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

SISTEMAS DE IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO

Semestre 2026-2

TURNO VESPERTINO

Integrantes de la academia: Alfredo Campos Guerrero

Fecha de Elaboración: 13/05/2026

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	Sistemas de identificación, autenticación y Control de acceso	**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:

Esta Unidad de Aprendizaje (**UA**) prepara al estudiante al campo conceptual, procedimental y actitudinal para el desarrollo de multimedia y Ambientes Virtuales que requiere la Industria. El estudiante al adquirir estas destrezas y habilidades relacionadas con el pensamiento eficaz favorecerán en él para el desarrollo de una visión crítica y holística, cuya puesta en práctica sea de forma autónoma. En el futuro le contribuirá a responder en forma eficiente y eficaz a los retos que se le presenten en la continuidad de sus estudios de nivel Superior y en su incorporación en la Industria. organización

Objetivos

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

- Esta Unidad de Aprendizaje contribuye a entender los protocolos, software y hardware que son requeridos para prevenir y supervisar acceso no autorizado
- Construir Sistemas de Control de Acceso que utilice medios electrónicos y digitales

Justificación

Las competencias profesionales (generales y particulares) implican como principales objetos de conocimiento los sistemas de acceso, identificación y control de acceso, que podrá vincular con su entorno socioeconómico y laboral. Asimismo, en la particularidad del estudiante:

- Diseño y construcción de Sistemas de Control de acceso, identificación y autenticación.
- Pruebas de control de acceso a sistemas informáticos

Estructura y contenidos

1. Identifica los controles de seguridad físicos/ lógicos para salvaguardar la integridad de los activos de acuerdo a una organización.

1.1 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

1.2 Conoce la definición y tipos de niveles de acceso.

- Identifica sistemas de acceso físicos/lógicos para generar las políticas y permisos de seguridad informática

2. Implementa procedimientos necesarios para su correcta autenticación y autorización de acuerdo con los estándares vigentes

2.1 Conoce diferentes procedimientos y mecanismos de seguridad que se implementan.

- Identifica procedimientos de autenticación, autorización y control.
- Conoce tipos de sistemas biométricos.

2.2. Identifica tipos de autenticación y control más utilizados en la actualidad y de acuerdo con los estándares vigentes.

3. Emplea diferentes protocolos estándar abierto, que permite la autenticación segura para brindar la protección necesaria a los activos de acuerdo con la organización.

3.1 Conoce diferentes protocolos tales como:

- OAuth, Oauth2
- OpenID Connect
- SAML
- Kerberos
- RADIUS.

3.2 Conoce y analiza procedimientos actuales en la aplicación de un protocolo

Materiales para la elaboración de la guía

No Aplica

Actividades de estudio

- Elabora esquema de la categoría y nivel de seguridad físicos/lógicos de los activos, y las medidas a tomar.
- Genera un plan de políticas de seguridad informática, con niveles de acceso, que permita mantener los activos salvaguardados de una organización.
- Genera un organizador gráfico donde muestra la estructura de los procedimientos, su implementación, mantenimiento y mejora de los procesos de autenticación y autorización.
- Documenta la implementación de un sistema haciendo uso de los protocolos que permita una identificación segura para brindar protección necesaria a los activos.

EJERCICIOS PRÁCTICOS:

Ejercicio. Sistema de Control de Acceso en una Red WiFi
Por medio del software de Cisco Packet Tracer realizar una configuración con un Access Point y un equipo laptop y proporcionales el acceso a la red Wifi con autenticación WPA2 Personal o Enterprise.

Ejercicio. Elaboración de un esquema de seguridad para una empresa

1. Identifica y da ejemplos de activos físicos en una empresa
2. Identifica y da ejemplos de activos lógicos en una empresa
3. Identifica y da ejemplos de dispositivos de red
4. Identifica y da ejemplos de dispositivos de red que proporcionan la seguridad a la red.

Ejercicio. Con el material de Arduino y el código proporcionado por el profesor realizar el circuito que se indique en el examen

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/
- Diferentes procedimientos y mecanismos de seguridad unidad 2 https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/ Identifica procedimientos de autenticación, autorización y control unidad 2 http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/mecanismos_bsicos_de_seguridad.html
- Tipos de sistemas biométricos unidad 2 https://recfaces.com/es/articles/tipos-de-identificacion-biometrica
- Tipos de autenticación y control más utilizados en la actualidad unidad 2 https://www.evidian.com/pdf/wp-strongauth-es.pdf http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp