📘 Glosario: Gestión de Sesiones, Autenticación y Autorización

---

1. Autenticación (Authentication)

El proceso mediante el cual se verifica la **identidad de un usuario** antes de permitirle acceder a un sistema. Este proceso puede implicar el uso de contraseñas, **autenticación multifactor (MFA)**, o biometría.

---

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

Método de autenticación que requiere múltiples factores para verificar la identidad del usuario. Generalmente, estos factores incluyen:

- **Algo que el usuario sabe** (contraseña).
- **Algo que el usuario tiene** (código enviado por SMS, token).
- **Algo que el usuario es** (biometría, como huella dactilar o reconocimiento facial).

---

3. Autorización (Authorization)

Proceso que determina qué recursos o acciones un usuario autenticado tiene permitido realizar dentro de un sistema. A menudo se implementa mediante **control de acceso** basado en roles (RBAC) o atributos (ABAC).

---

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

Modelo de autorización donde los permisos de acceso son asignados según el **rol** del usuario dentro de la organización. Por ejemplo, un **administrador** puede tener acceso completo, mientras que un **empleado** solo acceso a sus propios datos.

---

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

Modelo de control de acceso donde los permisos de acceso se determinan utilizando **atributos** de los usuarios, recursos, o el contexto en el que se realiza la solicitud. Los atributos pueden incluir el **hora**, **ubicación**, **tipo de dispositivo**, etc.

---

6. Sesión (Session)

Conjunto de interacciones entre un **usuario** y una **aplicación** que se mantiene durante un período determinado. La sesión es identificada a través de un **token de sesión** que asegura que el usuario no tenga que autenticarse repetidamente durante esa interacción.

---

7. Secuestro de Sesión (Session Hijacking)

Ataque en el que un atacante obtiene acceso no autorizado a una **sesión activa** de un usuario. Esto se puede hacer interceptando el **token de sesión** o explotando vulnerabilidades en la gestión de sesiones.

---

8. Token de Sesión (Session Token)

Identificador único que se genera al inicio de una sesión de usuario. Este token es almacenado en el cliente (en una **cookie** o almacenamiento local) y es utilizado para verificar la identidad del usuario en cada solicitud que realiza al servidor.

---

9. JWT (JSON Web Token)

Estándar abierto (RFC 7519) para la creación de **tokens compactos** que permiten representar de manera segura información entre dos partes. Se utiliza en la autenticación y autorización de aplicaciones web modernas, especialmente en **APIs** RESTful.

---

10. Cookies

Archivos pequeños que se almacenan en el navegador del usuario y que contienen información sobre la sesión, como el **token de sesión**. Las cookies deben configurarse adecuadamente con **flags** de seguridad (**Secure**, **HttpOnly**, **SameSite**) para prevenir ataques como **XSS** o **secuestramiento de sesión**.

---

11. HTTPOnly

Atributo de una cookie que impide que JavaScript acceda a su contenido, aumentando la seguridad frente a ataques de **Cross-Site Scripting (XSS)**.

---

12. Secure Cookie

Atributo de una cookie que asegura que solo será enviada a través de conexiones seguras HTTPS, protegiendo la información sensible de ser interceptada a través de **ataques Man-in-the-Middle (MITM)**.

---

13. SameSite Cookie Attribute

Atributo que ayuda a prevenir ataques de **Cross-Site Request Forgery (CSRF)** al restringir el envío de cookies con solicitudes de orígenes cruzados (diferentes dominios).

---

14. CSRF (Cross-Site Request Forgery)

Vulnerabilidad que permite a un atacante realizar acciones no autorizadas en una aplicación en la que el usuario está autenticado, mediante el envío de solicitudes maliciosas.

---

15. HTTPS (HyperText Transfer Protocol Secure)

Versión segura del **HTTP** que utiliza **SSL/TLS** para cifrar los datos transmitidos entre el cliente y el servidor, asegurando la privacidad e integridad de la información, incluidas las cookies de sesión.

---

16. Expiración de Sesión (Session Expiration)

Proceso por el cual una sesión de usuario es automáticamente cerrada después de un período de inactividad determinado. Esto ayuda a minimizar el riesgo de **secuestro de sesión**.

---

17. Reautenticación (Reauthentication)

Proceso en el que un usuario es solicitado a ingresar sus credenciales nuevamente para realizar una acción sensible, como cambiar la contraseña o realizar transacciones financieras.

---

18. Single Sign-On (SSO)

Sistema de autenticación que permite a un usuario iniciar sesión una sola vez y acceder a múltiples aplicaciones sin tener que autenticarse repetidamente. SSO se basa en protocolos como **OAuth** y **SAML**.

---

19. Expiración de Token

Proceso mediante el cual los **tokens de sesión** (como los **JWT**) tienen una fecha de expiración. Después de este período, el usuario debe autenticarse nuevamente para obtener un nuevo token.

---

20. Session Fixation

Ataque en el que el atacante logra fijar el valor de un token de sesión antes de que el usuario inicie sesión, lo que le permite secuestrar la sesión del usuario una vez que se autentica.
