INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA ACADÉMICA
DIRECCIÓN DE EDUCACION MEDIA SUPERIOR
CENTRO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS No. 13
"RICARDO FLORES MAGÓN"

G U Í A

d e e s t u d i o p a r a
presentar ETS de la
UNIDAD DE APRENDIZAJE
SEGURIDAD EN REDES
Semestre 2023-2
TURNO VESPERTINO

Integrantes de la academia: **Alfredo Campos Guerrero**

Fecha de Elaboración: **23/05 /2023**

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**Seguridad en Redes**	**Quinto**

Instrucciones generales de la guía:

Anotar aspectos que el alumno debe considerar antes de presentar el examen:

- Esta guía no tiene ningún valor sobre la calificación final

Presentación:

Preparar al estudiante para que desarrolle competencias para entender los protocolos, software y hardware que son requeridos para prevenir y supervisar acceso no autorizado o indebido a través de la red de datos que afectan la integridad de la información tanto en las empresas privadas, públicas y equipos de particulares y que pueden generar afectaciones económicas, políticas o legales.

Objetivos

Los principales objetos del conocimiento que se adquirirán y serán cuerpo de las acciones o desempeños a realizar son:

- Establecer la planificación para la implementación de una red de datos.
- Diseñar una red de datos a través de una metodología y requerimiento del usuario
- Conocer los medios de transmisión alámbricos e inalámbricos
- Conocer cuáles son los protocolos de red más utilizados para las redes de datos LAN, MAN y WAN.

Justificación

Las competencias profesionales (generales y particulares) implican como principales objetos de conocimiento de las redes de datos por medio de las bases metodológicas, que podrá vincular con su entorno socioeconómico y laboral. Asimismo, en la particularidad del estudiante:

- Diseña una red de datos en base a sistemas metodológicos establecidos.
- Hacer uso de herramientas informáticas que permiten diseñar Redes de datos

Estructura y contenidos

I. Identifica los elementos que conforman una red de datos y los dispositivos utilizados para saber cómo se comunican entre sí de acuerdo con la normatividad vigente Definición, explicación y características sobre los elementos que conforman una red de datos

- Uso de las redes de datos y su importancia
- Clasificación de las redes de acuerdo con su extensión geográfica
- Modelo de referencia OSI

II. Distingue los medios de transmisión, las topologías y tecnologías de redes haciendo uso de los elementos que conforman un sistema de cableado estructurado para su diseño físico de acuerdo con la normatividad vigente.

- Topologías y tecnologías de red
- Organismo Internacional IEEE
- Medios de transmisión
- Ensamblado cable de red UTP

III. Diseña la estructura lógica y la seguridad de una red para garantizar la transferencia de datos e integridad de la información mediante protocolos de red conforme a las necesidades de una organización

- Protocolos de Microsoft, IPX/SPX y TCP/IP
- Protocolos suite TCP/IP: FTP, TELNET, DHCP, DNS, TCP, IP, POP3, SMTP
- Modelo Cliente servidor

Materiales para la elaboración de la guía

No Aplica

Actividades de estudio

- Repaso de conceptos teóricos en esta guía detallados
- Se recomienda hacer uso del Software Cisco Packet Tracer para el diseño de redes de datos
- Se recomienda estudiar los siguientes temas:
  - ✓ Conoce la definición de seguridad en redes.
  - ✓ Identifica los conceptos asociados a la seguridad de redes.
  - ✓ Identifica en un esquema los componentes físicos de una red de datos.
  - ✓ Identifica en un esquema los elementos lógicos de una red de datos.
  - ✓ Conoce los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en una red de datos.
  - ✓ Conoce las políticas de seguridad de redes de datos.
  - ✓ Identifica a los miembros de la organización responsables de las TIC's para generar las políticas y permisos de seguridad informática.
  - ✓ Conoce los diferentes tipos de ataques en seguridad informática.
  - ✓ Identifica los niveles de servicio de seguridad dentro de una organización
  - ✓ Conoce los diferentes mecanismos de seguridad informática que abarquen la prevención, detección y recuperación de datos.
  - ✓ Identifica los mecanismos de seguridad aplicados en redes alámbricas e inalámbricas.
  - ✓ Conoce los diferentes componentes de una red segura de una organización tales como:
    - Zona militarizada y desmilitarizada.
    - Arquitectura de Firewalls.
    - Sistemas detectores de intrusos (IDS).
    - Analizadores de red.
    - AntiSpam.
    - Monitoreo de dispositivos conectados a la red
  - ✓ Conoce los términos de routing & switching.
  - ✓ Describe el uso de una Virtual Local Area Network (VLAN) en una red de datos.
  - ✓ Conoce las configuraciones de un switch y ruteador para segmentar una red de datos.

Información Adicional

- Ninguna

Bibliografía Básica

- Instalación Y Mantenimiento De Servicios De Redes locales. Autor: Francisco Molina. Edit. AlfaOmega
- Redes de Área Local. Autor: Francisco Molina. Edit. AlfaOmega
- Sistemas Informáticos Multiusuario y en Red. Autor: Laura Raya. Edit. Anaya Multimedia
- Construye y Configura Tu Red. Autor: Rosenda Hernández. Edit. Anaya Multimedia

Guía de estudio

1. Seguridad de red:

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.

- Incluye tecnologías de hardware y software.
- Está orientada a diversas amenazas.
- Evita que ingresen o se propaguen por la red.
- La seguridad de red eficaz administra el acceso a la red.

2. Cómo funciona la Seguridad de red:

La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.

3. Tipos de Seguridad en Redes

- **Firewalls**

Los firewalls ponen una barrera entre su red interna de confianza y las redes externas que no son de confianza, como Internet. Usan un conjunto de reglas definidas para permitir o bloquear el tráfico. Un firewall puede ser hardware, software o ambos.

- **Seguridad del correo electrónico**

Los gateways del correo electrónico son el principal vector de amenaza para las infracciones a la seguridad. Los atacantes usan la información personal y las tácticas de ingeniería social para desarrollar campañas de suplantación de identidad (phishing) sofisticadas para los destinatarios de los dispositivos a fin de dirigirlos a sitios con malware. Una aplicación de seguridad de correo electrónico bloquea los ataques entrantes y controla los mensajes salientes para prevenir la pérdida de datos sensibles.

- **Software antivirus y antimalware**

El "malware", abreviatura de "software malicioso", abarca los virus, gusanos, troyanos, ransomware y spyware. En algunos casos, el malware puede infectar una red y permanecer latente por días o incluso semanas. Los mejores programas antimalware no solo detectan la entrada de malware, sino que también hacen un seguimiento constante de los archivos para detectar anomalías, eliminar malware y reparar daños.

- **Segmentación de la red**

La segmentación definida por software clasifica el tráfico de red en distintas categorías y facilita la aplicación de políticas de seguridad. Lo ideal es que las clasificaciones se basen en la identidad de los EndPoints, no solo en las direcciones IP. Puede asignar derechos de acceso basados en roles, ubicación y demás, de modo que se otorgue el nivel de acceso correcto a las personas adecuadas y se contengan y reparen los dispositivos sospechosos.

- **Control de Acceso**

No todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos. Entonces podrá aplicar las políticas de seguridad. Puede bloquear dispositivos de EndPoint que no cumplen las políticas o proporcionarles acceso limitado. Este proceso se denomina control de acceso a la red (NAC).

- **Seguridad de las Aplicaciones**

Cualquier software que utilice para operar su negocio debe estar protegido, ya sea que su personal de TI lo construya o lo compre. Lamentablemente, todas las aplicaciones pueden tener vulnerabilidades que los atacantes pueden usar para infiltrarse a la red. La seguridad de las aplicaciones abarca el hardware, el software y los procesos que se usan para corregir estas vulnerabilidades.

- **Análisis de comportamiento**

Para detectar el comportamiento anómalo de la red, primero debe conocer el comportamiento normal. Las herramientas de análisis de comportamiento detectan automáticamente las actividades que se desvían de la norma. El equipo de seguridad entonces puede identificar mejor los indicadores de infiltración que pueden traer problemas y reaccionar rápidamente ante las amenazas.

- **Sistema de prevención de Intrusiones**

Un sistema de prevención de intrusiones (IPS) analiza el tráfico de red para bloquear ataques activamente. Los dispositivos del IPS de próxima generación (NGIPS) logran esto al correlacionar enormes cantidades de inteligencia de amenazas globales para bloquear las actividades maliciosas y hacer un seguimiento del progreso de los archivos sospechosos y el malware por la red a fin de evitar la propagación de brotes y la reinfección.

4. Pilares de la Seguridad de la Información

En virtud del creciente número de ataques virtuales y delitos cibernéticos, la protección de los datos se ha convertido en una prioridad para las organizaciones. No obstante, antes de implementar estrategias con la finalidad de incrementar la seguridad de la información, es indispensable conocer los pilares que la soportan:

1. Confidencialidad

2. Integridad

3. Disponibilidad

5. Responsables de las TICs en las organizaciones

El responsable de informática debe garantizar que en la empresa todo funcione correctamente. Mejorar los resultados del negocio usando las TIC y la gestión informática forma parte de sus responsabilidades. Sin embargo, no se trata de hacer informática, sino de utilizarla para que se cumplan los objetivos de la empresa.

6. Mejores prácticas para implementar un Plan de políticas de Seguridad de Redes de Datos

Las organizaciones de TI más eficaces adoptan las mejores prácticas de seguridad de red para maximizar la efectividad de su seguridad y proteger sus activos. Las siguientes son 10 mejores prácticas esenciales que toda organización debería usar para salvaguardar sus empresas hoy en día. Ten en cuenta que estos esfuerzos deben ser continuos para tener éxito. Además, estas prácticas deben revisarse periódicamente para medir su efectividad y, cuando sea necesario, ajustarse si las circunstancias cambian.

- Auditar la red y verificar los controles de seguridad
- Revisar y comunicar las políticas de seguridad
- Hacer una copia de seguridad de los datos e instituir un plan de recuperación
- Cifrar datos críticos
- Actualizar el software antimalware
- Establecer los controles de acceso adecuados y emplear la autenticación multifactor
- Establecer y comunicar una estructura de gobierno de seguridad
- Educar a los usuarios finales
- Tener un sistema de mantenimiento para la infraestructura de seguridad
- Mantenerse informado

7. Cisco Packet Tracer

Cisco Packet Tracer es una herramienta que te permite simular redes reales.

Realizar o revisar las siguientes prácticas:

- Conexión física de dispositivos de red con su respectivo cableado.
- Revisión del modo de simulación de Cisco Packet Tracer, analizando los siguientes paquetes:
  - ICMP
  - HTTP
  - POP3
  - SMTP
  - DNS

8. Análisis de datos con WireShark

WireShark es una herramienta que te permite el análisis de tráfico.

Revisar o revisar las siguientes prácticas:

- Creación de filtros
- Captura de paquetes ICMP
- Captura de paquetes HTTP
- Captura de paquetes HTTPS

9. Ruteo y Switcheo

- Dirección lógica (Protocolo IP)
- Dirección Física (MAC ADDRESS)
- Puertos
- Protocolos
- Modelo Cliente Servidor
- IP Pública e IP Privada
- IP V4
- Redes convergentes
- Práctica de Redes remotas con Cisco Packet Tracer unidas por medio de Routers
- Enrutamiento
  - Tablas de enrutamiento
  - Tipo de enrutamiento
  - Interpretación de Diagramas de Red
- Subneteo
  - Subredes
  - Hosts
  - Segmentación Clase A de 24 bits
  - Segmentación Clase A de 25 bits
  - Segmentación Clase A de 26 bits
  - Segmentación Clase A de 27 bits
  - Segmentación Clase A de 28 bits
  - Segmentación Clase A de 29 bits
  - Segmentación Clase A de 30 bits

10. Redes VLAN

- Definición y usos
- Creación de VLANS
- Asignación de puertos
- VLANS entre switches
- Protocolo 802.Q
- Práctica de VLAN con Cisco Packet Tracer