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
TURNO Matutino
Semestre 26-2

Presidente de academia: **Alejandro Morales Zavaleta** **Fecha de Elaboración:** **__Abril_ 2026**

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

Instrucciones generales de la guía:

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

- Esta guia no tiene ningun valor sobre la calificación final, es una ayuda para la presentación del examen

Procedimiento para la revisión del ETS.

El alumno deberá asistir al área correspondiente para solicitar el formato de revisión de examen, en dónde el jefe de área firmará e informará al profesor correspondiente para realizar dicha revisión.

Lo anterior debera realizarse en un plazo de 48 horas a partir de que se notifico la calificacion correspondiente.

El profesor tiene 24 hrs. a partir de la aplicación del examen para subir calificaciones de tal manera que el alumno puede solicitar la revisión a partir de que transcurra ese tiempo.

Presentación:

La presente guia de estudio , permitira al estudiante el desarrollo de habilidades y conmpetencias en el manejo y uso de sistema operativo como parte esencial en el funcionamiento de una computadora. Lo introduce al campo conceptual y procedimental, que permite al estudiante contar con una visión crítica, ampliando su panorama para que logre visualizar todos los elementos que lo componen, relacionándolo con la "Gestión de la Ciberseguridad"

Objetivos

Adquirir habilidades digitales, desarrollarlas y actualizarlas. Desarrollar procesos de enseñanza aprendizaje, utilizando métodos basados en administración de proyectos reales, aprovechando espacios educativos distintos a las aulas, para mejorar la calidad y pertinencia de la enseñanza. Conocimientos de leyes.

Establecer la planificacion para la implementacion de una red de datos
Diseñar una red a travez de una metodologia y requerimientos del usuario.
Conocer los dispositivos de red empleados para proteger una red de datos en un corporativo o empresa
Conocer cuales son los protocolos de la red mas utilizados para las redes de datos Lan, MAN y WAN

Justificación

Esta unidad de aprendizaje está enfocada al desarrollo de habilidades cognitivas y socioemocionales vinculadas con el ciberespacio y su relación con la sociedad para lo cual, las experiencias de aprendizaje se diseñan considerando el contexto real y las problemáticas del entorno global. En estas experiencias de aprendizaje se incluyen todas las relacionadas con las tecnologías de la Información para lograr tener un balance entre la tecnología, habilidades socioemocionales estables, la creatividad e iniciativa y la integración de varias disciplinas como el derecho, la ética y las redes.

Diseña una red de datoa en base a sistemas metodologicos establecidos
Hacer uso de herramienta informatica que permita diseñar redes de datos

Estructura y contenidos

En esta unidad de aprendizaje se abordan 3 unidades didácticas

Unidad 1: FUNDAMENTOS DE SEGURIDAD EN REDES DE DATOS
Unidad 2: ADMINISTRACIÓN DE LA SEGURIDAD EN UNA RED DE DATOS
Unidad 3 : APLICACIÓN DE LOS COMPONENTES DE SEGURIDAD EN UNA RED DE DATOS

Evaluación

La guía no tiene valor sobre el examen.

Materiales para la elaboración de la guía

Internet

Manuales o libros de consulta

Actividades de estudio

Repaso de conceptos teóricos en esta guía detallados
Hacer uso del Software Cisco Packet Tracer para el diseño de redes de datos
Investiga los siguientes temas:
Conoce los conceptos básicos de seguridad en redes.
Identifica los conceptos y componentes lógicos y físicos asociados a la seguridad de redes.
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)
Describe el uso de una Virtual Local Area Network (VLAN) en una red de datos.
Conoce los términos, conceptos de configuraciones de un switch y ruteador para segmentar una red de datos.

Información adicional

Que desarrolles los conocimientos básicos sobre las características de la ciencia y sus métodos de estudio para el manejo y uso de la seguridad en redes.

Bibliografía básica

Páginas en Internet

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

Integrantes de la academia

Alejandro Morales Zavaleta

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.

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.

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.

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: Confidencialidad, Integridad, . Disponibilidad

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.

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

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)

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

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

- o Tablas de enrutamiento
- o Tipo de enrutamiento
- o Interpretación de Diagramas de Red

Subneteo

- o Subredes
- o Hosts
- o Segmentación Clase A de 24 bits
- o Segmentación Clase A de 25 bits
- o Segmentación Clase A de 26 bits
- o Segmentación Clase A de 27 bits
- o Segmentación Clase A de 28 bits
- o Segmentación Clase A de 29 bits
- o Segmentación Clase A de 30 bits

Redes VLAN

Definición y usos

Creación de VLANS

Asignación de puertos

VLANS entre switches

Protocolo 802.Q

Práctica de VLAN con Cisco Packet Tracer