:** Explicación de conceptos clave de subnetting, incluidas máscaras de subred, cálculo de subredes y el proceso de asignación de direcciones IP.
    - Ejemplo en la pizarra sobre cómo dividir la red 192.168.1.0/24 en varias subredes.
2. **Planteamiento del Caso Práctico:** Dada la dirección IP 192.168.1.0/24 crear dos (2) subredes y posteriormente diseñar y realizar la configuración de la red en Packet Tracer. El router debe permitir la comunicación entre las subredes.

3. **Cálculo de Subredes:** Cada equipo calculará el número de subredes y asignará direcciones IP a los dispositivos en Cisco Packet Tracer.
4. **Configuración de Routers y Switches:** Cada equipo configurará routers y switches en Packet Tracer usando los comandos básicos
5. **Validación de la configuración:** Los equipos realizarán pruebas de conectividad utilizando el comando ping para verificar que los dispositivos en diferentes subredes pueden comunicarse entre sí. En caso de errores, se solucionarán los problemas de configuración.
6. **Presentación de Resultados:** Elaboración del informe final, Los aprendices redactaran el informe técnico donde se documente el cálculo de subredes, asignación de direcciones IP, configuración de routers y switches, pantallazos con la prueba de conectividad exitosa realizada entre los dispositivos de diferentes subredes validad mediante el comando ping.
7. **Cierre y retroalimentación:**
    - Discusión final: Reflexión sobre los retos encontrados durante la actividad y cómo se resolvieron.
    - Resumen de conceptos clave: Subnetting, rutas estáticas, y configuración básica de routers y switches.

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

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Análisis	Diagnosticar el estado de la infraestructur	Realizar una exposición sobre conceptos	Desempeño: El aprendiz realiza una exposición	Caracteriza pruebas de fallas en la red según	**Técnica:** Observación

	a de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.	relacionados con las subredes utilizando organizadores gráficos.	sobre conceptos relacionados con las subredes utilizando organizadores gráficos.	requerimientos técnicos. Efectúa pruebas de conectividad de hardware y/o software, operación de servicios y protocolos de infraestructura, disponibilidad, rendimiento y calidad, de acuerdo con normativa de telecomunicaciones, orden de trabajo, aplicando normas de SST y ambientales. Valida el estado de la red de acuerdo con la conectividad, el inventario tecnológico y su disponibilidad técnica según normativa.	**Instrumento:** Lista de chequeo desempeño
Análisis	Diagnosticar el estado de la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.	Diseñar y configurar una red dividida en múltiples subredes, interconectadas mediante routers y switches, utilizando Cisco Packet Tracer. Se trabajará con una red base y se dividirá en subredes	Producto: Informe técnico donde se documente el diseño y la configuración de dos (2) subredes y pantallazos de las pruebas de conectividad realizada entre los diferentes	Identificar estado de conectividad, operación de servicios y protocolos de infraestructura (DHCP, DNS, PROXY entre otros) de la red. Detectar fallas en la operación de la red Verificar operación disponibilidad y	**Técnica:** Observación **Instrumento:** Lista de chequeo producto

		específicas para satisfacer las necesidades de una empresa simulada, asegurando la correcta asignación de direcciones IP y la configuración de la conectividad.	dispositivos validadas mediante el comando ping.	capacidad de las redes de acceso.	

5. GLOSARIO DE TÉRMINOS

Access Point (Punto de Acceso): Dispositivo que permite la conexión de dispositivos inalámbricos a una red alámbrica.

Adaptadores: Dispositivos que permiten la conexión de diferentes tipos de hardware o interfaces, como adaptadores de red.

ARP (Address Resolution Protocol): Protocolo utilizado para mapear direcciones IP a direcciones MAC en una red local.

DNS (Domain Name System): Sistema que traduce nombres de dominio en direcciones IP para facilitar la localización de recursos en la red.

DHCP (Dynamic Host Configuration Protocol): Protocolo que asigna automáticamente direcciones IP y otros parámetros de configuración a los dispositivos en una red.

Dirección IP (Internet Protocol): Identificador numérico asignado a cada dispositivo en una red para su comunicación.

Equipos de Conectividad: Dispositivos que permiten la conexión y comunicación dentro de una red, clasificados en pasivos (por ejemplo, cables) y activos (por ejemplo, routers).

Host: Cualquier dispositivo o computadora en una red que puede enviar o recibir datos.

MAC (Media Access Control): Dirección física única asignada a cada interfaz de red para identificar dispositivos en una red local.

Máscara de Subred: Configuración que determina el rango de direcciones IP en una red local y cómo se dividen las direcciones IP en subredes.

NetBIOS (Network Basic Input/Output System): Interfaz de red que permite la comunicación entre aplicaciones en una red local.

Netstat (Network Statistics): Comando que muestra las conexiones de red activas y las estadísticas de red en un sistema.

Nbtstat: Comando que muestra la tabla de nombres NetBIOS y la caché de nombres NetBIOS en un sistema.

Ping: Comando utilizado para verificar la conectividad entre dos dispositivos de red enviando paquetes ICMP Echo Request y esperando respuestas.

Puerta de Enlace Predeterminada: Dispositivo que actúa como el punto de salida de una red local hacia otras redes, como Internet.

Routers (Enrutadores): Dispositivos que dirigen el tráfico entre redes, determinando la mejor ruta para los paquetes de datos.

Tracert (Trace Route): Comando que rastrea la ruta que sigue un paquete desde el origen hasta el destino a través de la red, mostrando el tiempo de respuesta de cada salto.

Netsh: Comando que permite la configuración y administración de la red en Windows, incluyendo ajustes de IP, DNS, y firewalls.

Route: Comando que muestra y modifica la tabla de enrutamiento IP de un sistema, gestionando las rutas utilizadas para dirigir el tráfico de red.

Ipconfig /all: Variación del comando ipconfig que muestra toda la información de configuración de IP, incluyendo detalles de servidores DNS y DHCP.

6. REFERENTES BILBIOGRÁFICOS (Webgrafía)

Cisco Networking Academy. (2018). ***CCNA Routing and Switching: Introduction to Networks*****. Recuperado de https://techandlan.blogspot.com/2018/02/curso-ccna-50.html**

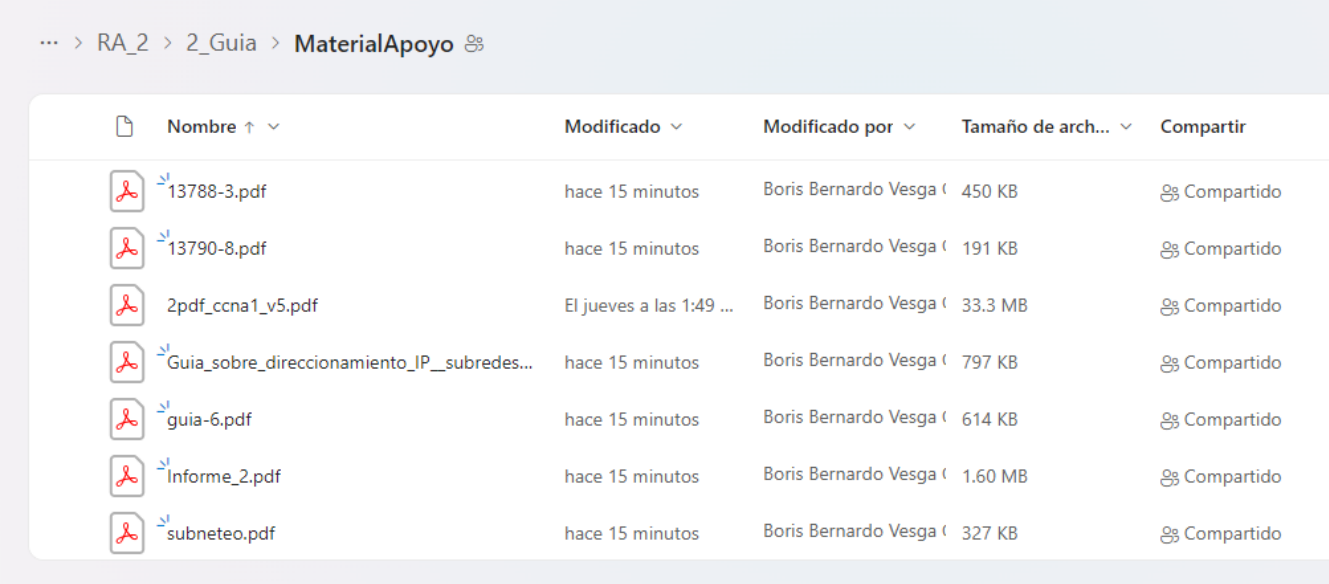
7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Boris Vesga Cardozo	Instructor	Centro de Innovación Agroindustrial y de Servicios	19/09/2024

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					

Material apoyo



INSTRUMENTO DE EVALUACIÓN
LISTA DE CHEQUEO PRODUCTO

1. DATOS GENERALES

Programa de formación:	Sistemas Teleinformáticos	**ID**	2961352
Proyecto formativo:	Fortalecimiento de los servicios Teleinformáticos de equipos y redes en las MIPYMES de la región de Boyacá.		
Fase proyecto:	Análisis		
Resultado de aprendizaje:	RAP02 - Comprobar la conectividad de la red, de acuerdo con normativa de telecomunicaciones y orden de trabajo.		
Actividad de aprendizaje:	Diseñar y configurar dos (2) subredes, interconectadas mediante un router, utilizando Cisco Packet Tracer asegurando la correcta asignación de direcciones IP y la configuración de la conectividad.		
Evidencia de producto:	Producto. Informe técnico donde se documente el diseño y la configuración de dos (2) subredes y pantallazos de las pruebas de conectividad realizada entre los diferentes dispositivos validadas mediante el comando ping.		

Criterios de evaluación:

- Caracteriza pruebas de fallas en la red según requerimientos técnicos.
- Efectúa pruebas de conectividad de hardware y/o software, operación de servicios y protocolos de infraestructura, disponibilidad, rendimiento y calidad, de acuerdo con normativa de telecomunicaciones, orden de trabajo, aplicando normas de SST y ambientales.
- Valida el estado de la red de acuerdo con la conectividad, el inventario tecnológico y su disponibilidad técnica según normativa.

2. LISTA DE VERIFICACIÓN

No.	VARIABLES/INDICADORES DE LOGRO	CUMPLE		Observaciones
		SÍ	NO	
1.	El informe evidencia el cálculo correcto de subredes			
2.	El informe detalla mediante capturas de pantalla la correcta configuración de los routers			
3.	El informe detalla mediante capturas de pantalla la correcta Configuración de los switches			

4.	El informe demuestra una asignación correcta de las direcciones IP a los hosts			
5.	El informe evidencia la prueba de conectividad entre subredes exitosa			
6.	Informe técnico claro, completo y bien estructurado			

3. EVALUACIÓN

Observaciones: _____

Juicio de valor: El aprendiz cumplió con los objetivos de la actividad de aprendizaje de manera satisfactoria.

_____ Firma Aprendiz

_____ Firma Instructor

Programa de formación

Sistemas Teleinformáticos

Guía de aprendizaje número 3

Competencia

Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica

Resultado de aprendizaje

RAP 03 - Documentar las acciones realizadas en la red de acuerdo con la normativa

PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Sistemas Teleinformáticos
- **Código del Programa de Formación:** 233108 V1
- **Nombre del Proyecto Formativo:** Fortalecimiento de los servicios Teleinformáticos de equipos y redes en las MIPYMES de la región de Boyacá cód. 2996750.
- F**ase del Proyecto:** Análisis
- **Actividad de Proyecto Formativo:** Diagnosticar el estado de la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.
- **Competencia:** 280102129 Evaluar red de acuerdo con procedimientos de telecomunicaciones y normativa técnica.
- **Resultados de Aprendizaje:** RAP 03 - Documentar las acciones realizadas en la red de acuerdo con la normativa
- **Duración de la Guía de Aprendizaje:** 40 horas

2. PRESENTACIÓN

Como aprendiz, usted será el protagonista de su proceso de formación, adquiriendo competencias clave para abordar los desafíos de seguridad en redes inalámbricas. En esta guía de aprendizaje, se le guiará para identificar los ataques más comunes en estas redes y diseñar protocolos efectivos de prevención y mitigación. A través de actividades teórico-prácticas, podrá relacionar conceptos previos con nuevos conocimientos, aplicándolos en situaciones reales y fortaleciendo su perfil profesional.

El aprendizaje se desarrollará mediante trabajo colaborativo y dinámicas participativas, donde se fomentará la interacción con sus compañeros para compartir ideas y construir soluciones. Además, utilizará organizadores gráficos que le permitirán estructurar la información de manera clara, facilitando su comprensión y exposición. Este enfoque integrador le ayudará a consolidar su capacidad analítica y su destreza para comunicar conocimientos técnicos de manera efectiva.

Con el apoyo del instructor, quien le orientará y proporcionará retroalimentación durante el proceso, usted avanzará en su formación de manera significativa. Al relacionar conocimientos teóricos con la práctica aplicada, podrá desarrollar habilidades críticas y técnicas necesarias para gestionar la seguridad en redes inalámbricas, preparándose para enfrentar con éxito los retos del entorno digital actual.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1. Actividades de reflexión inicial

Descripción de la actividad: En esta actividad, se llevará a cabo un conversatorio entre los aprendices sobre la importancia de la seguridad en redes inalámbricas. A través del intercambio de ideas, se fomentará la reflexión acerca de los riesgos y las consecuencias de los ataques en redes, así como las medidas preventivas que se pueden tomar para protegerlas.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

Discusión grupal: Los aprendices compartirán sus ideas, experiencias y opiniones sobre el tema en un entorno colaborativo.

Aprendizaje basado en preguntas: El instructor guiará la reflexión mediante preguntas orientadoras para provocar la reflexión y el análisis crítico.

Trabajo en equipo: Los aprendices discutirán en pequeños grupos para luego compartir sus conclusiones con el resto del grupo, promoviendo el intercambio de ideas.

Materiales de formación: N/A

Material de apoyo: N/A

Duración de la actividad: N/A

Desarrollo de la actividad:

1. **Introducción del tema:** El instructor plantea una situación hipotética sobre un ataque a una red inalámbrica y las consecuencias que ello podría traer.

   "Imagínese que una red inalámbrica en su hogar o lugar de trabajo ha sido vulnerable, permitiendo a un tercero acceder a información sensible o controlar dispositivos conectados. ¿Qué consecuencias podrían derivarse de este hecho?"

2. **Intervención de los aprendices:** Los aprendices participan activamente en la discusión, respondiendo a preguntas como:

   - ¿Por qué es importante la seguridad en las redes inalámbricas?

- ¿Qué riesgos existen si una red inalámbrica no está protegida?
- ¿Qué medidas tomarían para prevenir estos ataques?

3. **Cierre y reflexión final:** El instructor resume las ideas más relevantes de la discusión y las conecta con los temas que se abordarán en la guía de aprendizaje, destacando la importancia de la seguridad en redes inalámbricas y cómo las actividades siguientes ayudarán a desarrollar las competencias necesarias para proteger estas redes.

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

Descripción de la actividad: Esta actividad busca activar los conocimientos previos de los aprendices sobre las redes inalámbricas y su seguridad mediante un conversatorio. A través de preguntas, el instructor podrá identificar el nivel de comprensión que los aprendices tienen sobre los conceptos fundamentales relacionados con los ataques comunes a redes inalámbricas y las medidas de protección. La actividad fomenta la participación activa y el intercambio de ideas entre los aprendices, lo que permitirá ajustar la enseñanza a sus necesidades específicas.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

- **Interacción grupal:** Se fomentará una conversación abierta entre los aprendices para compartir sus ideas y conocimientos sobre el tema.
- **Preguntas dirigidas:** El instructor planteará preguntas orales que inviten a la reflexión y permitan evaluar el conocimiento previo de los aprendices.
- **Debate estructurado:** A medida que los aprendices respondan, se abrirá el espacio para discutir en grupo las respuestas y reflexionar sobre conceptos clave.

Materiales de formación: N/A

Material de apoyo: N/A

Duración de la actividad: N/A

Desarrollo de la actividad:

Introducción al conversatorio: El instructor explicará el propósito de la actividad, que es evaluar los conocimientos previos de los aprendices sobre redes inalámbricas a través de preguntas orales.

Interacción oral: El instructor realizará preguntas abiertas y de reflexión que inviten a los aprendices a compartir sus conocimientos. Algunas de las preguntas incluyen:

- ¿Qué entienden por redes inalámbricas?
- ¿Cuáles consideran que son los principales riesgos o ataques a una red inalámbrica?
- ¿Qué medidas creen que se deben tomar para proteger una red inalámbrica?

3.3. Actividades de apropiación:

Actividad de aprendizaje a desarrollar: Realizar una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.

Descripción de la actividad: El aprendiz realizará una exposición sobre los ataques más comunes a las redes inalámbricas, utilizando organizadores gráficos como mapas conceptuales, diagramas de flujo o tablas comparativas para representar visualmente los diferentes tipos de ataques y sus características. Esta actividad tiene como objetivo que los aprendices comprendan y puedan explicar, de forma clara y estructurada, los ataques más frecuentes a las redes inalámbricas, al tiempo que desarrollan habilidades en la organización de información visualmente.

Estrategias o técnicas didácticas activas:

Aprendizaje basado en la exposición: El aprendiz asume el rol de expositor, lo que le permite profundizar en el tema mientras organiza y sintetiza la información.

Uso de organizadores gráficos: Se fomenta el uso de mapas conceptuales y otros organizadores gráficos para facilitar la comprensión y estructuración de la información.

Trabajo autónomo y reflexión individual: El aprendiz investiga y organiza la información, reflexionando sobre cada tipo de ataque y cómo afecta a las redes inalámbricas.

Exposición oral: El aprendiz expone sus hallazgos a sus compañeros, fomentando la capacidad de comunicación efectiva sobre temas técnicos.

Materiales de formación:

- Computadoras con acceso a internet.

Material de apoyo:

- Fuentes bibliográficas, artículos o guías sobre los ataques más comunes a las redes inalámbricas, proporcionadas por el instructor.

Evidencias de aprendizaje:

Desempeño. El aprendiz realiza una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.

Instrumentos de evaluación: Lista de chequeo de desempeño

Duración de la actividad: 20 horas

Desarrollo de la actividad:

1. **Introducción al tema:** El instructor proporcionará una breve introducción sobre los ataques comunes a las redes inalámbricas, incluyendo ejemplos generales de ciberataques (como el ataque de denegación de servicio, spoofing, phishing, etc.), para dar contexto a la actividad.
2. **Investigación y elaboración de los organizadores gráficos:** Los aprendices investigarán sobre los distintos tipos de ataques a redes inalámbricas, como los ataques de fuerza bruta, el ataque Man-in-the-Middle (MITM), la falsificación de direcciones MAC, el sniffer, etc. Utilizando esta información, crearán un organizador gráfico (puede ser un mapa conceptual o un diagrama de flujo) para describir cada tipo de ataque, su funcionamiento, impacto y las medidas de mitigación.
3. **Exposición y análisis en grupo:** Cada aprendiz presentará su organizador gráfico a sus compañeros, explicando los ataques que ha investigado y detallando las estrategias para prevenirlos. Durante la exposición, los demás aprendices podrán hacer preguntas y el instructor proporcionará retroalimentación.

3.4. Actividades de Transferencia el Conocimiento:

Actividad de aprendizaje a desarrollar: Elaborar protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.

Descripción de la actividad: En esta actividad, los aprendices elaborarán un protocolo detallado para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a redes inalámbricas. A través de un enfoque práctico, los aprendices diseñarán procedimientos claros y específicos que permitan identificar, prevenir y mitigar las amenazas comunes a las redes inalámbricas. Este ejercicio les permitirá aplicar los conocimientos adquiridos sobre la seguridad en redes y desarrollar habilidades fundamentales para implementar medidas de protección en entornos reales.

Ambiente requerido: Sala de sistemas equipada con 24 computadoras Los equipos deben tener instalado software básico (sistema operativo, paquete ofimático, entre otros) y contar con conexión a internet.

Estrategias o técnicas didácticas activas:

- **Aprendizaje basado en problemas (ABP):** Los aprendices enfrentarán un desafío realista de seguridad en redes inalámbricas, lo que les motivará a aplicar soluciones prácticas basadas en la teoría.
- **Trabajo colaborativo:** Los aprendices trabajarán en grupos para estructurar un protocolo de seguridad, fomentando el intercambio de ideas y la toma de decisiones grupales.
- **Estudio de casos:** El instructor proporcionará ejemplos de incidentes de seguridad para ilustrar cómo las políticas de seguridad pueden prevenir ataques, y los aprendices deberán tomar estos ejemplos como referencia para su protocolo.
- **Discusión guiada:** A medida que los grupos desarrollen el protocolo, el instructor facilitará debates sobre las mejores prácticas de seguridad y las decisiones tomadas por los aprendices.

Materiales de formación:

- Computadoras con acceso a internet.

Material de apoyo:

- Fuentes bibliográficas, artículos o guías sobre los ataques más comunes a las redes inalámbricas, como evitarlos y mitigarlos.

Evidencias de aprendizaje:

Producto. Protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.

Instrumentos de evaluación: Lista de chequeo de producto

Duración de la actividad: 20 horas

Desarrollo de la actividad:

1. **Introducción:** El instructor comenzará con una breve presentación sobre la importancia de las políticas de seguridad informática y las amenazas más comunes a las redes inalámbricas. Se explicarán los conceptos clave como "prevención", "mitigación", y "respuesta ante incidentes".
    - Ejemplo de amenazas comunes: ataques de Denegación de Servicio (DoS), sniffing, spoofing, entre otros.
    - Definición de una política de seguridad informática y su importancia para proteger redes y datos sensibles.
2. **División en grupos:** Los aprendices se dividirán en parejas para colaborar en la elaboración de su protocolo. Cada grupo recibirá una plantilla que deberán completar, adaptando las recomendaciones teóricas a un protocolo práctico.
3. **Desarrollo del protocolo:** Los grupos trabajarán en la creación de su protocolo de seguridad. Cada grupo deberá incluir las siguientes secciones:

    - Objetivos de la política de seguridad: Qué se busca proteger, cuáles son los principales riesgos y las amenazas a las que se enfrentan las redes inalámbricas.
    - Acciones de prevención: Estrategias para evitar ataques a las redes inalámbricas (ej. encriptación, autenticación, cambios en contraseñas predeterminadas, uso de firewalls).
    - **Acciones de mitigación:** Medidas para reducir el impacto de un ataque, si llegara a ocurrir (ej. aislamiento de redes, alertas automáticas, monitoreo continuo).

- **Procedimientos en caso de ataque:** Qué hacer y cómo reaccionar ante un ataque a la red (ej. desconectar equipos afectados, notificar a los responsables, análisis forense).
- **Responsables:** Identificación de los roles y responsabilidades de cada miembro del equipo de seguridad.

4. **Presentación de los protocolos:** Cada grupo presentará su protocolo frente a la clase, explicando las decisiones tomadas y cómo su protocolo protegerá las redes inalámbricas frente a ataques. El instructor y los demás grupos podrán hacer preguntas o sugerir mejoras.
5. **Retroalimentación y cierre:** El instructor proporcionará retroalimentación sobre cada uno de los protocolos presentados, destacando las mejores prácticas y sugiriendo posibles mejoras. Se discutirá cómo aplicar este ejercicio en escenarios reales y la importancia de mantener una política de seguridad actualizada.

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

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Análisis	Diagnosticar el estado de la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.	Realizar una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.	**Desempeño:** El aprendiz realiza una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.	Registra información del estado de la red y su conectividad, de acuerdo con procedimientos y normativa. Mantiene al día el inventario tecnológico en los registros establecidos.	**Técnica:** Observación **Instrumento:** Lista de chequeo desempeño

Análisis	Diagnosticar el estado de la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presenta en el entorno de trabajo.	Elaborar protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.	**Producto:** Protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.	Registra información del estado de la red y su conectividad, de acuerdo con procedimientos y normativa. Mantiene al día el inventario tecnológico en los registros establecidos.	**Técnica:** Observación **Instrumento:** Lista de chequeo producto

5. GLOSARIO DE TÉRMINOS

Acción de mitigación: Medidas implementadas para reducir el impacto de un ataque o incidente de seguridad en una red.

Autenticación: Proceso de verificar la identidad de un usuario o dispositivo antes de conceder acceso a una red.

Ataque de Denegación de Servicio (DoS): Tipo de ataque donde se busca hacer que un servicio en línea no esté disponible, sobrecargando el sistema con tráfico.

Bluetooth: Tecnología de comunicación inalámbrica de corto alcance utilizada para intercambiar datos entre dispositivos.

BSSID (Basic Service Set Identifier): Identificador único asociado a un punto de acceso en una red Wi-Fi.

Cifrado (encriptación): Proceso de convertir datos en un formato ilegible para proteger la confidencialidad de la información durante la transmisión.

Contraseña: Secuencia de caracteres usada para verificar la identidad de un usuario y controlar el acceso a un sistema.

Cracking de contraseñas: Técnica utilizada para descifrar contraseñas de manera no autorizada, normalmente por fuerza bruta o pruebas sistemáticas.

Denegación de Servicio (DoS): "Ataque de Denegación de Servicio".

DNS (Domain Name System): Sistema de nombres de dominio que traduce los nombres de dominio legibles por los humanos a direcciones IP comprensibles por las computadoras.

EAP (Extensible Authentication Protocol): Protocolo utilizado para la autenticación en redes inalámbricas, como en Wi-Fi.

Escaneo de red: Proceso de examinar una red para identificar dispositivos y vulnerabilidades.

Firewall: Sistema de seguridad diseñado para proteger una red, filtrando el tráfico no deseado y permitiendo solo el tráfico autorizado.

Fuerza bruta: Método de ataque donde se prueban todas las combinaciones posibles para adivinar una contraseña o clave de seguridad.

Hotspot: Área geográfica donde se proporciona acceso a Internet a través de una red inalámbrica.

Hackeo: Acceso no autorizado a sistemas informáticos, generalmente con fines maliciosos.

IP (Internet Protocol): Protocolo utilizado para identificar dispositivos en una red mediante direcciones numéricas únicas.

Incidente de seguridad: Evento que compromete la seguridad de una red o sistema, como un ataque cibernético o una violación de datos.

LAN (Local Area Network): Red de área local que conecta dispositivos dentro de un área geográfica limitada, como una oficina o edificio.

WLAN (Wireless Local Area Network): Red de área local inalámbrica que permite la comunicación de dispositivos sin cables.

MITM (Man in the Middle): Tipo de ataque donde el atacante intercepta y manipula la comunicación entre dos partes sin que estas lo sepan.

MFA (Multi-factor Authentication): Método de autenticación que requiere más de un factor (como contraseña y código enviado al celular) para acceder a un sistema.

Phishing: Técnica de fraude en línea donde se engaña a las personas para que revelen información confidencial, como contraseñas, a través de correos electrónicos falsos.

Punto de acceso (AP): Dispositivo de red que permite que los dispositivos se conecten de manera inalámbrica a una red local.

Red inalámbrica: Conexión de dispositivos a una red sin la necesidad de cables, generalmente utilizando señales de radiofrecuencia.

Router: Dispositivo que dirige el tráfico entre redes, como entre una red local y la Internet.

Sniffing: Técnica utilizada para interceptar y analizar el tráfico de red, a menudo con fines maliciosos.

Spoofing: Ataque en el que un dispositivo o usuario se hace pasar por otro para obtener acceso a una red o sistema.

SSID (Service Set Identifier): Nombre único que identifica una red inalámbrica.

TLS (Transport Layer Security): Protocolo de seguridad utilizado para cifrar las comunicaciones entre dispositivos en una red.

Trojan (troyano): Tipo de malware que se disfraza de software legítimo para infectar un sistema y dar acceso no autorizado al atacante.

WEP (Wired Equivalent Privacy): Estándar de seguridad en redes Wi-Fi, ahora obsoleto, que cifra los datos transmitidos entre dispositivos y puntos de acceso.

WPA (Wi-Fi Protected Access): Protocolo de seguridad utilizado en redes inalámbricas, más seguro que WEP.

6. REFERENTES BILBIOGRÁFICOS (Webgrafía)

El empresario, U. G. de A. P. (s/f). en redes wifi: Incibe.es. Recuperado el 30 de noviembre de 2024, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

Introducción, 7. 1. (s/f). SEGURIDAD EN LAS REDES INALÁMBRICAS. Biblus.us.es. Recuperado el 30 de noviembre de 2024, de https://biblus.us.es/bibing/proyectos/abreproy/11138/fichero/memoria%252FCap%C3%ADtulo+7.pdf+

(S/f-a). Esetstatic.com. Recuperado el 30 de noviembre de 2024, de https://web-assets.esetstatic.com/wls/es/articulos/guias/documento_guia_de_wifi.pdf

(S/f-b). Edu.co. Recuperado el 30 de noviembre de 2024, de https://repositorio.utb.edu.co/bitstream/handle/20.500.12585/2637/0035911_organized.pdf?sequence=6&isAllowed=y

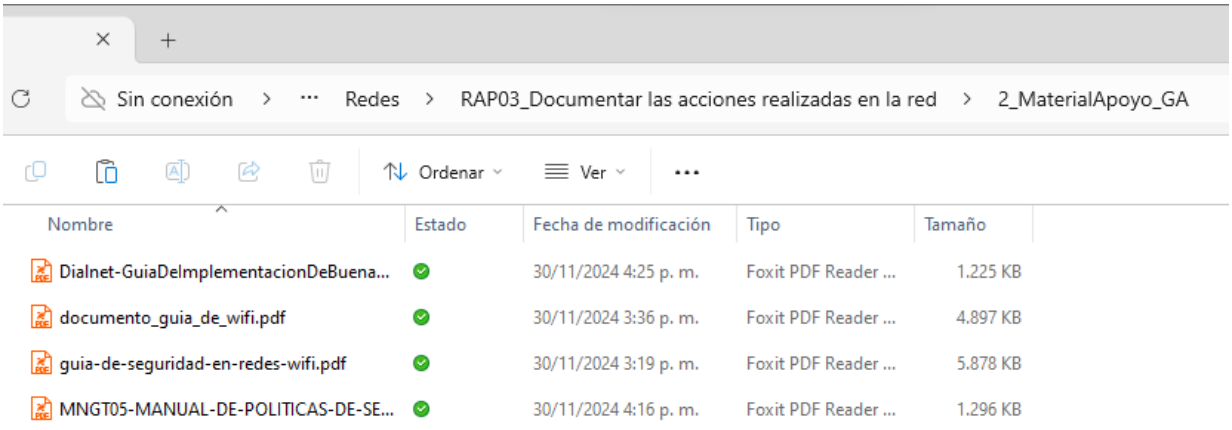
(S/f-c). Gov.co. Recuperado el 30 de noviembre de 2024, de https://www.insor.gov.co/home/descargar/MNGT05-MANUAL-DE-POLITICAS-DE-SEGURIDAD-Y-PRIVACIDAD-DE-LA-INFORMACION_copia_controlada-1.pdf

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Boris Vesga Cardozo	Instructor	Centro de Innovación Agroindustrial y de Servicios	04/11/2024

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					


Sin conexión
Redes
RAP03_Documentar las acciones realizadas en la red
2_MaterialApoyo_GA
Ordenar
Ver
Nombre
Estado
Fecha de modificación
Tipo
Tamaño
Dialnet-GuiaDeImplementacionDeBuena...
30/11/2024 4:25 p. m.
Foxit PDF Reader ...
1.225 KB
documento_guia_de_wifi.pdf
30/11/2024 3:36 p. m.
Foxit PDF Reader ...
4.897 KB
guia-de-seguridad-en-redes-wifi.pdf
30/11/2024 3:19 p. m.
Foxit PDF Reader ...
5.878 KB
MNGT05-MANUAL-DE-POLITICAS-DE-SE...
30/11/2024 4:16 p. m.
Foxit PDF Reader ...
1.296 KB

INSTRUMENTO DE EVALUACIÓN
LISTA DE CHEQUE DESEMPEÑO

1. DATOS GENERALES

Programa de formación:	Sistemas Teleinformáticos	**ID**	2961273
Proyecto formativo:	Fortalecimiento de los servicios Teleinformáticos de equipos y redes en las MIPYMES de la región de Boyacá.		
Fase proyecto:	Análisis		
Resultado de aprendizaje:	RAP 03 - Documentar las acciones realizadas en la red de acuerdo con la normativa		
Actividad de aprendizaje:	Realizar una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.		
Evidencia de desempeño:	El aprendiz realiza una exposición, utilizando organizadores gráficos, para describir los ataques más comunes a las redes inalámbricas.		

Criterios de evaluación:

- Registra información del estado de la red y su conectividad, de acuerdo con procedimientos y normativa.
- Mantiene al día el inventario tecnológico en los registros establecidos.

2. LISTA DE VERIFICACIÓN

No.	VARIABLES/INDICADORES DE LOGRO	CUMPLE		Observaciones
		SÍ	NO	
1.	Identifica y describe claramente al menos tres ataques comunes a redes inalámbricas.	X		
2.	Utiliza información técnica precisa y actualizada sobre los ataques descritos.	X		
3.	Describe correctamente ataques como sniffing, wardriving, man-in-the-middle, entre otros.	X		
4.	Explica cómo funciona cada ataque desde un enfoque técnico (procesos, herramientas usadas).	X		
5.	Detalla las vulnerabilidades específicas que explotan estos ataques en redes inalámbricas.	X		
6.	Analiza las posibles consecuencias de cada ataque (filtración de datos, interrupciones, etc.).	X		

7.	Menciona herramientas específicas usadas por atacantes (Wireshark, Aircrack-ng, Kali Linux).	X		
8.	Explica cómo dichas herramientas interactúan con las redes inalámbricas.	X		
9.	Describe ejemplos de daños reales ocasionados por estos ataques, en contextos personales o empresariales.	X		
10.	La exposición sigue una estructura lógica: introducción, desarrollo y conclusión.	X		
11.	Los conceptos se explican de manera clara y comprensible para el público objetivo.	X		
12.	Presenta organizadores gráficos adecuados al tema (mapas conceptuales, diagramas, etc.).	X		
13.	Los organizadores gráficos son claros, bien diseñados y relevantes para los ataques descritos.	X		
14.	Demuestra seguridad y dominio del tema durante la exposición.	X		
15.	Cumplió con los objetivos de la actividad	X		

3. EVALUACIÓN

Observaciones: _____

Juicio de valor: El aprendiz cumplió con los objetivos de la actividad de aprendizaje de manera satisfactoria.

_____ Firma Aprendiz

_____ Firma Instructor

INSTRUMENTO DE EVALUACIÓN
LISTA DE CHEQUEO PRODUCTO

1. DATOS GENERALES

Programa de formación:	Sistemas Teleinformáticos	**ID**	2961273
Proyecto formativo:	Fortalecimiento de los servicios Teleinformáticos de equipos y redes en las MIPYMES de la región de Boyacá.		
Fase proyecto:	Análisis		
Resultado de aprendizaje:	RAP 03 - Documentar las acciones realizadas en la red de acuerdo con la normativa		
Actividad de aprendizaje:	Elaborar protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.		
Evidencia de producto:	Protocolo para estructurar una política de seguridad informática con acciones de prevención y mitigación frente a posibles ataques a las redes inalámbricas.		

Criterios de evaluación:

- Registra información del estado de la red y su conectividad, de acuerdo con procedimientos y normativa.
- Mantiene al día el inventario tecnológico en los registros establecidos.

2. LISTA DE VERIFICACIÓN

No.	VARIABLES/INDICADORES DE LOGRO	CUMPLE		Observaciones
		SÍ	NO	
1.	El protocolo incluye un análisis de riesgos específico para redes inalámbricas.	X		
2.	El protocolo describe claramente las acciones preventivas para proteger redes inalámbricas.	X		
3.	El protocolo proporciona medidas de mitigación específicas frente a posibles ataques.	X		
4.	El protocolo contempla un plan de gestión de incidentes detallado y realista.	X		
5.	El protocolo define roles y responsabilidades de los actores involucrados en la implementación.	X		
6.	El protocolo propone políticas de acceso seguras, como autenticación multifactor, segmentación de redes y privilegios mínimos.	X		

7.	El protocolo incluye políticas de uso claras para los usuarios de redes inalámbricas (empleados, visitantes, etc.).	X		
8.	El protocolo define estrategias para el monitoreo y detección de amenazas en tiempo real.	X		
9.	El protocolo integra medidas de respuesta a incidentes que incluye pasos detallados para identificar, contener y resolver un ataque.	X		
10.	El protocolo propone un plan de contingencia para mantener la operación de la red en caso de incidentes graves.	X		
11.	El protocolo cumple con los requerimientos establecidos en la actividad	X		

3. EVALUACIÓN

Observaciones: _____

Juicio de valor: El aprendiz cumplió con los objetivos de la actividad de aprendizaje de manera satisfactoria.

_____ Firma Aprendiz

_____ Firma Instructor