INTRODUCCIÓN – CONCEPTOS

Seguridad vs **Riesgo**

Factores que influyen: **Amenaza** **Vulnerabilidad** **Valor del bien**

Amenaza vs **Vulnerabilidad**

Servicios que ofrece la seguridad informática – ¿Para qué sirve la seguridad informática?

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Responsabilidad**

Ciberseguridad vs Seguridad informática vs Seguridad de la información

Ciberseguridad vs **Ciberataque**

Incidente de seguridad: consecuencias

Herramientas y técnicas de seguridad vs **Herramientas y técnicas de ciberataque**

Responsable de seguridad vs **Delincuente**

Hacker
Analista de seguridad

Clasificación de herramientas y técnicas de seguridad:
Físicas vs **Lógicas**
Activas vs **Pasivas**
(Potencian – mejoran - priorizan la) **Confidencialidad** vs **Responsabilidad** vs **Integridad** vs **Disponibilidad**

Aplicación – **Relación de todo esto con el Desarrollo de Aplicaciones Web**

HTTPS
SSH
SFTP
AAA
…

INCIBE

Casos reales

Salidas profesionales

EJERCICIO 1:

El anexo I de la ORDEN EDU/411/2025 establece los siguientes **contenidos** en este módulo de **Fundamentos de ciberseguridad** de 2º curso del ciclo Desarrollo de Aplicaciones Web.

Realiza un diccionario de los términos **destacados** para familiarizarte con los conceptos que vamos a estudiar a lo largo del curso.

1. **Amenazas** y **vulnerabilidades** informáticas.

    a) Introducción a las amenazas y vulnerabilidades informáticas: conceptos básicos, diferencias entre amenazas activas y pasivas y su impacto, principios de **confidencialidad**, **integridad** y **disponibilidad**.
    b) Clasificación y características de las principales amenazas informáticas: Tipos de **malware**. Técnicas de **ingeniería social**. Ataques a la red: (**DoS y DDoS**) y (**Man-in-the-Middle**). **Exploits** y ataques a aplicaciones web: **Inyección SQL** y **Cross-Site Scripting (XSS)**.
    c) Clasificación de vulnerabilidades en sistemas, redes y aplicaciones. Vulnerabilidades en sistemas operativos, aplicaciones y redes. Redes inalámbricas sin **cifrar** o con cifrados obsoletos.
    d) Relación entre amenazas y vulnerabilidades. Mecánica de explotación: identificación de vulnerabilidades por los atacantes. Uso de Exploits y herramientas automatizadas. Ejemplos prácticos de explotación: **ransomware** en sistemas desactualizados e inyección SQL.
    e) Evaluación de las consecuencias de las amenazas y vulnerabilidades. Impacto sobre la confidencialidad, la integridad y la disponibilidad.
    f) Señales y síntomas de amenazas y vulnerabilidades activas. Detección de actividad sospechosa en sistemas. Señales de actividad maliciosa en redes.

2. Medidas de protección básicas.

    a) Importancia de las configuraciones seguras en la ciberseguridad. Conceptos básicos: servicios innecesarios, actualizaciones y vulnerabilidades conocidas. Procedimientos para desactivar servicios innecesarios en sistemas operativos. Herramientas para gestionar actualizaciones y parches de seguridad.
    b) Gestión de contraseñas robustas. Características de una contraseña segura. Políticas de gestión de contraseñas. Métodos de autenticación alternativos: **autenticación Multifactor (MFA).**
    c) Control de accesos y permisos. Principios de control de acceso. Gestión de **roles** y **permisos** en sistemas operativos. Configuración de accesos en redes.
    d) Implementación de **reglas** de **firewall**. Reglas básicas para controlar el tráfico: **filtrado** de **puertos** y **protocolos** y bloqueo de tráfico no autorizado. Configuración de cortafuegos en sistemas operativos y **routers**. Verificación y pruebas de las reglas implementadas.
    e) Herramientas de **monitoreo** y **auditoría**. Importancia del monitoreo en la ciberseguridad. Métodos para analizar registros y detectar incidentes o anomalías. Automatización del monitoreo mediante herramientas específicas.
    f) Corrección de configuraciones inseguras. Identificación de configuraciones inseguras o inconsistentes. Proceso de propuesta y ejecución de mejoras. Pruebas posteriores a la corrección para validar los cambios.

g) Documentación de medidas de protección implementadas. Importancia de la documentación en la seguridad informática. Estructura recomendada para documentar configuraciones y procedimientos. Uso de plantillas para la documentación eficiente.

3. Análisis de los **incidentes de seguridad**.

a) Concepto y clasificación de los incidentes de seguridad. **Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje**. Elementos clave de un incidente: amenazas, vulnerabilidades y consecuencias.
b) Clasificación de incidentes de seguridad. Tipos de incidentes: internos, externos, dirigidos y masivos. Criterios para clasificar los incidentes: naturaleza, alcance y objetivo.
c) **Indicadores de compromiso (IoC)**. Definición y tipos de IoC: basados en red, basados en sistema y basados en registros. Métodos para identificar IoC en sistemas y redes. Relación entre IoC y las técnicas de ataque utilizadas.
d) **Estrategias proactivas** para prevenir incidentes de seguridad: configuración de firewalls y herramientas de detección de intrusos e implementación de controles de acceso y gestión de contraseñas. Justificación de las medidas propuestas.
e) Evaluación del impacto de soluciones propuestas. Análisis de mitigación de riesgos. Consideraciones de coste-beneficio en las soluciones. Viabilidad técnica y operativa de las medidas implementadas.
f) Elaboración de informes sobre incidentes. Herramientas y formatos para la redacción de informes. Buenas prácticas en la comunicación de hallazgos técnicos.
g) Conceptos básicos del **análisis forense**: recopilación de evidencias digitales y preservación de la cadena de custodia. Técnicas fundamentales de análisis forense en sistemas y redes. Principios éticos y legales en la gestión de evidencias: cumplimiento normativo y privacidad y confidencialidad.

4. Herramientas y tecnologías de aplicación.

a) Introducción a las herramientas de ciberseguridad. Concepto y tipos. Funciones principales de **cortafuegos**, **IDS/IPS**, y software **antivirus**. Importancia de la configuración adecuada para la protección de sistemas.
b) Cortafuegos (firewalls). Tipos de **cortafuegos: basados en red y cortafuegos basados en host**. Instalación de cortafuegos: configuración básica y configuración avanzada. Pruebas funcionales.
c) Sistemas de detección y prevención de intrusos (IDS/IPS). Diferencias entre **IDS** y **IPS**. Instalación de IDS/IPS. Configuración de parámetros básicos. Ajustes avanzados. Verificación del funcionamiento.
d) Software **antivirus** y **antimalware**. Funciones y tipos de software antivirus. Instalación de software antivirus. Configuración inicial. Actualización de bases de datos y software. Validación del software antivirus: pruebas de detección y generación de informes.
e) Optimización de configuraciones y compatibilidad. Integración de herramientas de ciberseguridad con sistemas operativos y redes. Ajuste de configuraciones para maximizar el rendimiento. Resolución de conflictos entre herramientas y sistemas existentes.
f) Pruebas de efectividad de las herramientas configuradas. Métodos para simular escenarios de ataque. Evaluación de la respuesta de las herramientas ante amenazas simuladas. Identificación y resolución de configuraciones ineficientes o erróneas.

g) Documentación del proceso de configuración. Elementos básicos de la documentación técnica. Uso de plantillas para registrar procedimientos de instalación y configuración. Recomendaciones de mantenimiento y actualización.

5. Normativa y buenas prácticas de uso.

a) Concepto y objetivos de la seguridad de la información. Principios fundamentales: confidencialidad, integridad y disponibilidad. Importancia del cumplimiento normativo y las buenas prácticas en entornos profesionales.
b) Normativas y estándares internacionales en ciberseguridad. **Reglamento General de Protección de Datos (RGPD)**. **ISO/IEC 27001**. **Esquema Nacional de Seguridad (ENS)**.
c) Buenas prácticas en la gestión de la seguridad de la información. Clasificación de **datos sensibles**. Definición de **políticas de acceso**. Gestión del **ciclo de vida de la información**.
d) Evaluación de medidas de seguridad en escenarios prácticos. Análisis de casos. Uso de herramientas de auditoría. **Diagnóstico de fallos**. **Propuestas de mejora**.
e) Gestión de riesgos y mejora continua. Identificación de riesgos. Evaluación de riesgos. Desarrollo de planes de acción. Importancia de la revisión y actualización de las políticas de seguridad.
f) Documentación de la gestión de la seguridad de la información. Elaboración de procedimientos y políticas. **Registro de incidencias** y cumplimiento normativo. Uso de plantillas y formatos estándares para la documentación. Comunicación efectiva de las políticas y procedimientos a los usuarios.