📘 Glosario: Autenticación y Autorización en Aplicaciones Web

---

1. Autenticación (Authentication)

Proceso de verificar la identidad de un usuario o sistema. Se asegura de que una entidad que intenta acceder a un recurso sea quien dice ser. Comúnmente realizado a través de contraseñas, biometría, o métodos más complejos como **autenticación multifactor (MFA)**.

---

2. Autorización (Authorization)

Proceso de determinar qué recursos o acciones puede realizar un usuario o sistema después de ser autenticado. Dependiendo de los permisos otorgados, un usuario puede tener acceso a diferentes partes de un sistema o realizar ciertas acciones.

---

3. Autenticación Multifactor (MFA - Multi-Factor Authentication)

Método de autenticación que requiere más de una prueba de identidad antes de conceder acceso. Generalmente combina dos o más de los siguientes factores:

- **Algo que sabes** (como una contraseña o PIN).
- **Algo que tienes** (como un token o un teléfono móvil).
- **Algo que eres** (como una huella dactilar o reconocimiento facial).

---

4. Contraseña Hashing (Password Hashing)

Proceso de convertir una contraseña en una cadena de texto irreconocible utilizando un algoritmo matemático, generalmente acompañado de un **salting** (adición de datos aleatorios). Esto aumenta la seguridad de la contraseña almacenada al hacerla irrecuperable en su forma original.

---

5. Salting

Técnica utilizada en conjunto con el **hashing** para mejorar la seguridad de las contraseñas. Consiste en agregar un valor aleatorio (sal) a la contraseña antes de aplicar el algoritmo de hashing, de modo que contraseñas idénticas no generen el mismo hash.

---

6. JSON Web Token (JWT)

Un estándar abierto (RFC 7519) que define un método compacto y autónomo para transmitir información entre partes de manera segura, como parte de los procesos de autenticación y autorización. Generalmente se utiliza en **autenticación basada en tokens** y **autorización basada en roles**.

---

7. OAuth (Open Authorization)

Un protocolo abierto para autorización que permite a los usuarios otorgar acceso a sus recursos en un servidor sin compartir sus credenciales. OAuth se utiliza ampliamente en la **autenticación delegada** y es fundamental en la autorización de aplicaciones de terceros.

---

8. OpenID Connect (OIDC)

Una capa de identidad basada en OAuth 2.0 que permite a las aplicaciones verificar la identidad de un usuario basándose en la autenticación realizada por un servidor de autorización. OIDC es un estándar moderno para implementar la **autenticación única (SSO)**.

---

9. Single Sign-On (SSO)

Método de autenticación que permite a un usuario acceder a múltiples aplicaciones utilizando un solo conjunto de credenciales, mejorando la experiencia del usuario y aumentando la seguridad al reducir el número de contraseñas necesarias.

---

10. Control de Acceso Basado en Roles (RBAC - Role-Based Access Control)

Modelo de autorización que limita el acceso a recursos en función de los roles asignados a los usuarios dentro de un sistema. Los permisos se asignan a los roles y los usuarios obtienen permisos a través de los roles que se les asignan.

---

11. Control de Acceso Basado en Atributos (ABAC - Attribute-Based Access Control)

Modelo de control de acceso que determina si se permite o deniega el acceso a un recurso en función de los **atributos** del usuario, del recurso, o del entorno. Es más flexible que RBAC porque tiene en cuenta más factores en tiempo real.

---

12. Control de Acceso Basado en Reglas (RBAC - Rule-Based Access Control)

Modelo de autorización que permite definir reglas específicas para determinar el acceso a recursos, a menudo basado en el contexto o atributos dinámicos, como la ubicación del usuario o la hora del día.

---

13. Access Control List (ACL)

Conjunto de reglas que definen qué usuarios o sistemas tienen acceso a qué recursos dentro de una red o sistema. Se utilizan para **controlar el acceso** a directorios, archivos, dispositivos y servicios dentro de un sistema.

---

14. Token de Acceso (Access Token)

Elemento clave en el proceso de **autorización delegada**, utilizado para otorgar acceso a recursos protegidos sin necesidad de compartir las credenciales del usuario. Es comúnmente usado en protocolos como **OAuth** y **OpenID Connect**.

---

15. Web Application Firewall (WAF)

Dispositivo o servicio que filtra, monitorea y bloquea el tráfico HTTP hacia y desde una aplicación web. Su objetivo principal es proteger contra ataques como **inyección SQL**, **XSS**, y **CSRF**. Actúa como una capa de defensa adicional entre la aplicación web y el tráfico malicioso.

---

16. Cross-Site Scripting (XSS)

Vulnerabilidad de seguridad que permite a los atacantes inyectar scripts maliciosos en las páginas web vistas por otros usuarios. Existen varios tipos de XSS: **reflejado**, **almacenado** y **basado en DOM**.

17. Cross-Site Request Forgery (CSRF)

Ataque en el que un atacante engaña a un usuario autenticado para realizar acciones no deseadas en una aplicación web en la que el usuario está autenticado. Para mitigar este riesgo, se utiliza la **verificación de tokens** en los formularios.

---

18. HTTP Strict Transport Security (HSTS)

Mecanismo de seguridad que obliga a los navegadores a interactuar con un servidor web solo a través de conexiones seguras (HTTPS), impidiendo que los usuarios se conecten a través de HTTP, lo que previene los ataques de **downgrade**.

---

19. Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

Protocolos criptográficos que proporcionan seguridad en la comunicación a través de redes. SSL ha sido reemplazado por TLS debido a vulnerabilidades en versiones anteriores de SSL.

---

20. Least Privilege

Principio de seguridad según el cual los usuarios deben recibir solo los permisos mínimos necesarios para realizar sus tareas. Aplicar el principio de **mínimo privilegio** ayuda a reducir el impacto de posibles vulnerabilidades o compromisos de seguridad.
