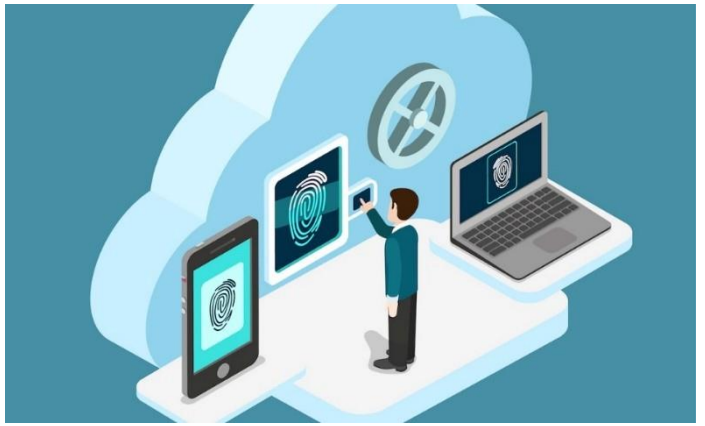
GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPCV
Formació Professional Comunitat Valenciana

M1 - Introducción y Legalidad en el Hacking Ético.

Objetivo: Proporcionar una visión general sobre la seguridad, identificar amenazas críticas (OWASP Top Ten) y conocer normativas relevantes.

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

¿Qué es la Ciberseguridad?



"protección de los activos de información frente a las amenazas procesada, almacenada y transportada por los sistemas de información interconectados" *ISACA*

Conocer los factores de negocio y las tecnologías que afecten a la seguridad de la información.

- ❑ Los planes de negocio y el entorno empresarial.
- ❑ La tecnología de la información disponible en la entidad.

https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Diferencias entre Seguridad de la información y Ciberseguridad

La **Ciberseguridad** es parte de la seguridad de la información.

Se refiere a la protección de **activos digitales** (información, hardware y redes), mientras que en la **seguridad de la información,** se incluye tanto **activos digitales,** como **activos en papel.**

5 funciones claves necesarias para la protección de activos digitales:

- ❑ **Identificar**
- ❑ **Proteger**
- ❑ **Detectar**
- ❑ **Responder**
- ❑ **Recuperar**

https://www.nist.gov/
https://www.enisa.europa.eu/

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Conceptos Clave de Seguridad Informática (S.I.)

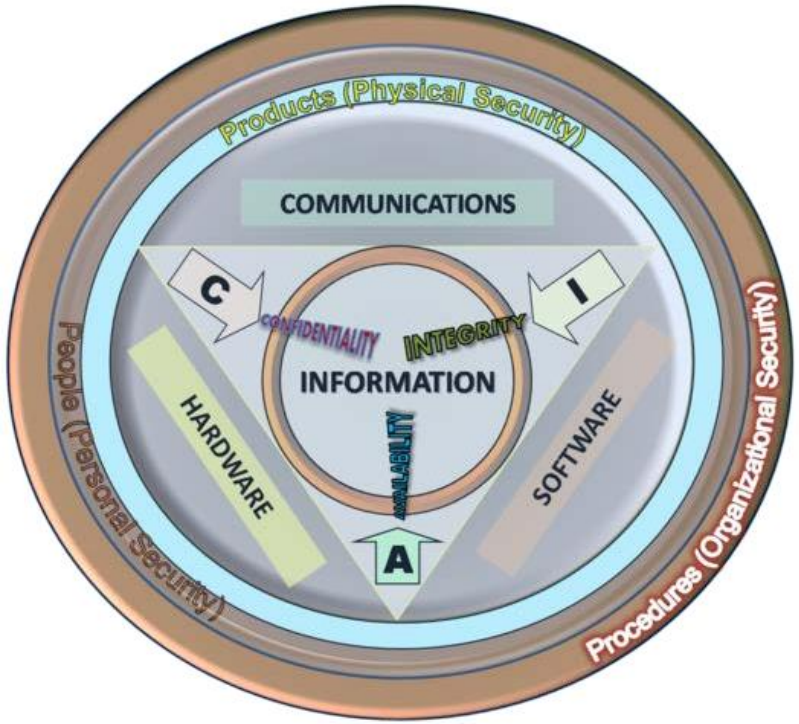
La Seguridad de la Información se basa en 3 dimensiones:

Conjunto de medidas preventivas y reactivas que permiten **resguardar y proteger la información** buscando **mantener la confidencialidad, la disponibilidad e integridad de la misma**.

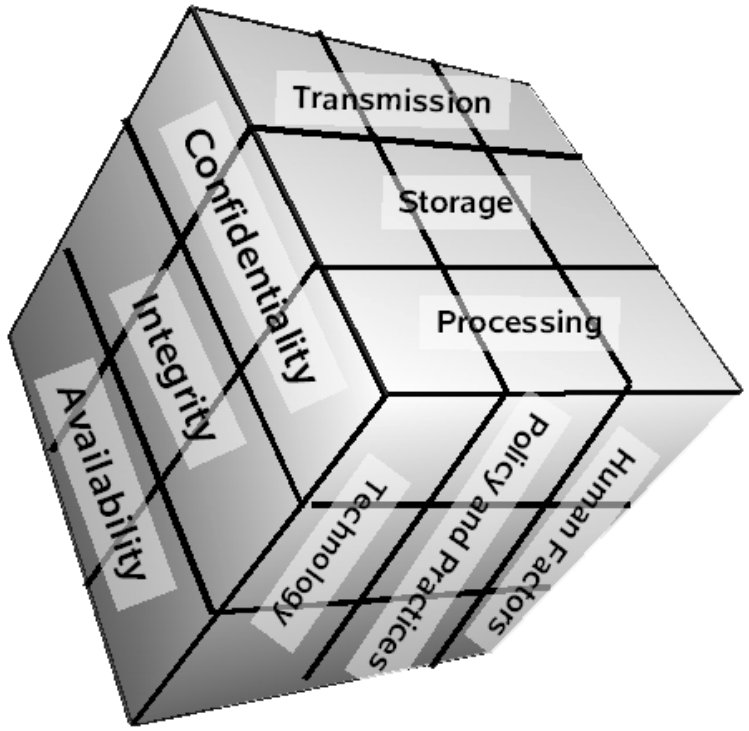
- **Confidencialidad:** Garantizar que la información solo sea accesible por quienes tienen permiso.
- **Integridad:** Proteger la exactitud y completitud de los datos contra alteraciones no autorizadas.
- **Disponibilidad:** Asegurar que los sistemas estén accesibles cuando sean necesarios.

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Conceptos Clave de Seguridad Informática (S.I.)



Tríada CIA



Cubo Mc Cumber (1991)

https://es.linkedin.com/pulse/qu%C3%A9-es-la-triada-cia-o-cid-n%C3%A9stor-mu%C3%B1oz
https://www.alexmilla.net/mccumber-cube-el-cubo/

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Conceptos Clave de Seguridad Informática (S.I.)

Pero existen otras dimensiones:

- **Autenticación:** Verificar la identidad de usuarios o sistemas.
- **Autorización:** Controlar los permisos según la identidad autenticada.
- **Auditoría:** Registro de eventos y monitoreo para detectar accesos no autorizados.

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPCV
Formació Professional Comunitat Valenciana

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

https://www.welivesecurity.com/la-es/2019/01/22/como-analizar-dispositivos-iot/

https://www.shodan.io/

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

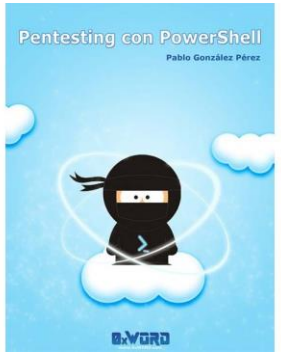
Tipos de Auditoria

Auditorías Normativas

Evaluar el cumplimiento de determinados estándares o requisitos legales.

Auditorías Técnicas

Comprobar el estado de nuestra tecnología, compañía o servicio respecto a distintas situaciones.



FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Auditoria Normativas

Primera parte

Evaluación interna por personal con experiencia e independiente.

Segunda parte

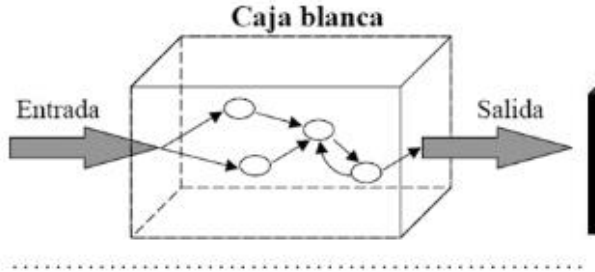
Aquella en que los auditores del cliente de la organización auditen a sus proveedores o aun proveedor potencial para determinar la viabilidad de sus incorporación a la empresa en calidad de tal.

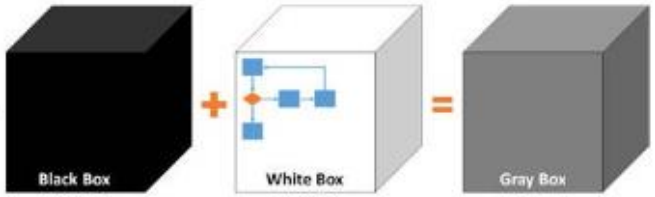
Tercera parte

Auditoria de certificación, es decir, cuando una organización independiente, acreditada, audita a una organización, para determinar si cumple con una determinada norma.

FUNDAMENTOS DE SEGURIDAD EN APLICACIONES

Auditoria Técnicas





Se enfoca en el rol de un usuario interno de la organización o empresa, el cual dispone de acceso a los sistemas internos o a la totalidad o parte de los datos críticos.

La auditoría de caja gris permite al atacante tomar el rol de un cliente, un empleado con pocos o ningún privilegio, un empleado de una ubicación concreta. El auditor dispone de una visión a medias.

La auditoría de caja negra permite al auditor tomar el rol de un atacante que no conoce ninguna característica del interior de la empresa o la organización. La visión global del sistema es ciega.

*El **rol** que se asume en una auditoria **es de vital importancia***

OWASP TOP TEN Y PRINCIPALES VULNERABILIDADES

Introducción a OWASP

https://owasp.org/

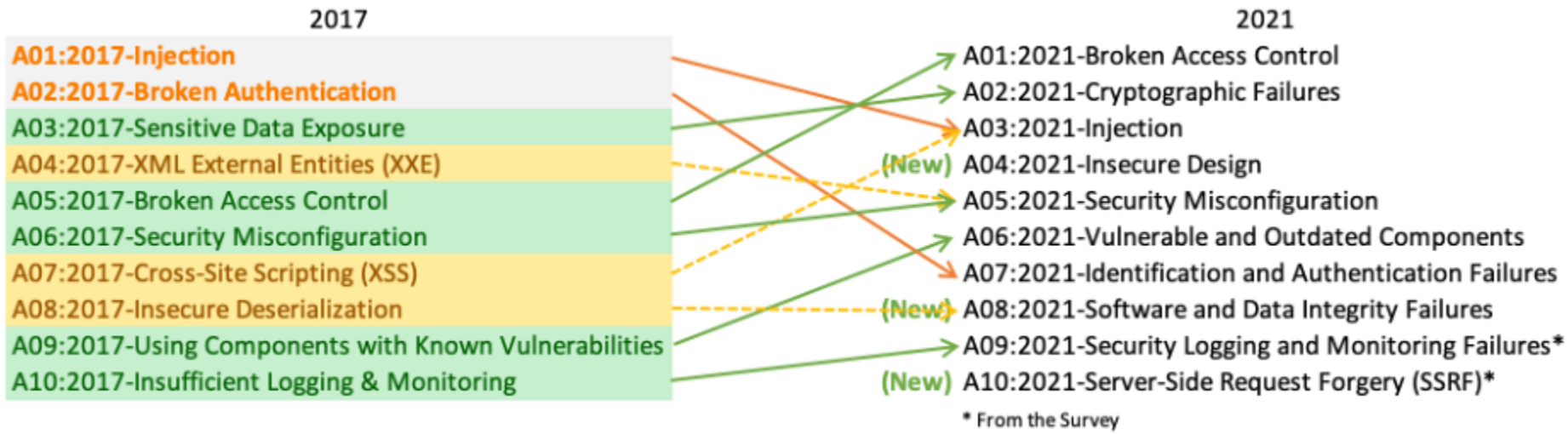
¿Qué es OWASP?

Open Web Application Security Project, comunidad enfocada en la seguridad de aplicaciones.

¿Por qué es relevante?

- Proporciona recursos gratuitos y estándares reconocidos mundialmente.
- OWASP Top Ten es una guía clave para el desarrollo seguro.

OWASP TOP 10



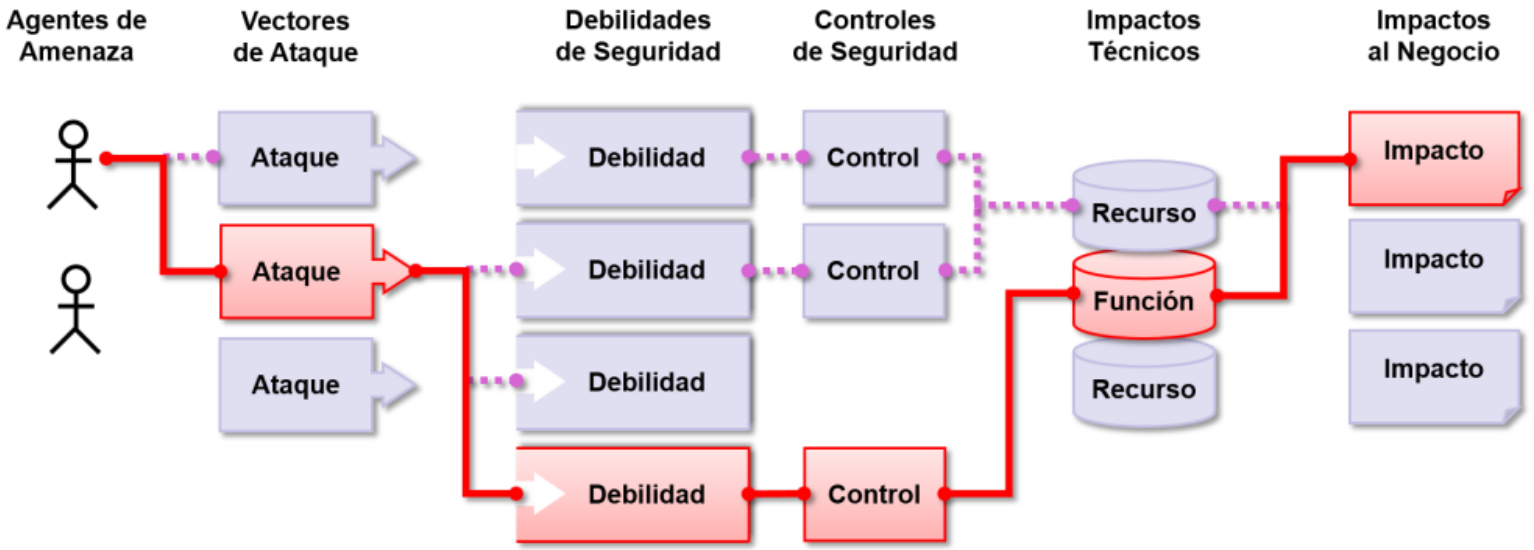
https://owasp.org/Top10/

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPCV
Formació Professional Comunitat Valenciana

Risk Riesgos en la Seguridad de las Aplicaciones

¿Cuáles son los riesgos en seguridad de aplicaciones?

Los atacantes pueden, potencialmente, utilizar diferentes rutas a través de su aplicación para perjudicar su negocio u organización. Cada uno de estos caminos representa un riesgo que puede o no ser suficientemente grave como para merecer atención.



Algunas veces, estos caminos son fáciles de encontrar y explotar, mientras que otras son extremadamente difíciles. De la misma manera, el perjuicio ocasionado puede no tener consecuencias, o puede dejarlo en la quiebra. A fin de determinar el riesgo para su organización, puede evaluar la probabilidad asociada a cada agente de amenaza, vector de ataque, debilidad de seguridad y combinarlo con una estimación del impacto técnico y de negocio para su organización. Juntos, estos factores determinan su riesgo general.

https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP TOP TEN

A01:2021 - Broken Access Control (Control de Acceso Vulnerable)

Descripción:

Ocurre cuando las restricciones de acceso no están correctamente implementadas, permitiendo a usuarios no autorizados realizar acciones o acceder a datos restringidos.

Ejemplos de ataque:

- Modificación de un parámetro en la URL para acceder a recursos de otro usuario.
- Uso de cuentas con privilegios elevados sin autenticación adecuada.

Consecuencias:

- Filtración de datos sensibles.
- Modificación no autorizada de información.

Mitigación:

- Implementar controles de acceso a nivel de servidor.
- Aplicar el principio de **menor privilegio** en los permisos.
- Validar el acceso a cada recurso mediante autenticación y autorización estricta.

OWASP TOP TEN

A02:2021 - Cryptographic Failures (Fallos Criptográficos)

Descripción:

Se produce cuando los datos sensibles no se protegen correctamente con cifrado fuerte o protocolos adecuados.

Ejemplos de ataque:

- Almacenamiento de contraseñas en texto plano.
- Uso de cifrados obsoletos como MD5 o SHA-1.
- Transmisión de datos sin cifrado (HTTP en lugar de HTTPS).

Consecuencias:

- Robo de credenciales o datos personales.
- Ataques de intercepción (Man-in-the-Middle).

Mitigación:

- Implementar TLS 1.2 o 1.3 en todas las conexiones.
- Usar algoritmos seguros: AES-256 para cifrado, Argon2 para contraseñas.
- Nunca almacenar datos sensibles sin cifrado.

OWASP TOP TEN

A03:2021 - Injection (Inyección de Código: SQL, XSS, LDAP, etc.)

Descripción:

Ocurre cuando un atacante logra inyectar código malicioso en una aplicación, manipulando consultas o comandos.

Ejemplos de ataque:

- **SQL Injection:** Modificación de consultas SQL para acceder o manipular bases de datos.
- **Cross-Site Scripting (XSS):** Inyección de scripts en páginas web para robar información o manipular la interfaz.
- **Command Injection:** Ejecución de comandos en el sistema operativo.

Consecuencias:

- Robo de información confidencial.
- Ejecución remota de código en el servidor.

Mitigación:

- Usar **consultas parametrizadas** y ORM en bases de datos.
- Sanitizar entradas de usuario para evitar scripts maliciosos.
- Aplicar **Content Security Policy (CSP)** para prevenir XSS.

OWASP TOP TEN

A04:2021 - Insecure Design (Diseño Inseguro)

Descripción:

Se refiere a sistemas que no fueron diseñados con medidas de seguridad adecuadas.

Ejemplos de ataque:

- Falta de controles de acceso en APIs.
- Autenticación débil sin doble factor (2FA).
- Sin análisis de amenazas en la fase de diseño.

Consecuencias:

- Aplicaciones vulnerables desde su desarrollo.
- Explotación de errores de lógica de negocio.

Mitigación:

- Aplicar el principio de **seguridad por diseño**.
- Implementar modelos de amenazas desde el inicio del desarrollo.
- Realizar auditorías de código y pruebas de seguridad.

OWASP TOP TEN

A05:2021 - Security Misconfiguration (Mala Configuración de Seguridad)

Descripción:

Errores en la configuración de servidores, aplicaciones y bases de datos que exponen vulnerabilidades.

Ejemplos de ataque:

- Consolas de administración accesibles sin autenticación.
- Permisos excesivos en archivos o bases de datos.
- Uso de contraseñas por defecto en sistemas en producción.

Consecuencias:

- Acceso no autorizado a sistemas internos.
- Exposición de datos sensibles.

Mitigación:

- Aplicar el **principio de menor privilegio** en configuraciones.
- Realizar revisiones y auditorías de seguridad periódicas.
- Deshabilitar características innecesarias en servidores.

OWASP TOP TEN

A06:2021 - Vulnerable and Outdated Components

Descripción:

Uso de librerías, frameworks o software con vulnerabilidades conocidas.

Ejemplos de ataque:

- Explotación de fallos en versiones obsoletas de Apache, PHP o WordPress.
- Uso de librerías desactualizadas con fallas conocidas.

Consecuencias:

- Ataques de ejecución remota de código (RCE).
- Compromiso total de la aplicación.

Mitigación:

- Actualizar regularmente los componentes utilizados.
- Aplicar parches de seguridad de forma constante.
- Utilizar herramientas de análisis de dependencias como **OWASP Dependency-Check**.

OWASP TOP TEN

A07:2021 - Identification and Authentication Failures

Descripción:

Problemas en la autenticación de usuarios, permitiendo accesos indebidos.

Ejemplos de ataque:

- Uso de contraseñas débiles sin restricciones.
- Falta de 2FA en accesos críticos.
- Almacenamiento inseguro de credenciales.

Consecuencias:

- Robo de credenciales y acceso a cuentas.
- Suplantación de identidad (phishing).

Mitigación:

- Implementar autenticación fuerte con **2FA**.
- Almacenar contraseñas con hashing seguro (**Argon2, bcrypt**).
- Bloquear cuentas después de múltiples intentos fallidos.

OWASP TOP TEN

A08:2021 - Software and Data Integrity Failures

Descripción:

Uso de software manipulado o alteraciones no controladas en datos.

Ejemplos de ataque:

- Actualizaciones de software sin firma digital.
- Manipulación de datos por falta de integridad.

Consecuencias:

- Ejecución de código malicioso en actualizaciones.
- Alteración de registros críticos.

Mitigación:

- Usar **firmas digitales en software**.
- Implementar controles de integridad en bases de datos.

OWASP TOP TEN

A09:2021 - Security Logging and Monitoring Failures

Descripción:

Falta de registros y monitoreo adecuados para detectar ataques.

Ejemplos de ataque:

- No registrar intentos de acceso fallidos.
- Falta de monitoreo en cambios de configuración.

Consecuencias:

- Detección tardía de ataques.
- Incapacidad de realizar auditorías forenses.

Mitigación:

- Implementar **SIEM** y herramientas de monitoreo.
- Registrar eventos críticos y alertas en tiempo real.

OWASP TOP TEN

A10:2021 - Server-Side Request Forgery (SSRF)

Descripción:

El atacante engaña al servidor para hacer peticiones a recursos internos.

Ejemplos de ataque:

- Acceso a servicios internos a través de URLs manipuladas.

Mitigación:

- Validar y restringir URLs externas en peticiones del servidor.

OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

- Metodología cuyo manual se puede descargar de manera libre y gratuita.
- Está estructurada en **15 capítulos** donde se explica como llevar las distintas pruebas.
- Propone una vía de **generación de informes estandarizada.**

http://www.isecom.org/

EJEMPLOS PRÁCTICOS DE EXPLOTACIÓN Y MITIGACIÓN

Ejemplo de Explotación – Inyección SQL

Escenario:

- Una aplicación web tiene un formulario de inicio de sesión vulnerable a SQL Injection.
- Un atacante introduce ' OR '1'='1 en el campo de contraseña.

Resultado del ataque:

- Se ejecuta la consulta con lógica alterada, permitiendo acceso sin conocer credenciales.

Mitigación:

- Uso de consultas parametrizadas (Prepared Statements).
- Validación y saneamiento de entradas de usuario.
- Configurar roles mínimos de acceso en la base de datos.

EJEMPLOS PRÁCTICOS DE EXPLOTACIÓN Y MITIGACIÓN

Ejemplo de Explotación – Cross-Site Scripting (XSS)

Escenario:

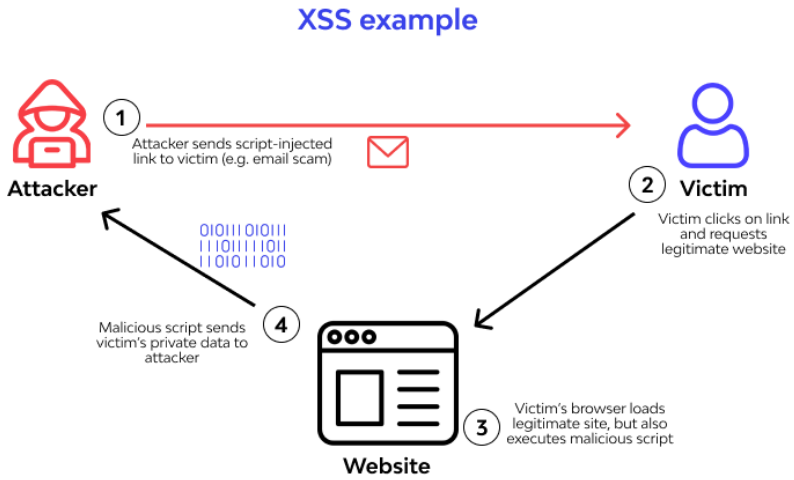
- Un foro permite a los usuarios publicar comentarios sin filtrar entradas.
- Un atacante inserta *<script>alert('Hacked!')</script>.*

Resultado del ataque:

- Los usuarios ven el mensaje, lo que confirma la inyección de scripts maliciosos.
- Posible robo de cookies y credenciales.

Mitigación:

- Sanitización de entradas con *HTML Entities*.
- Implementación de **Content Security Policy (CSP)**.
- Uso de bibliotecas de escape como DOMPurify.



ANÁLISIS DE CASOS REALES DE ATAQUES

Caso Real – Equifax (2017)

Breve descripción:

- Hackers explotaron una vulnerabilidad en Apache Struts para acceder a datos de 147 millones de usuarios.

Factores clave del ataque:

- No actualización de software con parches de seguridad.
- Falta de monitoreo adecuado en la red.

Lecciones aprendidas:

- Aplicar parches de seguridad sin demora.
- Implementar segmentación de redes y controles de acceso.

https://www.linkedin.com/pulse/el-ciberataque-equifax-fallos-cr%C3%ADticos-detectados-una-catherine-txnwe/

ANÁLISIS DE CASOS REALES DE ATAQUES

Caso Real – Ataque a Facebook (2019)

Breve descripción:

- Fallo en la autenticación OAuth permitió que atacantes accedieran a más de 50 millones de cuentas.

Factores clave del ataque:

- Tokens de acceso comprometidos.
- Deficiencia en la gestión de sesiones.

Lecciones aprendidas:

- Implementación de autenticación reforzada (2FA).
- Caducidad automática de sesiones y tokens.

https://www.equipodecomunicacion.com/la-caida-mundial-de-facebook-y-su-comunicacion-de-crisis/

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació

CFR | CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES

FPCV
Formació Professional Comunitat Valenciana

ACTIVIDAD

M1-A1-Ética y Legalidad en Casos Reales

Objetivo: Diferenciar acciones éticas, dudosas o ilegales en situaciones relacionadas con la ciberseguridad.

ESTRATEGIAS DE PREVENCIÓN Y BUENAS PRÁCTICAS

Estrategias de Prevención Generales

Principios fundamentales de seguridad:

- Seguridad por diseño.
- Principio de menor privilegio.
- Defensa en profundidad.

Técnicas esenciales:

- Filtrado y validación de datos.
- Uso de HTTPS y cifrado en tránsito.
- Implementación de autenticación multifactor (MFA).

ESTRATEGIAS DE PREVENCIÓN Y BUENAS PRÁCTICAS

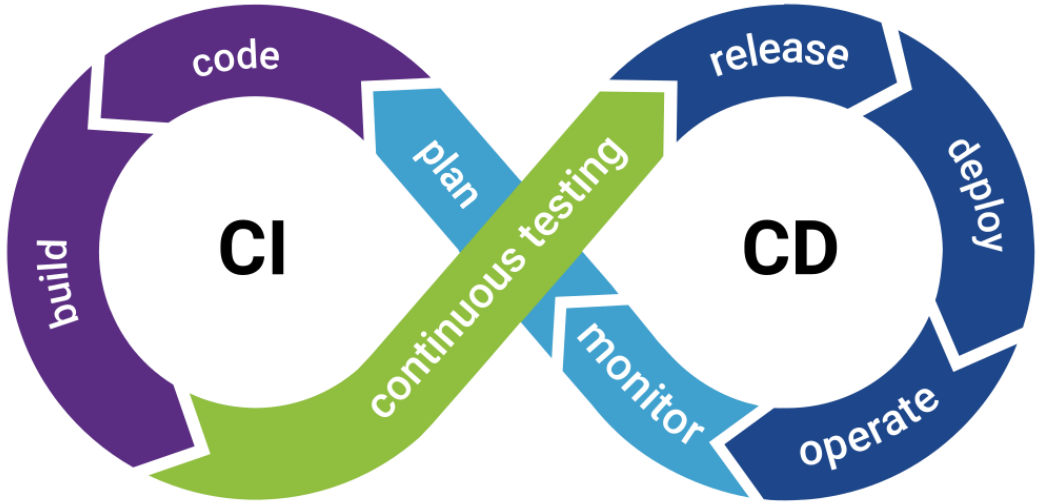
Buenas Prácticas en Desarrollo Seguro

Seguridad en el código:

- Uso de herramientas de análisis estático y dinámico.
- Evitar contraseñas en código fuente.

Pruebas de seguridad:

- Integración de pruebas automatizadas en CI/CD.
- Análisis de dependencias de software.



GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPCV
Formació Professional Comunitat Valenciana

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Importancia de las Normativas y Estándares

¿Por qué son necesarias?

- Garantizan la seguridad de datos y sistemas.
- Facilitan el cumplimiento legal y regulatorio.
- Reducen riesgos de ciberataques y sanciones legales.

Tipos de normativas:

- Globales: *ISO 27001, NIST.*
- Sectoriales: *PCI-DSS, GDPR.*

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Norma General:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)
- Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal (LOPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD)

Normas Sectoriales:

- La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y comercio electrónico (LSSI-CE)
- Ley 32/2003, General de Telecomunicaciones
- Ley 59/2003, de 19 de diciembre, de firma electrónica

Otras

- Real Decreto Legislativo 1/1996, Ley de Propiedad Intelectual (LPI)
- Real Decreto 3/2010, en el que se regula el Esquema Nacional de Seguridad (ENS)
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, en el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica. (ENI)
- Ley 8/2011, de 28 de abril, Ley de protección de Infraestructuras Críticas (LPIC)

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

ISO/IEC 27001 y 27002 – Gestión de Seguridad de la Información

Objetivo:

- Establecer un Sistema de Gestión de Seguridad de la Información (SGSI).

Principales requisitos:

- Evaluación de riesgos.
- Implementación de controles de seguridad.
- Auditorías periódicas.

Aplicación en empresas:

- Protección de información confidencial.
- Cumplimiento con regulaciones y auditorías.

https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

https://tienda.aenor.com/norma-une-en-iso-iec-27002-2023-n0071321

https://tienda.aenor.com/norma-une-en-iso-iec-27001-2023-n0071764

https://secureframe.com/es-es/hub/iso-27001/vs-iso-27002

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

GDPR y Regulaciones de Privacidad

¿Qué es GDPR?

- Reglamento General de Protección de Datos de la UE.

Principios clave:

- Transparencia en el uso de datos.
- Derecho al olvido y portabilidad de datos.
- Notificación de brechas de seguridad.

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

RGPD o GDPR

Reglamento relativo a la protección de las personas físicas en lo que respecta al **tratamiento de datos personales y a la libre circulación de estos datos**.

Normativa a **Nivel Europeo.**

Las **multas por el no cumplimiento** del RGPD pueden llegar a los 20 millones de euros.

Fuente: www.coregistros.com

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

LOPDGDD

Regula el uso que se hace de los **datos personales, imágenes, o videos de terceros, y estipula fuertes** multas.

Todas las empresas y/o profesionales tienen **obligación de adaptarse a la LOPDGDD y su** normativa de desarrollo

Ámbito de aplicación

https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

LOPDGDD / RGPD

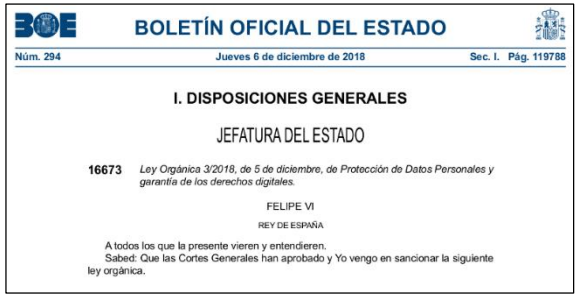
En España, se actualizó la **Ley Orgánica de Protección de Datos de Carácter Personales y garantía de los derechos digitales** (L.O. 3/2018, de 5 de diciembre) vigente desde 1993 para adaptarse al nuevo reglamento europeo.

Reglamento General de Protección de Datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Contiene una serie de importantes cambios que exigen la actualización de los procedimientos en todas las organizaciones.

- ❑ **Delegado de Protección de Datos** .
- ❑ Nuevos derechos que el RGPD otorga a los ciudadanos.
- ❑ Análisis de riesgos y las evaluaciones de impacto.
- ❑ Establecimiento de códigos de conducta.
- ❑ …

https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf



BOLETÍN OFICIAL DEL ESTADO
Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119788

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

16673 *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

FELIPE VI
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Infracciones y sanciones

Impacto en empresas:

- Multas de hasta el 4% del ingreso anual por incumplimiento.

https://protecciondatos-lopd.com/empresas/procedimiento-sancionador-rgpd-lopdgdd/

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

PCI-DSS – Seguridad en Transacciones de Pago

¿Qué es PCI-DSS?

- Estándar de seguridad para datos de tarjetas de pago.

Principales requisitos:

- Uso de cifrado en almacenamiento y transmisión.
- Control de accesos y monitoreo de actividad.
- Pruebas de seguridad regulares.

Consecuencias del incumplimiento:

- Multas, restricciones en transacciones y daños reputacionales.

https://www.pcisecuritystandards.org/minisite/es-es/

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

NIST Cybersecurity Framework

Objetivo:

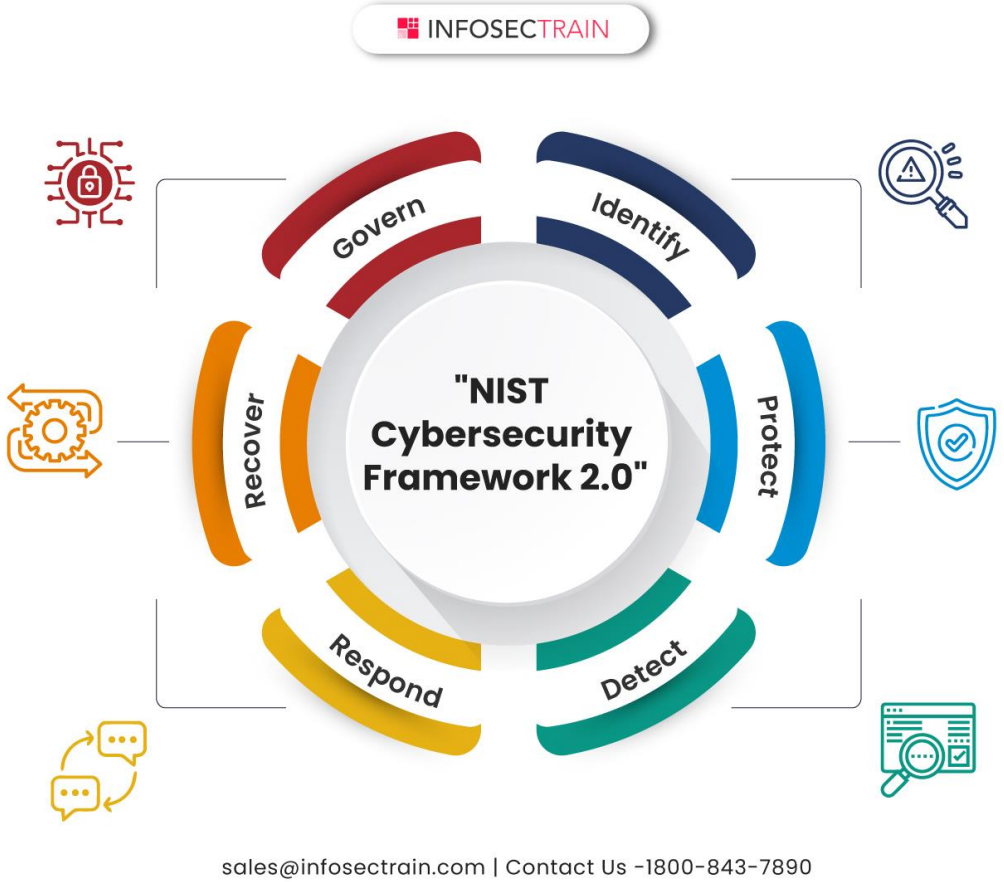
- Proporcionar un marco para gestionar riesgos de ciberseguridad.

Funciones clave:

- Identificar, Proteger, Detectar, Responder y Recuperar.

Uso en la industria:

- Adoptado por empresas y gobiernos para fortalecer la seguridad.



https://www.nist.gov/cyberframework

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Ley de Ciberseguridad de la UE

7.6.2019 ES Diario Oficial de la Unión Europea L 151/15

REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 17 de abril de 2019

relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»)

(Texto pertinente a efectos del EEE)

https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-act

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

LSSI-CE

La **Ley 34/2002, de Servicios de Seguridad de la Información y Comercio Electrónico** fue modificada por la Ley 2/2011, de Economía Sostenible y posteriormente, por el Real Decreto-Ley 13/2012.

Objeto:

- Regular el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica.

Ámbito de aplicación:

- Prestadores de Servicio establecidos en España.
- Prestadores de Servicio residentes o domiciliados en otro Estado pero con establecimiento permanente en España.
- Prestadores de Servicio establecidos en otro Estado Miembro de la UE o EEE.
- Prestadores de Servicio establecidos en un Estado no perteneciente a la UE o EEE.

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones 32/2003 fue modificada en Mayo de 2014, por la llamada **Ley 9/2014, de Telecomunicaciones.**

Exclusiones de manera expresa:

- Servicios de **comunicación audiovisual** y los **contenidos audiovisuales** transmitidos a través de las redes.
- Servicios que suministren **contenidos transmitidos mediante** redes y servicios de comunicaciones electrónicas, las actividades que consistan en el ejercicio del **control editorial** sobre dichos contenidos y los **servicios de la Sociedad de la Información**, que **no consistan**, en su totalidad o principalmente, en el **transporte de señales** a través de redes de comunicaciones electrónicas.

Ámbito de aplicación:

- La regulación de las telecomunicaciones, que comprenden la **explotación de las redes** y la **prestación de los servicios de comunicaciones electrónicas** y los recursos asociados

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Ley de firma electrónica

La Ley 59/2003, de 19 de diciembre, de firma electrónica establece los siguientes conceptos:

- **Firma electrónica**
- **Firma electrónica avanzada**
- **Firma electrónica reconocida**

Sede Electrónica
Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

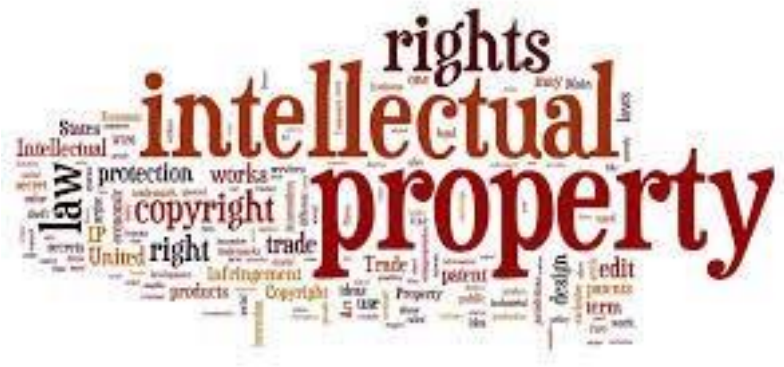
NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Ley de propiedad intelectual

El Real Decreto 1/1996, de Propiedad Intelectual fue modificada por la Ley 21/2014.

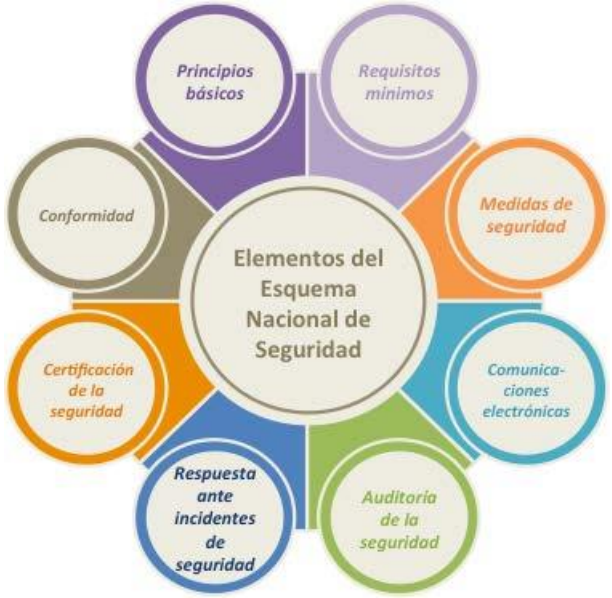
Objeto:

- Proteger el conjunto de derechos que corresponden a los autores y a otros titulares respecto de las obras y prestaciones fruto de su creación.



NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Esquema Nacional de Seguridad

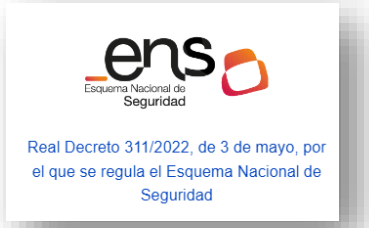


Objeto:

Establecer la política de seguridad en la utilización de medios electrónicos .
Constituido por principios básicos y requisitos mínimos

Objetivos:

- ❑ **Crear las condiciones necesarias de confianza en el uso de los medios electrónicos**
- ❑ **Establecer la política de seguridad** en la utilización de medios electrónicos
- ❑ **Introducir los elementos comunes** que han de guiar la actuación de las Administraciones públicas
- ❑ **Aportar un lenguaje común** para facilitar la interacción de las Administraciones públicas
- ❑ **Aportar un tratamiento homogéneo de la seguridad**
- ❑ **Facilitar un tratamiento continuado de la seguridad.**



https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf


BOLETÍN OFICIAL DEL ESTADO
Núm. 106 Miércoles 4 de mayo de 2022 Sec. I. Pág. 61715

I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

7191 *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

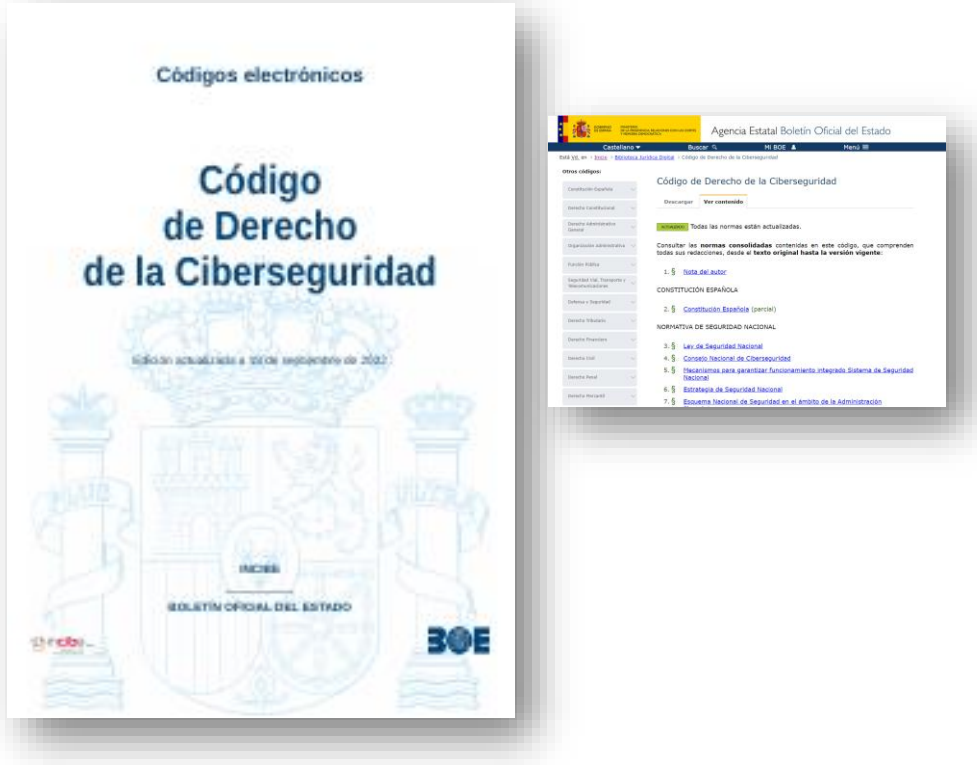
ÍNDICE

Capítulo I. Disposiciones generales.

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Código de Derecho de la Ciberseguridad

El **Código del Derecho de la Ciberseguridad** es un iniciativa conjunta del **Instituto Nacional de Ciberseguridad (INCIBE)** y el **Boletín Oficial del Estado (BOE)** que pone a disposición de todos los profesionales del Derecho, en un compendio de normas, el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimiento en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado.



https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173&modo=2&nota=0&tab=2

https://www.boe.es/biblioteca_juridica/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho_de_la_Ciberseguridad.pdf

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Infracciones y sanciones

LEGISLACIÓN	LEVES	GRAVES	MUY GRAVES
LOPD	No atender por motivos formales la solicitud de rectificación o cancelación, Obtener datos personales sin informar a los afectados, según el artículo 5 LOPD, Incumplir el deber de secreto establecido por la LOPD,... Sanciones: 900 € a 40.000 €	Recogida de datos sin consentimiento expreso, cuando sea necesario, la obstrucción de la función inspectora, ... *40.001 € a 300.000 €*	*La cesión de datos sin permiso, la recogida de datos de forma engañosa y fraudulenta,.. Sanciones: 300.001 € a 600.000 €*
LSSI-CE	incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, ... *Multa de hasta 30.000 euros*	Envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos legales, incumplimiento por no permitir la revocación del consentimiento, resistencia, excusa o negativa a la actuación inspectora, etc. *Multa de 30.001 hasta 150.000 euros*	No informar en la forma prescrita al afectado, No facilitar la información al afectado, incumplimiento de la obligación de confirmar la recepción de una petición, Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento, ... *Multa de 150.001 hasta 600.000 euros Prohibición de actuación en España si existe reiteración*
Ley general de telecomunicaciones	Producción de cualquier tipo de emisión radioeléctrica no autorizada, Establecimiento de comunicaciones utilizando estaciones no autorizadas, No facilitar los datos requeridos por la Administración o retrasar injustificadamente su aportación, Incumplimiento de las obligaciones en materia de calidad de servicio,... *Hasta 50.000 euros*	Instalación de estaciones radioeléctricas sin autorización, Emisión de señales de identificación falsas o engañosas, Negativa o la obstrucción a ser inspeccionado, Instalación negligente de infraestructuras comunes de telecomunicación en el interior de edificios, Negativa a cumplir las obligaciones de servicio público, Incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones,... *Hasta 2.000.000 euros*	*Realización de actividades sin disponer de la habilitación oportuna, Incumplimiento grave de las características y condiciones establecidas para la conservación de los números, Incumplimiento de las resoluciones firmes en vía administrativa,... hasta 20.000.000 euros*

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Outsourcing

Movilizar recursos hacia una empresa externa a través de un contrato.

Las **operaciones** se caracterizan por ser **complejas, importantes o incómodas de efectuar.**

Importante en la actualidad dada la complejidad de los ataques

Permite a las organizaciones centrarse en la consecución de los objetivos propios de su negocio.

Utiliza en su beneficio todo el conocimiento sobre las últimas tecnologías y recursos que acumula una empresa de seguridad.

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Outsourcing

Situaciones

- ❑ Amenazas cada vez más sofisticadas
- ❑ Nuevas formas de phishing
- ❑ Nuevos entornos y tecnologías susceptibles de sufrir ataques
- ❑ Regulaciones cada vez más exigentes

Beneficios

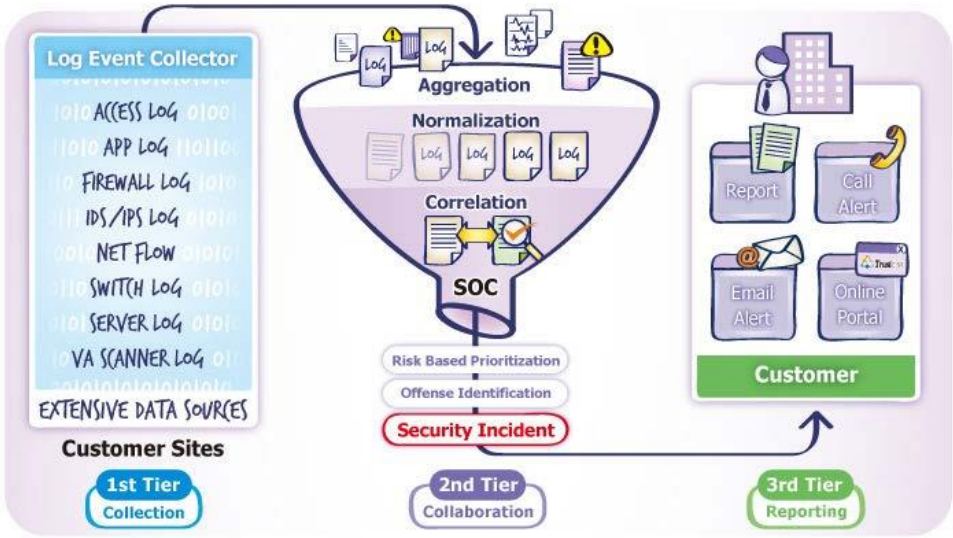
- ❑ Sumar experiencia y **están en condiciones de mantenerse permanentemente actualizadas** sobre las nuevas vulnerabilidades, las herramientas, productos de seguridad y últimas versiones de software.
- ❑ Permite transferir el conocimiento de los especialistas a la organización.
- ❑ Permite exigir niveles de rendimiento en función de unos acuerdos de nivel de servicio y ofrecer la posibilidad de acceder a niveles de seguridad más elevados

NORMATIVAS Y ESTÁNDARES DE SEGURIDAD

Outsourcing

Servicios que suelen externalizarse

- ❑ **Monitorización de la seguridad** *(son servicios especializado como la gestión de firewalls, IDS, IPS…)*
- ❑ **Protección y defensa**
- ❑ **Vigilancia digital** y **respuesta** a posibles **incidentes** o ataques
- ❑ **Análisis forense**



GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació

CFR | CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES

FPCV
Formació Professional Comunitat Valenciana

ACTIVIDAD

M1-A2-Marco Legal en España y Europa

Objetivo: Identificar obligaciones y limitaciones legales que afectan a un hacker ético en España y la UE.

BUENAS PRÁCTICAS Y FRAMEWORKS DE SEGURIDAD

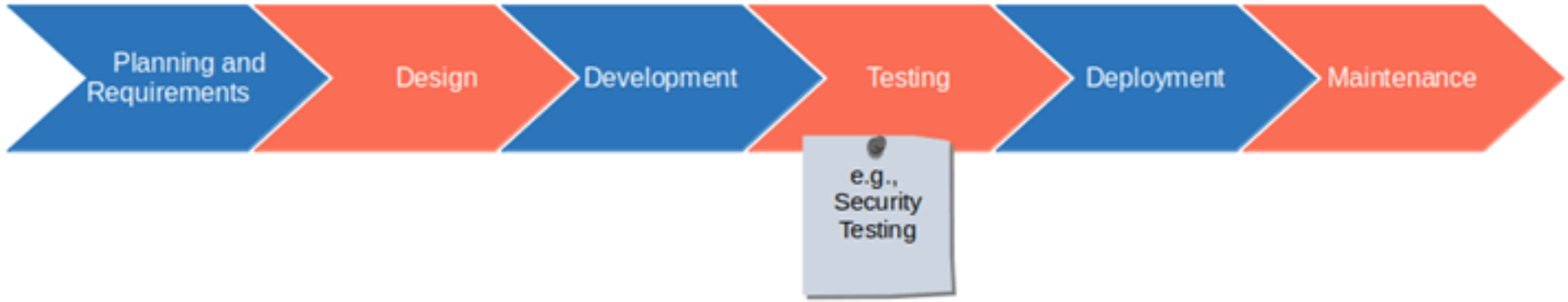
Proceso del Ciclo de Vida del Desarrollo de Software (SDLC)

1. **Planificación y Requisitos**
2. **Diseño**
3. **Desarrollo**
4. **Pruebas** (*pruebas de seguridad*)
5. **Despliegue**
6. **Mantenimiento**

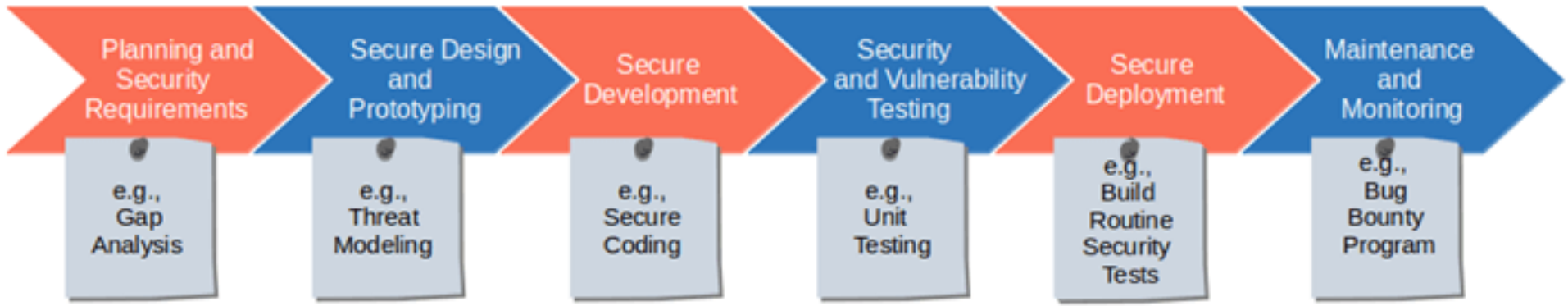
Proceso del Ciclo de Vida del Desarrollo de Software Seguro (SSDLC)

1. **Planificación y Requisitos de Seguridad** (*análisis de brechas*)
2. **Diseño Seguro y Prototipado** (*modelado de amenazas*)
3. **Desarrollo Seguro** (*codificación segura*)
4. **Pruebas de Seguridad y Vulnerabilidad** (*pruebas unitarias*)
5. **Despliegue Seguro** (*pruebas de seguridad rutinarias de compilación*)
6. **Mantenimiento y Monitoreo** (*programa de recompensas por errores - bug bounty program*)

Software Development Life Cycle (SDLC) Process



Secure Software Development Life Cycle (SSDLC) Process



BUENAS PRÁCTICAS Y FRAMEWORKS DE SEGURIDAD

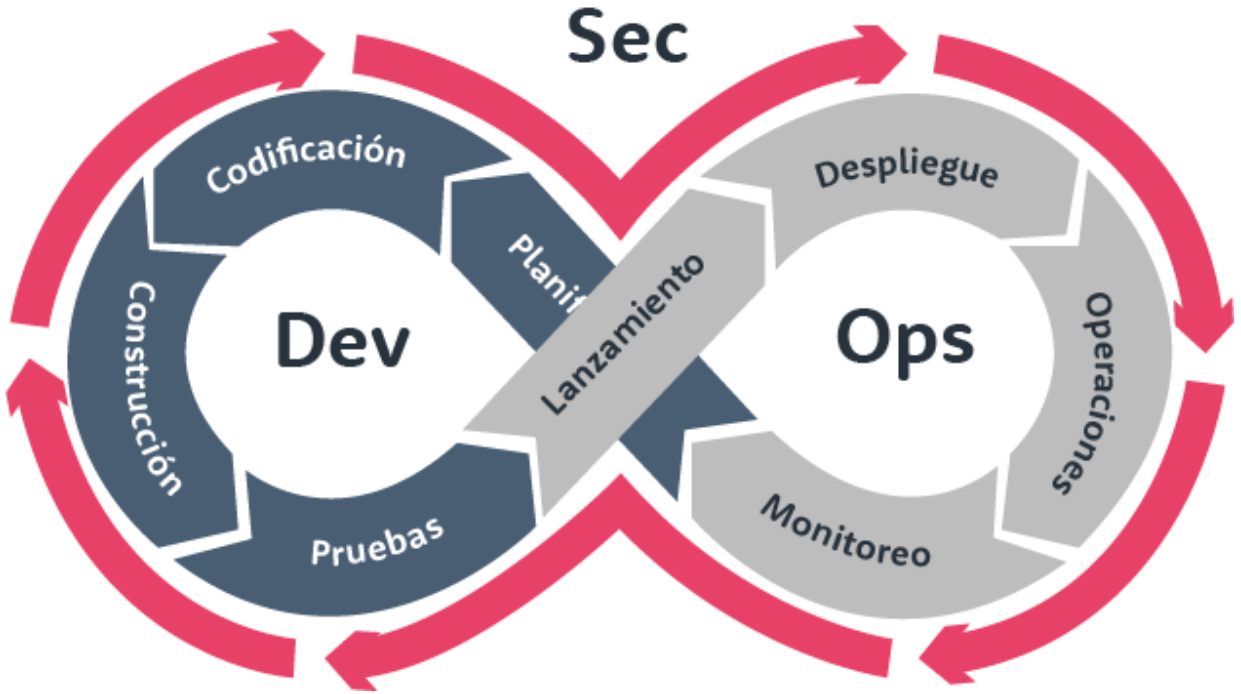
DevSecOps – Seguridad en Desarrollo Ágil

¿Qué es DevSecOps?

- Integración de seguridad en DevOps.

Principales prácticas:

- Automatización de pruebas de seguridad.
- Análisis continuo de vulnerabilidades.



BUENAS PRÁCTICAS Y FRAMEWORKS DE SEGURIDAD

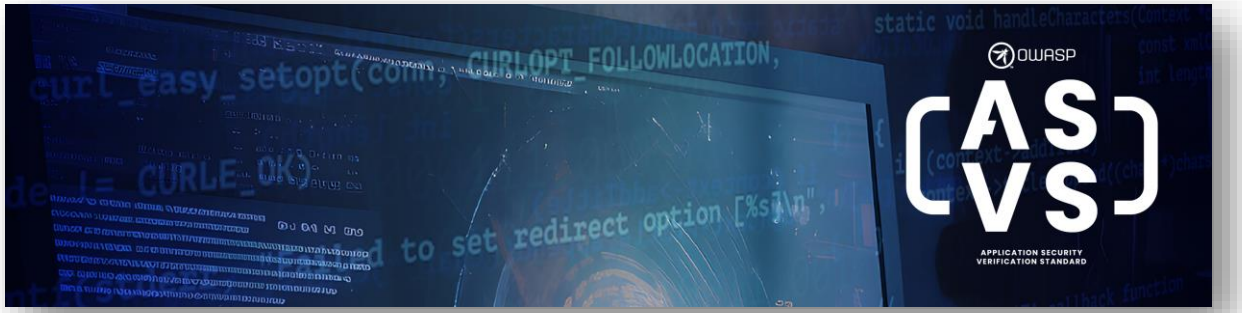
OWASP ASVS – Application Security Verification Standard

Objetivo:

- Proporcionar un marco para verificar la seguridad de aplicaciones web.

Niveles de seguridad:

- Nivel 1: Protección básica contra amenazas comunes.
- Nivel 2: Mayor protección en aplicaciones sensibles.
- Nivel 3: Seguridad avanzada para aplicaciones críticas.



https://owasp.org/www-project-application-security-verification-standard/

EVALUACIONES DE CUMPLIMIENTO Y AUDITORÍAS DE SEGURIDAD

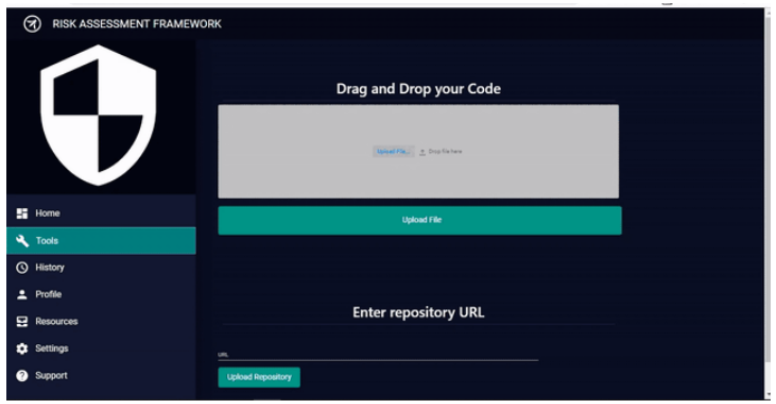
Análisis de Riesgos en Aplicaciones Web

Proceso:

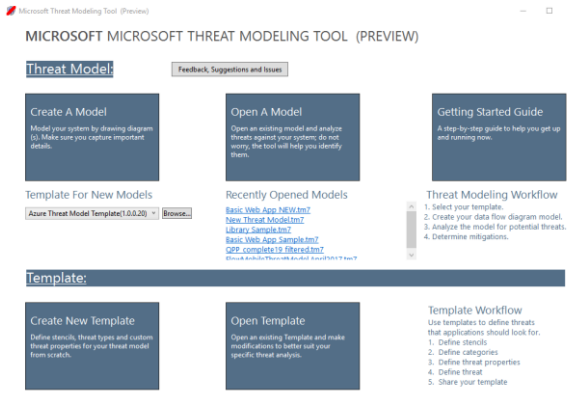
- Identificación de activos y amenazas.
- Evaluación de impacto y probabilidad.

Herramientas recomendadas:

- OWASP Risk Assessment Framework.
- Microsoft Threat Modeling Tool.



https://github.com/OWASP/RiskAssessmentFramework



https://learn.microsoft.com/es-es/azure/security/develop/threat-modeling-tool

EVALUACIONES DE CUMPLIMIENTO Y AUDITORÍAS DE SEGURIDAD

Pruebas de Penetración (Pentesting) y Metodologías

¿Qué es Pentesting?

- Simulación de ataques para identificar vulnerabilidades.

Metodologías:

- OWASP Testing Guide.
- NIST 800-115.

https://owasp.org/www-project-web-security-testing-guide/

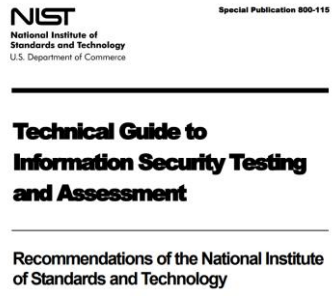
https://owasp.org/www-project-web-security-testing-guide/v42/

https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

Fases del Pentesting:

- Recolección de información, escaneo, explotación, informe.

https://www.nist.gov/privacy-framework/nist-sp-800-115


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-115

Technical Guide to Information Security Testing and Assessment

Recommendations of the National Institute of Standards and Technology

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació

CFR | CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES

FPCV
Formació Professional Comunitat Valenciana

ACTIVIDAD

M1-A3-Tipos de Hackers y Metodologías

Objetivo: Identificar distintos perfiles de hackers y asociar metodologías estándar a un escenario real.

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació
CFR CEFIRE
FORMACIÓ PROFESSIONAL ENSENYANCES ARTÍSTIQUES I ESPORTIVES
FPCV
Formació Professional Comunitat Valenciana

M1 - Introducción y Legalidad en el Hacking Ético.

Objetivo: Proporcionar una visión general sobre la seguridad, identificar amenazas críticas (OWASP Top Ten) y conocer normativas relevantes.