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	**SISTEMAS DE BASES DE DATOS Y DE RESPALDO DE 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 Modelos de Seguridad de la Información. Siga estas instrucciones para aprovechar al máximo el contenido:

1. **Lee con atención y comprende los modelos de seguridad.**
2. **Resuelve casos prácticos aplicando la teoría de las unidades.**
3. **Vincula los conceptos de las tres unidades del programa.**
4. **Consulta las referencias bibliográficas oficiales en formato APA.**
5. **Autoevalúate honestamente para identificar y reforzar tus debilidades.**

Presentación:

Esta guía está diseñada para ayudar a los estudiantes a prepararse para el examen ETS de la Unidad de Aprendizaje para evaluar los conocimientos, habilidades y actitudes relacionados con las Modelos de Seguridad de la información

Objetivos:

Proporcionar los conceptos clave y casos prácticos de las tres unidades para que el alumno desarrolle las competencias necesarias y acredite exitosamente el examen ETS.

Justificación:

Esta guía responde a la necesidad de regularizar a los estudiantes que no acreditaron la unidad, estructurando los temas de forma sencilla para asegurar que comprendan la aplicación real de los modelos de seguridad.

Estructura y contenidos

- **Conceptos Clave**
- **Casos Prácticos**
- **Recomendaciones de Estudio**

Evaluación

Sin valor.

Materiales para la elaboración de la guía

- Computadoras personales.
- Internet.
- Plataformas educativas.
- Recursos Didácticos:

Actividades de estudio

Unidad 1 - Seguridad de la Información

1. El Concepto y la Importancia de la Seguridad

La seguridad de la información no es solo un tema técnico, sino una necesidad vital tanto en el ámbito empresarial como en el público.

- **¿Qué es la Seguridad?** Se define como el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información.
- **Información en Informática:** Es el activo más valioso de una organización. Se debe distinguir entre el "dato" (materia prima) y la "información" (datos procesados con significado).
- **Clasificación de la Información:** No toda la información tiene el mismo valor. Las empresas suelen clasificarla para saber cuánto invertir en su protección (ej. Pública, Interna, Confidencial, Secreta).

2. Los Tres Pilares: La Tríada CIA

Este es el concepto más importante de la unidad. Los objetivos fundamentales de la seguridad de la información son tres:

1. **Confidencialidad:** Garantizar que la información sea accesible solo para aquellas personas autorizadas a tener acceso.
2. **Integridad:** Mantener la exactitud y completitud de la información y los métodos de procesamiento. Es decir, que los datos no sean modificados de forma no autorizada.
3. **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los activos relacionados cuando lo requieran.

3. Seguridad de la Información vs. Ciberseguridad

Un error común en el examen es confundir estos términos. Aquí la diferencia clave:

- **Seguridad de la Información:** Es el concepto general. Protege la información en **cualquier formato** (papel, digital, verbal, etc.).
- **Ciberseguridad:** Es una parte de la anterior. Se enfoca específicamente en proteger la información en **formato digital** y los sistemas/redes que la procesan y almacenan.

4. Evolución de las Amenazas: Historia, Malware y Hackers

Para entender el presente, hay que conocer el pasado de las vulnerabilidades

Historia: La seguridad ha evolucionado de proteger documentos físicos a proteger infraestructuras críticas en la nube.

- **Malware:** Software malicioso diseñado para infiltrarse o dañar un sistema (virus, troyanos, ransomware, etc.).
- **Hackers:** El estudio de sus perfiles permite entender las motivaciones de los ataques. En este nivel, se analizan como actores que identifican y explotan vulnerabilidades.

5. Ética y Sociedad Digital (Práctica 1)

En la actualidad, la seguridad no solo depende de software, sino de los **valores y la ética** de las personas.

- **Tecnologías Emergentes:** La innovación constante (IA, IoT, Blockchain) genera nuevas oportunidades pero también nuevas vulnerabilidades que deben ser analizadas.
- **Impacto Organizacional:** Una falla en la seguridad de la información puede destruir la reputación de una empresa y afectar su estructura socioeconómica.

PREGUNTAS:
Si un empleado borra por error una base de datos de la que no hay respaldo, ¿qué pilar de la tríada se vio afectado? (Respuesta: Disponibilidad e Integridad).

¿Por qué un archivo en papel guardado en una caja fuerte es "Seguridad de la Información" pero NO es "Ciberseguridad"?

Menciona tres criterios para clasificar la información en una empresa pequeña (ej. Nóminas, Datos de clientes, Recetas de cocina).

Unidad 2 - Modelos de la Seguridad de la Información

1. Importancia y Gestión de los Modelos

Un modelo de seguridad es un esquema teórico que ayuda a las organizaciones a implementar políticas de seguridad de manera estructurada.

- **Política de Seguridad:** Es el conjunto de reglas y normas que dictan cómo se gestionan y protegen los activos de información.
- **Alineación Estratégica:** La seguridad no es aislada; los procesos de control deben garantizar que las Tecnologías de la Información (TI) soporten los objetivos y estrategias de la organización.
- **Gestión de Protocolos:** Implica validar, definir y distribuir las normas técnicas que rigen el comportamiento de los sistemas dentro de la empresa.

2. Modelos de Seguridad Vigentes

A. Modelos de Confidencialidad e Integridad

- **Bell-Lapadula (BLP):** Su objetivo principal es la **Confidencialidad**. Se basa en reglas estrictas para evitar que la información clasificada "se filtre" hacia niveles inferiores (ej. "No leer hacia arriba" y "No escribir hacia abajo").
- **Clark-Wilson (CW):** Su objetivo principal es la **Integridad** de los datos. Se enfoca en que la información no sea modificada de forma malintencionada o accidental, utilizando la separación de obligaciones.

B. Otros Modelos de Control de Acceso

- **Matriz de Accesos:** Una tabla que define qué derechos (leer, escribir, ejecutar) tiene cada sujeto (usuario) sobre cada objeto (archivo/sistema).
- **Take-Grant (TG):** Analiza cómo se pueden transferir o quitar permisos de acceso entre usuarios mediante reglas de "tomar" y "conceder".
- **Harrison, Ruzzo y Ullman (HRU):** Estudia si es posible determinar si un sistema de acceso es "seguro" mediante operaciones elementales en la matriz de accesos.
- **Graham-Denning (GD):** Se centra en cómo se crean y eliminan de forma segura los sujetos y objetos, y cómo se asignan sus derechos iniciales.

3. Estándares y Marcos de Referencia (Governance)

Para que los modelos funcionen en el mundo real, se utilizan estándares internacionales:

1. **ISO 27001:** Es la norma internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).
2. **COBIT:** Marco de referencia para el **Gobierno y Gestión de las TI** empresariales.
3. **ITIL:** Se enfoca en la **Gestión de Servicios de TI** para asegurar que los servicios (incluyendo la seguridad) se entreguen con calidad.
4. **ISM3:** Un modelo de madurez que ayuda a medir qué tan robusta es la seguridad de una organización en comparación con sus objetivos.

• Pregunta de Análisis: Una empresa militar necesita que sus soldados no puedan ver documentos de generales, pero los generales sí deben ver lo de los soldados. ¿Qué modelo aplicarías?

• Respuesta sugerida: Bell-Lapadula, porque su prioridad es la confidencialidad y el control de flujo de información por niveles jerárquicos.

• Diferenciación: Explica la diferencia entre un modelo (como BLP) y un estándar (como ISO 27001).

• Respuesta sugerida: El modelo es la teoría matemática/lógica de cómo se permite el acceso; el estándar es la guía práctica y administrativa de cómo gestionar toda la seguridad en la empresa.

• Relación con el Negocio: ¿Por qué es importante que las TI soporten las estrategias organizacionales?.

Haz un cuadro comparativo de los modelos (BLP, TG, CW, HRU) anotando su objetivo principal (Confidencialidad vs. Integridad)

Unidad 3 - Diseño y Aplicación de Modelos

1. Función de la Seguridad en la Organización (Estrategia y Gestión)

En esta etapa, la seguridad deja de ser solo "configurar equipos" y se convierte en una función de gestión. Debes comprender cómo la seguridad ayuda a que la empresa cumpla sus objetivos.

Estrategias de Seguridad: Son los planes de alto nivel que definen cómo la organización protegerá sus activos a largo plazo.

Procesos de Seguridad: Son las series de pasos repetibles (como el control de acceso o la gestión de respaldos) que ejecutan la estrategia día a día.

Métricas de Seguridad: Son indicadores numéricos que permiten medir si los controles están funcionando (ej. "Número de intentos de acceso fallidos" o "Tiempo de recuperación tras una falla").

2. Modelos de Implementación Clave

A. Modelo Take-Grant (TG)

Este modelo se utiliza para analizar cómo se pueden transferir o ganar derechos de acceso en un sistema.

Concepto clave: Se visualiza como un grafo donde los nodos son sujetos/objetos y las flechas son los permisos.

Reglas principales:

Take (Tomar): Un sujeto puede "tomar" los derechos de otro objeto si tiene el permiso adecuado.

Grant (Conceder): Un sujeto puede "conceder" sus propios derechos a otro sujeto.

Aplicación práctica: Sirve para detectar si un usuario podría llegar a obtener permisos que no debería tener mediante una cadena de transferencias.

B. Modelo Bell-Lapadula (BLP) - Repaso de Aplicación

- Aunque se ve en la Unidad 2, en la Unidad 3 se debe saber implementar.
- Enfoque: Seguridad multinivel (Confidencialidad).
- Regla de Oro: "No leer hacia arriba" (No read up) y "No escribir hacia abajo" (No write down).
- Planificación e Implementación del Proceso

Realiza lo siguiente:

1. Definición de Requisitos: Identificar qué necesita proteger la empresa (activos críticos).
2. Selección del Modelo: Elegir si se necesita BLP (confidencialidad) o TG (gestión de permisos) según el giro de la empresa.
3. Calendario de Planificación: Definir fechas y responsables para instalar y configurar los controles.
4. Gestión de Recursos: Determinar qué hardware, software y personal se requiere.
5. Análisis de Pros y Contras: Documentar qué beneficios trae el modelo y qué dificultades de operación podría generar.

Escenario: Una aplicación bancaria necesita asegurar que un cajero no pueda otorgarse a sí mismo permisos de gerente para autorizar créditos.

¿Qué modelo usarías? El modelo Take-Grant (TG) para analizar el flujo de permisos y evitar que se "tomen" facultades no autorizadas.

¿Cuál sería el proceso? Implementar una Matriz de Accesos donde se definan roles estrictos y se auditen periódicamente los derechos concedidos.

CASO PRÁCTICO

La empresa "Salud Digital S.A." es una startup que ha desarrollado una plataforma donde pacientes, médicos y laboratorios comparten información médica sensible (recetas, diagnósticos y estudios). La empresa está creciendo y necesita formalizar su seguridad para cumplir con la ley y proteger su reputación.

1. Identificación de Activos: Identifica el activo de información más valioso de la empresa.

2. Análisis de la Tríada CIA: Explica qué pilar (Confidencialidad, Integridad o Disponibilidad) se ve afectado en los dos problemas mencionados (el correo sospechoso y el acceso de los recepcionistas).

3. Ciberseguridad vs. Seguridad de la Información: Si un médico deja un expediente de papel sobre el escritorio y un extraño lo lee, ¿esto es un problema de Ciberseguridad o de Seguridad de la Información? Justifica.

El Director de TI decide que para proteger los expedientes médicos se deben aplicar reglas matemáticas y lógicas estrictas. Se requiere que:

Nadie pueda "leer hacia arriba" (un médico general no debe leer casos de alta especialidad si no tiene el nivel).

La información de las recetas no sea alterada por personas no autorizadas (Integridad).

1. Modelo de Confidencialidad: Si la prioridad es evitar filtraciones por niveles jerárquicos, ¿qué modelo es más adecuado: Bell-LaPadula o Take-Grant? Explica la regla de "No leer hacia arriba".

2. Modelo de Integridad: Para asegurar que los diagnósticos solo sean modificados mediante procedimientos autorizados y por las personas correctas, explica cómo se aplicaría el Modelo de Clark-Wilson.

3. Estándares: Menciona qué norma internacional (ISO 27001, COBIT o ITIL) debería usar la empresa para certificar que tiene un Sistema de Gestión de Seguridad sólido.

Diseño e Implementación (Unidad 3)

Situación: Ya se eligieron los modelos. Ahora hay que planificar cómo se van a ejecutar en la vida real para que la empresa pueda operar sin riesgos y sea eficiente.

Tareas:

Diseño del Proceso: Diseña un Proceso de Control de Acceso para un nuevo médico que entra a la empresa. ¿Quién autoriza, quién da la clave y cómo se verifica que solo vea lo que le corresponde?

Modelo Take-Grant en la práctica: Dibuja o explica un pequeño grafo donde un "Médico A" le otorga (Grant) permiso de "Lectura" a un "Especialista B" sobre el "Expediente X".

Métricas y Alineación:

Propón una métrica para saber si el modelo de seguridad está funcionando (Ej. número de accesos denegados).

Explica cómo esta seguridad ayuda a que la empresa gane más dinero o sea más exitosa (Alineación con el negocio).

Información Adicional

- **Practica:** Desarrolla pequeñas bases de datos y aplica la jerarquía de control y la jerarquía de seguridad considera los comandos de control de acceso
- **Investiga:** Consulta tutoriales, documentación oficial y ejemplos.
- **Simula el Examen:** Resuelve ejercicios prácticos relacionados con cada unidad.

¡Éxito en tu examen de ETS!

Bibliografía Básica

Centro Criptológico Nacional. (s.f.). Esquema Nacional de Seguridad (ENS). CCN-CERT. https://www.ccn-cert.cener.es/ens.html

Miranda Cairo, M., y Vega, O. (2016). Metodología para la Gestión de la Seguridad de la Información. Instituciones SLD. https://instituciones.sld.cu/files/2013/08/Metodologiasparalagestiondelaseguridaddelainformacion.pdf

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001). https://www.iso.org/standard/27001

ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. https://www.isaca.org/resources/cobit