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
## MODELOS DE SEGURIDAD DE LA INFORMACIÓN
## Semestre 2026-2
## TURNO MATUTINO

**Integrantes de la academia:** María de Lourdes Garcés Vanegas

**Fecha de Elaboración:** __11/mayo/26

# FORMATO DE LA GUÍA DE ESTUDIO

| Área: | Nombre de la Unidad de Aprendizaje: | Nivel/semestre: |
|---|---|---|
| **Tecnológica** | **MODELOS DE SEGURIDAD DE LA INFORMACIÓN** | **Medio/QUINTO** |

## Instrucciones generales de la guía:

**Esta guía está diseñada para ayudar a los estudiantes a prepararse para el examen ETS de la Unidad de Aprendizaje Modelos de Seguridad de la Información. Siga estas instrucciones para aprovechar al máximo el contenido:**

1. **Estudie cada sección detenidamente: La guía está organizada en conceptos clave, preguntas de opción múltiple, casos prácticos y recomendaciones.**
2. **Resuelva las preguntas de opción múltiple: Utilice estas preguntas para autoevaluarse.**
3. **Analice los casos prácticos: Desarrolle respuestas detalladas y justificadas para cada situación.**
4. **Utilice recursos complementarios: Consulte libros, artículos y sitios web recomendados para ampliar su comprensión.**
5. **Practique en equipo: Estudiar en grupos puede ayudar a discutir y aclarar conceptos complejos.**
6. **Gestione su tiempo: Dedique suficiente tiempo a cada sección para comprender los temas en profundidad.**

## Presentación:

Esta guía está diseñada para ayudar a los estudiantes a prepararse para el examen ETS de la Unidad de Aprendizaje Modelos de Seguridad de la Información. Incluye conceptos clave, preguntas de opción múltiple, casos prácticos y recomendaciones para comprender mejor los temas centrales del programa de estudios.

## Objetivos

Esta Unidad de Aprendizaje contribuye a conocer los modelos de la seguridad de la información para su implementación y gestión en las organizaciones, aplicando las normas, técnicas y estándares nacionales e internacionales, así como mantener actualizadas las tecnologías de la información y comunicación. Introduce al estudiante para que cuente con una visión de los modelos para tomar responsablemente decisiones sobre qué normas, estándares o técnicas aplicar de acuerdo a las formas y usos que se esté aplicando en la organización

## Justificación

La presente guía de estudio está diseñada para proporcionar a los estudiantes un recurso completo y estructurado que les permita prepararse adecuadamente para el examen ETS de la Unidad de Aprendizaje Modelos de Seguridad de la Información. Esta guía combina conceptos teóricos, ejercicios prácticos y preguntas de opción múltiple, enfocándose en las competencias clave establecidas en el programa oficial.

El objetivo principal es desarrollar habilidades de análisis, comprensión y aplicación en temas relacionados con la gestión de la seguridad de la información, los modelos de seguridad y los procesos de implementación en contextos organizacionales. La guía permite a los estudiantes reforzar sus conocimientos y desarrollar una visión integral para enfrentar con éxito el examen..

## Estructura y contenidos

- **Conceptos Clave**
- **Preguntas de Opción Múltiple**
- **Casos Prácticos**
- **Recomendaciones de Estudio**

## Evaluación

**Sin valor.**

## Materiales para la elaboración de la guía

- Computadora o dispositivo móvil: Para acceder a recursos en línea y realizar investigaciones.
- Manuales y guías de seguridad informática: Incluyendo estándares como ISO 27001, COBIT e ITIL.
- Libros de texto recomendados: Relacionados con seguridad de la información.
- Acceso a Internet: Para investigaciones y consultas en bases de datos académicas.
- Cuaderno y bolígrafos: Para realizar anotaciones y esquemas.

## Actividades de estudio

### I. Conceptos Clave

Unidad 1: Seguridad de la Información

- Seguridad de la Información: Protección de datos contra acceso no autorizado.
- Confidencialidad, Integridad y Disponibilidad (CID): Principios fundamentales de la seguridad de la información.
- Malware: Software malicioso (virus, troyanos, ransomware).
- Hackers: Actores que buscan explotar vulnerabilidades.

Unidad 2: Modelos de la Seguridad de la Información

- Política de Seguridad: Normas y procedimientos para proteger los datos.
- Modelos de Seguridad:
- BLP (Bell-Lapadula): Controla el acceso basado en la confidencialidad.
- TG (Take GranT): Gestión de permisos y privilegios.
- ISO 27001, COBIT e ITIL: Estándares y marcos de trabajo.

Unidad 3: Diseño y Análisis de los Modelos de Seguridad

- Gestión de la Seguridad: Incluye estrategias, procesos y métricas. Procesos de Implementación: Planificación y aplicación de modelos según normas vigentes.

## II. Preguntas de Opción Múltiple

1. ¿Qué representa la integridad en la seguridad de la información?

A) Protección frente a usuarios externos

B) Evitar la modificación no autorizada de los datos (Correcta)

C) Garantizar el acceso a los datos las 24 horas

D) Proteger el equipo físico

2. ¿Qué modelo se centra en el control de acceso basado en niveles de confidencialidad?

A) Modelo TG (Take GranT)

B) Modelo BLP (Bell-Lapadula) (Correcta)

C) ISO 27001

D) COBIT

3. ¿Cuál es un ejemplo de malware?

A) Contraseña segura

B) Firewalls

C) Virus informático (Correcta)

D) Políticas de acceso

4. ¿Qué principio se ve comprometido en un ataque de denegación de servicio (DoS)?

A) Confidencialidad

B) Integridad

C) Disponibilidad (Correcta)

D) Privacidad

5. ¿Qué estándar se utiliza para la gestión de la seguridad de la información?

A) ISO 27001 (Correcta)

B) GDPR

C) ITIL

D) COBIT

6. ¿Qué acción corresponde a la gestión de la seguridad?

A) Monitorear redes sociales

B) Definir estrategias y métricas de seguridad (Correcta)

C) Eliminar antivirus

D) Compartir datos sin control

7. ¿Qué modelo gestiona permisos y privilegios de acceso?

A) BLP (Bell-Lapadula)

B) TG (Take GranT) (Correcta)

C) Clark-Wilson

D) Matriz de accesos

8. ¿Qué principio de seguridad asegura que solo usuarios autorizados accedan a la información?

A) Disponibilidad

B) Confidencialidad (Correcta)

C) Integridad

D) Autenticación

9. ¿Qué estándar define buenas prácticas de gestión de servicios de TI?

A) COBIT

B) ITIL (Correcta)

C) ISO 9001

D) GDPR

10. ¿Qué tipo de ataque implica el robo de datos mediante engaño a usuarios?

A) Phishing (Correcta)

B) Ransomware

C) DoS

D) Keylogger

11. ¿Qué técnica garantiza la disponibilidad de datos en caso de fallo del sistema?

A) Cifrado de datos

B) Realización de copias de seguridad (Correcta)

C) Control de acceso

D) Uso de firewalls

12. ¿Qué significa implementar una política de seguridad en una empresa?

A) Eliminar datos confidenciales

B) Definir reglas y procedimientos de protección (Correcta)

C) Dar acceso a todos los empleados

D) Desactivar sistemas de seguridad

13. ¿Qué tipo de malware bloquea el acceso a los datos hasta recibir un pago?

A) Spyware

B) Ransomware (Correcta)

C) Adware

D) Keylogger

14. ¿Qué técnica permite verificar si los datos han sido alterados?

A) Uso de firewalls

B) Control de accesos

C) Cifrado de datos

D) Hashing (Correcta)

15. ¿Cuál es el objetivo principal de la gestión de seguridad en una organización?

A) Desarrollar software

B) Proteger los activos informáticos (Correcta)

C) Aumentar el número de usuarios

D) Compartir información con terceros

**III. Casos Prácticos**

Caso 1: Implementación de un Modelo de Seguridad

Una empresa de desarrollo de software necesita proteger sus datos confidenciales. Deben seleccionar un modelo de seguridad adecuado y justificar su elección.

- Tareas:
  - Identificar amenazas principales.
  - Seleccionar un modelo (BLP o TG).

- Justificar su elección y describir la implementación.

Caso 2: Análisis de un Ataque Informático

Una universidad detectó un ataque de malware que afectó la disponibilidad de sus servicios de TI.

- Tareas:
  - Identificar el tipo de malware.
  - Explicar el principio afectado (CID).
  - Proponer soluciones para prevenir futuros ataques.

Caso 3: Diseño de una Política de Seguridad

- Una empresa quiere crear una política de seguridad para proteger su red interna.
- Tareas:
  - Establecer los objetivos de la política.
  - Incluir normas de acceso y control de datos.
  - Proponer medidas de seguridad técnicas y administrativas.

Información Adicional

- Revisar Conceptos Clave: Asegúrate de comprender los términos técnicos.
- Practicar Preguntas: Resuelve preguntas de opción múltiple.
- Estudiar Casos Prácticos: Desarrolla respuestas detalladas y justificadas.
- Usar Recursos Digitales: Consulta materiales en línea y manuales de seguridad.

## Bibliografía Básica


- Arturo Cuellar Feradez, 2015, Seguridad Integral dela Empresa, México, Trillas
- Alvaro Gómez Vieites, 2014. Enciclopedia de la Seguridad Informática, Espala RA MA
- Becerra., L. C.(2019). Diseño de un modelo de seguridad informática a una empresa en sus sitemas de monitoreo del área de tencnología. Colobia: Tesis


Normativas y Estándares

- Norma ISO/IEC 27001 - Sistema de gestión de la seguridad de la información.
- COBIT 2019 - Marco para la gestión de TI.
- ITIL 4 - Gestión de servicios de TI.

Recursos Digitales

- Sitio Web de la ISO - https://www.iso.org
- NIST Cybersecurity Framework - https://www.nist.gov
- Artículos y Publicaciones Académicas - Google Scholar, IEEE Xplore.