SEGURIDAD EN APP WEB

Leon Ernesto Marmolejo Torres

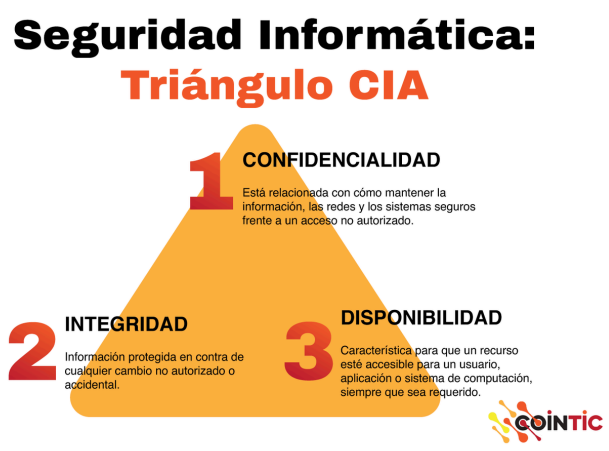
Conjunto de prácticas, herramientas y políticas diseñadas para proteger sistemas, redes, programas y datos de ataques, daños o accesos no autorizados.

¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

- Confidencialidad: La información solo es accesible para usuarios autorizados.
- Integridad: Los datos son exactos y no han sido alterados de forma no autorizada.
- Disponibilidad: Los sistemas y datos son accesibles cuando se necesitan.

EL TRIÁNGULO DE LA SEGURIDAD

Este modelo representa los tres pilares fundamentales que toda estrategia de seguridad debe equilibrar.



ESTRATEGIAS DE SEGURIDAD POR CAPAS

SEGURIDAD EN EL FRONT-END (Cliente)

- Validación de Entrada: Siempre validar y sanitizar los datos en el cliente para una mejor experiencia de usuario, pero NUNCA confiar únicamente en esto.
  -
- Protección XSS (Cross-Site Scripting): Sanitizar el contenido renderizado para evitar la inyección de scripts maliciosos.
  -
- Headers de Seguridad (CSP): Usar Content Security Policy para restringir qué recursos (scripts, estilos) puede cargar el navegador.
  -
- Autenticación Segura: Implementar flujos robustos (OAuth, JWT) y almacenar tokens de forma segura (HttpOnly cookies).

SEGURIDAD EN EL BACK-END (SERVIDOR)

- Validación y Sanitización Estrictas: Validar SIEMPRE toda la entrada del usuario en el servidor. Nunca confiar en el front-end.
-
- Protección contra Inyección SQL: Usar consultas parametrizadas o ORMs para evitar que se ejecuten comandos SQL maliciosos.
-
- Autenticación y Autorización Robustas:
- Autenticación: Verificar identidad (ej. con bcrypt para contraseñas).
- Autorización: Verificar permisos (ej. Middleware, RBAC).
-
- Gestión Segura de Sesiones: Implementar sesiones con tokens únicos, tiempos de expiración y regeneración de ID de sesión.
- Rate Limiting: Limitar el número de peticiones de un usuario/IP para prevenir fuerza bruta y abuso.

SESIONES VS. COOKIES

SESIONES	COOKIES
En el servidor (en memoria, BD o cache).	**En el navegador del cliente** (dispositivo del usuario).
Más seguras. La información sensible no sale del servidor.	**Menos seguras.** Son accesibles y modificables por el cliente.
ID de sesión, datos del usuario, carrito de compras.	Preferencias, ID de sesión (ej. `sessionId`), tokens de rastreo.
Generalmente caducan tras un periodo de inactividad.	Pueden tener fecha de expiración (persistentes) o ser de sesión (se borran al cerrar el navegador).
Mayor, ya que se deben gestionar y almacenar los estados.	Menor, el servidor no almacena el estado de cada usuario.