MF0489_3 Sistemas seguros de acceso y transmisión de datos

Módulo 4

UNIDAD DIDÁCTICA 1. CRIPTOGRAFÍA

Perspectiva histórica y objetivos de la criptografía.

Perspectiva histórica de la criptografía:

- **Orígenes antiguos:**
  - La criptografía tiene raíces que se remontan a miles de años. Civilizaciones antiguas como la egipcia, la griega y la romana ya utilizaban técnicas rudimentarias para ocultar mensajes.
  - El cifrado César, utilizado por Julio César, es un ejemplo clásico de cifrado por sustitución.
- **Desarrollo a lo largo de la historia:**
  - A lo largo de la Edad Media y el Renacimiento, la criptografía evolucionó con la invención de cifrados más complejos.

- Durante las guerras mundiales, la criptografía desempeñó un papel crucial en la comunicación militar. La máquina Enigma, utilizada por los alemanes en la Segunda Guerra Mundial, es un ejemplo destacado.

- **Era moderna:**
  - Con la llegada de las computadoras, la criptografía experimentó una revolución. Los algoritmos modernos son mucho más sofisticados y seguros.
  - La criptografía se ha convertido en una herramienta esencial para la protección de la información en el mundo digital, desde la banca en línea hasta la comunicación segura.

Objetivos de la criptografía:

La criptografía tiene cuatro objetivos principales:

- **Confidencialidad:**
  - Garantizar que solo las personas autorizadas puedan acceder a la información.
  - Se logra mediante el cifrado, que transforma la información en un formato ilegible para quienes no tienen la clave de descifrado.
- **Integridad:**
  - Asegurar que la información no ha sido modificada o alterada sin autorización.
  - Se utilizan técnicas como las funciones hash y las firmas digitales para detectar cualquier manipulación de los datos.
- **Autenticación:**
  - Verificar la identidad del remitente o del destinatario de la información.
  - Se utilizan contraseñas, certificados digitales y otros métodos para confirmar la autenticidad de las partes involucradas.
- **No repudio:**
  - Evitar que una persona niegue haber enviado o recibido un mensaje o realizado una transacción.
  - Las firmas digitales y otros mecanismos garantizan que una vez que se realiza una acción, no se pueda negar su autoría.

Importancia en la seguridad de la información:

- La criptografía es fundamental para proteger la información confidencial, como datos bancarios, información personal y secretos comerciales.

- Permite la comunicación segura a través de Internet y otras redes.
- Es esencial para la protección de la propiedad intelectual y la prevención del fraude.

Teoría de la información.

¿Qué es la Teoría de la Información?

- Es una rama de las matemáticas aplicadas y la ingeniería eléctrica que se centra en la cuantificación, el almacenamiento y la comunicación de la información.
- Su objetivo principal es comprender los límites de la transmisión de datos y la eficiencia de la codificación de la información.
- Fue desarrollada principalmente por Claude Shannon en su artículo seminal de 1948, "Una teoría matemática de la comunicación".

Conceptos Clave:

- **Información:**
  - En la teoría de la información, la información se mide en bits, que representan la cantidad de incertidumbre reducida al recibir un mensaje.
  - Cuanto más improbable sea un mensaje, más información contiene.
- **Entropía:**
  - La entropía mide la cantidad de incertidumbre o aleatoriedad en un conjunto de datos.
  - Una alta entropía indica una mayor imprevisibilidad y, por lo tanto, más información.
- **Capacidad del Canal:**
  - La capacidad del canal representa la máxima velocidad a la que se puede transmitir información a través de un canal de comunicación sin errores.
  - El teorema de Shannon-Hartley establece los límites de la capacidad del canal en función del ancho de banda y la relación señal/ruido.
- **Codificación:**
  - La codificación implica la conversión de información en un formato adecuado para la transmisión o el almacenamiento.
  - La teoría de la información proporciona principios para diseñar códigos eficientes que minimicen la redundancia y maximicen la capacidad del canal.

Importancia en la Seguridad Informática:

- **Criptografía:**
  - La teoría de la información es fundamental para la criptografía, ya que proporciona herramientas para analizar la seguridad de los sistemas de cifrado.
  - La entropía se utiliza para evaluar la aleatoriedad de las claves de cifrado, lo que es crucial para la seguridad de los algoritmos criptográficos.
- **Compresión de Datos:**
  - La teoría de la información permite comprender las técnicas de compresión de datos, tanto sin pérdida como con pérdida, que se utilizan extensivamente para comprimir vídeo, audio o ficheros de datos.
- **Detección y Corrección de Errores:**
  - La teoría de la información proporciona los fundamentos para diseñar códigos de detección y corrección de errores, que son esenciales para garantizar la integridad de los datos durante la transmisión.
- **Análisis de Tráfico de Red:**
  - la teoría de la información se utiliza para analizar patrones de tráfico de red y detectar anomalías que pueden indicar ataques cibernéticos.

En resumen:

La teoría de la información proporciona un marco matemático riguroso para comprender la naturaleza de la información y sus límites. Sus principios son esenciales en muchos campos, incluida la seguridad informática, donde se utilizan para diseñar sistemas seguros y eficientes.

Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos.

1. Confidencialidad:

- **Definición:** Garantiza que la información solo sea accesible para personas autorizadas.
- **Criptografía:** Se logra mediante el cifrado, que transforma los datos en un formato ilegible (texto cifrado) utilizando claves criptográficas. Solo quienes posean la clave correcta podrán descifrar la información y acceder al texto original.

- **Ejemplo:** Cifrado de correos electrónicos, mensajes de chat o archivos almacenados en la nube.

2. Integridad:

- **Definición:** Asegura que la información no ha sido alterada durante su transmisión o almacenamiento.
- **Criptografía:** Se utilizan funciones hash criptográficas, que generan una "huella digital" única de los datos. Cualquier modificación en los datos resultará en una huella digital diferente, lo que permite detectar alteraciones.
- **Ejemplo:** Firmas digitales en documentos electrónicos, verificación de la integridad de archivos descargados de Internet.

3. Autenticidad:

- **Definición:** Verifica la identidad del emisor o receptor de la información.
- **Criptografía:** Se utilizan firmas digitales y certificados digitales, que asocian una identidad única a una clave criptográfica. Esto permite confirmar que la información proviene de la fuente declarada.
- **Ejemplo:** Certificados SSL/TLS en sitios web, firmas digitales en transacciones bancarias en línea.

4. No repudio:

- **Definición:** Impide que una persona niegue haber enviado o recibido un mensaje o realizado una transacción.
- **Criptografía:** Se combina la firma digital con el sellado de tiempo, lo que proporciona una prueba irrefutable de la autoría y el momento exacto de la acción.
- **Ejemplo:** Transacciones de comercio electrónico, contratos digitales.

5. Imputabilidad:

- **Definición:** Permite atribuir una acción o información a una persona o entidad específica.
- **Criptografía:** Se logra mediante el uso de claves criptográficas personales y registros de auditoría, que permiten rastrear las acciones realizadas por cada usuario.
- **Ejemplo:** Registros de acceso a sistemas informáticos, auditorías de seguridad.

6. Sellado de tiempo:

- **Definición:** Proporciona una prueba irrefutable del momento exacto en que se creó o modificó una información.

- **Criptografía:** Se utilizan servicios de sellado de tiempo confiables, que generan un certificado digital con la fecha y hora exacta, firmado por una autoridad de confianza.
- **Ejemplo:** Evidencia digital en investigaciones forenses, validación de la antigüedad de documentos electrónicos.

En resumen:

La criptografía es una herramienta esencial para garantizar la seguridad de la información en el mundo digital. Al aplicar técnicas criptográficas adecuadas, se pueden controlar de manera efectiva las propiedades de confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempo, lo que permite proteger la información contra una amplia gama de amenazas.

Elementos fundamentales de la criptografía de clave privada y de clave publica.

Criptografía de Clave Privada (Simétrica)

- **Elementos Fundamentales:**
  - **Clave Secreta:**
    - Se utiliza una única clave para cifrar y descifrar la información.
    - Esta clave debe mantenerse en secreto y compartirse de forma segura entre el emisor y el receptor.
  - **Algoritmo de Cifrado:**
    - Se aplica un algoritmo matemático para transformar el texto plano en texto cifrado utilizando la clave secreta.
  - **Algoritmo de Descifrado:**
    - Se utiliza el mismo algoritmo y la misma clave para revertir el proceso y obtener el texto plano original.
- **Características:**
  - Velocidad: Los algoritmos de clave privada son generalmente más rápidos y eficientes.
  - Simplicidad: Suelen ser más sencillos de implementar.
  - Desafío: La distribución segura de la clave secreta es el principal desafío.
- **Ejemplos:**

- AES (Advanced Encryption Standard).
- DES (Data Encryption Standard).

Criptografía de Clave Pública (Asimétrica)

- **Elementos Fundamentales:**
  - **Par de Claves:**
    - Se generan dos claves relacionadas: una clave pública y una clave privada.
    - La clave pública se puede compartir libremente, mientras que la clave privada debe mantenerse en secreto.
  - **Clave Pública:**
    - Se utiliza para cifrar la información.
    - Cualquier persona puede usarla para enviar mensajes cifrados al propietario de la clave privada.
  - **Clave Privada:**
    - Se utiliza para descifrar la información cifrada con la clave pública correspondiente.
    - Solo el propietario de la clave privada puede descifrar los mensajes.
  - **Algoritmos de Cifrado y Descifrado:**
    - Se utilizan algoritmos matemáticos complejos que hacen que sea computacionalmente inviable derivar la clave privada a partir de la clave pública.
- **Características:**
  - Seguridad: Elimina el problema de la distribución de claves secretas.
  - Flexibilidad: Permite la autenticación y la firma digital.
  - Desafío: Los algoritmos de clave pública son más lentos y requieren más recursos computacionales.
- **Ejemplos:**
  - RSA (Rivest-Shamir-Adleman).
  - Criptografía de curva elíptica (ECC).

Diferencias Clave:

- **Claves:**
  - Clave privada: Una clave.
  - Clave pública: Un par de claves (pública y privada).
- **Velocidad:**
  - Clave privada: Más rápida.
  - Clave pública: Más lenta.
- **Uso:**
  - Clave privada: Cifrado de grandes cantidades de datos.
  - Clave pública: Intercambio seguro de claves, firmas digitales y autenticación.

Características y atributos de los certificados digitales.

Los certificados digitales son herramientas fundamentales en la seguridad informática, actuando como "pasaportes digitales" que verifican la identidad de entidades en línea. Aquí te presento sus características y atributos clave:

Características Principales:

- **Autenticación de Identidad:**
  - Su función primordial es confirmar que una entidad (persona, organización o dispositivo) es quien dice ser.
  - Esto se logra vinculando la identidad de la entidad a una clave pública.
- **Integridad de la Información:**
  - Garantizan que la información contenida en el certificado no ha sido alterada.
  - La firma digital de la Autoridad de Certificación (AC) protege contra manipulaciones.
- **No Repudio:**
  - Proporcionan evidencia de que una entidad realizó una acción, impidiendo que niegue su participación.
  - Esto es crucial en transacciones y comunicaciones importantes.
- **Cifrado de Comunicaciones:**
  - Permiten establecer canales de comunicación seguros mediante el cifrado de datos.

- Esto protege la información confidencial de accesos no autorizados.

Atributos Clave:

- **Información del Titular:**
  - Nombre de la entidad (persona o organización).
  - Dirección de correo electrónico.
  - Otros datos de identificación relevantes.
- **Clave Pública:**
  - La clave pública asociada a la entidad, utilizada para cifrar información.
- **Información de la Autoridad de Certificación (AC):**
  - Nombre de la AC que emitió el certificado.
  - Firma digital de la AC, que valida la autenticidad del certificado.
- **Período de Validez:**
  - Fecha de emisión y fecha de expiración del certificado.
  - Esto limita el tiempo durante el cual el certificado es considerado válido.
- **Número de Serie:**
  - Un identificador único para cada certificado.
- **Información de Uso:**
  - Indicaciones sobre los propósitos para los que se puede utilizar el certificado (por ejemplo, firma digital, cifrado de correo electrónico, autenticación de sitios web).

Importancia:

- Los certificados digitales son esenciales para la seguridad en Internet, permitiendo transacciones en línea seguras, comunicaciones protegidas y autenticación confiable.
- Son utilizados en una amplia gama de aplicaciones, desde el comercio electrónico y la banca en línea hasta la firma digital de documentos y la autenticación de usuarios en sistemas informáticos.
- Es importante recordar que los certificados digitales son emitidos por Autoridades de Certificación, que son entidades de confianza que verifican la identidad de los titulares de los certificados.

Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente.

1. Intercambio de Claves Diffie-Hellman (DH):

- **Funcionamiento:**
  - Permite a dos partes generar una clave secreta compartida a través de un canal inseguro.
  - Se basa en la dificultad del problema del logaritmo discreto en campos finitos.
  - Las partes intercambian información pública y realizan cálculos matemáticos para derivar la clave secreta.
- **Características:**
  - No requiere el intercambio previo de claves secretas.
  - Vulnerable a ataques de "man-in-the-middle" si no se autentican las partes.
  - Existen variantes como el Diffie-Hellman efímero (DHE) y el Diffie-Hellman de curva elíptica (ECDH) que mejoran la seguridad y eficiencia.
- **Uso:**
  - Se utiliza en protocolos como SSH, IPsec y TLS para establecer canales de comunicación seguros.

2. RSA (Rivest-Shamir-Adleman):

- **Funcionamiento:**
  - Es un algoritmo de clave pública que se utiliza tanto para el cifrado como para la firma digital.
  - Se basa en la dificultad de factorizar números enteros grandes.
  - Una parte genera un par de claves (pública y privada) y comparte la clave pública.
  - La otra parte utiliza la clave pública para cifrar la clave secreta y enviarla a la primera parte, que la descifra con su clave privada.
- **Características:**
  - Permite el intercambio seguro de claves secretas.
  - También se utiliza para la autenticación y la firma digital.
  - Puede ser más lento que otros protocolos de intercambio de claves.

- **Uso:**
    - Se utiliza en protocolos como TLS/SSL y en sistemas de firma digital.

3. Intercambio de claves de curva elíptica Diffie-Hellman (ECDH):

- **Funcionamiento:**
    - Es una variante del Diffie-Hellman que utiliza curvas elípticas en lugar de campos finitos.
    - Ofrece una seguridad equivalente con claves más cortas, lo que lo hace más eficiente.
- **Características:**
    - Muy eficiente y seguro.
    - Se utiliza ampliamente en dispositivos móviles y en aplicaciones con recursos limitados.
    - Existen variantes como ECDHE (Diffie-Hellman efímero de curva elíptica) que proporcionan secreto perfecto hacia adelante.
- **Uso:**
    - Se utiliza en protocolos como TLS 1.3, SSH y VPNs.

Puntos clave:

- Es crucial que los protocolos de intercambio de claves se utilicen junto con mecanismos de autenticación para prevenir ataques de "man-in-the-middle".
- La elección del protocolo adecuado depende de los requisitos de seguridad, rendimiento y compatibilidad de la aplicación.
- Es importante mantener actualizadas las librerías criptográficas que se utilicen, para garantizar la seguridad de los protocolos.

Algoritmos criptográficos mas frecuentemente utilizados.

Algoritmos de Cifrado Simétrico (Clave Privada):

- **AES (Advanced Encryption Standard):**
    - Es el estándar de cifrado más utilizado en la actualidad.
    - Ofrece alta seguridad y eficiencia.
    - Se utiliza en una amplia gama de aplicaciones, desde el cifrado de archivos hasta la seguridad de redes.

- **DES (Data Encryption Standard):**
    - Fue un estándar ampliamente utilizado, pero ahora se considera obsoleto debido a su clave corta (56 bits).
    - Aún se puede encontrar en algunos sistemas heredados.
- **3DES (Triple DES):**
    - Una mejora de DES que aplica el algoritmo tres veces, aumentando la seguridad.
    - Aunque es más seguro que DES, es más lento que AES.

Algoritmos de Cifrado Asimétrico (Clave Pública):

- **RSA (Rivest-Shamir-Adleman):**
    - Uno de los algoritmos de clave pública más utilizados.
    - Se basa en la dificultad de factorizar números enteros grandes.
    - Se utiliza para el cifrado, la firma digital y el intercambio de claves.
- **Criptografía de Curva Elíptica (ECC):**
    - Ofrece una seguridad equivalente a RSA con claves más cortas.
    - Es más eficiente en términos de rendimiento y consumo de energía.
    - Se utiliza cada vez más en dispositivos móviles y aplicaciones con recursos limitados.
- **Diffie-Hellman:**
    - Este algoritmo se usa para el intercambio seguro de claves.
    - Permite que dos partes generen una clave secreta compartida a través de un canal inseguro.

Funciones Hash:

- **SHA-2 (Secure Hash Algorithm 2):**
    - Una familia de funciones hash que incluye SHA-256 y SHA-512.
    - Se utiliza para verificar la integridad de los datos y generar firmas digitales.
- **SHA-3 (Secure Hash Algorithm 3):**
    - La última versión de SHA, diseñada para ser más segura que SHA-2.
    - Se utiliza para verificar la integridad de datos.

Puntos Clave:

- La elección del algoritmo adecuado depende de los requisitos de seguridad, rendimiento y compatibilidad de la aplicación.
- Es importante utilizar algoritmos criptográficos actualizados y considerados seguros por la comunidad criptográfica.
- Es importante recordar que la potencia de los algoritmos criptográficos puede cambiar con el tiempo, debido a los avances en la potencia de la computación.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización.

Elementos Clave de un Certificado Digital:

- **Información del Titular:**
  - Nombre de la entidad (persona, organización o dispositivo).
  - Dirección de correo electrónico.
  - Otros datos de identificación relevantes.
- **Clave Pública:**
  - La clave pública asociada al titular, utilizada para cifrar información.
- **Información de la Autoridad de Certificación (AC):**
  - Nombre de la AC que emitió el certificado.
  - Firma digital de la AC, que valida la autenticidad del certificado.
- **Período de Validez:**
  - Fecha de emisión y fecha de expiración del certificado.
  - Esto limita el tiempo durante el cual el certificado es considerado válido.
- **Número de Serie:**
  - Un identificador único para cada certificado.
- **Información de Uso:**
  - Indicaciones sobre los propósitos para los que se puede utilizar el certificado (por ejemplo, firma digital, cifrado de correo electrónico, autenticación de sitios web).
- **Algoritmo de Firma:**

- Especifica el algoritmo utilizado para crear la firma digital de la autoridad de certificación.

Formatos Comúnmente Aceptados:

- **X.509:**
  - Es el estándar más utilizado para certificados digitales.
  - Define el formato y los campos de un certificado.
  - Se utiliza en una amplia gama de aplicaciones, desde la seguridad de sitios web (HTTPS) hasta la firma digital de documentos.
  - Dentro de este estandar los formatos mas comunes son:
    - **.PEM (Privacy Enhanced Mail):**
    - Codificado en Base64, común para certificados y claves.
    - **.DER (Distinguished Encoding Rules):**
    - Formato binario, también común para certificados y claves.
    - **.P12 o .PFX (Personal Information Exchange):**
    - Contiene tanto el certificado como la clave privada, protegido con contraseña.

Utilización de Certificados Digitales:

- **Seguridad de Sitios Web (HTTPS):**
  - Los certificados SSL/TLS permiten establecer conexiones seguras entre un navegador y un servidor web.
  - Esto protege la información confidencial, como contraseñas y datos bancarios, de accesos no autorizados.
- **Firma Digital de Documentos:**
  - Los certificados digitales permiten firmar documentos electrónicos, garantizando su autenticidad e integridad.
  - Esto es esencial para transacciones comerciales, contratos y otros documentos importantes.
- **Cifrado de Correo Electrónico (S/MIME):**
  - Los certificados digitales permiten cifrar y firmar correos electrónicos, protegiendo su confidencialidad y autenticidad.

- **Autenticación de Usuarios:**
  - Los certificados digitales se utilizan para autenticar usuarios en sistemas informáticos y aplicaciones en línea.
  - Esto proporciona un nivel adicional de seguridad más allá de las contraseñas.
- **Firma de Código:**
  - Los certificados son usados para firmar digitalmente software, esto verifica que el software no fue alterado y que proviene de una fuente confiable.
- **VPNs (Redes Privadas Virtuales):**
  - Los certificados digitales ayudan a autenticar los servidores VPN y los clientes, ayudando a crear tuneles de comunicación seguros.

Consideraciones Importantes:

- Es fundamental obtener certificados digitales de Autoridades de Certificación (AC) confiables.
- Es importante mantener las claves privadas seguras y protegerlas contra accesos no autorizados.
- Los certificados digitales deben renovarse antes de su fecha de expiración para garantizar su validez.

Elementos fundamentales de las funciones resumen y los criterios para su utilización.

Las funciones resumen, también conocidas como funciones hash, son herramientas criptográficas fundamentales en la seguridad de la información. Su capacidad para generar "huellas digitales" únicas de datos las hace esenciales para garantizar la integridad y autenticidad de la información.

Elementos Fundamentales de las Funciones Resumen:

- **Entrada Variable, Salida Fija:**
  - Una función hash puede tomar como entrada datos de cualquier tamaño, pero siempre produce una salida de longitud fija, conocida como "hash" o "resumen".
- **Determinismo:**
  - La misma entrada siempre producirá la misma salida hash.
- **Unidireccionalidad:**

- Es computacionalmente inviable revertir el proceso y obtener la entrada original a partir del hash.

- **Resistencia a Colisiones:**
  - Es extremadamente difícil encontrar dos entradas diferentes que produzcan el mismo hash.
    - Resistencia a colisiones débiles: dado un mensaje, es difícil encontrar otro mensaje que produzca el mismo hash.
    - Resistencia a colisiones fuertes: es difícil encontrar dos mensajes cualesquiera que produzcan el mismo hash.
- **Efecto Avalancha:**
  - Un pequeño cambio en la entrada debe producir un cambio drástico en la salida hash.

Criterios para su Utilización:

- **Integridad de Datos:**
  - Las funciones hash se utilizan para verificar que los datos no han sido alterados. Al comparar el hash de un archivo antes y después de su transmisión o almacenamiento, se puede detectar cualquier modificación.
- **Autenticación de Mensajes:**
  - Las funciones hash se combinan con claves secretas para generar códigos de autenticación de mensajes (MAC), que permiten verificar la autenticidad y la integridad de los mensajes.
- **Almacenamiento Seguro de Contraseñas:**
  - En lugar de almacenar las contraseñas en texto plano, se almacenan sus hashes. Esto protege las contraseñas en caso de una brecha de seguridad.
- **Firmas Digitales:**
  - Las funciones hash se utilizan para generar un resumen del documento que se va a firmar. Este resumen se cifra con la clave privada del firmante, creando una firma digital que garantiza la autenticidad y la integridad del documento.
- **Generación de Números Aleatorios:**
  - Algunas funciones hash se utilizan en la creación de generadores de números pseudoaleatorios criptográficamente seguros.
- **Detección de malware:**

- las funciones hash se utilizan para identificar archivos maliciosos, creando listas de hashes de malware conocidos.

Consideraciones Importantes:

- Es fundamental elegir funciones hash criptográficas fuertes y actualizadas, como SHA-2 o SHA-3.
- La longitud del hash debe ser suficiente para garantizar la seguridad contra ataques de colisión.
- Es importante utilizar las funciones hash de manera adecuada para cada aplicación específica.

Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece el marco legal para el uso de firmas electrónicas en España. Aquí se resumen los requerimientos legales clave:

Conceptos Fundamentales:

- **Firma Electrónica:**
  - Se define como el conjunto de datos en forma electrónica asociados a un documento, que se utilizan como medio de identificación del firmante.
- **Firma Electrónica Reconocida:**
  - Es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro1 de creación de firma. Esta firma tiene el mismo valor jurídico que la firma manuscrita.

Requerimientos Legales Clave:

- **Validez Jurídica:**
  - La ley reconoce la validez jurídica de la firma electrónica, especialmente la firma electrónica reconocida, que se equipara a la firma manuscrita.
- **Certificados Electrónicos:**
  - Los certificados electrónicos son esenciales para la firma electrónica reconocida. Deben ser emitidos por prestadores de servicios de certificación acreditados.
- **Prestadores de Servicios de Certificación:**

- La ley regula la actividad de los prestadores de servicios de certificación, estableciendo sus obligaciones y responsabilidades. Deben garantizar la seguridad y fiabilidad de los certificados que emiten.

- **Dispositivos Seguros de Creación de Firma:**
  - La firma electrónica reconocida debe ser generada mediante dispositivos seguros que garanticen la confidencialidad de la clave privada del firmante.
- **Documento Nacional de Identidad Electrónico (DNIe):**
  - El DNIe se reconoce como un documento de acreditación electrónica y de firma electrónica, cumpliendo los requisitos de la firma electrónica reconocida.
- **Obligaciones de los Prestadores de Servicios:**
  - Los prestadores de servicios de certificación deben comunicar al Ministerio de Industria, Turismo y Comercio, sus datos de identificación, los datos que permitan establecer comunicación con el prestador, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen.

Objetivos Principales de la Ley:

- Fomentar el uso de la firma electrónica para facilitar las transacciones electrónicas.
- Garantizar la seguridad y confianza en las comunicaciones electrónicas.
- Equiparar la firma electrónica reconocida a la firma manuscrita en términos de validez jurídica.

Es importante tener en cuenta que, aunque la Ley 59/2003 estableció el marco inicial, el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior3 (Reglamento eIDAS), ha armonizado la legislación sobre firma electrónica en la Unión Europea.

Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización.

Elementos Fundamentales de la Firma Digital:

- **Función Hash:**

- Se utiliza para generar un resumen único del documento, conocido como "hash" o "huella digital".
- Esto garantiza la integridad del documento, ya que cualquier modificación alterará el hash.

- **Criptografía de Clave Pública:**
  - Se utiliza un par de claves: una clave privada, que solo conoce el firmante, y una clave pública, que puede ser conocida por cualquiera.
  - El hash del documento se cifra con la clave privada del firmante, creando la firma digital.
- **Certificado Digital:**
  - Asocia la identidad del firmante a su clave pública.
  - Es emitido por una Autoridad de Certificación (AC) de confianza.

Funcionamiento Básico:

1. El firmante genera el hash del documento.
2. El firmante cifra el hash con su clave privada, creando la firma digital.
3. El firmante envía el documento y la firma digital al destinatario.
4. El destinatario utiliza la clave pública del firmante (obtenida del certificado digital) para descifrar la firma digital y obtener el hash original.
5. El destinatario genera su propio hash del documento.
6. El destinatario compara los dos hashes. Si son idénticos, el documento es auténtico e íntegro.

Tipos de Firma Digital:

- **Firma Electrónica Simple:**
  - Es la forma más básica de firma electrónica.
  - No requiere certificados digitales ni criptografía de clave pública.
  - Su validez jurídica es limitada.
- **Firma Electrónica Avanzada:**
  - Cumple con requisitos más estrictos, como la vinculación única al firmante y la capacidad de detectar cualquier cambio posterior en los datos firmados.
  - Suele basarse en certificados digitales.

- **Firma Electrónica Cualificada:**
  - Es el tipo de firma digital con mayor validez jurídica.
  - Se basa en un certificado cualificado y se crea mediante un dispositivo cualificado de creación de firmas.
  - Tiene el mismo valor legal que la firma manuscrita.

Criterios para su Utilización:

- **Validez Legal:**
  - Para documentos legales o transacciones importantes, se recomienda utilizar firmas electrónicas cualificadas.
- **Integridad y Autenticidad:**
  - Las firmas digitales son esenciales para garantizar que los documentos no han sido alterados y que provienen de la fuente correcta.
- **No Repudio:**
  - Las firmas digitales impiden que el firmante niegue haber firmado el documento.
- **Eficiencia:**
  - Las firmas digitales agilizan los procesos de firma y reducen el uso de papel.
- **Seguridad:**
  - Es fundamental utilizar certificados digitales emitidos por AC de confianza y proteger las claves privadas.

Consideraciones Adicionales:

- El reglamento eIDAS, es el reglamento de la Unión Europea relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior,1 y aporta un marco legal homogeneo para las firmas digitales dentro de la UE.
- Es importante conocer la legislación aplicable en cada país o región, ya que puede haber variaciones en los requisitos y la validez jurídica de las firmas digitales.

Criterios para la utilización de técnicas de cifrado de flujo y de bloque.

La elección entre técnicas de cifrado de flujo y de bloque depende de diversos factores, como la velocidad, la seguridad y el tipo de datos que se van a cifrar. Aquí te presento los criterios clave para su utilización:

Cifrado de Flujo:

- **Características:**
  - Cifra los datos bit a bit o byte a byte.
  - Genera una secuencia de claves pseudoaleatoria que se combina con el texto plano.
  - Suele ser más rápido que el cifrado de bloque.
- **Criterios de Utilización:**
  - **Transmisión de datos en tiempo real:** Adecuado para aplicaciones que requieren cifrado rápido y continuo, como la transmisión de audio y video.
  - **Recursos limitados:** Ideal para dispositivos con poca potencia de procesamiento, como dispositivos móviles o sistemas embebidos.
  - **Flujos de datos largos e ininterrumpidos:** Eficiente para cifrar grandes cantidades de datos que se transmiten de forma continua.
  - **Cuando el error de propagación no es un problema:** Un error en la transmisión solo afecta a un bit o byte, no a bloques completos.
- **Consideraciones de seguridad:**
  - Es crucial evitar la reutilización de la clave, ya que esto puede comprometer la seguridad.
  - La calidad del generador de claves pseudoaleatorias es fundamental.

Cifrado de Bloque:

- **Características:**
  - Cifra los datos en bloques de tamaño fijo.
  - Utiliza modos de operación para cifrar datos de longitud variable.
  - Suele ser más seguro que el cifrado de flujo para ciertos tipos de ataques.
- **Criterios de Utilización:**
  - **Almacenamiento de datos:** Adecuado para cifrar archivos y bases de datos.
  - **Transmisión de datos en paquetes:** Ideal para aplicaciones que transmiten datos en bloques, como el correo electrónico o la transferencia de archivos.
  - **Requisitos de alta seguridad:** Preferible para aplicaciones que requieren una fuerte protección contra ataques, como transacciones financieras.

- **Cuando el error de propagación es aceptable:** Un error en un bloque afecta a todo el bloque cifrado.

- **Modos de operación:**
  - Es importante elegir el modo de operación adecuado para cada aplicación, ya que cada modo ofrece diferentes niveles de seguridad y rendimiento.
  - Ejemplos de modos de operación: ECB, CBC, CTR, GCM.

En resumen:

- El cifrado de flujo es más rápido y adecuado para la transmisión de datos en tiempo real, mientras que el cifrado de bloque es más seguro y adecuado para el almacenamiento de datos.
- La elección entre ambos tipos de cifrado depende de los requisitos específicos de cada aplicación.
- Es esencial considerar las implicaciones de seguridad de cada técnica de cifrado y seguir las mejores prácticas para garantizar la protección de los datos.

Protocolos de intercambio de claves.

Los protocolos de intercambio de claves son esenciales en criptografía, ya que permiten a dos o más partes establecer una clave secreta compartida a través de un canal de comunicación, que a menudo se considera inseguro. Esta clave compartida se utiliza posteriormente para cifrar y descifrar mensajes, garantizando la confidencialidad de la comunicación.

Tipos principales de protocolos de intercambio de claves:

- **Diffie-Hellman (DH):**
  - Es uno de los protocolos más antiguos y ampliamente utilizados.
  - Permite a dos partes generar una clave secreta compartida sin intercambiar información secreta directamente.
  - Se basa en la dificultad del problema del logaritmo discreto.
  - Existen variantes como el Diffie-Hellman efímero (DHE) y el Diffie-Hellman de curva elíptica (ECDH), que ofrecen mayor seguridad y eficiencia.
- **RSA:**
  - Aunque RSA se utiliza principalmente para cifrado y firmas digitales, también se puede utilizar para el intercambio de claves.

    - Una de las partes genera un par de claves (pública y privada) y comparte la clave pública.
    - La otra parte cifra la clave secreta con la clave pública y la envía a la primera parte, que la descifra con su clave privada.
- **Intercambio de claves de curva elíptica Diffie-Hellman (ECDH):**
    - Es una variante del Diffie-Hellman que utiliza curvas elípticas.
    - Ofrece una seguridad equivalente con claves más cortas, lo que lo hace más eficiente para dispositivos con recursos limitados.
    - Se utiliza ampliamente en aplicaciones móviles y protocolos como TLS 1.3.
- **Protocolo de intercambio de claves por Internet (IKE):**
    - IKE es un protocolo de administración segura de claves que se utiliza para configurar un canal de comunicaciones seguro y autenticado entre dos dispositivos.
    - IKE1 se utiliza ampliamente junto con IPsec para establecer VPNs.

Consideraciones importantes:

- Es fundamental que los protocolos de intercambio de claves se utilicen junto con mecanismos de autenticación para prevenir ataques de "man-in-the-middle".
- La elección del protocolo adecuado depende de los requisitos de seguridad, rendimiento y compatibilidad de la aplicación.
- Es importante mantener actualizadas las librerías criptográficas que se utilicen, para garantizar la seguridad de los protocolos.

Los protocolos de intercambio de claves son una pieza fundamental de la criptografía moderna, ya que permiten establecer comunicaciones seguras en un mundo digital cada vez más conectado.

Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

Las herramientas de cifrado como PGP (Pretty Good Privacy), GPG (GNU Privacy Guard) y CryptoLoop son fundamentales para proteger la privacidad y la seguridad de la información en el mundo digital.

PGP y GPG:

- **Funcionalidad principal:**
    - Cifrado y descifrado de archivos y mensajes de correo electrónico.

    - Firma digital de documentos para garantizar su autenticidad e integridad.
    - Generación y gestión de claves criptográficas.
- **Características:**
    - Utilizan criptografía de clave pública, lo que permite el intercambio seguro de claves.
    - Ofrecen una fuerte protección contra accesos no autorizados y manipulaciones de datos.
    - Son ampliamente utilizados para proteger la privacidad de las comunicaciones y la información confidencial.
    - GPG es la implementación de código abierto del estandar OpenPGP, por lo que son muy compatibles.
- **Usos comunes:**
    - Cifrado de correos electrónicos para proteger la confidencialidad de la comunicación.
    - Firma digital de documentos para garantizar su autenticidad e integridad.
    - Cifrado de archivos y carpetas para proteger la información confidencial.
    - Verificación de la autenticidad de software y actualizaciones.

CryptoLoop:

- Aunque menos conocido que PGP y GPG, CryptoLoop se refiere a un concepto de cifrado, y existen herramientas que lo implementan.
- Estas herramientas suelen enfocarse en el cifrado de archivos y carpetas de forma transparente, integrándose con el sistema operativo.
- El objetivo es proporcionar una protección continua y automática de la información confidencial.
- Suelen usar el cifrado de bloques, y pueden integrar la capacidad de generar contenedores cifrados.

Consideraciones generales:

- Es fundamental mantener las claves privadas seguras y protegerlas contra accesos no autorizados.
- Es importante utilizar versiones actualizadas de estas herramientas para garantizar la seguridad.

- El uso adecuado de estas herramientas requiere comprender los conceptos básicos de la criptografía de clave pública.
- Es importante recordar que estas herramientas son muy utiles para proteger la información, pero no son infalibles.

En resumen, PGP, GPG y herramientas que usan conceptos como CryptoLoop son herramientas poderosas para proteger la privacidad y la seguridad de la información. Su uso adecuado puede ayudar a proteger la información confidencial de accesos no autorizados y manipulaciones.

UNIDAD DIDÁCTICA 2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

Identificación de los componentes de una PKI y su modelo de relaciones.

Una Infraestructura de Clave Pública (PKI) es un sistema que permite gestionar certificados digitales y claves públicas, facilitando la autenticación, el cifrado y la firma digital en entornos digitales. Sus componentes y relaciones son esenciales para establecer un ecosistema de confianza.

Componentes Principales de una PKI:

- **Autoridad de Certificación (CA):**
  - Es el componente central de la PKI.
  - Su función es emitir, revocar y renovar certificados digitales.
  - Establece y mantiene la "cadena de confianza".
  - Puede haber CA raíz (la más alta jerarquía) y CA intermedias.
- **Autoridad de Registro (RA):**
  - Verifica la identidad de los solicitantes de certificados.
  - Actúa como intermediario entre los solicitantes y la CA.
  - Puede ser parte de la CA o una entidad separada.
- **Repositorio de Certificados:**
  - Almacena los certificados digitales emitidos.
  - Permite a los usuarios verificar la validez de los certificados.

- Suele ser accesible a través de protocolos como LDAP o HTTP.

- **Certificados Digitales:**
  - Contienen la clave pública del titular y su información de identidad.
  - Son firmados digitalmente por la CA para garantizar su autenticidad.
  - Se utilizan para autenticar entidades y cifrar comunicaciones.
- **Claves Públicas y Privadas:**
  - Pares de claves criptográficas utilizadas para cifrado y firma digital.
  - La clave privada se mantiene en secreto, mientras que la clave pública se distribuye a través de certificados.
- **Usuarios Finales:**
  - Son las personas o sistemas que utilizan los certificados digitales para sus distintas tareas.

Modelo de Relaciones:

- **Cadena de Confianza:**
  - Se establece a través de la jerarquía de CA.
  - La CA raíz es la base de la confianza, y las CA intermedias heredan su confianza.
  - Los certificados emitidos por una CA son confiables si se puede verificar su firma con la clave pública de la CA superior.
- **Relación CA-RA:**
  - La RA actúa en nombre de la CA para verificar la identidad de los solicitantes.
  - La CA confía en la RA para realizar estas verificaciones.
- **Relación CA-Repositorio:**
  - La CA publica los certificados en el repositorio.
  - Los usuarios acceden al repositorio para obtener y verificar certificados.
- **Relación CA-Usuarios:**
  - La CA emite los certificados a los usuarios.
  - Los usuarios confían en la CA para emitir certificados válidos.

Utilización de la PKI:

- La PKI se utiliza en una amplia variedad de aplicaciones, como:
  - HTTPS para la seguridad de sitios web.
  - Firma digital de documentos electrónicos.
  - Cifrado de correo electrónico (S/MIME).
  - VPNs (Redes Privadas Virtuales).
  - Autenticación de usuarios en sistemas informáticos.

En resumen, una PKI establece un marco de confianza que permite a las entidades digitales identificarse y comunicarse de forma segura.

Autoridad de certificación y sus elementos.

Una Autoridad de Certificación (CA) es una entidad de confianza que desempeña un papel crucial en la seguridad de las comunicaciones digitales. Su función principal es emitir, gestionar y revocar certificados digitales, que son esenciales para verificar la identidad de entidades en línea.

Elementos Fundamentales de una CA:

- **Infraestructura de Clave Pública (PKI):**
  - La CA opera dentro de una PKI, que es un sistema que permite gestionar certificados digitales y claves públicas. La PKI proporciona el marco para establecer la confianza en las comunicaciones digitales.
- **Certificados Digitales:**
  - La CA emite certificados digitales que vinculan una identidad (persona, organización o dispositivo) a una clave pública. Estos certificados son la base para la autenticación y el cifrado en línea.
- **Políticas de Certificación:**
  - La CA establece políticas y procedimientos para la emisión y gestión de certificados. Estas políticas definen los requisitos para la verificación de identidad, la validez de los certificados y otros aspectos importantes.
- **Procesos de Verificación de Identidad:**
  - La CA implementa procesos rigurosos para verificar la identidad de los solicitantes de certificados. Esto puede incluir la verificación de documentos de identidad, la comprobación de información en bases de datos y otros métodos.

- **Sistema de Gestión de Certificados:**
    - La CA utiliza un sistema para gestionar el ciclo de vida de los certificados, que incluye la emisión, renovación, revocación y publicación de certificados.
- **Repositorio de Certificados:**
    - La CA mantiene un repositorio donde se publican los certificados emitidos. Esto permite a los usuarios verificar la validez de los certificados y obtener información sobre los titulares de los certificados.
- **Listas de Revocación de Certificados (CRL):**
    - La CA publica CRL que contienen información sobre los certificados que han sido revocados. Esto permite a los usuarios verificar si un certificado ha sido revocado y, por lo tanto, ya no es válido.
- **Clave Privada de la CA:**
    - La CA dispone de una clave privada, que es de vital importancia, y la cual se usa para firmar los certificados que emite. Esta clave privada, debe de estar muy bien protegida.

Funciones Clave de una CA:

- **Emisión de Certificados:**
    - La CA emite certificados digitales a entidades que han verificado su identidad.
- **Gestión de Certificados:**
    - La CA gestiona el ciclo de vida de los certificados, incluyendo la renovación y revocación.
- **Publicación de Certificados:**
    - La CA publica los certificados en un repositorio para que puedan ser verificados.
- **Revocación de Certificados:**
    - La CA revoca los certificados que han sido comprometidos o que ya no son válidos.

En resumen, una CA es una entidad de confianza que garantiza la autenticidad y la integridad de las comunicaciones digitales mediante la emisión y gestión de certificados digitales.

Política de certificado y declaración de practicas de certificación (CPS)

La Política de Certificados (CP) y la Declaración de Prácticas de Certificación (CPS) son documentos fundamentales en el ámbito de las Infraestructuras de Clave Pública (PKI). Ambos documentos establecen las reglas y procedimientos que rigen la emisión, gestión y uso de certificados digitales, pero difieren en su alcance y nivel de detalle.

Política de Certificados (CP)

- **Definición**:
  - La CP es un documento de alto nivel que define las reglas generales que rigen la emisión y uso de certificados digitales.
  - Establece los requisitos de seguridad, los tipos de certificados y los usos permitidos.
- **Contenido**:
  - Identificación de la CA.
  - Tipos de certificados emitidos.
  - Usos previstos de los certificados.
  - Requisitos de seguridad y confianza.
  - Responsabilidades de la CA y de los usuarios.
- **Propósito**:
  - Establecer un marco general de confianza y seguridad para la emisión y uso de certificados.
  - Definir los requisitos mínimos que deben cumplir los certificados y las CA.

Declaración de Prácticas de Certificación (CPS)

- **Definición**:
  - La CPS es un documento más detallado que describe las prácticas y procedimientos específicos que sigue una CA en la emisión, gestión y revocación de certificados.
  - Proporciona información detallada sobre los procesos operativos de la CA.
- **Contenido**:
  - Procedimientos de verificación de identidad.
  - Procesos de emisión, renovación y revocación de certificados.

  - Medidas de seguridad físicas y lógicas.
  - Procedimientos de gestión de incidentes.
  - Políticas de auditoría y cumplimiento.
- **Propósito**:
  - Proporcionar transparencia sobre las prácticas operativas de la CA.
  - Permitir a los usuarios evaluar el nivel de confianza y seguridad de la CA.

Relación entre CP y CPS

- La CP establece el marco general, mientras que la CPS proporciona los detalles operativos.
- La CPS debe cumplir con los requisitos establecidos en la CP.
- Ambos documentos son esenciales para establecer la confianza en una PKI.

Importancia

- Estos documentos son vitales para generar confianza en el uso de certificados digitales.
- Permiten a los usuarios entender las políticas y prácticas de la CA.
- Son importantes para el cumplimiento de normativas y estándares de seguridad.

En resumen, la CP y la CPS son documentos complementarios que garantizan la seguridad y la confianza en el uso de certificados digitales.

Lista de certificados revocados (CRL)

Una Lista de Certificados Revocados (CRL, por sus siglas en inglés) es un componente esencial de una Infraestructura de Clave Pública (PKI).

¿Qué es una CRL?

- Una CRL es una lista de certificados digitales que han sido revocados por una Autoridad de Certificación (CA) antes de su fecha de expiración.
- Esto es necesario porque los certificados pueden quedar invalidados por diversas razones, como:
  - Compromiso de la clave privada del titular.
  - Cambio de la información del titular.
  - Cese de la actividad del titular.

Componentes Clave de una CRL:

- **Número de serie de los certificados revocados:**
  - La CRL contiene los números de serie únicos de los certificados que han sido revocados.
- **Fecha de revocación:**
  - Indica cuándo se revocó cada certificado.
- **Información de la CA emisora:**
  - Identifica la CA que emitió la CRL.
- **Firma digital de la CA:**
  - Garantiza la autenticidad e integridad de la CRL.
- **Fecha de emisión de la CRL:**
  - Indica cuando fue publicada la lista.
- **Fecha de próxima actualización:**
  - Indica cuando se publicara la proxima lista actualizada.

Funcionamiento y Uso de las CRL:

- **Publicación:**
  - Las CA publican periódicamente CRL en repositorios accesibles, como servidores LDAP o sitios web.
- **Verificación:**
  - Las aplicaciones y los sistemas que utilizan certificados digitales deben verificar las CRL para asegurarse de que los certificados que utilizan no han sido revocados.
  - Este proceso de verificación es crucial para mantener la seguridad y la confianza en las comunicaciones digitales.
- **Actualización:**
  - Las CRL deben actualizarse periódicamente para reflejar los cambios en el estado de los certificados.
  - La frecuencia de actualización depende de la política de la CA y del nivel de riesgo asociado a los certificados.

Importancia de las CRL:

- **Garantizan la seguridad:**
  - Las CRL son esenciales para evitar el uso de certificados comprometidos, lo que podría poner en peligro la confidencialidad y la integridad de la información.
- **Establecen la confianza:**
  - Al verificar las CRL, los usuarios pueden confiar en que los certificados que utilizan son válidos y confiables.
- **Cumplimiento normativo:**
  - En muchos sectores, el uso de CRL es un requisito normativo para garantizar la seguridad de las transacciones electrónicas.

En resumen, las CRL desempeñan un papel fundamental en la seguridad de las PKI al proporcionar un mecanismo para verificar el estado de los certificados digitales.

Funcionamiento de las solicitudes de firma de certificados (CSR)

Una Solicitud de Firma de Certificado (CSR, por sus siglas en inglés) es un archivo esencial en el proceso de obtención de un certificado digital. Su función principal es proporcionar a una Autoridad de Certificación (CA) la información necesaria para emitir un certificado que valide la identidad de una entidad en línea.

Funcionamiento de una CSR:

1. **Generación del par de claves:**
   a. El primer paso es generar un par de claves criptográficas: una clave privada y una clave pública.
   b. La clave privada se mantiene segura y confidencial, mientras que la clave pública se incluye en la CSR.
2. **Creación de la CSR:**
   a. La CSR se genera utilizando la clave privada.
   b. Contiene información sobre la entidad que solicita el certificado, como:
      i. Nombre común (CN): El nombre de dominio o la entidad a la que se asocia el certificado.
      ii. Organización (O): El nombre de la organización.
      iii. Unidad organizativa (OU): La división o departamento dentro de la organización.

iv. Localidad (L): La ciudad.

v. Estado o provincia (S): El estado o provincia.

vi. País (C): El código de país de dos letras.

vii. Clave pública: La clave pública generada en el primer paso.

3. **Envío de la CSR a la CA:**
    a. La CSR se envía a la CA, que la utiliza para verificar la información del solicitante.
4. **Verificación y emisión del certificado:**
    a. La CA verifica la información de la CSR y, si todo es correcto, emite un certificado digital.
    b. El certificado contiene la clave pública del solicitante, la información de identidad y la firma digital de la CA.
5. **Instalación del certificado:**
    a. El certificado emitido se instala en el servidor o dispositivo del solicitante, junto con la clave privada.

Elementos Clave de una CSR:

- **Clave pública:** La clave pública del solicitante.
- **Información de identidad:** Datos sobre la entidad que solicita el certificado.
- **Firma digital (opcional):** Algunas CSR pueden estar firmadas digitalmente para garantizar su integridad.

Importancia de las CSR:

- Las CSR son esenciales para obtener certificados digitales que permitan establecer comunicaciones seguras en línea.
- Garantizan que la información de identidad del solicitante sea verificada por una CA de confianza.
- Permiten establecer la confianza en las transacciones electrónicas y las comunicaciones en línea.

En resumen, las CSR son un paso fundamental en el proceso de obtención de certificados digitales, ya que proporcionan a las CA la información necesaria para verificar la identidad de los solicitantes y emitir certificados confiables.

Infraestructura de gestión de privilegios (PMI)

La Infraestructura de Gestión de Privilegios (PMI, por sus siglas en inglés) es un marco de seguridad esencial diseñado para controlar y administrar los privilegios de acceso dentro de un entorno digital. A diferencia de la Infraestructura de Clave Pública (PKI), que se centra en la gestión de certificados digitales, la PMI se enfoca en la autorización y el control de acceso a recursos y aplicaciones.

Elementos Clave de una PMI:

- **Atributos de Privilegio:**
  - Son las características que definen los privilegios de acceso de un usuario o entidad. Pueden incluir roles, permisos, grupos y otros atributos específicos.
- **Autoridad de Atributos (AA):**
  - Es la entidad responsable de emitir y gestionar los atributos de privilegio. Similar a una CA en una PKI, la AA establece la confianza en los atributos de privilegio.
- **Certificados de Atributos:**
  - Son documentos digitales que contienen los atributos de privilegio de un usuario o entidad. Son emitidos por la AA y se utilizan para verificar la autorización de acceso.
- **Política de Privilegios:**
  - Define las reglas y restricciones que rigen el acceso a los recursos. Establece qué usuarios o entidades tienen permiso para realizar qué acciones.
- **Puntos de Decisión de Políticas (PDP):**
  - Son los componentes que evalúan las solicitudes de acceso en función de las políticas de privilegios y los atributos de privilegio. Deciden si se concede o deniega el acceso.
- **Puntos de Aplicación de Políticas (PAP):**
  - Son los componentes que aplican las decisiones de acceso tomadas por los PDP. Controlan el acceso real a los recursos.

Funcionamiento de una PMI:

1. **Emisión de Certificados de Atributos:**
   a. La AA emite certificados de atributos que contienen los privilegios de acceso de un usuario o entidad.

2. **Solicitud de Acceso:**
    a. Un usuario o entidad solicita acceso a un recurso.
3. **Evaluación de Políticas:**
    a. El PDP evalúa la solicitud de acceso en función de las políticas de privilegios y los atributos de privilegio del solicitante.
4. **Decisión de Acceso:**
    a. El PDP decide si se concede o deniega el acceso.
5. **Aplicación de la Decisión:**
    a. El PAP aplica la decisión de acceso, permitiendo o denegando el acceso al recurso.

Importancia de la PMI:

- **Control de Acceso Granular:**
    - La PMI permite un control de acceso preciso y detallado, lo que reduce el riesgo de accesos no autorizados.
- **Gestión de Privilegios Centralizada:**
    - La PMI proporciona un marco centralizado para gestionar los privilegios de acceso, lo que simplifica la administración y mejora la seguridad.
- **Cumplimiento Normativo:**
    - La PMI ayuda a las organizaciones a cumplir con las normativas y los estándares de seguridad que exigen un control estricto del acceso a los datos.
- **Minimización de Riesgos:**
    - Al aplicar el principio de mínimo privilegio, las organizaciones pueden reducir la superficie de ataque y mitigar el riesgo de usuarios internos malintencionados o de ciberataques externos.1

En resumen, la PMI es un componente fundamental de la seguridad de la información que permite a las organizaciones controlar y administrar los privilegios de acceso de manera efectiva.

Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales.

Los certificados de atributos son una extensión de los certificados digitales que permiten añadir información adicional sobre los privilegios y roles de un usuario o entidad. A diferencia de los certificados digitales tradicionales, que se centran en la identidad, los certificados de atributos se centran en la autorización.

Campos de Certificados de Atributos:

- **Identificador del titular:**
  - Este campo vincula el certificado de atributos a un certificado digital existente, estableciendo la relación entre la identidad y los privilegios.
- **Atributos:**
  - Este es el campo principal del certificado de atributos. Contiene información sobre los roles, permisos y privilegios del titular. Los atributos pueden ser definidos por la organización o por estándares específicos.
- **Emisor:**
  - Identifica la Autoridad de Atributos (AA) que emitió el certificado.
- **Período de validez:**
  - Define el período durante el cual el certificado de atributos es válido.
- **Firma digital:**
  - La firma digital de la AA garantiza la autenticidad e integridad del certificado de atributos.

Usos Habituales:

- **Control de acceso basado en roles (RBAC):**
  - Los certificados de atributos se utilizan para asignar roles y permisos a los usuarios, simplificando la gestión de acceso a recursos y aplicaciones.
- **Autorización de transacciones:**
  - Se utilizan para autorizar transacciones específicas, como transferencias bancarias o firmas de documentos electrónicos.
- **Control de acceso a aplicaciones:**
  - Se utilizan para controlar el acceso a aplicaciones y sistemas, permitiendo o denegando el acceso a funciones específicas.

- **Delegación de privilegios:**
    - Permiten delegar privilegios a otros usuarios o entidades de forma segura y controlada.

Relación con los Certificados Digitales:

- Los certificados de atributos complementan a los certificados digitales, proporcionando información adicional sobre la autorización.
- Un certificado de atributos está vinculado a un certificado digital, estableciendo la relación entre la identidad y los privilegios.
- Esta relación permite un control de acceso más granular y flexible, ya que se pueden combinar la identidad y los privilegios para tomar decisiones de autorización.

En resumen:

Los certificados de atributos son una herramienta poderosa para gestionar la autorización en entornos digitales. Al combinar la identidad proporcionada por los certificados digitales con los privilegios definidos en los certificados de atributos, las organizaciones pueden implementar un control de acceso más seguro y eficiente.

Aplicaciones que se apoyan en la existencia de una PKI

Una Infraestructura de Clave Pública (PKI) es fundamental para una amplia gama de aplicaciones que requieren seguridad y confianza en las comunicaciones digitales. Aquí te presento algunas de las aplicaciones más comunes que se apoyan en la existencia de una PKI:

1. Seguridad de Sitios Web (HTTPS):

- Los certificados SSL/TLS, emitidos por una CA dentro de una PKI, permiten establecer conexiones seguras entre navegadores y servidores web.
- Esto garantiza la confidencialidad e integridad de la información transmitida, protegiendo datos sensibles como contraseñas, información bancaria y datos personales.

2. Firma Digital de Documentos:

- La PKI permite la firma digital de documentos electrónicos, garantizando su autenticidad e integridad.
- Esto es esencial para transacciones comerciales, contratos, documentos legales y otros documentos importantes.

3. Cifrado de Correo Electrónico (S/MIME):

- Los certificados digitales permiten cifrar y firmar correos electrónicos, protegiendo su confidencialidad y autenticidad.
- Esto es crucial para comunicaciones confidenciales en entornos corporativos y gubernamentales.

4. Autenticación de Usuarios:

- La PKI se utiliza para autenticar usuarios en sistemas informáticos y aplicaciones en línea, proporcionando un nivel adicional de seguridad más allá de las contraseñas.
- Esto es común en VPNs, redes corporativas y aplicaciones de banca en línea.

5. Banca en Línea y Comercio Electrónico:

- La PKI es esencial para garantizar la seguridad de las transacciones en línea, protegiendo la información financiera y personal de los clientes.
- Se utiliza para autenticar usuarios, cifrar comunicaciones y firmar transacciones.

6. Redes Privadas Virtuales (VPNs):

- La PKI se utiliza para autenticar servidores VPN y clientes, estableciendo túneles de comunicación seguros.
- Esto permite a los usuarios acceder a redes privadas de forma segura a través de Internet.

7. Firma de Código:

- Los certificados digitales se utilizan para firmar digitalmente software, garantizando que el software no ha sido alterado y que proviene de una fuente confiable.
- Esto protege a los usuarios contra software malicioso y falsificado.

8. Internet de las Cosas (IoT):

- La PKI se utiliza para autenticar y proteger dispositivos IoT, garantizando la seguridad de las comunicaciones y la integridad de los datos.
- Esto es crucial para aplicaciones IoT en sectores como la salud, la industria y la infraestructura crítica.

9. Administración Pública Electrónica:

- La PKI se utiliza para autenticar ciudadanos y funcionarios públicos en transacciones electrónicas con la administración pública.
- Esto facilita la realización de trámites en línea de forma segura y confiable.

UNIDAD DIDÁCTICA 3. COMUNICACIONES SEGURAS

Definición, finalidad y funcionalidad de redes privadas virtuales.

Este es un tema crucial para comprender cómo se establecen comunicaciones seguras a través de redes públicas.

Definición de Red Privada Virtual (VPN):

- Una VPN es una tecnología que crea una conexión segura y cifrada a través de una red pública, como Internet.
- Permite a los usuarios acceder a recursos de red privada de forma remota, como si estuvieran conectados directamente a la red.
- En esencia, una VPN crea un "túnel" seguro a través de Internet, protegiendo los datos de accesos no autorizados.

Finalidad de las VPN:

- **Confidencialidad:**
  - Cifrar el tráfico de datos para proteger la información sensible de espionaje y robo.
- **Integridad:**
  - Garantizar que los datos no sean modificados durante la transmisión.
- **Autenticación:**
  - Verificar la identidad de los usuarios que acceden a la red privada.
- **Acceso Remoto Seguro:**
  - Permitir a los empleados acceder a los recursos de la empresa de forma segura desde cualquier ubicación.
- **Anonimato:**
  - Ocultar la dirección IP del usuario, proporcionando un cierto grado de anonimato en línea.
- **Evitar Restricciones Geográficas:**
  - Permite acceder a contenido que puede estar bloqueado en determinadas regiones.

Funcionalidad de las VPN:

- **Creación de un Túnel Cifrado:**
  - La VPN establece un túnel cifrado entre el dispositivo del usuario y el servidor VPN.
  - Todo el tráfico de datos que pasa a través de este túnel está cifrado, lo que lo hace ilegible para terceros.
- **Protocolos de Túnel:**
  - Las VPN utilizan diversos protocolos para crear el túnel cifrado, como:
    - IPsec (Internet Protocol Security)
    - OpenVPN
    - L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security)
    - Wireguard.
- **Servidores VPN:**
  - Los proveedores de VPN mantienen servidores en diferentes ubicaciones geográficas.
  - Los usuarios pueden conectarse a estos servidores para cambiar su dirección IP y acceder a contenido bloqueado geográficamente.
- **Cifrado de Datos:**
  - Las VPN utilizan algoritmos de cifrado para proteger los datos durante la transmisión.
  - Los algoritmos de cifrado más comunes incluyen AES (Advanced Encryption Standard).
- **Autenticación de Usuarios:**
  - Las VPN requieren que los usuarios se autentiquen antes de permitir el acceso a la red privada.
  - Esto puede implicar el uso de contraseñas, certificados digitales u otros métodos de autenticación.

Protocolo IPSec.

El protocolo IPsec (Internet Protocol Security) es un conjunto de protocolos de seguridad que opera en la capa de red del modelo OSI. Su principal objetivo es proporcionar seguridad a las comunicaciones IP, garantizando la confidencialidad, integridad y autenticación de los datos transmitidos a través de redes IP, ya sean públicas o privadas.

Características Principales:

- **Seguridad de Capa de Red:**
  - IPsec opera en la capa de red, lo que significa que protege todo el tráfico IP, independientemente de la aplicación que se esté utilizando.
- **Confidencialidad:**
  - Cifra los datos para protegerlos de accesos no autorizados.
- **Integridad:**
  - Utiliza funciones hash para garantizar que los datos no han sido alterados durante la transmisión.
- **Autenticación:**
  - Verifica la identidad de los dispositivos que se comunican.

Componentes de IPsec:

IPsec se compone de dos protocolos principales:

- **AH (Authentication Header):**
  - Proporciona autenticación e integridad, pero no confidencialidad.
  - Verifica que los paquetes no han sido modificados y que provienen de la fuente correcta.
- **ESP (Encapsulating Security Payload):**
  - Proporciona confidencialidad, integridad y autenticación.
  - Cifra los datos y los autentica.

Modos de Operación:

IPsec puede operar en dos modos:

- **Modo de Transporte:**
  - Cifra solo la carga útil del paquete IP.
  - Se utiliza para proteger la comunicación entre dos hosts.
- **Modo de Túnel:**
  - Cifra todo el paquete IP original y lo encapsula en un nuevo paquete IP.
  - Se utiliza para crear VPNs.

Intercambio de Claves:

IPsec utiliza el protocolo IKE (Internet Key Exchange) para establecer asociaciones de seguridad (SA) y gestionar las claves criptográficas.

Usos Comunes:

- **VPNs:**
  - IPsec se utiliza ampliamente para crear VPNs seguras, permitiendo a los usuarios acceder a redes privadas de forma remota.
- **Comunicaciones Seguras entre Sitios:**
  - IPsec se utiliza para proteger las comunicaciones entre oficinas remotas de una misma organización.
- **Protección de Tráfico Sensible:**
  - IPsec se utiliza para proteger el tráfico de datos sensibles en redes públicas.

Ventajas de IPsec:

- **Seguridad robusta:**
  - Proporciona un alto nivel de seguridad para las comunicaciones IP.
- **Transparencia:**
  - Opera en la capa de red, lo que lo hace transparente para las aplicaciones.
- **Flexibilidad:**
  - Puede utilizarse en una amplia variedad de aplicaciones y entornos.

Protocolos SSL y SSH.

Los protocolos SSL (Secure Sockets Layer) y SSH (Secure Shell) son dos protocolos de seguridad ampliamente utilizados que desempeñan funciones distintas en la protección de las comunicaciones en línea.

Protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security):

- **Función principal:**
  - SSL/TLS se utiliza para establecer conexiones seguras y cifradas entre un cliente (como un navegador web) y un servidor.
  - Su objetivo principal es proteger la confidencialidad e integridad de los datos transmitidos entre estas dos partes.
- **Características clave:**

- Cifrado de datos: SSL/TLS cifra los datos transmitidos, lo que los hace ilegibles para terceros no autorizados.
- Autenticación: Permite la autenticación del servidor, lo que garantiza que el cliente se está comunicando con el servidor correcto.
- Integridad de datos: Utiliza funciones hash para verificar que los datos no han sido alterados durante la transmisión.

- **Usos comunes:**
  - Navegación web segura (HTTPS): SSL/TLS es esencial para proteger la información sensible transmitida a través de sitios web, como contraseñas, información bancaria y datos personales.
  - Comercio electrónico: Se utiliza para proteger las transacciones en línea, garantizando la seguridad de los pagos y la información del cliente.
  - Correo electrónico seguro: S/MIME (Secure/Multipurpose Internet Mail Extensions) utiliza SSL/TLS para cifrar y firmar correos electrónicos.
- **Capa de protocolo:**
  - Opera en la capa de transporte del modelo OSI.

Protocolo SSH (Secure Shell):

- **Función principal:**
  - SSH se utiliza para establecer conexiones seguras y cifradas para el acceso remoto a servidores y dispositivos de red.
  - Permite a los usuarios ejecutar comandos y transferir archivos de forma segura a través de una red insegura.
- **Características clave:**
  - Acceso remoto seguro: SSH proporciona un canal cifrado para el acceso remoto a servidores, lo que protege las credenciales de inicio de sesión y los datos transmitidos.
  - Transferencia de archivos segura: Permite la transferencia segura de archivos a través de protocolos como SFTP (SSH File Transfer Protocol) y SCP (Secure Copy Protocol).
  - Túneles SSH: Permite la creación de túneles SSH para redirigir el tráfico de red de forma segura.
- **Usos comunes:**

- Administración de servidores remotos: SSH es ampliamente utilizado por los administradores de sistemas para acceder y administrar servidores Linux y otros dispositivos de red.
- Transferencia de archivos segura: Se utiliza para transferir archivos de forma segura entre computadoras.
- Acceso a dispositivos de red: Permite el acceso seguro a enrutadores, conmutadores y otros dispositivos de red.

- **Capa de protocolo:**
  - Opera en la capa de aplicación del modelo OSI.

Diferencias clave:

- **Propósito:**
  - SSL/TLS: Protege la comunicación entre un cliente y un servidor, principalmente para la navegación web y el comercio electrónico.
  - SSH: Proporciona acceso remoto seguro a servidores y dispositivos de red.
- **Capa de protocolo:**
  - SSL/TLS: Capa de transporte.
  - SSH: Capa de aplicación.
- **Autenticación:**
  - SSH soporta varios métodos de autenticación, incluyendo contraseñas, claves SSH y certificados SSH.
  - SSL/TLS se basa principalmente en certificados digitales emitidos por autoridades de certificación (CA).

Sistemas SSL VPN.

Un sistema SSL VPN (Red Privada Virtual SSL) es una solución de acceso remoto seguro que utiliza el protocolo SSL/TLS para establecer conexiones cifradas a través de Internet. A diferencia de las VPNs IPsec tradicionales, que requieren la instalación de software cliente específico, las SSL VPNs suelen funcionar a través de navegadores web, lo que las hace más fáciles de implementar y utilizar.

Características y Funcionamiento:

- **Acceso basado en navegador:**

    - Los usuarios pueden acceder a los recursos de la red privada a través de un navegador web, lo que elimina la necesidad de instalar software cliente adicional.

- **Cifrado SSL/TLS:**
    - Utiliza el protocolo SSL/TLS para cifrar el tráfico de datos, garantizando la confidencialidad e integridad de la información transmitida.
- **Autenticación:**
    - Implementa mecanismos de autenticación para verificar la identidad de los usuarios, como nombres de usuario y contraseñas, certificados digitales o autenticación de dos factores.
- **Control de acceso granular:**
    - Permite definir políticas de acceso detalladas, controlando qué recursos pueden acceder los usuarios.
- **Acceso a aplicaciones y recursos web:**
    - Principalmente se utiliza para dar acceso a aplicaciones web internas y otros recursos basados en web. Aunque tambien hay soluciones que permiten el acceso a nivel de red.

Ventajas de los Sistemas SSL VPN:

- **Facilidad de implementación y uso:**
    - No requiere la instalación de software cliente, lo que simplifica la implementación y reduce los costos de soporte.
- **Compatibilidad:**
    - Funciona con la mayoría de los navegadores web y sistemas operativos, lo que facilita el acceso desde diversos dispositivos.
- **Acceso remoto seguro:**
    - Proporciona un acceso seguro a los recursos de la red privada desde cualquier ubicación con conexión a Internet.
- **Control de acceso granular:**
    - Permite definir políticas de acceso detalladas, controlando qué recursos pueden acceder los usuarios.

Usos Comunes:

- **Acceso remoto a aplicaciones web corporativas:**

- Permite a los empleados acceder a aplicaciones web internas desde fuera de la oficina.

- **Acceso a portales de intranet:**
  - Facilita el acceso seguro a portales de intranet y otros recursos internos.
- **Acceso a escritorios remotos:**
  - Algunas soluciones SSL VPN permiten el acceso a escritorios remotos, lo que permite a los usuarios controlar sus equipos de trabajo desde cualquier lugar.

Consideraciones de seguridad:

- Es fundamental mantener actualizados los servidores SSL VPN y los navegadores web para evitar vulnerabilidades.
- Se recomienda utilizar mecanismos de autenticación fuertes, como la autenticación de dos factores, para proteger las cuentas de usuario.
- Es importante definir políticas de acceso detalladas para controlar qué recursos pueden acceder los usuarios.

Túneles cifrados.

¿Qué es un túnel cifrado?

- Un túnel cifrado es una conexión segura y privada creada a través de una red pública, como Internet.
- Funciona encapsulando los datos dentro de otro protocolo, creando un "túnel" virtual a través del cual viajan los datos cifrados.
- El cifrado garantiza que los datos sean ilegibles para cualquier persona que no tenga la clave de descifrado, protegiéndolos de la interceptación y el espionaje.

¿Cómo funcionan?

1. **Encapsulación:**
   a. Los datos originales se encapsulan dentro de otro protocolo, como IPsec o SSL/TLS.
   b. Esto crea un paquete de datos que contiene tanto los datos originales como la información de enrutamiento necesaria para llegar al destino.
2. **Cifrado:**
   a. Los datos encapsulados se cifran utilizando algoritmos criptográficos.

    b. Esto garantiza que los datos sean ilegibles para cualquier persona que intercepte el tráfico.

3. **Transmisión:**
    a. Los datos cifrados se transmiten a través de la red pública.
    b. Debido al cifrado, los datos son seguros incluso si son interceptados.
4. **Descifrado y desencapsulación:**
    a. En el destino, los datos cifrados se descifran y desencapsulan.
    b. Los datos originales se extraen y se entregan al destinatario.

Usos comunes:

- **VPNs:**
    - Los túneles cifrados son la base de las VPNs, que permiten a los usuarios acceder a redes privadas de forma segura a través de Internet.
- **Acceso remoto seguro:**
    - Se utilizan para proporcionar acceso remoto seguro a servidores y aplicaciones.
- **Comunicaciones seguras entre sitios:**
    - Se utilizan para proteger las comunicaciones entre oficinas remotas de una misma organización.
- **Protección de datos sensibles:**
    - Se utilizan para proteger la transmisión de datos sensibles, como información financiera o datos personales.

Protocolos de túnel:

- **IPsec (Internet Protocol Security):**
    - Un conjunto de protocolos que proporciona seguridad a las comunicaciones IP.
- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):**
    - Un protocolo que proporciona seguridad a las comunicaciones web.
- **SSH (Secure Shell):**
    - Un protocolo que proporciona acceso remoto seguro a servidores y dispositivos de red.
- **OpenVPN:**

  - Protocolo VPN de código abierto muy utilizado.

- **WireGuard:**
  - Protocolo VPN moderno, con gran velocidad y seguridad.

Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

La implementación de una Red Privada Virtual (VPN) ofrece diversas alternativas, cada una con sus propias ventajas e inconvenientes.

1. VPNs basadas en hardware:

- **Ventajas:**
  - Alto rendimiento: Los dispositivos VPN de hardware están diseñados para manejar grandes volúmenes de tráfico de forma eficiente.
  - Seguridad robusta: Suelen ofrecer características de seguridad avanzadas y cifrado de alta calidad.
  - Fiabilidad: Son dispositivos dedicados, lo que reduce el riesgo de fallos y cuelgues.
- **Inconvenientes:**
  - Costo elevado: La adquisición e instalación de dispositivos VPN de hardware puede ser costosa.
  - Complejidad: La configuración y administración de estos dispositivos pueden requerir conocimientos técnicos especializados.
  - Escalabilidad limitada: la ampliación de la capacidad puede requerir la compra de hardware adicional.

2. VPNs basadas en software:

- **Ventajas:**
  - Costo reducido: Las soluciones VPN de software suelen ser más económicas que las basadas en hardware.
  - Flexibilidad: Se pueden instalar en servidores o equipos existentes, lo que facilita la implementación.
  - Escalabilidad: es mas sencillo ampliar la capacidad añadiendo mas recursos al servidor.

- **Inconvenientes:**
    - Rendimiento variable: El rendimiento puede depender de la capacidad del servidor o equipo donde se instale.
    - Mayor carga de trabajo: El software VPN consume recursos del sistema, lo que puede afectar al rendimiento de otras aplicaciones.
    - Dependencia del sistema operativo: pueden surgir problemas de compatibilidad.

3. VPNs SSL:

- **Ventajas:**
    - Facilidad de uso: El acceso a la VPN se realiza a través de un navegador web, sin necesidad de instalar software cliente.
    - Compatibilidad: Funciona con la mayoría de los sistemas operativos y dispositivos.
    - Acceso granular: permite definir politicas de acceso a aplicaciones.
- **Inconvenientes:**
    - Limitaciones de aplicaciones: Principalmente se utiliza para el acceso a aplicaciones web.
    - Rendimiento: puede ser inferior a las VPNs IPsec.
    - Dependencia del navegador: las actualizaciones del navegador pueden afectar a la compatibilidad.

4. VPNs IPsec:

- **Ventajas:**
    - Alta seguridad: El protocolo IPsec proporciona un cifrado robusto y autenticación sólida.
    - Compatibilidad: Ampliamente soportado por dispositivos de red y sistemas operativos.
    - Protege todo el trafico IP.
- **Inconvenientes:**
    - Complejidad: La configuración de IPsec puede ser compleja y requerir conocimientos técnicos.

- Problemas de NAT: La traducción de direcciones de red (NAT) puede dificultar la configuración de VPNs IPsec.
- Compatibilidad de cortafuegos: algunos cortafuegos pueden bloquear el trafico IPsec.

5. VPNs de proveedores de servicios:

- **Ventajas:**
  - Facilidad de uso: Los proveedores de servicios VPN suelen ofrecer aplicaciones fáciles de usar.
  - Anonimato: Ocultan la dirección IP del usuario, proporcionando un cierto grado de anonimato.
  - Acceso a contenido restringido: permiten saltarse las restricciones geograficas.
- **Inconvenientes:**
  - Confianza en el proveedor: El usuario debe confiar en que el proveedor protege su privacidad y seguridad.
  - Rendimiento variable: El rendimiento puede depender de la congestión de los servidores del proveedor.
  - Posible registro de datos: algunos proveedores pueden registrar la actividad del usuario.