

# Puesta en Producción Segura

Unidad 0.

## Fundamentos de Seguridad Informática



JUNTA DE EXTREMADURA

★  Plan de  
Recuperación,  
Transformación  
y Resiliencia



Financiado por  
la Unión Europea  
NextGenerationEU

 MINISTERIO  
DE EDUCACIÓN,  
FORMACIÓN PROFESIONAL  
Y DEPORTES

*"Si crees que lo sabes todo sobre ciberseguridad, esta disciplina probablemente no te fue bien explicada "*

*—Stephane Nappo. Vicepresidente y  
**Global Chief Information Security Officer (CISO) del Grupo SEB***

# Objetivos

- Conocer el concepto de seguridad informática.
- Conocer los diferentes conceptos en ciberseguridad.
- Conocer las principales amenazas de los sistemas informáticos y cómo actúan.
- Comprender los riesgos que del uso de sistemas de información interconectados.
- Cambiar “el chip” para encaminarnos hacia el desarrollo seguro.
- Tener un primer acercamiento a las estrategias de prevención y a las buenas prácticas.
- Tener una visión de la necesidad de normativas y estándares en ciberseguridad



# Contenidos

**01** Introducción

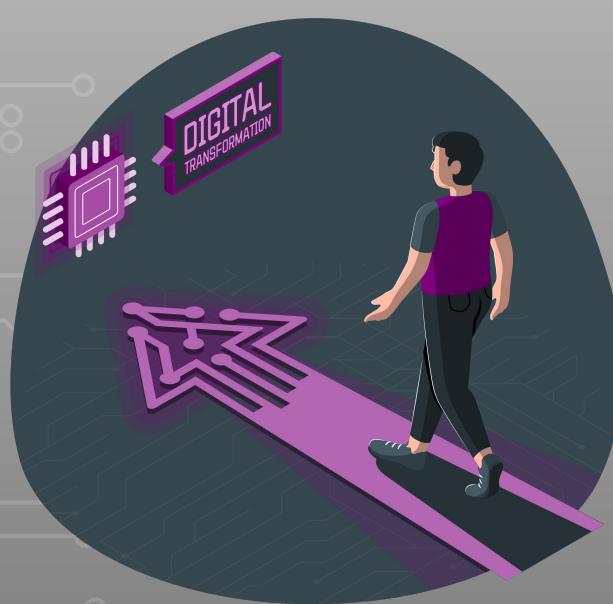
**02** Conceptos básicos de seguridad

**03** Ciberataques

**04** Modelos de amenazas

**05** Estrategias de prevención y buenas prácticas

**06** Normativas y estándares de seguridad WEB



01

# Introducción



# Introducción: Seguridad informática

La **ciberseguridad** o **seguridad informática** es la práctica de proteger sistemas, redes y programas contra la interrupción o el desvío de los servicios que provocan los ciberataques.



- La seguridad informática tiene como finalidad proteger la integridad y privacidad de la información almacenada o tratada por un sistema informático frente a cualquier amenaza.

**Amenaza:** factor que puede afectar al desempeño directo del sistema informático y los resultados obtenidos del mismo.

# Introducción: Seguridad informática

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).
- La **seguridad de la información**, se incluye tanto activos digitales, como activos en papel.

# Introducción: Seguridad informática

- Aunque ningún sistema puede considerarse seguro al 100%, sí podemos aplicar una serie de protocolos, normas, restricciones, políticas de acceso y planes de contingencia para mantener la seguridad en un nivel óptimo.
- Algunos expertos prefieren hablar de *fiabilidad* del sistema.
  - *Fiabilidad* es la probabilidad de que un sistema se comporte tal y como se espera de él.
- El factor humano es fundamental para lograr un nivel de seguridad óptimo

# Introducción: Seguridad informática

El **factor humano** es fundamental para lograr un nivel de seguridad óptimo, por ello el objetivo de la **ciberseguridad** no solamente es aplicar diferentes sistemas de seguridad con el fin de prevenir y/o contrarrestar dichos ataques, sino que también es educar a los usuarios sobre cómo evitar riesgos innecesarios.



# Introducción: Seguridad informática

- Podemos encontrar dos tipos de técnicas de seguridad para proteger los equipos informáticos:
  - La **seguridad activa**: se encarga de evitar que los sistemas informáticos sufran algún daño.
  - La **seguridad pasiva**: consiste en minimizar los efectos o desastres causados por un accidente, un usuario o un malware a los sistemas informáticos.



02

# Conceptos Básicos de seguridad



# Conceptos básicos: Triada CIA

La Seguridad de la Información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Se basa en 3 dimensiones:

- **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.



<https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/>

# Conceptos básicos: Conceptos clave

Pero existen otras **dimensiones o conceptos clave**:

- ❑ **Autenticación**: Verificar la identidad de usuarios o sistemas.
- ❑ **Autorización**: Controlar los permisos según la identidad autenticada.
- ❑ **Irrefutabilidad o no repudio**: permite probar la participación de las partes en una comunicación.
- ❑ **Auditoría**: Registro de eventos y monitoreo para detectar accesos no Autorizados.



<https://www.redeszone.net/app/uploads-redeszone.net/2020/06/autenticacion-autorizacion.jpg?quality=80>

# Conceptos básicos: Integridad

**Integridad:** modificación de la información sólo por entidades debidamente autorizadas.

- La información ha de mantenerse con exactitud, tal cual fue generada, sin ser alterada por personas o procesos informáticos no autorizados para ello.
- La modificación de los datos por personas autorizadas debe quedar registrada, asegurando su precisión y confiabilidad.

Se produce una violación de la integridad cuando una persona, aplicación o proceso modifica o borra datos importantes, bien accidentalmente, bien de forma dolosa.



# Conceptos básicos: Confidencialidad

**Confidencialidad:** garantiza que la información sea accesible únicamente a personas, entidades o procesos autorizados.

- La pérdida o violación de la confidencialidad de la información puede adoptar múltiples formas, por ejemplo:

Si en una transacción electrónica el número de nuestra tarjeta de crédito no se envía cifrado.



# Conceptos básicos: Disponibilidad

**Disponibilidad:** La información ha de estar disponible para las personas, procesos o aplicaciones que deban acceder a ella en el momento en el que lo requieran.

- ¿Qué entendemos por **alta disponibilidad**?<sup>4</sup>

Hablamos de **alta disponibilidad** cuando un sistema garantiza la continuidad operacional, es decir, que va a estar disponible en todo momento, evitando cualquier interrupción del servicio (ya sea por cortes de energía, fallos del hardware o problemas de software).



# Conceptos básicos: Autentificación

**Autentificación** (autenticación): El generador de la información, o el que acceda o la edite, ha de estar perfectamente identificado en todo momento de forma unívoca e inequívoca → El usuario es quién dice ser.

- La autenticación se implementa mediante la gestión de cuentas de usuario y contraseña, que gradúa el privilegio de acceso a los distintos niveles de información.



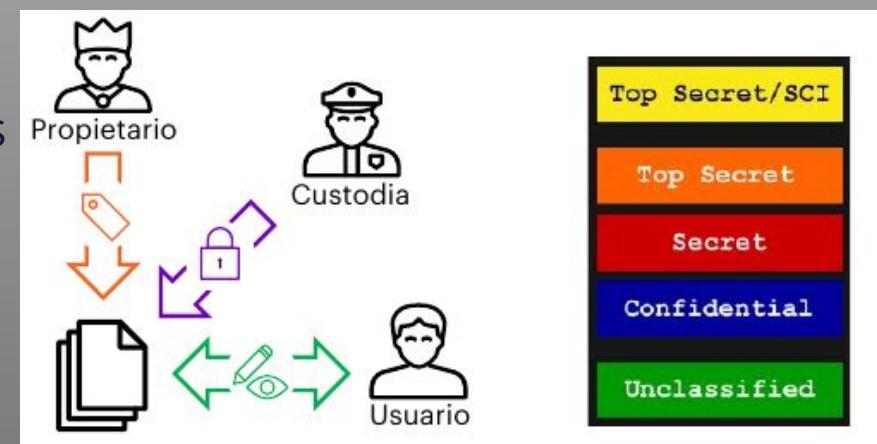
# Conceptos Básicos: Autorización

Validación de los **permisos** de un actor para la realización de acciones sobre recursos del sistema.

- Busca establecer controles de lectura, escritura o ejecución según las políticas de **control de acceso**.

Conceptos relacionados:

- Propiedad y privacidad de datos
- Clasificación de la información



# Conceptos básicos: Irrefutabilidad

**Irrefutabilidad** (no rechazo o no repudio): Imposibilidad, para una persona usuaria, programa o proceso, de negar (rechazar) la autoría de una acción.

En caso de participar en un proceso de comunicación, podemos hablar de:

- **No repudio de origen:** la persona emisora no puede negar que realizó un envío porque la receptora tiene una prueba infalsificable del origen del envío.
- **No repudio de destino:** la persona receptora no puede negar que recibió el mensaje porque la persona emisora tiene pruebas de la recepción.

# Conceptos Básicos: Otros conceptos importantes

- **Auditabilidad:** Permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados.
- **Protección a la réplica:** impedir la realización de "ataques de repetición", como podría ser efectuar varias veces una misma transacción bancaria.
- **Huella digital:** rastro que dejas cuando navegas por Internet. Se recopilan a través de cookies.

# Conceptos Básicos: Debilidad y vulnerabilidad

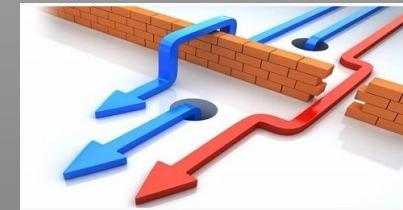
- Un error o **debilidad** es un defecto de software, hardware o firmware.
- Una **vulnerabilidad** es la debilidad de cualquier tipo que compromete la seguridad de un sistema informático.

Es usualmente desconocida tanto para las personas programadoras del software como para el gran público (que ignoran que tienen una brecha potencialmente peligrosa en sus sistemas), pero no así para los potenciales atacantes.

¿Cómo se encuentran entonces estos puntos débiles?

- Por un análisis minucioso y detallado
- Por un uso indebido
- Sencillamente, de manera accidental.

Cuando se produce una vulnerabilidad, el punto débil puede causar que los programas o los sistemas operativos se comporten de manera extraña, no deseada o no planificada.



# Conceptos Básicos: Debilidad y vulnerabilidad

Cuando se produce una vulnerabilidad, el punto débil puede causar que los programas o los sistemas operativos se comporten de manera extraña, no deseada o no planificada.

Un atacante que conozca una vulnerabilidad puede utilizar este comportamiento extraño para crear una brecha por donde apoderarse de información sensible o penetrar en el sistema y lograr que se ejecute su código malicioso.



# Conceptos Básicos: Vector de ataque

Un **vector de ataque** es la ruta o método que un atacante utiliza para acceder a un sistema o red con el fin de explotar vulnerabilidades y causar daño.

Esencialmente, es la forma en que un ciberdelincuente intenta entrar en un sistema para obtener acceso no autorizado a datos confidenciales o interrumpir operaciones.

Algunos de los principales vectores de ataque son el correo electrónico (phishing, malware), la navegación web (malware, sitios web falsos), contraseñas débiles, configuraciones erróneas, vulnerabilidades en software y hardware y la Ingeniería Social.



# Conceptos Básicos: Amenaza y Riesgo

El **riesgo** se puede definir como Probabilidad x Impacto. El impacto es el resultado en caso de la explotación exitosa de una debilidad y la probabilidad es la posibilidad de que suceda.

Una **amenaza** es cualquier indicio perjudicial hacia un componente o flujo de datos que pueda materializarse en un compromiso de confidencialidad, integridad o disponibilidad de los datos.





03

# Ciberataques



# Ciberataques: Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.



<https://www.nexotur.com/noticia/127870/nexotur/el-61-de-los-ciberataques-a-empresas-turisticas-ocurren-en-verano.html#images>

# Ciberataques

Vamos a ver los principales tipos de ciberataque a través del documento:

## Guía de ciberataques

Este documento ha sido elaborado y publicado por la Oficina de Seguridad del Internauta (OSI) del Instituto del Instituto Nacional de Ciberseguridad (INCIBE).



04

# Modelos de amenazas



# Modelos de amenazas: Amenaza

**Amenazas:** Según la RAE: "Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo."

En informática el bien máspreciado es la información, y nuestro esfuerzo se va a encaminar a proteger los datos.

Podemos agrupar las amenazas en dos bloques principales:

- **Amenazas físicas.**
- **Amenazas lógicas.**

Aunque también tenemos otra categoría especial que puede ir relacionada con las anteriores:

- **Ingeniería social**

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- **Personas**
- **Programas o aplicaciones** específicas
- **Catástrofes naturales.**

# Modelos de amenazas: amenazas físicas

Las amenazas físicas más comunes de los sistemas informáticos pueden dividirse en cuatro puntos principales:

- Acceso físico.
- Desastres del entorno y averías del hardware.
- Desastres naturales.
- Radiaciones electromagnéticas.



# Modelos de amenazas: Amenazas físicas

**Acceso físico:** cuando existe acceso físico a un recurso ya no existe seguridad alguna sobre el mismo, con el consiguiente riesgo.

- Un error típico de seguridad por acceso físico es el de tomas de conexión a la red informática no controladas, de acceso libre: un atacante con los suficientes conocimientos técnicos puede causar graves daños.
- Las redes de acceso público y la red interna del instituto están virtualizadas y aisladas.



<https://www.piqsels.com/es/public-domain-photo-fhgei>

# Modelos de amenazas: amenazas físicas

En el apartado 3: **Ciberataques**, en el documento : [\*\*Guía de ciberataques\*\*](#), concretamente en el punto 1 del documento: **Ataques a contraseñas**, hemos podido ver alguno de los tipos de amenazas físicas, aunque en este caso no es acceso físico sino **acceso remoto**.



# Modelos de amenazas: Amenazas físicas

**Desastres del entorno y averías del hardware:** picos de sobretensión que puedan quemar componentes, apagones que afecten a los servidores, incendios, etc.

- Pueden tener un impacto importante si no se habilitan las medidas de protección adecuadas.
- Lo mismo ocurre con los desastres naturales.



# Modelos de amenazas: amenazas físicas

**Radiaciones electromagnéticas:** Cualquier aparato eléctrico emite radiaciones y éstas se pueden capturar y reproducir si se dispone del equipamiento adecuado.

- Un posible atacante podría capturar los datos tecleados en un teclado inalámbrico (no decimos que sea fácil, pero es factible), por no hablar de las redes WiFi abiertas, un auténtico coladero de seguridad.



<https://www.publicdomainpictures.net/pictures/520000/nahled/data-hacker.jpg>

# Modelos de amenazas: amenazas lógicas

En el apartado 3: **Ciberataques**, en el documento : [Guía de ciberataques](#), concretamente en los puntos 3 y 4 del documento: **Ataques a las conexiones** y **Ataques por malware**, podemos ver las principales amenazas lógicas.



# Modelos de amenazas: Ingeniería Social

El punto más frágil de un sistema informático lo constituyen, casi siempre, las personas relacionadas con él.

Ataques al **eslabón más débil → las personas.**



Para acceder a un sistema bien protegido lo más sencillo es hacerlo a través de los usuarios que tienen acceso al mismo (mediante engaño o manipulación).

# Modelos de amenazas: Ingeniería Social



Fuente:  
<https://www.incibe.es/aprendeciberseguridad/ingenieria-social>

# Modelos de amenazas: Ingeniería Social

En el apartado 3: **Ciberataques**, en el documento : [\*\*Guía de ciberataques\*\*](#), concretamente en el punto 2 del documento: **Ataques por ingeniería social**, hemos podido ver alguno de los tipos de amenazas por Ingeniería Social. Vemos como en la mayoría de las ataques somos los usuarios y empleados los que proporcionamos el acceso o los datos para acceder.



# Modelos de amenazas: Amenazas en entornos Web

## Seguridad en Cliente vs. Seguridad en Servidor

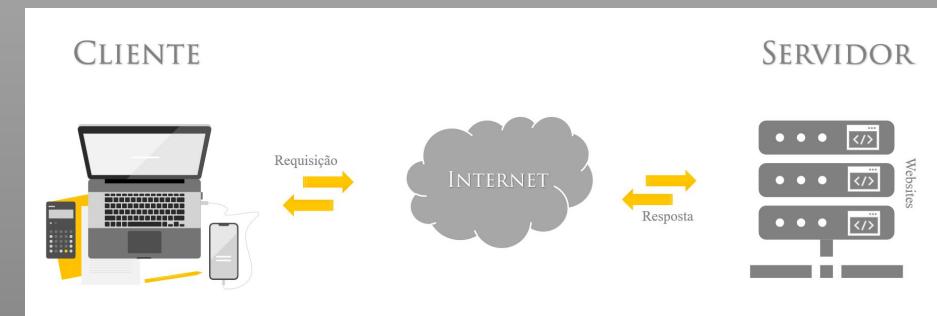
- **Cliente:** Protección contra ataques como XSS, CSRF.
- **Servidor:** Protección contra inyecciones, desbordamientos de buffer, accesos indebidos.

## Vectores de Ataque Comunes

- Ingeniería social
- Malware y Ransomware
- Phishing
- Vulnerabilidades de software

## Evaluación de Riesgos

- Identificación de activos
- Análisis de Amenazas y Vulnerabilidades
- Planes de Mitigación



[https://upload.wikimedia.org/wikipedia/commons/0/09/Cliente\\_servidor.png](https://upload.wikimedia.org/wikipedia/commons/0/09/Cliente_servidor.png)

# Modelos de amenazas

## ¿Cómo se explota una página web?

El sistema informático que soporta una aplicación se puede explotar en varios niveles: a nivel del sistema, a nivel del servidor y a nivel de aplicación.

## ¿Qué debilidades se pueden encontrar?

A cada uno de los niveles, existen varias debilidades típicas que pueden ser utilizadas como vector de ataque.

Sistema	Servidor	Aplicación
<input type="checkbox"/> Software desactualizado	<input type="checkbox"/> Autorización incorrecta	<input type="checkbox"/> Parámetros no controlados
<input type="checkbox"/> Autenticaciones débiles	<input type="checkbox"/> Exposición de información	<input type="checkbox"/> Lógica de negocio no controlada
<input type="checkbox"/> Servicios innecesarios	<input type="checkbox"/> Funcionalidades no controladas	<input type="checkbox"/> Abuso de valores por defecto
<input type="checkbox"/> Cifrados débiles	<input type="checkbox"/> Seguridad por defecto	<input type="checkbox"/> Prácticas de desarrollo inseguras

# Modelos de amenazas: Seguridad en el Cliente

Los ataques en el cliente afectan principalmente al usuario final y a su navegador.

Algunos de los **ataques más comunes** son:

- o **Cross-Site Scripting (XSS)**: Permite a un atacante injectar scripts maliciosos en sitios web legítimos, robando información del usuario o redirigiéndolo a sitios fraudulentos.
- o **Cross-Site Request Forgery (CSRF)**: Engaña al usuario para que ejecute acciones no deseadas en un sitio donde ya está autenticado.
- o **Clickjacking**: Manipulación de la interfaz web para que el usuario haga clic en elementos invisibles, permitiendo acciones involuntarias.
- o **Uso de contenido inseguro**: Descarga de archivos maliciosos o ejecución de scripts dañinos.

**Medidas de seguridad:** Uso de Content Security Policy (CSP), SameSite Cookies, validación de entradas, autenticación segura.

JUNTA DE EXTREMADURA



Financiado por  
la Unión Europea  
NextGenerationEU



# Modelos de amenazas: Seguridad en el Servidor

**Los ataques en el servidor afectan la infraestructura del sitio web y los datos almacenados.**

Ejemplos incluyen:

- **Inyección SQL:** Inserción de código SQL malicioso para acceder, modificar o eliminar datos de la base de datos.
- **Desbordamiento de buffer:** Manipulación de la memoria del servidor para ejecutar código malicioso.
- **Accesos indebidos:** Uso de credenciales robadas o forzadas para ingresar a sistemas sin autorización.
- **Denegación de Servicio (DoS/DDoS):** Sobrecarga de tráfico para dejar inoperativo un servidor.

**Medidas de seguridad:** Uso de firewalls, autenticación multifactor (MFA), cifrado de datos, actualización de software.

# Modelos de amenazas: Evaluación de riesgos

La evaluación de riesgos en entornos web es clave para prevenir ataques y proteger los datos. Se basa en tres fases:

## 1. Identificación de Activos.

- Listar los elementos críticos de la infraestructura web. Ejemplo: Bases de datos, servidores, aplicaciones, APIs, credenciales.

## 2. Análisis de Amenazas y Vulnerabilidades

- Identificar posibles amenazas y evaluar su impacto. Métodos: Pruebas de penetración (pen testing), escaneos de vulnerabilidades.  
Ejemplo: Un firewall mal configurado puede permitir accesos no autorizados.

## 3. Planes de Mitigación

- Definir estrategias para reducir riesgos y responder a incidentes.  
Ejemplo: Implementar copias de seguridad cifradas y segmentación de red.



05

# Estrategias de Protección y Buenas Prácticas



# Estrategias de prevención generales



Fuente:  
[https://www.incibe.es/empresas/  
/blog/decálogo-de-ciberseguridad-mejora-el-nivel-de-protección-de-tu-empresa](https://www.incibe.es/empresas/blog/decálogo-de-ciberseguridad-mejora-el-nivel-de-protección-de-tu-empresa)

# 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).



<https://topofthelist.net/is-your-website-secure/>

JUNTA DE EXTREMADURA



Plan de  
Recuperación,  
Transformación  
y Resiliencia



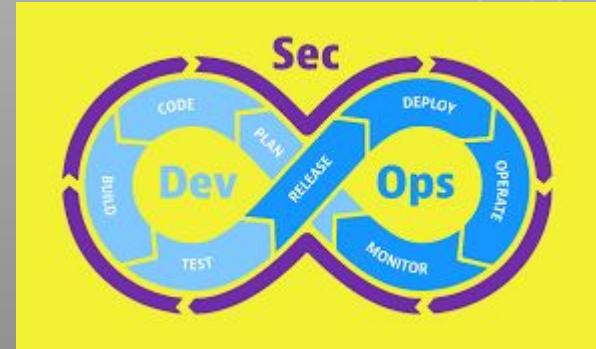
Financiado por  
la Unión Europea  
NextGenerationEU



# Buenas prácticas

## 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.

<https://commons.wikimedia.org/wiki/File:DevSecOps.jpg>



06

# NORMATIVAS Y ESTÁNDARES DE SEGURIDAD WEB



# NORMATIVAS Y ESTÁNDARES DE SEGURIDAD WEB

## 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.
- Otros...



<https://freesvg.org/1542668244>



# NORMATIVAS Y ESTÁNDARES DE SEGURIDAD WEB

## 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](#))

# Bibliografía y Webgrafía

- **Puesta en Producción Segura.** *Rafael López García*
- **Introducción a la Seguridad Web: Fundamentos de seguridad, OWASP Top Ten, Normativas.** *Rafael Ferrer.*
- **Basic Principles for Secure Application Development.** *Accenture Security. CNE-Cert*
- **Introducción a la ciberseguridad.** *INCIBE*



# Gracias!

¿Alguna pregunta?



[informatica.iesvalledeljerteplasencia.es](http://informatica.iesvalledeljerteplasencia.es)



[coordinacion.cenfp@iesvp.es](mailto:coordinacion.cenfp@iesvp.es)



C/ Pedro y Francisco González, s/n  
10600, Plasencia (Cáceres)



927 01 77 74

