Cifrado

Los controles de cifrado de información se han convertido en un elemento de gran importancia para la gestión de la seguridad de la información, ya que nos permite proteger la privacidad de la misma al evitar que esta sea interpretada por persona no autorizadas. El cifrado es **"el proceso mediante el cual se codifica algo, de modo que no resulte fácil de entender para quienes no tienen acceso autorizado"** (WeLiveSecurity, 2021)

En este mismo sentido, además de adentrar la atención en los aspectos de cifrado, es necesario conocer sobre los procesos de Criptografía.

Criptografía: procesos mediante los cuales se aplican métodos de cifrado a una información para ser transmitida, estos procesos tienen como objetivos:

- Garantizar la privacidad y confidencialidad de tal manera que únicamente el destinatario interesado pueda leerla.
- Integridad, evitando que esta sea modificada sin autorización.
- Autenticación, garantizando que solo se pueda interpretar por los interesados.
- No repudio, para evitar que se niegue que alguno de los interesados ha podido accederla.

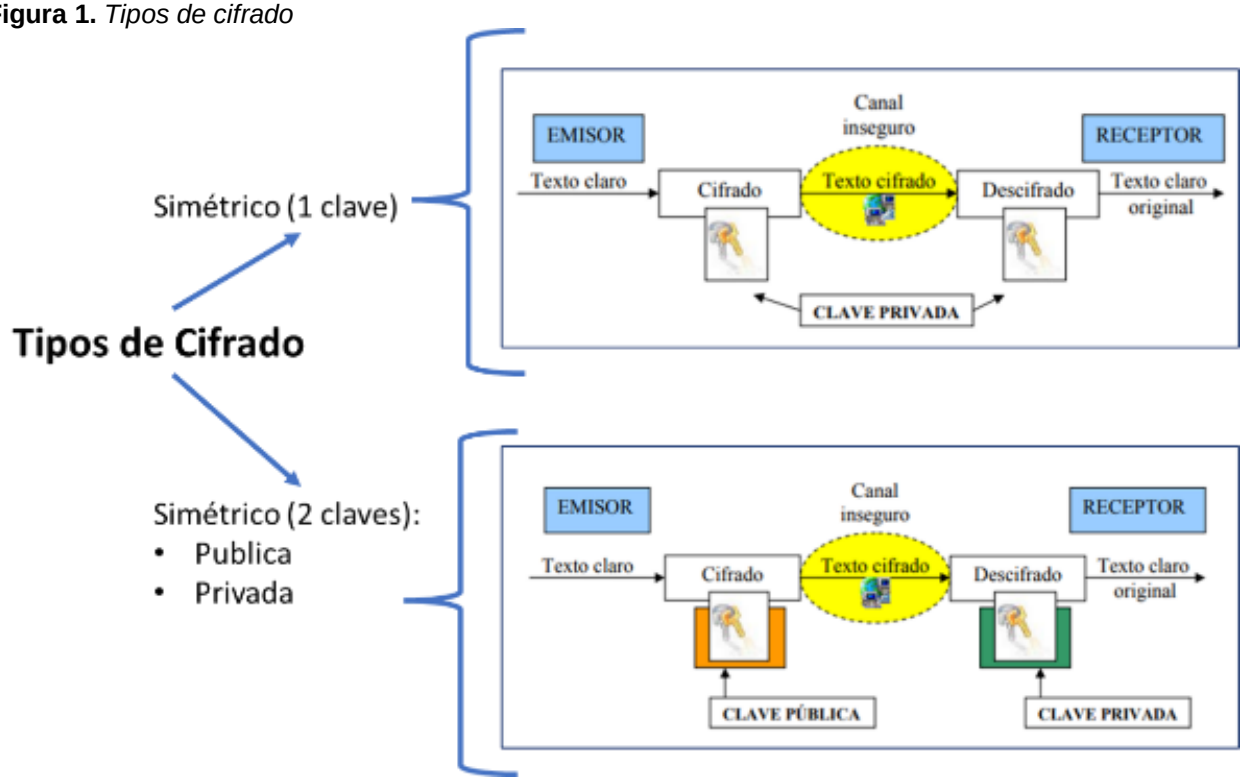
1. Tipos de cifrado

Actualmente, se pueden identificar dos tipos de cifrado, como son:

- **Cifrado simétrico**: este tipo de cifrado hace uso de una sola llave para cifrar un mensaje como para recuperarlo.
- **Cifrado asimétrico**: este tipo de cifrado hace uso de dos llaves.
- **Llave pública**: la cual se puede compartir.
- **Llave privada**: esta únicamente debe ser conocida por el destinatario o interesado.

En la figura 9, observe el proceso para cifrar mensaje a partir de estos 2 tipos de cifrado.

Figura 1. *Tipos de cifrado*



2. Comunicaciones Cifradas

Los controles de cifrado deben ser integrados en cualquier estrategia de seguridad como mecanismos vitales para salvaguardar la información confidencial y garantizar los pilares de la seguridad de la información. A continuación, identifique algunas aplicaciones específicas en servicios de red.

HTTPS

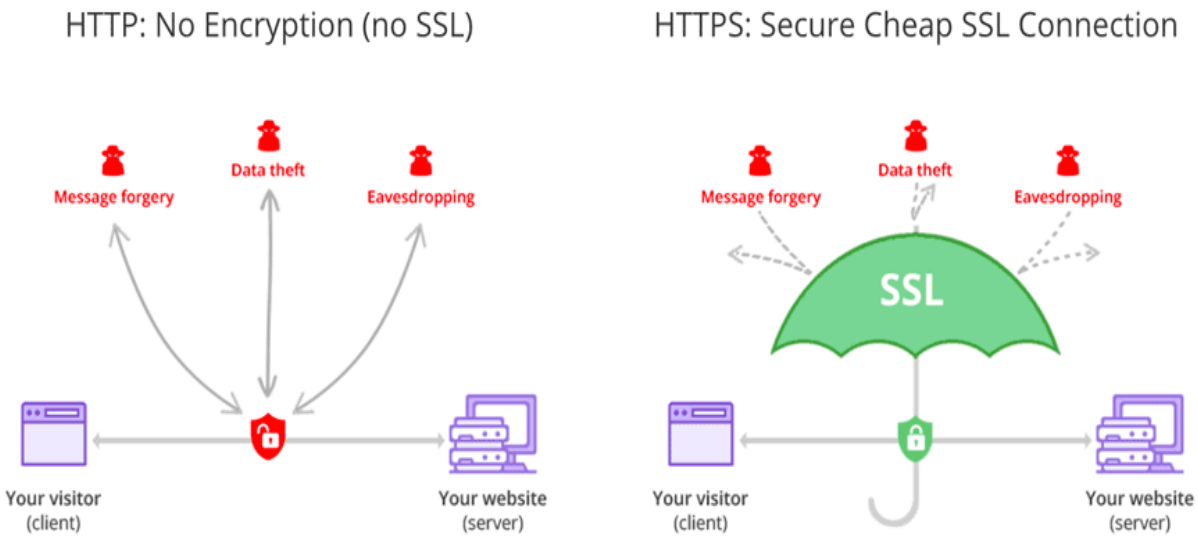
El protocolo de servicio web HTTP viaja de manera plana a través de los medios de comunicación, lo que lo hace vulnerable a cualquier interceptación permitiendo recuperar información sensible, alterar y/o aplicar sentencias dañinas; para mejorar la seguridad de este protocolo se realizan implementaciones como SSL acrónimo de *Secure Sockets Layer* la cual permite realizar un cifrado a la información transmitida entre dos puntos.

Así mismo, se cuenta con TLS *Transport Layer Security*, la cual es una mejora al SSL, agregando una capa de seguridad al transporte; los certificados web, se distribuyen actualmente con tecnología TLS aunque continúen llamándose SSL.

Estas implementaciones se realizan con la inclusión de un certificado digital en la operación del servidor web como apache, *ngnix* ó IIS, por nombrar algunos, habilitando el protocolo HTTPS.

En la figura 10, observe cómo la implementación de cifrado SSL evita que el contenido que circula a través de la red pueda ser leída por terceros no autorizados.

Figura 2. *Trafico HTTP vs HTTPS*



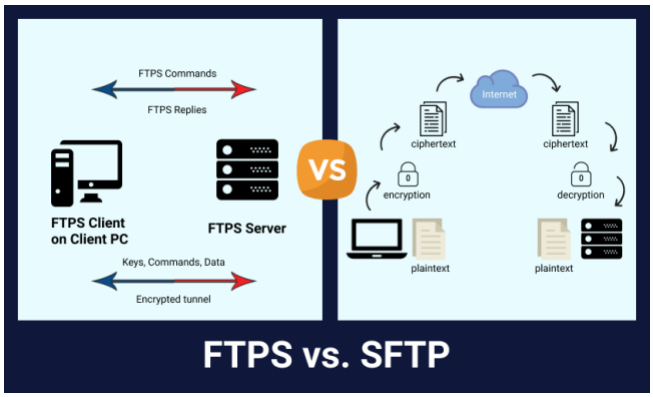
FTPS

La transferencia de archivos aún sigue siendo un servicio que se consume en algunas organizaciones y es muy útil cuando se realiza transferencia de gran cantidad de archivos o estos son de gran tamaño; para ello se hace uso de protocolos como el FTP. Lastimosamente este servicio en su implementación es muy sensible y apetecido por ciberdelincuentes; para reducir estos inconvenientes se puede realizar la implementación de FTPS (Protocolo de transferencia de archivos con soporte para Seguridad de la capa de transporte (SSL / TLS)).

Esta implementación también se realiza incorporando un certificado digital sobre el servicio FTP como, por ejemplo, *Vsftpd, Proftpd o Pure-FTPd.*

No se debe confundir con SFTP (Protocolo de transferencia de archivos SSH) el cual es un protocolo que permite transferir y manipular archivos a través de cualquier medio. Por lo general, se usa con el protocolo SSH-2, en la figura 11 podemos observar algunas de las diferencias en operación de esto protocolos.

Figura 3. *Diferencias entre FTPS Y SFTP*

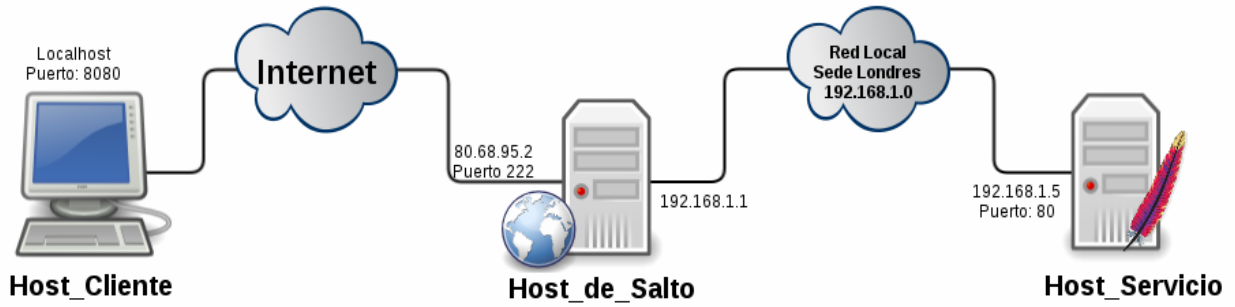


SSH

Uno de los controles que no deben faltar en cualquier estrategia de seguridad es la que sugiere asegurar los accesos remotos y seguros, en especial para la administración de dispositivos críticos así como de consolas y aplicaciones de seguridad; para abordar este control se sugiere la implementación de acceso seguro a través de SSH (*Secure SHell*) el cual es un servicio que hace uso de protocolo de cifrado como RSA y DSA. Este establece las conexiones estableciendo canales seguros y cifrados entre los dos puntos de la conexión, resguardando la información que fluye por el medio.

En la figura No. 12, identifique cómo, desde el exterior, haciendo uso de una conexión ssh puede establecer conexión con un *host* al interior de la red, implementando un canal cifrado a través de la red pública. Este servicio puede utilizarse a través de programas para la conexión remota como *Putty* y de transferencia de archivos segura como *WinSCP*.

Figura 4. *Funcionamiento de conexión SSH*



LDAPS

Uno de los controles sugeridos en las organizaciones son los relacionados con una adecuada gestión de usuarios y sobre su administración responsable, por el cual es muy común encontrar soluciones de servicio de directorio basados en protocolo LDAP *(Lightweight Directory Access Protocol*) como *OpenLDAP* o *Active de Directory* de Microsoft.

Estos servicios basados en LDAP permiten implementar directorio de objetos (unidades organizacionales, grupos, usuarios, equipos, entre otros), está estructurado bajo el protocolo X.500 y contiene una estructura de manera jerárquica; esto permite su gestión centralizada, así como la asignación de privilegios a diferentes recursos de la red.

Este servicio se aprovecha a nivel de aplicación para que los usuarios se autentiquen y hagan uso de servicios, por ejemplo: inicio de sesión, escritorio remoto, carpetas compartidas, dns, dhcp, autenticación desde otras aplicaciones, entre otros.

Al igual que los servicios anteriormente nombrados, para mejorar la seguridad en la transmisión de información, se recomienda la implementación de LDAPS (LDAP Seguro), esto se puede realizar con implementación de protocolos como SSL y TLS los cuales requieren un certificado digital. Observe y analice la figura No. 13.

Figura 5. *Implementación de protocolo LDAPS*