Glosario

Terminología de seguridad informática y ciberseguridad:

1. **Amenaza:** Cualquier evento o circunstancia que puede causar daño o perjuicio a los sistemas de información.
2. **Ataque:** Acción intencional realizada por un individuo o grupo para comprometer la seguridad de un sistema o red.
3. **Autenticación:** Proceso de verificar la identidad de un usuario o dispositivo antes de permitir el acceso a un sistema o red.
4. **Cortafuegos (Firewall):** Un cortafuegos es un sistema de seguridad que controla el tráfico de red y filtra las comunicaciones entrantes y salientes según una serie de reglas predefinidas.
5. **Criptografía:** Conjunto de técnicas y algoritmos utilizados para proteger la confidencialidad y la integridad de la información mediante la encriptación y el cifrado.
6. **Malware:** Software malicioso diseñado para dañar, alterar o robar información de un sistema sin el consentimiento del usuario.
7. **Phishing:** Técnica de ingeniería social utilizada para engañar a los usuarios y obtener información confidencial, como contraseñas o datos bancarios, haciéndose pasar por una entidad confiable.
8. **Ransomware:** Tipo de malware que bloquea el acceso a los archivos o sistemas de un usuario hasta que se pague un rescate.
9. **Vulnerabilidad:** Debilidad o fallo en un sistema o software que podría ser aprovechado por atacantes para comprometer la seguridad.
10. **Exploit:** Un exploit es un código o técnica utilizada para aprovechar una vulnerabilidad y comprometer la seguridad de un sistema.
11. **Firewall de aplicación web (WAF):** Es un firewall específicamente diseñado para proteger aplicaciones web de ataques como inyección de SQL, cross-site scripting (XSS) u otros ataques comunes.
12. **Ingeniería social:** Táctica utilizada para manipular y engañar a las personas con el fin de obtener información confidencial o acceso a sistemas protegidos.
13. **VPN (Red Privada Virtual):** Una VPN permite establecer una conexión segura y encriptada entre un dispositivo y una red privada a través de Internet, proporcionando anonimato y protección de datos.
14. **Auditoría de seguridad:** Proceso de evaluación de la seguridad de un sistema o red para identificar vulnerabilidades, debilidades y posibles riesgos.
15. **Incidente de seguridad:** Evento o suceso que compromete o intenta comprometer la confidencialidad, integridad o disponibilidad de los sistemas de información.
16. **La autenticación multifactor (multi factor authentication o MFA):** es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción.

Legislación en Argentina:

Bajo la dirección del Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el **Gobierno de Argentina** ha desarrollado un proyecto de **Estrategia Nacional de Seguridad Cibernética.**
Además, se han aprobado diversas normas relacionadas con la ciberseguridad:

- **Ley 26.388 de Delito informático**

Esta ley especial introduce la tipificación de nuevos delitos a distintos artículos del Código Penal de la Nación. En esta ley se incorporan sanciones en los siguientes casos:

  - Posesión de pornografía infantil con la finalidad de distribuirla por Internet o a través de otros medios electrónicos.
  - La apropiación, violación y difusión de comunicaciones electrónicas.
  - Interceptar cualquier tipo de comunicaciones electrónicas.
  - Suspensión de las comunicaciones electrónicas.
  - Acceder ilícitamente a sistemas informáticos.
  - Acceder a bases de datos personales.
  - Comunicar información almacenada en bases de datos personales.
  - Causar daños informático y propagar virus.
  - Introducir datos falsos en un archivo de datos personales.
  - Cometer fraude informático.
  - Causar daño o sabotaje informático.

- **Ley 25.326 de Protección de Datos Personales**

Esta ley tiene por objeto la protección integral de los datos personales recogidos en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

- **Decreto Reglamentario N°1558/2001**

Este reglamento desarrolla la ley de Protección de datos. Establece los principios generales relativos a la Protección de datos personales, los derechos de los titulares de los datos, usuarios y responsables de archivos, registros y bancos de datos, los controles necesarios y las sanciones.

- **Ley 25.506 de Firma Digital**
  Con esta ley se admite y se fijan las condiciones para el uso de la firma electrónica y de la firma digital reconociendo su eficacia jurídica. También se instaura la Infraestructura de Firma Digital de la República Argentina.

- **Ley 26.904 de Grooming**
  En esta ley se regula el grooming y se considera un delito castigado con penas de 6 meses a 4 años a los adultos que se contacten por medio de comunicaciones electrónicas a menores de edad con el propósito de cometer cualquier delito contra la integridad sexual.

- **Ley 27.126 de Inteligencia Nacional**
  Esta ley define el marco jurídico dentro del que deben llevarse a cabo las actuaciones de inteligencia del Estado. Concreta que esas actuaciones tendrán que realizarse conforme la Constitución Nacional, los tratados de derechos humanos y cualquier otra ley que recoja derechos y garantías.
  Además, en esta ley se crea la **Agencia Federal de Inteligencia**, dependiente del Poder Ejecutivo Nacional. Se considera el órgano superior del Sistema de Inteligencia Nacional. A este órgano se le atribuyen funciones relacionadas con la creación de inteligencia nacional y la producción de inteligencia criminal.

Seguridad de las aplicaciones bancarias

1. **Autenticación de dos factores (2FA)**: Un método de seguridad que requiere dos formas diferentes de autenticación (por ejemplo, contraseña y código enviado por SMS) para verificar la identidad de un usuario.
2. **Phishing:** Técnica utilizada por ciberdelincuentes para obtener información confidencial, como contraseñas o datos bancarios, haciéndose pasar por una entidad legítima a través de mensajes de correo electrónico, SMS o llamadas telefónicas.
3. **Malware móvil:** Software malicioso diseñado específicamente para atacar dispositivos móviles, como smartphones o tablets, con el objetivo de robar información o acceder a cuentas bancarias.
4. **Actualizaciones de seguridad:** Parches y actualizaciones proporcionados por el proveedor de la aplicación bancaria para corregir vulnerabilidades y mejorar la seguridad. Los usuarios deben asegurarse de mantener su aplicación siempre actualizada.
5. **Contraseñas seguras:** Combinaciones de letras, números y símbolos utilizados para proteger el acceso a la aplicación bancaria. Las contraseñas seguras deben ser únicas, largas y difíciles de adivinar.
6. **Pharming:** Técnica en la que los ciberdelincuentes redirigen a los usuarios a sitios web falsos y maliciosos para robar su información personal y financiera.
7. **Transacciones no autorizadas**: Actividades realizadas en una cuenta bancaria sin el consentimiento del titular. Puede incluir cargos fraudulentos, transferencias no autorizadas o retiros indebidos.
8. **Ataques de fuerza bruta:** Método utilizado por los atacantes para probar una amplia gama de combinaciones de contraseñas hasta encontrar la correcta y obtener acceso no autorizado a una cuenta bancaria.
9. **Suplantación de identidad (Identity Theft):** El acto de robar información personal y financiera de una persona para hacerse pasar por ella y realizar actividades fraudulentas, como abrir cuentas bancarias o solicitar préstamos a su nombre.
10. **Seguridad en redes Wi-Fi públicas:** Las redes Wi-Fi públicas pueden ser inseguras y propensas a ataques. Los usuarios deben evitar realizar transacciones financieras sensibles o acceder a aplicaciones bancarias en redes Wi-Fi abiertas y utilizar una conexión VPN para mayor seguridad.
11. **Autorización de transacciones:** Proceso de verificación y aprobación de una transacción financiera antes de que se lleve a cabo. Los usuarios deben revisar cuidadosamente y confirmar cualquier transacción antes de autorizarla.
12. **Actualización de información de contacto:** Mantener actualizados los datos de contacto asociados a la cuenta bancaria, como número de teléfono y dirección de correo electrónico, para recibir notificaciones de seguridad y alertas relacionadas con la cuenta.