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
SISTEMAS DE IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO
CICLO ESCOLAR 2026-2
TURNO MATUTINO

Presidente de academia: GODELINDA MELGOZA PONCE **Fecha de Elaboración: MAYO/2026**

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
TECNOLOGICA	**SISTEMAS DE IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO**	**QUINTO**

Instrucciones generales de la guía:

1. **Para poder presentar el examen el alumno debe conocer:**
   - Identificar los conceptos clave así como el marco normativo vigente que lo regula
   - Reconocer
   - Adaptar protocolos

La guía no tiene valor.

Presentación:

Esta Unidad de Aprendizaje contribuye a entender los protocolos, software y hardware que son requeridos para prevenir y supervisar acceso no autorizado o indebido a través de un sistema que afectan la integridad de la información tanto en las empresas privadas, públicas y equipos de particulares y que pueden generar afectaciones económicas, políticas, legales y sociales. Introduce al campo conceptual y procedimental, que permite al estudiante contar con una visión crítica sobre las vulnerabilidades en los sistemas informáticos ampliando su panorama para que logre visualizar los elementos de la seguridad en Sistemas, clasificación de los tipos de ataques en las redes de datos, softwares y equipos que permiten proteger la información de las empresas. Forma al estudiante con los principios básicos para proponer sistemas y equipos de seguridad y control para mantener la información debidamente resguardada.

Objetivos

Esta unidad de aprendizaje contribuye a conocer que la Auditoría informática es una entidad de conocimientos, normas, técnicas, modelos y buenas prácticas aplicadas a la evaluación y aseguramiento de la calidad, la seguridad, el razonamiento y la disponibilidad de la información, manejada y almacenada a través de sistemas de cómputo y tecnologías afines, así como también, la eficiencia, eficacia y mejorar la economía con que la gestión informática de una organización están manejando esta información así como todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Con el único propósito de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoría de alta aceptación general y un conocimiento técnico específico. Permitirá al alumno el desarrollo de habilidades y destrezas para analizar y desarrollar nuevas técnicas y procesos para el control de los recursos informáticos disponibles en las organizaciones, facilitando así la obtención de información y propicie en él, un entendimiento óptimo de conocimientos integrales para efectuar una auditoría informática, esto conlleva a un alto grado de competitividad en su futuro desempeño profesional.

Justificación

La Unidad de Aprendizaje de "Sistemas de Identificación, Autenticación y Control de Acceso" propone fortalecer en el estudiante la construcción de un ser ético y creativo a fin de que colabore en su entorno, diseñando e innovando técnicas aplicadas en las Tecnologías de Información y Comunicaciones (TIC) a partir del conocimiento de protocolos, equipos y softwares que permiten mantener la integridad de información digital de las empresas y así difundir buenas prácticas de uso y ética en el diseño de la seguridad en redes de datos.

Estructura y contenidos

SISTEMAS DE IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO

Implementa un sistema de seguridad para los procesos de identificación, autenticación y acceso de acuerdo con los estándares vigentes

UNIDAD DIDÁCTICA 1: INTRODUCCIÓN A LOS PROCESOS DE SEGURIDAD

1. Identifica los controles de seguridad físicos/ lógicos para salvaguardar la integridad de los activos de acuerdo a una organización.
   Reconoce las categorías comunes y tipos de niveles de seguridad para salvaguardar la integridad de los activos, de acuerdo a los estándares vigentes.
   CONCEPTUALES ● Introducción a los controles de seguridad. ● Conoce la definición de niveles de seguridad. ● Identifica las categorías y tipos de niveles de seguridad en activos físicos/lógicos. ● Identifica como utilizar los niveles de seguridad.
   Identifica la seguridad adecuada en procesos físicos/lógicos para aplicar el control de acceso a usuario autorizado orientado a proteger la confidencialidad e integridad de activos de acuerdo con la organización.
   CONCEPTUALES ● Conoce la definición y tipos de niveles de acceso. ● Identifica sistemas de acceso físicos/lógicos para generar las políticas y permisos de seguridad informática.

UNIDAD DIDÁCTICA 2: PROCEDIMIENTOS PARA LA AUTENTICACIÓN Y AUTORIZACIÓN

2. Implementa procedimientos necesarios para su correcta autenticación y autorización de acuerdo con los estándares vigentes.
   Conoce la implementación, mantenimiento y mejora de procedimientos para la seguridad de autenticación y autorización de acuerdo con los estándares vigentes. CONCEPTUALES ● Conoce diferentes procedimientos y mecanismos de seguridad que se implementan. ● Identifica procedimientos de autenticación, autorización y control. ● Conoce tipos de sistemas biométricos.
   Implementa un procedimiento sobre autenticación y control en la seguridad de los activos de acuerdo con los estándares vigentes.
   CONCEPTUALES • Identifica tipos de autenticación y control más utilizados en la actualidad y de acuerdo con los estándares vigentes.

UNIDAD DIDÁCTICA 3: PROTOCOLOS DE AUTENTICACIÓN Y CONTROLES DE ACCESO

3. Emplea diferentes protocolos estándar abierto, que permite la autenticación segura para brindar la protección necesaria a los activos de acuerdo con la organización.
   Diseña un protocolo para implementar la seguridad de un activo, haciendo uso de los diferentes estándares vigentes.

CONCEPTUALES Conoce diferentes protocolos tales como: ● OAuth, Oauth2 ● OpenID Connect ● SAML ● Kerberos ● Radius
Implementa un protocolo de identificación y acceso, para la seguridad de un activo, con base en las normas y estándares de control de la organización.
CONCEPTUALES • Conoce y analiza procedimientos actuales en la aplicación de un protocolo.

Evaluación

Sin valor.

Materiales para la elaboración de la guía

Computadoras personales.

Recursos Adicionales

- **Libros: Textos especializados en seguridad de la información, autenticación y autorización.**
- **Artículos: Publicaciones académicas y profesionales sobre el tema.**
- **Software: Herramientas de seguridad, simuladores de ataques.**
- **Plataformas en línea: Cursos en línea y comunidades de práctica.**

Actividades de estudio

Esta guía tiene como objetivo proporcionar una base sólida en los conceptos y prácticas de seguridad relacionadas con la identificación, autenticación y control de acceso. Al finalizar el curso, los estudiantes serán capaces de implementar sistemas de seguridad robustos y eficaces para proteger los activos de una organización.

Unidad Didáctica 1: Introducción a los Controles de Seguridad

- **Conceptos básicos: Seguridad de la información, activos, amenazas, vulnerabilidades.**
- **Controles de seguridad: Físicos (cerraduras, alarmas), lógicos (firewalls, contraseñas), administrativos (políticas, procedimientos).**
- **Niveles de seguridad: Bajo, medio, alto.**
- **Principios de seguridad: Confidencialidad, integridad, disponibilidad.**
- **Control de acceso: Concepto, importancia y tipos (físico, lógico, discrecional, mandatorio).**

Unidad Didáctica 2: Procedimientos para la Autenticación y Autorización

- **Autenticación: Proceso de verificar la identidad de un usuario.**
- **Autorización: Proceso de determinar los permisos de acceso de un usuario autenticado.**
- **Métodos de autenticación: Contraseñas, tokens, biometría, multifactor.**
- **Gestión de identidades y accesos (IAM): Concepto y componentes.**
- **Mejores prácticas: Recomendaciones para implementar sistemas de autenticación y autorización seguros.**

Unidad Didáctica 3: Protocolos de Autenticación y Control de Acceso

- **Protocolos estándares: OAuth, OpenID Connect, SAML, Kerberos, RADIUS.**
- **Comparación de protocolos: Características, ventajas y desventajas.**
- **Implementación: Cómo configurar y utilizar estos protocolos en diferentes entornos.**
- **Consideraciones de seguridad: Riesgos y amenazas asociados a cada protocolo.**

Actividades de Aprendizaje

- **Investigación: Realizar investigaciones sobre temas específicos de seguridad, como ataques cibernéticos, vulnerabilidades y mejores prácticas.**
- **Análisis de casos: Estudiar casos reales de incidentes de seguridad y analizar las causas y consecuencias.**
- **Simulaciones: Participar en simulaciones de ataques cibernéticos para comprender las técnicas utilizadas por los atacantes.**

Laboratorios: Configurar y probar diferentes sistemas de autenticación y autorización.

- **Elaboración de informes: Redactar informes sobre los resultados de las actividades realizadas.**

Evaluación

- **Examenes escritos: Preguntas teóricas y prácticas sobre los contenidos del curso.**
- **Trabajos prácticos: Desarrollo de proyectos de implementación de sistemas de seguridad.**

Información adicional

NINGUNA

Bibliografía básica

niveles de seguridad unidad 1 https://blog.mdcloud.es/niveles-de-seguridad-que-son-y-su-importancia-en-la-empresa/ tipos de niveles unidad 1 https://www.ceac.es/blog/tipos-de-seguridad-informatica como se utilizan los niveles de seguridad unidad 1 https://blog.mdcloud.es/niveles-de-seguridad-que-son-y-su-importancia-en-la-empresa/ https://www.ibm.com/docs/es/i/7.2?topic=authority-security-levels

diferentes procedimientos y mecanismos de seguridad unidad 2 https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/

OAuth, OAuth2 (Hawai, 2020) OpenID (OpenID, 2020) SAML (guevara, 2021) Kerberos (Kerberos, 2021) Radias (Help, 2018)

Integrantes de la academia

GODELINDA MELGOZA PONCE.