

# Cifrado De La Información

## Introducción

En el siguiente estudio sobre el cifrado de la información dentro de las redes de ordenadores, hemos considerado oportuno, realizar una breve síntesis sobre la necesidad de las redes, así como describir escuetamente la estructura de estudio de una red. Sin embargo, no por ello realizamos un análisis profundo y formal de la estructura y funcionamiento de la red, sino que nos limitamos a contar someramente en qué consiste. Conocer qué y cómo es una red es necesario para entender la necesidad de la seguridad de las redes y por tanto la necesidad del cifrado de la información.

La aparición del ordenador personal hace posible llevar la capacidad de proceso y almacenamiento a cada uno de los puestos de trabajo, creándose así espectro de equipos en los que tanto unos como otros pueden ser depositarios de información a la que se puede acceder desde cualquier punto de la organización. Precisamente esta posibilidad de acceder a la información desde cualquier punto implica un aumento en la necesidad de interconectar equipos.

Las redes se han convertido por lo tanto en un recurso importante de la empresa para el desarrollo de sus actividades y por lo tanto deben responder a ésta eficazmente con **fiabilidad** y **disponibilidad**.

Los requisitos de fiabilidad y disponibilidad de la red hacen que sea necesaria herramientas para preservar la **capacidad de respuesta** y mantener la **calidad del servicio** que la red debe proporcionar.

En definitiva, la función básica de una red informática es poder establecer entre distintos equipos informáticos una comunicación.

Las funciones elementales de una comunicación establecida mediante una red pueden resumirse en:

- **Conectabilidad de datos:** Conjunto de mecanismos que permite el trabajo cooperativo entre los equipos de datos (nodos de la red), tanto para el acceso a la información como para su proceso y almacenamiento.

- **Transformación:** Funciones que permiten la interoperación entre sistemas heterogéneos, es decir, arquitecturas distintas.
- **Gestión de ancho de banda:** Conjunto de elementos y funciones que permiten optimizar y gestionar el uso de los recursos básicos de los medios de transmisión, para conseguir una adecuada relación coste/rendimiento de estos medios.
- **Integración voz/datos:** El tratamiento digital de la voz la hace susceptible de ser procesada como un elemento más de información.
- **Gestión y control de la red:** El conjunto de funciones que integran la gestión de la red son fundamentales ya que las comunicaciones son un importante recurso importantísimo dentro de las organizaciones, y como tal, ha de ser controlado y administrado para optimizar su uso y rendimiento. La optimización de la disponibilidad sólo puede garantizarse si se pueden anticipar los problemas potenciales, detectar su ocurrencia, solucionarlos en el menor tiempo posible y controlar su evolución. Además todo esto debe hacerse con un enfoque global, que incluya desde el más importante programa o aplicación hasta el último de los terminales de la organización.

# Arquitectura De Redes

En el apartado anterior hemos descrito de una forma muy básica la necesidad de las redes telemáticas y los requisitos elementales que debe ofrecer al los usuarios. En el apartado actual presentamos, también de manera muy somera, como se inicia o prepara el estudio de las redes ya que al ser un conjunto particularmente complejo, necesita una estructuración que permita descomponer el sistema en sus elementos directamente realizables. Introducimos así el modelo de referencia para la **Interconexión de Sistemas Abiertos (OSI Open Systems Interconnection)**. Tras esta breve introducción dedicaremos un mayor detalle en el estudio de la **Capa de Presentación** que es la que se encarga en mayor medida de la seguridad y cifrado de los datos intercambiados.

## Estructura En Niveles

El modelo OSI de **ISO** (*International Standards Organization*) surge, en el año 1984, ante la necesidad imperante de interconectar sistemas de procedencia diversa —diverso fabricantes—, cada uno de los cuales empleaba sus propios protocolos para el intercambio de señales. El término *abierto* se seleccionó con la idea de realzar la facilidad básica del modelo que do origen al mismo, frente a otros modelos *propietarios* y, por tanto, cerrados.

El modelo OSI está compuesto por una pila de 7 niveles o capas, cada uno de ellos con una funcionalidad específica, para permitir la interconexión e interoperatividad de sistemas heterogéneos. La utilidad radica en la separación que en él se hace de las distintas tareas que son necesarias para comunicar datos entre dos sistemas independientes.

Es importante señalar que este modelo no es una arquitectura de red en sí mismo, dado que no se especifica, en forma exacta, los servicios y protocolos que se utilizarán en cada nivel, sino que solamente indica la funcionalidad de cada uno de ellos. Sin embargo, ISO también ha generado normas para la mayoría de los niveles, aunque éstas no forman parte del modelo OSI, habiéndose publicado todas ellas como normas independientes.

Num.	Nivel	Función
7	Aplicación	Datos normalizados
6	Presentación	Interpretación de los datos
5	Sesión	Diálogos de control
4	Transporte	Integridad de los mensajes
3	Red	Encaminamiento
2	Enlace	Detección de errores
1	Físico	Conexión de equipos

Tabla 1 Niveles OSI de ISO

Los tres niveles inferiores están orientados al acceso del usuario — comunicaciones de datos —; el cuarto nivel al transporte extremo a extremo de la información, y los tres superiores a la aplicación.

## Nivel 1 — Físico

El nivel físico —el más bajo y más antiguo— proporciona los medios mecánicos, electrónicos, funcionales y de procedimiento para mantener y desactivar las conexiones físicas para la transmisión de bits entre entidades de enlace de datos.

La misión básica de este nivel consiste en transmitir bits por un canal de comunicación, de manera tal que cuanto envíe el receptor llegue sin alteración al receptor.

Algunas de las normas dentro de este nivel son:

- **X.24** Definiciones relativas a los circuitos de unión establecidos entre dos equipos sobre redes públicas de datos.
- **V.10** Características eléctricas de los circuitos de intercambio de doble corriente asimétrica para uso general en teleinformática.
- **V.11** Como V.10 pero para corriente simétrica.
- **V.24/V.28** Características funcionales/eléctricas para los circuitos de enlace entre dos equipos.
- **V.35** Recomendación CCITT<sup>\*</sup> para transmisión de datos a 48 Kbit/s por medio de circuitos en grupo primario de 60 a 108 KHz.
- **ISO 2110** Características mecánicas.
- **EIA-232** Estándares a nivel físico, eléctrico y funcional de EIA<sup>\*\*</sup>.

## Nivel 2 — Enlace

El objetivo de este nivel es facilitar los medios funcionales y procedimentales para establecer, mantener y liberar conexiones de enlace de datos entre entidades de red y para transferir unidades de datos del servicio de enlace de datos.

Las funciones básicas que realiza este nivel están orientadas a resolver los problemas planteados por la falta de fiabilidad de los circuitos de datos, agrupándose los datos recogidos del nivel de red para su transmisión, formando tramas, que incluyen además bits de redundancia y control para corregir los errores de transmisión; además regula el flujo de las tramas, para sincronizar su emisión y recepción.

Pertenecen a este nivel:

- **HDLC** (*High-level Data Link control*): Protocolo de alto nivel, orientado al bit (especificado por ISO 3309), para el control del enlace de datos, en modo síncrono.
- **LAP-B** (*Link Access Procedure-Balanced*): Subconjunto del protocolo HDLC, definido por OSI, para acceso al enlace a redes X.25.
- **IEEE 802.2-7**: Para LAN's

### ***Nivel 3 — Red***

El nivel de red proporciona los medios para establecer, mantener y liberar la conexión, a través de una red donde existe una malla compuesta de enlaces y nodos, entre sistemas abiertos que contienen entidades de aplicación en comunicación, así como los medios funcionales y de procedimiento para el intercambio de unidades de datos del servicio de red entre entidades de transporte por conexiones de red.

Es el responsable de las funciones de conmutación y encaminamiento de la información; proporciona los procedimientos precisos necesarios para el intercambio de datos entre el origen y el destino por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.

Pertenecen a este nivel:

- **X.25**- Interconexión sobre redes públicas de equipos ETD\* y ETCD\*\* para terminales con funcionamiento en modo paquete, conectados a una red pública de transmisión de datos, con línea dedicada.
- **X.32** Interfase entre un ETD y un ETCD para terminales que transmiten en modo paquete y acceden a la red pública X.25 a través de la red telefónica conmutada.
- **X.3** Servicio complementario de ensamblado y desensamblado de paquetes en una red pública de datos.
- **X.28** Interconexión entre ETD/ETCD para el acceso de un ETD asíncrono al servicio de ensamblado y desensamblado de paquetes (DEP), en una red pública de datos.

- **X.29** Procedimientos de intercambio de información de control y de datos de usuario entre un DEP y un ETD modo paquete u otro DEP.
- **ISO 9542** Protocolo de encaminamiento para LAN's.

## ***Nivel 4 — Transporte***

El nivel de transporte efectúa la transferencia de datos entre entidades de sesión y las libera de toda otra función relativa a conseguir una transferencia de datos segura y económica.

Su misión básica es la de optimizar los servicios del nivel de red y corregir las posibles deficiencias en la calidad del servicio, con el auxilio de mecanismos de recuperación para condiciones anormales en los niveles inferiores. Proporciona los procedimientos de transporte precisos, con independencia de la red o soporte físico empleado.

Este nivel está muy relacionado con la calidad del servicio ofrecido por la red, ya que si no es suficiente es este nivel el encargado de establecer el puente entre las carencias de la red y las necesidades del usuario.

Se encuadran dentro de este nivel:

- **X.214 (ISO -8072)** Servicio de Transporte
- **X.224 (ISO 8073)** Especificación del protocolo de Transporte
- **ISO 8073**

## ***Nivel 5 — Sesión***

El nivel de sesión proporciona el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos.

Su función básica consiste en realizar el mapeo de la dirección de sesión hacia el usuario con las direcciones de transporte orientadas a la red y gestionar y sincronizar los datos intercambiados entre los usuarios de una sesión.

En el nivel de sesión tenemos las siguientes recomendaciones:

- **X.215 (ISO 8326)** Servicio de Sesión
- **X.225 (ISO 8327)** Especificación del Protocolo de Sesión

## ***Nivel 6 — Presentación***

Éste permite la representación de la información que las entidades de aplicación comunican o mencionan en su comunicación. Es el responsable de que la información se entregue al proceso de aplicación de manera que pueda ser entendida y utilizada.

Es responsable de la obtención y liberación de la conexión de sesión cuando existan varias alternativas disponibles, y de establecer el contexto sintáctico del diálogo. A través de él, los procesos de aplicación adquieren independencia de la representación de los datos, incluyendo en su entorno las posibles transformaciones de códigos y la selección de sintaxis.

A este nivel corresponden:

- **Normas para VideoText**
- **Normas para TeleFax**
- **Normas para TeleTex**
- **X.225**

## ***Nivel 7 — Aplicación***

Al ser el nivel más alto del modelo de referencia, el nivel de aplicación es el medio por el cual los procesos de aplicación acceden al entorno OSI. Por ello, este nivel no interactúa con uno superior a él.

Su función es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones. Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, controladas por protocolos de aplicación y utilizando los servicios del nivel de presentación.

La transferencia de ficheros es una de las aplicaciones más comunes de este nivel.

Pertenecen a este nivel, entre otras:

- **X.400** Describe el modelo básico del sistema de tratamiento de mensajes en la aplicación de *Correo Electrónico*
- **X.500** Servicio de *Directorio* en la aplicación de Correo electrónico.

# Nivel De Presentación

En este apartado veremos con mayor detalle el nivel o capa de presentación ya que, como hemos indicado, es, dentro del modelo de referencia OSI de ISO, el encargado de la gestión de la seguridad en las redes teleinformáticas.

El nivel de presentación se ocupa de la sintaxis de los datos, es decir la representación de los datos extremo a extremo.

Así pues es responsable de alcanzar un acuerdo en los códigos y formatos que se usarán en el intercambio de datos de aplicación durante una sesión. El nivel de presentación puede ser responsable del formateo de chorros de datos para su correcta salida a una impresora o a una determinada pantalla. También puede realizar compresión de datos y descompresión.

Las funciones del nivel de presentación son soportadas frecuentemente por las aplicaciones de los usuarios, y por tanto a menudo se omite el nivel de presentación.

Este límite tan sutil, entre el nivel de presentación y el nivel de aplicación, es debido a que durante mucho tiempo fue una capa sin función determinada. En principio se concibió como el lugar en donde se pudiesen llevar a cabo las conversiones para permitir que las máquinas ASCII se comunicaran con máquinas EBCDIC. Después se le asignó como medio para permitir que los programas orientados al despliegue visual, pudiesen trabajar con una gran variedad de terminales.

Finalmente, se ha decidido que la capa de presentación tratara todos los problemas relacionados con la representación de los datos transmitidos. Por lo tanto incluye los aspectos de:

- **Conversión**
- **Cifrado**
- **Compresión de datos**

Cuando se establece comunicación entre dos entidades o capas de aplicación se producen tres representaciones sintácticas de los datos transferidos entre dichas entidades de aplicación:

- La **sintaxis** usada por la entidad que origina los datos, **entidad emisora**.
- La **sintaxis** usada por la entidad que los recibe los datos o **entidad receptora**.
- La **sintaxis** usada por el **proceso de transferencia**, es decir como son representados en el cable (mientras viajan de una aplicación a otra).



Por lo tanto, y como ya hemos indicado, la capa de presentación se encarga de codificar los datos estructurados del formato interno utilizado en la máquina transmisora, a un flujo de bits adecuado para la transmisión y, después, decodificarlos para representarlos en el formato del extremo destinatario.

Ya hemos visto qué funciones tiene la capa de presentación. Vamos a explicar a continuación por qué es importante la representación de los datos entre el camino desde el origen hasta el destino, la compresión de datos y la seguridad y confidencialidad en las redes.

## **Representación De Datos**

Los diferentes ordenadores tienen diferentes representaciones internas para los datos. Estas representaciones son establecidas por los fabricantes en su momento y que ahora les es muy difícil de cambiar, dado que tienen que mantener la compatibilidad con sus antiguos sistemas.

Las redes informáticas permiten establecer comunicaciones entre los distintos ordenadores sin tener en cuenta su arquitectura interna. Por ello el modelo de referencia OSI de ISO establece que en la capa de presentación se realice la conversión entre las representaciones internas de los equipos conectados.

Para resolver este problema se han propuesto varias alternativas:

- El extremo transmisor realiza la conversión.
- El extremo receptor realiza la conversión.
- Establecer un formato normalizado y que cada uno de los extremos realice la conversión hacia y desde este formato normalizado de red.

Este tema es muy importante para el correcto funcionamiento de la capa de aplicación pero se aleja del objeto de nuestro análisis. Por ello y a nuestro pesar lo dejamos para mejor ocasión.

## **Compresión De Datos**

El costo por utilizar una red depende, normalmente de la cantidad de datos transmitidos. Por lo tanto y a fin de rebajar la factura se utiliza la compresión de datos antes de expedirlos al receptor para reducir la cantidad de datos a transmitir.

La compresión de datos está muy relacionada con la representación de los datos, ya que, lo que intentamos es transmitir la misma información, con menor número de bytes, representada mediante algún código especial pero con el mismo significado.

Igualmente que en el apartado anterior este tema escapa del interés de nuestro estudio.

## **Seguridad y Confidencialidad En Las Redes**

Con el desarrollo de las redes actuales las medidas de seguridad que se tienen que aplicar, para evitar al máximo que los datos emitidos sean interceptados por personas no autorizadas, se han disparado. Existe pues la necesidad de establecer algún tipo de mecanismo de **cifrado** para conseguir que los datos sean ininteligibles para aquellos que lo intercepten sin autorización.

La seguridad de los datos en la red debe contemplar los siguientes aspectos:

- Proteger los datos para que no puedan ser leídos por personas que no tienen autorización para hacerlo.
- Impedir que las personas sin autorización inserten o borren mensajes.
- Verificar al emisor de cada uno de los mensajes.
- Hacer posible que los usuarios transmitan electrónicamente documentos firmados.

El cifrado es un método que permite llevar a cabo los objetivos descritos.

El cifrado, no obstante, no es un elemento que pertenece en exclusiva a la capa de presentación sino que podemos encontrarlo en otras capas.

### ***Cifrado De Enlace***

En este caso el cifrado se realiza en la capa física. Para ello se utiliza una unidad de puesta en clave o cifrado entre cada ordenador, participante de la comunicación, y el medio físico, de manera que cada bit que sale de la máquina emisora sufre un proceso de cifrado, y a cada bit que entra en la máquina receptora se le practica el proceso inverso.

La ventaja del cifrado de enlace es que tanto las cabeceras como los datos se cifran.

### ***Cifrado En Transporte***

Si introducimos el cifrado en la capa de transporte ocasionamos que el cifrado se realice en la sesión completa. Se entiende que este cifrado tan general, conlleva una sobrecarga de trabajo de cifrado y que en muchas ocasiones será innecesario para algunos de los datos cifrados.

### ***Cifrado En Presentación***

Es quizás una solución más elaborada ya que el cifrado es sufrido sólo por aquellas partes de los datos que sean consideradas necesarias, consiguiendo de este modo que la sobrecarga del proceso de cifrado sea menor.

## ***Análisis De Tráfico***

Otro aspecto relacionado con la seguridad en las redes es el conocimiento de los patrones de tráfico, es decir, se estudia la longitud y frecuencia de los mensajes. Con este análisis se consigue determinar los lugares donde se está produciendo un intenso movimiento de datos. De todas maneras es fácil engañar a este análisis introduciendo en el mensaje grandes cantidades de datos de relleno o incluso enviando mensajes inútiles.

# SEGURIDAD EN LAS REDES

Hasta el momento hemos visto por qué las redes son necesarias, cómo se estructura su estudio, las distintas capas de una red dentro del modelo de referencia OSI de ISO y en mayor detalle la capa de Presentación la más adecuada para conseguir la privacidad de los datos transmitidos. Ahora llevaremos a cabo un estudio más general de la importancia de la seguridad en las redes, qué métodos de violación de seguridad se utilizan y qué medidas de protección existen para resolver la vulnerabilidad de los datos dentro de las redes.

Es cada vez más habitual oír casos de intrusión en ordenadores o redes de comunicación, bien con unos objetivos económicos bien con unos objetivos políticos, mientras que en otras ocasiones son simplemente malintencionados. Con el paso del tiempo los usuarios están cada vez más preparados para la utilización de ordenadores y redes, lo que supone que la preparación se está convirtiendo en un problema cada vez más grave para la industria informática y de comunicaciones.

En la gráfica expuesta se representa la curva de vulnerabilidad, de manera que se puede apreciar que cada vez es mayor el número de personas dotadas de los suficientes conocimientos como para causar daño el sistema informático de una organización. Debido a esta tendencia, cada vez se establecen mayores medidas preventivas y se dedica más atención a la seguridad en las redes.

## *Tipos De Violación De Los Sistemas De Seguridad*

Una de las formas más usuales y sencillas de quebrantar la seguridad es el **falseamiento**, es decir, la modificación previa a la introducción de los datos en el sistema informático o en una red. —un individuo, hace unos años, modificó una tarjeta de depósito en la ventanilla de un banco, con lo que consigue que le ingresaran fondos en su cuenta de forma ilegal—.

Otra forma de violación de la seguridad es el **ataque ínfimo "salami attack"**, que consiste en la realización de acciones repetitivas pero muy pequeñas, cada una de las cuales es casi indetectable —así, esta el caso de un programador que redondeaba las fracciones de moneda de las operaciones y las hacía ingresar en su propia cuenta—.

Una de las formas más eficaces de violación de la seguridad en una red, es la **suplantación de personalidad**, que aparece cuando un individuo accede a una red mediante el empleo de contraseñas o de códigos no autorizados. La contraseña suele obtenerse directamente del usuario autorizado de la red, muchas veces sin que éste se dé cuenta. Hay incluso algunos sistemas de acceso a la red que pueden burlarse

utilizando un ordenador para calcular todas las posibles combinaciones de contraseñas.

Una forma de combatir el empleo no autorizado de contraseñas consiste en instalar un sistema de palabras de acceso entre el canal de comunicaciones y el ordenador. Este dispositivo, un vez que recibe la contraseña, desconecta automáticamente la línea, consulta en una tabla cuál es el número de teléfono asociado a ella, y vuelve a marcar para conectar con el usuario que posee el número de teléfono designado.

Con este mecanismo, el intruso ha de disponer de la palabra de acceso o contraseña, y ha de encontrarse físicamente en el lugar en el que se supone que debe estar el usuario autorizado. No es una solución muy buena ya que hace verdaderos estragos en funciones como la redirección de llamadas hacia otros números o contestación automática.

Las redes también pueden ser violadas mediante lo que se conoce como "**puertas traseras**". Este problema se producirá cuando los dispositivos o los programas de seguridad sean inadecuados o incluyan errores de programación, lo que permitirá que alguien pueda encontrar el punto vulnerable del sistema. Los delitos cometidos mediante puertas traseras suelen deberse a la candidez del gestor de la red, lo cual queda de manifiesto especialmente cuando la red dispone de capacidades criptográficas. El gestor supone que el texto cifrado es completamente ininteligible, pero existen muchos sistemas en la actualidad que usan técnicas de cifrado sencillas, que pueden violarse con bastante facilidad.

Las redes también se ven comprometidas como consecuencia de la **intercepción y monitorización de los canales**. Así, por ejemplo, las señales de microondas o de satélites pueden interceptarse, si el intruso encuentra la frecuencia adecuada. Algunos casos de intercepción de las señales de satélite han originado serios problemas de seguridad a algunas compañías que transmitían informaciones secretas o delicadas.

## ***Métodos De Protección***

Para garantizar la confidencialidad de la información se utilizan las técnicas de cifrado de claves.

Una clave es un algoritmo software o un dispositivo hardware que codifica y bloquea el acceso a la información. Sólo la misma clave o una clave asociada puede descifrar la información.

Consideremos, por ejemplo, el envío de datos confidenciales a través de un enlace telefónico. Se pueden utilizar técnicas de cifrado para que los datos sean confidenciales, pero si se usa una clave para cifrar los datos, *¿cómo hacer que la clave llegue al receptor para que así pueda descifrarlos?*

Si se envía la clave a través de la línea, entonces estaría a disposición de cualquiera que estuviese conectado. Se podría enviar la clave a través de una línea diferente o utilizar un servicio de distribución urgente, pero, *¿se puede estar completamente seguro de que la clave llegó a su destino sin ser interceptada?*

Una solución consiste en intercambiar las claves antes de llevar a cabo las transmisiones. Un banco podría hacerlo así para comunicarse con sus sucursales. Pero *¿qué ocurre si lo que se quiere es enviar un mensaje confidencial aislado a un receptor que no se conoce?*

Las técnicas de **cifrado de claves públicas** proporcionan una solución.

Hay distintas técnicas que proporcionan seguridad en entornos de informática distribuida, tales como:

- **Servicios de Autenticación.**

Estos servicios de encargan de identificar a los usuarios que inician sesiones en las redes y sirven como prueba de su autenticidad para el resto de los dispositivos de la red.

- **Servicios de Autorización.**

Proporcionan al usuario el acceso a la red de acuerdo con los derechos de acceso que correspondan.

- **Servicios de Confidencialidad.**

Ocultan los datos frente a accesos no autorizados y asegurar que la información transmitida entre el emisor y el receptor no ha sido interceptada.

- **Servicios de Integridad.**

Garantizan que los mensajes son auténticos y no se han alterado.

- **No Repudiación.**

Sirven como prueba de que un mensaje ha sido enviado por un emisor específico y así evitar que éste pueda ocultar quién es el propietario.

## **CIFRADO CON CLAVES PRIVADAS**

Una técnica muy usada para aumentar la seguridad de las redes informáticas es el cifrado. Esta técnica convierte el texto normal en algo ininteligible, por medio de algún esquema reversible de codificación desarrollado en torno a un clave privada que sólo conocen el emisor y el receptor. El proceso inverso es el descifrado , mediante el cual el texto

en clave vuelve a convertirse en texto legible. El cifrado suele tener lugar en el emisor, mientras que el descifrado suele realizarse en el receptor.

El cifrado se clasifica en dos tipos: **cifrado por sustitución** y **cifrado por transposición**.

- **Sustitución:** Es la forma más sencilla de cifrado. Casi todas hemos utilizado alguna vez esta técnica en alguna de nuestras actividades personales, o incluso como un juego de niños. Consiste en reemplazar una letra o un grupo de letras del original por otra letra o grupo de letras.

Uno de los esquemas más sencillos es el **CIFRADO DE CÉSAR**, en este mecanismo cada letra del alfabeto es sustituida por otra.

Texto legible:            ABCDEFGHIJKLMNOPQRSTUVWXYZ

Letras de sustitución:       FGQRASEPTHUIBVJWKLXYZCONMD

Este tipo descifrado se conoce como **sustitución monoalfabética**, ya que cada una de las letras se sustituye por otra del mismo alfabeto.

Aunque este método ofrece  $4 \times 10^{26}$  claves distintas, la propia clave puede revelar bastante sobre la inteligibilidad del mensaje. Si no se conocen las claves, o si éstas no presentan ninguna regularidad, se calcula que un ordenador tardaría 1013 años en probar con todas las claves, si se dedica un microsegundo a probar con cada clave.

Sin embargo, los lenguajes presentan ciertas propiedades que permiten descifrar mucho más rápido. Así, por ejemplo, las vocales son mucho más frecuentes que las consonantes. Además, existen algunas combinaciones de dos letras —*digramas*— que aparecen muy a menudo, por ejemplo, en español, de, en, etc. En muchos idiomas también son frecuentes determinadas combinaciones de tres letras —*trigramas*— como en español, des, con, que, etc.

La tarea del criptoanalista consiste en estudiar las apariciones de cada letra, digrama, trigramas e incluso de algunas palabras. Una vez que el criptoanalista y su ordenador han establecido el cifrado correspondiente a las letras, digramas, trigramas y palabras más frecuente, puede generar un intento de texto legible basándose en los datos descodificados.

El descifrado final del código se convierte en algo relativamente sencillo, sobre todo si se utiliza un ordenador de alta velocidad.

Hay otros métodos de cifrado por sustitución más eficaces. Así, por ejemplo, algunos sistemas usan la **sustitución polialfabética**, en la cual existen varios alfabetos de cifrado que se emplean en rotación. Una variación del cifrado por sustitución consiste en utilizar una clave más

larga que el texto legible. Se usa como clave una secuencia aleatoria de bits, que se cambia periódicamente.

La principal desventaja de todas las estructuras basadas en una clave privada es que todos los nodos de la red han de conocer cuál es la clave común.

La distribución y confidencialidad de las claves acarrea algunos problemas administrativos y logísticos.

Hasta hace poco, la idea de una clave privada era el esquema de cifrado predominante en las redes. Los nodos de la red cambian la clave periódicamente; por ejemplo, cada 24 horas, o incluso, si es necesario, cada pocos minutos.

- **Cifrado por transposición.** Es un método criptográfico más sofisticado. En él las claves de las letras se reordenan, pero no se disfrazan necesariamente.

En la siguiente ilustración se muestra un ejemplo de cifrado por transposición.

La clave utilizada para el ejemplo es SEGURIDAD, que no es demasiado buena para un sistema de seguridad. La clave se emplea para numerar las columnas. La columna 1 se coloca bajo la letra de la clave más próxima al comienzo del alfabeto, es decir, A, B, C, ...

Si la clave incluye alguna letra repetida, puede adoptarse el criterio de numerar de izquierda a derecha. Por ejemplo:

A continuación se escribe el texto legible como una serie de renglones que se colocan debajo de la clave. Después se lee el texto cifrado por columnas, empezando por aquella columna cuya letra clave sea la más próxima al principio del alfabeto. Así, la frase *"compra barato vende caro y hazlo hoy"* quedará como sigue:

<b>S</b>	<b>E</b>	<b>G</b>	<b>U</b>	<b>R</b>	<b>I</b>	<b>D</b>	<b>A</b>	<b>D</b>
8	4	5	9	7	6	2	1	3
C	O	M	P	R	A	B	A	R
A	T	O	V	E	N	D	E	C
A	R	O	Y	H	A	Z	L	O
H	O	Y	A	B	C	D	E	F



Y el texto cifrado será el siguiente:

**AELEBDZDRCOFOTROMOOYANACREHBCAAHPVYA**

## El Algoritmo DES\*

En 1977, el Departamento de Comercio y la Oficina Nacional de Estándares de Estados Unidos publicaron la norma **DES** (estándar de cifrado de datos, publicación 46 del FIPS\*\*).

DES es un esquema de cifrado de claves privadas. El algoritmo DES es un sistema monoalfabético que fue desarrollado en colaboración con IBM y se presentó al público con la intención de proporcionar un algoritmo de cifrado normalizado para redes de ordenadores.

DES se basa en el desarrollo de un algoritmo de cifrado que modifica el texto con tantas combinaciones que el criptoanalista no podría deducir el texto original aunque dispusiese de numerosas copias.

El cifrado comienza con la **función de permutación** "*función P*", en este caso la entrada a la función P consta de 8 bits. La sustitución de los bits sigue una serie de reglas lógicas. La salida está formada por los mismos bits cambiados de orden. La caja P puede estar cableada o estar realizada mediante programa con el fin de llevar a cabo diversos tipos de permutaciones. La segunda **función** que se realiza es la de **sustitución**. En este caso, una entrada de 5 bits (el decodificador) selecciona una de las ocho posibles líneas que entran en la caja S. La "*función*" S lleva a cabo la sustitución de las líneas, con lo cual las 8 líneas vuelven a convertirse en 5 tras pasar por el codificador.

La filosofía del algoritmo DES consiste en llevar a cabo varias etapas de permutación y sustitución, como se ve en la tercera figura. DES utiliza una clave de 64 bits, de los cuales 56 son utilizados directamente por el algoritmo DES y otros 8 se emplean para la detección de errores. Existen unos setenta mil billones de claves posibles de 56 bits. Evidentemente para romper una clave semejante sería necesaria una enorme cantidad de potencia de cálculo. Sin embargo, no es una tarea imposible. Los ordenadores de alta velocidad, mediante análisis estadísticos, no necesitan emplear todas las posibles combinaciones para romper la clave. A pesar de ello, el objetivo de DES no es proporcionar una seguridad absoluta, sino únicamente un nivel de seguridad razonable para las redes orientadas a aplicaciones comerciales.

En el método DES el texto legible que debe ser que debe ser cifrado se somete a una permutación inicial (ip) con un bloque de entrada de 64 bits que se permuta de la siguiente forma:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Es decir, la entrada permutada tiene como primer bit el bit 58 del original, como segundo bit el bit 50 del original, y así sucesivamente, hasta llegar al último bit, que corresponderá al bit 7 del texto sin cifrar. A continuación, el bloque de entrada permutado sirve de entrada a un complejo cálculo dependiente de la clave, que consta de 16 etapas. El funcionamiento de cada etapa es el mismo, pero la función de cifrado utiliza la clave (K) de distintas formas.

A continuación, el resultado final se somete a la siguiente permutación, que es la inversa de la permutación inicial:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Las 16 etapas emplean los dos bloques (L y R) de 32 bits para generar dos bloques de 32 bits de salida. Las copias derecha e izquierda se

intercambian antes de cada etapa. La "función  $F$ " lleva a cabo cuatro pasos sobre la salida derecha, mediante una transposición basada en la operación o-exclusivo.

1. La mitad derecha R de 32 bits se convierte, mediante una regla de transposición y duplicación, en el número E, de 48 bits.
1. E y K se combinan mediante un o-exclusivo. En cada etapa se escoge un bloque K de bits dentro de la clave de 64 bits.
1. Los 48 bits generados en la etapa 2 se dividen en ocho grupos de 6 bits que se introducen en sendas cajas S, cada una de las cuales produce 4 bits de salida.
1. Los 32 bits restantes se introducen en la caja P.

Este algoritmo ha sido motivo de gran controversia parte de ella se debe al secreto que rodeó a su desarrollo. IBM trabajó en colaboración con la Agencia Nacional de Seguridad de Estados Unidos y ambas guardaron el secreto de los aspectos del diseño del algoritmo.

Muchas de las críticas obtenidas se encuentran en el hecho de usar sólo 56 bits de parte de la clave para conseguir el cifrado, ya es considerado por muchos insuficientes. El diseño de IBM incluía una clave de 128 bits, que habría hecho radicalmente imposible romper la clave, incluso con los ordenadores más rápidos existentes.

También hay quien piensa que el gobierno no quiere dar al público una clave completamente inviolable.

La digitalización de la voz es algo que ya incorporan algunos aparatos telefónicos, de modo que usando la tecnología de los semiconductores, no sería difícil instalar un circuito integrado capaz de calcular el algoritmo DES, que sea capaz de descifrar cualquier transmisión.

## Cifrado Con claves Públicas

Muchos sistemas comerciales emplean métodos de cifrado/descifrado basados en claves públicas. Este sistema está basado en el uso de claves independientemente para el cifrado y para el descifrado de los datos. La particularidad y enorme ventaja es que la clave y el algoritmo de cifrado pueden ser de dominio público, siendo la clave de descifrado la que se mantiene en secreto. Este método elimina los problemas logísticos y administrativos relacionados con la distribución y gestión de las claves públicas.

Los métodos inventados en la Universidad de Stanford y en el MIT<sup>\*</sup> incluyen la generación de un par de enteros positivos "**E y N**" que se usan para cifrar los datos, según la fórmula ***texto legible*<sup>E</sup> / N = *textocifrado***. El mismo proceso que genera E y N da como resultado el

valor D, que se emplea para descifrar, según la fórmula:  $\text{textocifrado}^D/N = \text{texto legible}$ . Los enteros E, N y D se calculan generando dos grandes números aleatorios primos.

Los sistemas basados en claves públicas no son tampoco infalibles ya que también pueden romperse.

En cualquier caso, y para evitar que la clave pueda ser detectada, es posible generar una clave distinta para cada transmisión, o de una forma más realista, a intervalos periódicos o aleatorios. El cambio de clave frecuente aumenta la seguridad de las transmisiones, ya que el posible intruso deberá intentar romper la clave cada vez que ésta cambia.

Puede incluso añadirse otro nivel de seguridad, utilizando un sistema de claves privadas para cifrar las claves públicas, es decir, pueden emplearse dos niveles de cifrado para los datos más delicados.

## Técnicas Que Proporcionan Seguridad

Con anterioridad hemos nombrado algunas técnicas que se utilizan para poder evitar que los datos transmitidos por la red puedan ser leídos o modificados por usuarios no autorizados. A continuación estudiamos estas técnicas con mayor detalle.

### Autenticación y Autorización

En un entorno de informática distribuida, generalmente los usuarios acceden a algunos recursos que no sean los unidos a sus servidores locales. Tradicionalmente, un usuario inicia una sesión para acceder a los recursos locales. Cuando accede a los recursos remotos, el usuario debe iniciar de nuevo una sesión.

Este método de iniciar una sesión por cada recurso no solo es incómodo, sino que dificulta la gestión. Se debe mantener una cuenta de usuario con la clave actual de cada servidor. Además, la conexión a dispositivos remotos no es fiablemente segura y los intrusos podrían controlar la línea e interceptar la información de inicio de sesión para su propio uso. Claramente, se necesitan métodos mejores.

UNIX, NetWare 4.X y otros sistemas operativos usan el concepto de "**anfitrión de confianza**", donde un sistema confía en que otro sistema haya verificado correctamente la identidad de un usuario.

Los sistemas de autenticación en los entornos de las redes de área local suelen ir asociados a los procedimientos de inicio de sesión.

Una palabra clave —**password**— que tan sólo conoce un usuario y que está asociada con su cuenta en la red, garantiza la autenticidad de dicho usuario. En algunos casos extremos es necesario utilizar alguna otra técnica adicional para la identificación de los usuarios, tales como la verificación de determinadas características físicas y biológicas, como, huellas digitales y patrones de voz.

Son habituales los sistemas de **identificación mediante tarjetas**. Los cajeros automáticos ATM\* de los bancos utilizan este método. El usuario debe insertar primero una tarjeta donde está codificada la información de su cuenta, y luego ha de introducir una palabra clave o un número de identificación personal que sirve de comprobación adicional.

**Kerberos** es un sistema de autenticación, desarrollado por el Proyecto Athena del Instituto Tecnológico de Massachusetts—MIT—. Se usa en el Entorno de informática distribuida —CE— de la Fundación del software abierto —OSF— y también lo emplean diversos fabricantes de sistemas operativos de la red.

Kerberos proporciona un modo de autenticación de los clientes y los servidores sin necesidad de transmitir información a través de la red, con el consiguiente riesgo que esa transmisión implica para la seguridad. así podemos ver que sus características son:

- Autentifica a los clientes cuando inician la sesión (logon). Otros clientes confían en que los servidores de autenticación Kerberos han identificado a los clientes debidamente.
- Los usuarios deben adquirir un billete desde un servidor de autenticación con objeto de utilizar un servicio disponible en un servidor determinado. Se genera un autenticador, que contiene información adicional sobre el usuario que el servidor deseado compara con un billete para la verificación de la identidad correcta. Este proceso tiene lugar en segundo plano.
- Los billetes proporcionan la autorización requerida a los usuarios autenticados que van a acceder al servicio.
- Los billetes son claves privadas y cifradas, y contienen la identidad de un cliente, su dirección, marcas de tiempo y otra información. Las marcas de tiempo aseguran que la información que cruza la red expira después de unas pocas horas, con objeto de desbaratar las acciones de los intrusos.
- Todas las sesiones entre clientes y servidores son temporales. Si un cliente necesita establecer una nueva sesión, debe obtener un nuevo identificador. Los billetes expiran después de un periodo de tiempo, de modo que los clientes necesitan periódicamente la adquisición de nuevos billetes para el acceso a un servidor particular.

Para el uso del sistema Kerberos se requiere que cada servicio de red se modifique. También requiere un servidor especial que gobierne el servicio de autenticación Kerberos. Este sistema debe situarse en lugar seguro. Además, se recomienda un servidor redundante, debido a que el acceso a la red se corta si el servidor Kerberos sufre una caída. Aunque

los costes son altos, Kerberos proporciona un entorno seguro para las organizaciones que lo necesitan.

Una vez que el usuario ha sido autenticado dentro del sistema, es la autorización quién se encarga de que acceda a los recursos. La autorización consiste en una serie de listas de control de acceso ACLs definidas por los supervisores y los administradores de la red. Una ACL otorga al usuario de acceso a los directorios, los archivos, los objetos y/o los recursos de la red.

## Servicios Criptográficos

Los sistemas criptográficos permiten el envío de información a través de sistemas de comunicación poco fiables, en lo que se refiere a la seguridad, de forma que aquellos que puedan estar interceptando la línea no sean capaces de desvelar el contenido de dicha información.

Estos sistemas garantizan la confidencialidad y pueden servir también como prueba de que no se han interceptado o alterado una transmisión. sin embargo, el propio sistema criptográfico debe ser fiable. *¿Cómo garantizar que un sistema criptográfico es seguro?, ¿Existe alguna persona no autorizada que posea la clave para descifrar los mensajes cifrados?* Es debido a estas dudas que los esquemas de cifrado extensamente probados, de dominio público y bien documentados son los más populares. Existen **esquemas de cifrado simétricos y asimétricos**.

El propósito de cualquier programa de cifrado, es asegurar la comunicación privada. El crecimiento de las redes internacionales, los sistemas de correo electrónico públicos y privados, y las comunicaciones por radio requieren mayores necesidades de seguridad. Afortunadamente, los avances en microelectrónica ofrecen medidas de seguridad más fáciles y económicas de implementar. Quizás la justificación de que los técnicos utilicen analizadores de protocolos que supervisan el tráfico de red, ha liberado a los gestores del hecho de que sus transmisiones de datos no sean seguras.

Los algoritmos de cifrado son relativamente lentos y el método de la clave pública es el más lento de todos. La implementación de algoritmos en hardware mejora las prestaciones y proporciona otro nivel de seguridad frente a la piratería informática con la que se encuentra un producto software.

## Esquemas De Claves Privadas

En los sistemas de claves privadas la información se transforma mediante un algoritmo que se basa en alguna clave privada que poseen tanto el emisor como el receptor del mensaje.

El mensaje transformado es ilegible y se puede transmitir a través de sistemas que no sean fiables. El receptor puede descifrar el mensaje mediante la clave privada que posee. El problema consiste en hacer llegar a los receptores una copia de las claves, sin que la misma se vea comprometida.

Para evitar la distribución de las claves con el consiguiente riesgo para el sistema, se pueden utilizar métodos de claves públicas en conjunción con los métodos de clave privadas.

## *Claves En Depósito*

Desde 1995, el gobierno de Estados Unidos se ha interesado en la normalización de un método de cifrado calificado "**CLAVE ESCROW**", en el cual se mantiene en secreto la clave para descifrar las comunicaciones de cualquier organización que el gobierno desee controlar.

El método divide la clave en partes y se da cada una a una persona de confianza diferente. De esta manera, una clave sólo es útil cuando estas personas se reúnen y cada una de ellas entrega su parte de la clave. El Ministro de Justicia de los Estados Unidos supervisaría el acceso a las claves y las agencias jurídicas sólo podrían conseguir las claves con mandatos judiciales. Esto es algo que inquieta al servicio de seguridad.

A mediados de 1993, el Instituto Nacional de Normas y Tecnologías — *NIST* — propuso la tecnología de la clave de escrow como el núcleo de una norma federal para procesamiento de información y el Departamento de Justicia se comprometió a utilizarla.

## *Chip Clipper*

El chip Clipper utiliza una clave de 80 bits para cifrar tanto datos como voz digitalizada y se instalará en los equipos de comunicación de datos propiedad del gobierno de los Estados Unidos, tales como computadoras, modems, fax y teléfonos.

El chip de cifrado de datos Clipper permitirá que las agencias federales y las empresas se protejan de los intrusos, de aquellos que intenten violentar los sistemas informáticos y de los criminales.

Es un coprocesador de cifrado de 12Mbits/seg diseñado por Mykotronix y fabricado por VLSI. El chip está protegido para evitar que pueda ser abierto, de forma que no se puede estudiar su diseño — *ingeniería inversa* —. Lo desarrollaron conjuntamente la Agencia Nacional de Seguridad — *NSA* — y el Instituto Nacional de Normalización y Tecnología.

El chip Clipper es muy controvertido. A pesar de que se ha utilizado un algoritmo secreto, se plantean dudas acerca de si su implementación ha sido la correcta, y si el algoritmo de cifrado tiene una "**puerta-falsa**" para descifrar los mensajes que sólo conocen las personas que lo han diseñado.

## Esquemas De Claves Públicas —Asimétricas—

Los esquemas de cifrado de claves públicas resuelven el problema del envío de las claves a los receptores de los mensajes. De hecho, permiten que una persona envíe un mensaje cifrado a otra sin que se haya realizado ningún intercambio previo. Ni siquiera es necesario que ninguna de las otras dos partes conozca a la otra, o que pertenezcan a la misma organización o estén conectadas a la misma red. Tan sólo es necesario que ambas partes tengan acceso a un servidor común que las gestione la seguridad de la clave pública.

El sistema de clave pública consta de dos claves. Cada usuario dispone de una clave privada junto con otra pública, que deja para que esté disponible en alguna ubicación pública. Cuando un usuario desea enviar un mensaje confidencial a otro usuario, cifra el mensaje con su propia clave privada. Los mensajes cifrados con clave pública tan sólo pueden ser descifrados con claves privadas.

## Firmas Digitales

Las firmas digitales son métodos de cifrado que tienen dos propósitos:

- **Validar el contenido** de un mensaje electrónico y se puede utilizar posteriormente para comprobar que un emisor envió de hecho ese mensaje.
- **Probar que no se ha falsificado un mensaje durante su envío.** Las firmas digitales respaldan la autenticidad del correo electrónico, transacciones de contabilidad, órdenes de empresa, documentos para grupos de trabajo y otros mensajes y archivos que se trasladan entre sistemas, usuarios u organizaciones.

Las firmas digitales se basan en el hecho de que dos grupos pueden autenticarse el uno al otro para el intercambio seguro de documentos, pero la relación entre ellos no se basa en una confianza total.

Por ejemplo, una persona podría enviar un mensaje para apostar a un caballo de carreras y después, si el caballo perdió la carrera, y niega haber enviado dicho mensaje. Aunque se sabe a través del proceso de autenticación que esta persona realmente envió ese mensaje, sin una firma digital no se podría probar técnicamente que el mensaje no se modificó. El emisor podría decir, "sí, yo le mandé un mensaje, pero usted lo cambió"



Las firmas digitales autentifican los mensajes y se usan para validar compras, transferencias de fondos y otras transacciones de negocios. Un formulario con una firma digital debe incluir el nombre del emisor, la fecha y hora, junto con una secuencia numérica o identificación que identifique positivamente a la persona o a la transmisión.

A continuación perfilamos un procedimiento que usa cifrado de clave pública con firma digital:

1. El emisor crea la firma digital con el uso de su clave privada, con la que cifra la información de identificación en el documento.
2. Antes de enviar el mensaje, el emisor cifra todo el documento de nuevo con el uso de la clave pública del receptor. Ah ora el mensaje original cifrado se incrusta en el documento nuevamente cifrado.
3. El mensaje se envía al receptor que lo descifra con su clave.

El primer cifrado protege la firma y la información que identifica al emisor de la falsificación y proporciona una forma de autentificar el mensaje. El segundo cifrado protege la parte del texto o la información del documento que se transmite y permite que el receptor descifre y lea la información recibida.

La seguridad de una firma digital, como otros métodos de cifrado, se basa en un algoritmo matemático que asegura que dos firmas nunca son iguales. Imagina el tiempo que llevaría desbloquear los modernos códigos de cifrado generados por las computadoras y que durante décadas han utilizado las supercomputadoras. De hecho, los mejores sistemas de seguridad están bajo el "ataque" constante de los expertos en este tema.

Con los algoritmos de cifrado proporcionados por RSA Data Security la probabilidad de que por casualidad diferentes documentos tengan el mismo código es menor de 1 entre un billón de billones.

Las necesidades de seguridad crecen diariamente debido al aumento de la informática distribuida, que sitúa los recursos de las computadoras y las bases de datos en localizaciones remotas. La autentificación, certificación, el cifrado de clave pública, proporcionan otros tipos distintos de seguridad.

## **Sistemas De Certificación**

Los servidores de certificados y certificación son un medio de autentificación para aquellos clientes que desean acceder a los servidores en entornos distribuidos, sin necesidad de autentificar a los usuarios cada vez que éstos acceden a un servicio protegido.

El procedimiento de certificación se desarrolló originalmente en el Instituto de Tecnología de Massachusetts —MIT— y está implementado en el sistema de seguridad de Kerberos, sus normas actualmente están en X.509 del CCITT.

Considérese una red de gran tamaño donde muchos usuarios necesitan acceder a los datos y las aplicaciones de muchos servidores. En un entorno tan grande como éste, no sería realista pretender autenticar a los usuarios cada vez que intentan en acceder a uno de los servidores. No se debe olvidar que las palabras de acceso, incluso aquellas que estén cifradas, han de permanecer fuera de las líneas donde los intrusos puedan interceptarlas para conseguir el acceso al sistema. Con la certificación se autentifica a los usuarios una sola vez, cuando inician una sesión en el sistema, y luego se informa a los demás servidores de que el usuario es quién dice ser. Se basa en la **"relación de confianza"**

La verificación proviene de un tercero en quien se confía, denominado servidor de certificación. Es más fácil describir con un ejemplo el proceso de certificación que utilizan el servidor de certificación, el cliente y el servidor de la aplicación.

Este ejemplo podría ser:

Se necesita consultar los informes secretos de la oficina de tu compañía en Madrid y que trabajamos en Alicante y el jefe que es quien puede autorizarnos está en Toledo.

Lo normal sería llamar al jefe y solicitarle el acceso a los archivos. El escribe un certificado autorizado donde se incluye su nombre y fotografía, junto con otra información que pueda ser necesaria y que pueda identificar sin ninguna duda la oficina de Madrid.

Esta información se guarda en una caja cerrada de la cual posee llave el jefe de seguridad de la oficina de Madrid. Esta caja se guarda en una segunda caja cerrada de la cual nosotros tenemos la llave. De modo que si alguien intenta abrirla se detectaría, ya que necesitan la llave que tenemos en Alicante o la de Madrid.

Una vez que hemos recibido la caja la abrimos y avisamos al jefe de seguridad de Madrid, este verificará nuestra identidad y autorizará a darnos los archivos. Si la caja mostrase señales de haber sido manipulada el jefe de seguridad nos denegará el acceso.

Los sistemas de computadoras pueden gestionar fácilmente este tedioso proceso. Y lo lleva a cabo de la siguiente forma:

1. En un principio, el servidor de certificación obtiene las claves "llaves" de todos los clientes y los servidores de aplicaciones, así como las palabras claves para iniciar las sesiones.
2. Cuando se inicia una sesión en el sistema, el servidor de certificación solicita una identificación y una palabra clave que identifican al usuario.

3. Para acceder a un servidor basta con conectarse a él, pero, en segundo plano, hay un proceso que solicita un certificado del servidor de certificación para acceder al servidor de la aplicación y lo envía en un mensaje cifrado es cifrado una segunda vez con la clave pública del usuario. Así se garantiza que la transmisión del certificado de acceso del usuario sea segura.
4. Cuando el sistema del usuario recibe el paquete certificado, lo descifra con su clave personal. El sistema está ahora en posesión del certificado que da acceso al servidor. A continuación, el certificado se envía al servidor de la aplicación que lo descifra con su propia clave.
5. De esta forma el usuario ha sido autenticado para el servidor de la aplicación a partir del certificado y de la información acerca de la sesión que éste contiene.

Si la seguridad se ve comprometida durante el intercambio del certificado, se invalida a éste. El proceso utiliza una serie de funciones que pueden detectar los intentos de interceptación.

En el ejemplo anterior, se ha supuesto que todos los sistemas pertenecen a la misma organización, pero la certificación también puede controlar el acceso a los recursos de organizaciones diferentes.

Por ejemplo, los usuarios de Internet pueden obtener del gobierno de los Estados Unidos la certificación necesaria para acceder a sistemas y redes protegidas. O también, podría darse el caso o de una compañía que permitiese el acceso a algunos de sus servidores a una empresa auditora o de contabilidad.

Un aspecto importante de la certificación es **que existe algún tipo de autoridad que se encarga de autenticar al usuario**. Esta autoridad era un servidor de certificación en el ejemplo anterior, pero también se podría tratar de una tercera organización o de una agencia del gobierno. La autoridad es la encargada de proporcionar los certificados que verifican a los usuarios. También es necesario verificar que la autoridad encargada de la certificación es quién dice ser. En este caso, se puede recurrir a algún tipo de organización notarial para que sirva como mediador entre un usuario y una organización.

## Servicios De Integridad

Las firmas digitales y los códigos de autenticación de mensajes — *MAC*— proporcionan un medio de autenticar el origen de un mensaje y de estar seguros de que el contenido del mensaje no ha sido alterado durante la transmisión.

Un MAC es un mecanismo que calcula un único valor a partir del contenido del mensaje, algo similar a los códigos de paridad. Tanto el emisor como el receptor deben ser capaces de realizar el mismo cálculo y obtener el mismo resultado: de no ser así el mensaje está corrompido.

Para garantizar la seguridad, se utilizan en el cálculo las claves privadas del emisor y el receptor.

Las firmas digitales son posibles cuando se emplean esquemas de cifrado de claves públicas. Se usa un algoritmo para generar un valor hash a partir de la información de una parte del mensaje. A continuación se cifra este valor mediante la clave privada del emisor, para así obtener la firma digital.

Para verificar el mensaje el receptor debe, en primer lugar, ejecutar el mismo algoritmo hash. Los resultados de este algoritmo se comparan con la firma digital descifrada. El receptor utiliza la clave pública del emisor para descifrar la firma.

Dado que para verificar la autenticidad del mensaje se utiliza la clave pública, las firmas digitales son más versátiles que los esquemas MAC, en los que se requiere que las dos partes hayan intercambiado primero sus claves privadas.

De cualquier forma, ambos métodos sirven para que tanto el emisor como el receptor sepan si el mensaje ha sido modificado. Esto es de enorme utilidad en los negocios y otras transacciones.

Imagínese que le envía a su agente de bolsa un mensaje diciéndole que adquiera determinadas acciones. Tanto MAC como una firma digital le pueden servir al agente de bolsa para asegurarse de que el mensaje proviene de usted y de que no ha sido alterado, y podrá conservar el mensaje como prueba de su transacción. No se puede repudiar el mensaje una vez recibido puesto que tanto MAC como la firma digital permiten demostrar su origen. Y lo que es más, el agente de bolsa no puede modificar el contenido del mensaje puesto que cualquier alteración se pondría de manifiesto si se hiciese una verificación de la firma digital o de MAC.

## **Recomendaciones ISO Relativas a La Seguridad**

Por último hemos considerado necesario enumerar las recomendaciones del organismo ISO para la seguridad, con la intención de guiar a los posibles lectores de este documento sobre la misma.

El Organismo Internacional de Normalización (ISO) recomienda establecer el cifrado en el nivel de presentación de la configuración según el modelo ISA. Estas son las razones que aduce el ISO para ello:

1. Es **importante colocar los servicios de cifrado en un nivel superior de red**, para poder simplificar el cifrado de extremo a extremo, y como el nivel más bajo donde se dan los servicios extremo a extremo es en el nivel de transporte, es por ello, que el cifrado se ha de realizar en un nivel superior a él.
2. Los **servicios de cifrado han de estar en un nivel superior al de transporte** si se quiere minimizar la cantidad de programas a los que ha de confiarse el texto legible. O sea, cuantos menos programas manejen el texto vulnerable mejor, lo que nos lleva a deducir que el cifrado se debe realizar en el nivel superior al de transporte.
3. El **cifrado ha de establecerse por debajo del nivel de aplicación**, ya que de lo contrario las transformaciones sintácticas, sobre los datos cifrados serían bastantes difíciles. Además, si el nivel de presentación se llevan a cabo transformaciones sintácticas, éstas han de tener lugar antes de que se realice el cifrado.
4. También se ha tenido en cuenta que **el cifrado de datos se puede hacer de forma selectiva**, el organismo de ISO cree que donde mejor puede hacerse esta selección es **en el nivel de presentación** o en uno superior, ya que por debajo de este nivel no existe constancia de la división en campos de la corriente de datos.
5. Aunque el cifrado se puede realizar en cualquier nivel, **la protección adicional que obtienen los datos de usuario puede no compensar la sobrecarga de trabajo que supone el cifrado**.

## Sistemas Y Protocolos Para Terminales

Como ya se ha intuido antes, en el nivel de presentación asigna una sintaxis a los datos, determinando la forma de representación de los datos, sin preocuparse de su significado o semántica. En realidad, sus funciones son bastantes limitadas, este nivel consta de muchas tablas sintácticas —correspondientes a códigos como el teletipo, ASCII, VideoText...—. El nivel de presentación es capaz de crear visualizaciones de terminales virtuales.

## Servicios Telemáticos

Los servicios telemáticos son los que conocemos como **videotex, o teletex**.

El videotex es un servicio de información de carácter bidireccional entre el dispositivo del usuario y una determinada fuente de información.

Mientras el **teletexto** se refiere a un servicio unidireccional. El teletexto usa un sistema convencional de difusión televisiva, que introduce los datos de unidireccionalmente y de forma cíclica en el terminal del usuario.

Cada página permanece en pantalla hasta que otra página del ciclo la sustituya automáticamente o por indicación del usuario. Pero el videotex, implica un sistema dotado de una determinada estructura de

comunicación de datos , se emplean componentes convencionales, com o módems y redes telefónicas, para conseguir la bidireccionalidad.

La idea de los servicios de Videotex y Teletexto es ofrecer un sistema capaz de distribuir dentro de amplias áreas informaciones de carácter gráfico o textual.

La información se disemina de forma electrónica para su visualización en terminales de bajo coste. El receptor de la información controla de forma selectiva la visualización, mediante procedimientos de fácil comprensión.

La telemática y el teletexto proporcionan servicios que para muchos de nosotros son ya parte de nuestras vidas. Así, incluyen información como: telecompra, difusión de publicidad de teletexto, transacciones bancarias a través de un teléfono, diarios electrónicos, juegos y entretenimientos, correo electrónico, servicios de apoyo a ordenadores personales.

## Teletex

Los primeros sistemas estaban limitados a comunicaciones punto a punto, luego poco a poco se vio que la potencia de las comunicaciones a través de teleimpresor o máquina de escribir a distancia podía verse aumentada considerablemente con el empleo de equipos de conmutación.

El CCITT se ocupó de los estándares TELEX y publicó diversos documentos en los que se describían las funciones de control y señalización. Originariamente, el CCITT reconoció dos tipos distintos de señales, conocidas como señales de Tipo A y de Tipo B. Las dos clases de señalización proporcionan las mismas señales funcionales la diferencia está sobre todo en el Tipo B, que ha venido utilizándose generalmente en los sistemas de acceso por marcado.

A medida que el TeleTex fue evolucionando hasta formar sistemas intercontinentales, el coste de los cables transoceánicos y de los circuitos de satélite necesarios obligó a mantener los circuitos al máximo de utilización, para compensar el incremento de precio del canal. Por ese motivo se idearon técnicas de multiplexado que permitían compatir un canal entre varios usuarios.

También fue pergeñándose el plan de numeración internacional de la red TELEX, que facilitón considerablemente el empleo de este servicio en comunicaciones internacionales.

Además de esto, el CCITT desarrolló un nuevo esquema mejorado de señalización, cononido como **tipo c**. Del mismo modo mejoraron las funciones de teclado del TELEX, como son las señales de acuse de recio, y se idearon señales de "*continuar la selección*"—para evitar el efecto de los grandes tiempos de propagación—.

# Bibliografía

## ***Sistemas Y Redes Teleinformáticas***

Jesús García Tomas

Editorial Sepa

## ***Comunicaciones***

José M. Huidobro

Editorial Paraninfo

## ***Telemática***

Guy Pujolle

Editorial Paraninfo

## ***Redes de Ordenadores***

Andrew S. Tanenbaum

Editorial Prentice Hall

## ***Redes de TeleComunicación y Ordenadores***

Michael Purser

Editorial Díaz de Santos, S.A.

## ***Redes de Ordenadores. Protocolos, Normas e Interfases***

Uyless Black

Editorial Rama

## ***Enciclopedia Lan Times De Redes (NetWorking)***

Tom Sheldon

McGraw-Hill 1995