# ARQUITECTURAS DE SEGURIDAD

## 1.1 Introducción

Los requisitos en seguridad de la información manejada dentro de una organización ha evolucionado sustancialmente en las últimas décadas. Si en un principio la seguridad de la información reaía en medios físico y administrativos, con la llegada y enorme evolución de los sistemas informáticos ha surgido la necesidad de desarrollar herramientas automáticas para proteger los ficheros y otras informaciones almacenadas en memoria. Estas necesidades de seguridad han conducido a la evolución de los sistemas operativos con el objeto de proteger los recursos del sistema y dar acceso a usuarios autorizados.

Por otro lado el desarrollo en paralelo de los sistemas distribuido y redes de datos ha dado lugar a la aparición de nuevos riesgos de seguridad relativos a la distribución de la información entre los sistemas informáticos y a la necesidad de reforzar o incluso adaptar al nuevo entorno los controles de seguridad de los sistemas individuales.

El objetivo de este trabajo será el análisis de los riesgos de seguridad en la distribución de la información en redes de comunicaciones. En este sentido, como ya es sabido, para que dos sistemas informáticos intercambien información es necesario junto con unos medios de transmisión físicos la existencia de una *arquitectura de comunicaciones* común estructurada en niveles. Cada uno de estos niveles realizará un subconjunto de las funcionalidades propias necesarias para el intercambio de datos. Es por ello que se hace necesario integrar las funcionalidades propias de la seguridad en las arquitecturas de comunicaciones existentes. Este proceso de integración implicará la implementación de mecanismos y servicios y funciones de seguridad de seguridad que se apoyarán en muchos casos en servicios, mecanismos y funciones ya implementados en la propia arquitectura de comunicaciones. El resultado final será lo que denominaremos ***Arquitectura de seguridad.***

Para estimar las necesidades de seguridad de una organización y evaluar y elegir los productos y políticas de seguridad en la comunicaciones, objetivo de nuestro estudio, el gestor responsable de la seguridad necesita evaluar los siguientes aspectos en la seguridad de la información:

1. ***Ataques a la seguridad***: Qué acciones pueden comprometer la seguridad de la información que pertenece a una organización.

2. ***Mecanismos de seguridad***: Qué mecanismos hay que implementar para detectar, prevenir o recuperarse de un ataque a la seguridad de la información.

3. ***Servicios de seguridad***: Qué servicios ofrecer al usuario respecto a la transferencia de información en una red de datos. Los servicios de seguridad tratan de contrarestar los ataques y para ello hacen uso de los mecanismos de seguridad para proporcionar ese servicio.

Visto desde otro punto de vista se pueden definir una serie de pasos a la hora de la implantación de seguridad en redes de datos:

1. En primer lugar hay que definir una serie de objetivos o requisitos de seguridad que se desea que cumpla la información que se distribuye en redes de datos en función de los posibles o potenciales ataques a la seguridad. Es decir hay que definir una ***política de seguridad***. Estos objetivos o requisitos de seguridad se van a articular en forma de servicios de seguridad que se van a ofrecer al usuario.

2. Una vez especificados una serie de requisitos de seguridad para la información habría que implementar los mecanismos necesarios para garantizar esos requisitos. La implementación de estos mecanismos puede ser más o menos compleja dependiendo de la tecnología de la red de datos a considerar. Así tengase en cuenta los mecanismos de seguridad se van a implementar utilizando el protocolo de comunicaciones propio de la red de datos lo cual implica que hay que tener ciertas garantias respecto a este protocolo (por ejemplo respecto a temporizaciones, retransmisiones etc). A la hora de implementar un mecanismo de seguridad es muy importante considerar también las posibles contrapartidas o coste que puede tener dicho mecanismo en las comunicaciones (por ejemplo en tiempo de proceso o retardo en la red).

3. Una vez decidido que mecanismos de seguridad implementar habría que determinar donde situarlos. Este aspecto tiene dos implicaciones: por un lado habría que determinar en que lugar físico de la red de datos localizar estos mecanismos y por otro lado en que lugar de la arquitectura de comunicaciones (en que nivel de esta estructura) situar estos mecanismos.

## 1.2 Arquitectura de seguridad en el modelo ISA

El objetivo del modelo de referencia ISA (Interconexión de Sistemas Abiertos) es permitir la interconexión de sistemas informaticos de modo que se pueda alcanzar una comunicación util entre procesos de aplicación. Para ello se deben establecer mecanismos de seguridad para protejer la información intercambiada entre procesos. Tales mecanismos deberían hacer que el coste de obtener o modificar los datos sea mayor que el valor potencial de obtener o modificar los datos.

Es necesario por tanto un estándar de arquitectura de seguridad en el modelo ISA que permita comenzar la tarea de implementar los servicios de seguridad en productos comerciales de modo que no sólo un sistema ISA pueda comunicarse con otro, sino que además pueda hacerlo con la adecuada seguridad.

La *arquietectura de seguridad* propuesta para el modelo ISA definida en el estandar ***ISO 7498 (Part 2)*** proporciona una descripción de los servicios de seguridad y mecanismos asociados, los cuales pueden ser proporcionados por los niveles del modelo de referencia ISA y define los niveles dentro del modelo de referencia donde se pueden proporcionar los servicios y mecanismos.

La arquietectura de seguridad propuesta para el modelo ISA contempla cinco elementos: definición de servicios de seguridad, definición de mecanismos de seguridad, definición de una serie de principios de estructuración de servicios de seguridad en los niveles de la arquitectura ISA, implantación de servicios de seguridad en los niveles ISA y finalmente definición de los mecanismos asociados a cada servicio de seguridad

El estandar *ISO 7498* hace uso de las siguientes definiciones:

- *Servicio de Seguridad (N):* Es la capacidad que el nivel N y de los niveles inferiores ofrecen a las entidades de nivel N+1 en el campo de la seguridad en el interfaz entre el nivel N y el nivel N+1 por medio de las primitivas de servicio.

- *Función de seguridad (N):* Es una función relativa a la seguridad de acuerdo al servicio proporcionado al nivel N, controlado por el control lógico de la entidad (N).

- *Mecanismo de seguridad (N):* Mecanismo de nivel N que realiza una parte de una función de seguridad de nivel N.

Los **servicios de seguridad** definidos son autenticación de entidad par, control de acceso, confidencialidad de datos, integridad de datos, no repudio (con prueba de origen, con prueba de entrega). Para proporcionar estos servicios de seguridad es

necesario incorporar en niveles apropiados del modelo de referencia ISA **mecanismos de seguridad (**cifrado, firma digital, mecanismos de control de acceso, integridad de datos, intercambio de autenticación, etc).

En este modelo una entidad de nivel N se compone de tres partes:

- ***Control Lógico:*** Realiza la lógica del protocolo usando funciones y variables.

- ***Mecanismos:*** Controlados por el elemento de control opera con la variables realizando funciones.

- ***Variables:*** La mayoria de las cuales son locales a cada entidad.

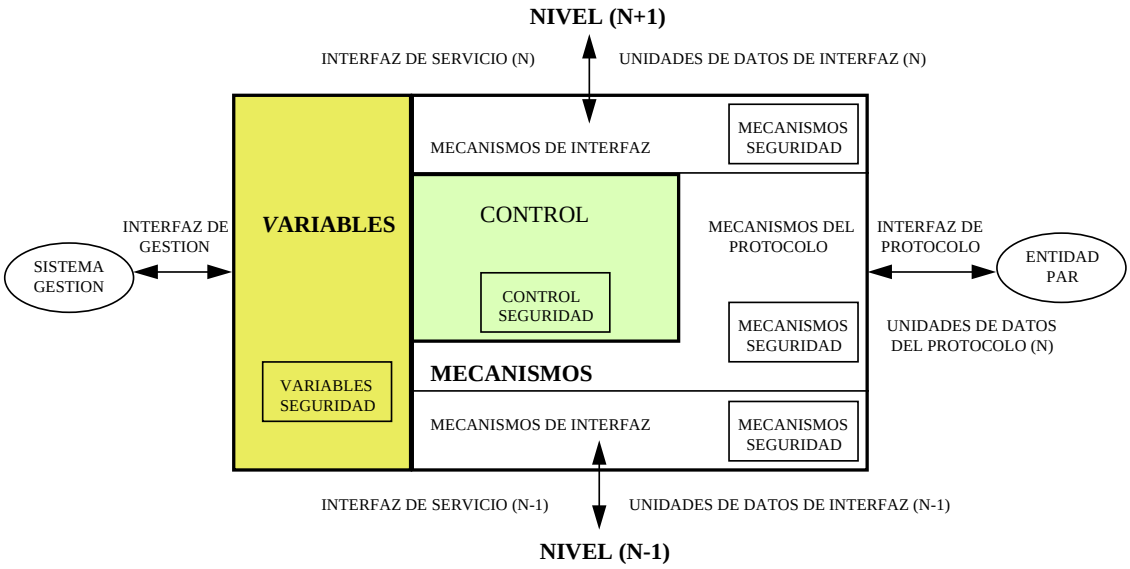
El *control lógico* puede ser modelado como una máquina de estado finita extendida. Los *mecanismos* se pueden a su vez dividir en tres grupos cada uno realizando su misión en un interfaz del nivel N:

- ***Mecanismos de Interfaz de Nivel Superior:*** Realizados en el interfaz entre el nivel N+1 y el nivel N.

- ***Mecanismos de Interfaz de Nivel Inferior:*** Realizados en el interfaz entre el nivel N y el nivel N-1.

- ***Mecanismos de Protocolo***: Es el mecanismo que consiste en el dialogo entre entidades pares.

Una descripción gráfica de la estructura de una entidad par de un nivel (N) así como su interrelación con el entorno se muestra en la siguiente figura:



Formalmente una entidad de nivel ***N*** en un sistema ***A*** , $A_N$, puede ser modelada como una tripleta: $(C_{A_N}, V_{A_N}, M_A)$, donde $C_{A_N}$ es el Control Lógico, $M_{A_N}$ es el conjunto de mecanismos y $V_{A_N}$ es el conjunto de variables.

El conjunto de variables de la entidad $A_N$ es la unión del conjunto de *variables de protocolo* de la entidad $A_N$ y el conjunto de *variables de seguridad* de la entidad $A_N$.

$$V_{A_N} = V_{A_N,P} \bigcup V_{A_N,S}$$

Similarmente el conjunto de mecanismos de la entidad $A_N$ es la unión del conjunto de *mecanismos de protocolo*, el conjunto de *mecanismos de interfaz* , el conjunto de *mecanismos de seguridad* y el conjunto de otros mecanismos:

$$M_{A_N} = M_{A_N,P} \bigcup M_{A_N,I}, M_{A_N,S} \bigcup M_{A_N,O}$$

Las variables de seguridad incluyen claves e información que controla la selección y uso de varios mecanismos de seguridad. Los valores de las variables de seguridad pueden ser establecidas por el gestor del sistema, o peuden ser resultado de la negociación con n nivel superior del nivel ISA, o como parte de control de la entidad

Un ***contexto de seguridad de nivel N*** entre instancias de dos Sistemas A y B, $A_{N,i}$ y $B_{N,j}$ se puede definir formalmente como:

$$SC_{A_{N,i},B_{N,i}} = (V_{A_{N,i},S}, V_{B_{N,j},S}) \bigcup (M_{A_{N,i},S}, M_{B_{N,j},S})$$

El uso de un contexto de seguridad en una comunicacion real implica por ejemplo que necesitamos conocer los mecanismos criptográficos empleados, claves usadas, funciones de seguridad requeridas, etc. Un contexto de seguridad puede ser establecido por medio de un acuerdo previo, gestion y negociación. Es posible negociar varios contextos de seguridad y manejarlos del mismo modo que son manejados los contextos de presentación en el nivel de presentación.

Las funciones de seguridad pueden ser autónomas, (es decir, estar siempre activas o o con posibilidad de ser activadas por los sistemas de gestión guiados por una *política de seguridad*) o bién pueden ser activadas en un momento dado significando en este caso que su uso es negociado y controlado por el usurio final mediante la invocación de primitivas.

El análisis de las funciones y mecanismos de seguridad junto con el concepto de *contexto de seguridad* nos da idea de la relación entre funciones y mecanismos en sistemas abiertos así como nos permite dividir el problema de la seguridad de sistemas

abiertos en unidades más manejables. Desarrollando una técnica formal para describir y analizar los contextos de seguridad y las transferencias entre ellos se pueden deducir y probar la seguridad de los sistemas abiertos.

### 1.2.1 Objetivos de seguridad

Se pueden definir una serie de objetivos o requisitos que la arquitectura de seguridad definida para el modelo ISA debe garantizar respecto de los datos que manejan las redes de comunicaciones. Estos objetivos son los siguientes:

1. Protección de los datos frente a modificaciones no autorizadas.

2. Protección de los datos frente a pérdidas/repeticiones.

3. Protección de los datos frente a revelaciones no autorizadas.

4. Garantía de la correcta identidad del emisor de los datos.

5. Garantía de la correcta identidad del receptor de los datos.

Alcanzar estos objetivos en la arquitectura ISA asegurará que los datos que son transmitidos de un sistema ISA a otro no han sido modificados revelados, retransmitidos o perdidos en la red sin que el emisor o el pretendido receptor haya sido notificado y sin que las partes que intervienen en el protocolo hayan sido correctamente identificadas.

Otros objetivos de seguridad identificados como deseables incluyen: no revelación ni de la cantidad ni de la estructura de la información; probar a una tercera parte que la comunicación ocurrió y que la información fue recibida; obtención de la autorización explicita para acceder a un sistema etc.

### 1.2.2 Servicios de seguridad

En el contexto del modelo ISA un servicio de seguridad se va a suministrar como parte de un servicio de nivel (N). Cada servicio de seguridad en el interfaz entre los niveles (N) y (N+1) está soportado por uno o más mecanismos incorporados a las entidades de nivel (N) y al protocolo de nivel (N).

Por lo tanto cuando se habla de servicios de seguridad en el modelo ISA habría que determinar por un lado el conjunto de servicios que contemplen los objetivos de

seguridad definidos, por otro lado que mecanismos son adecuados o cuáles se deberían implementar para cada servicio y finalmente dónde deberían estar situados dichos servicios en la arquitectura ISA y que repercusiones tendría este aspecto. Empezaremos por enumerar los servicios de seguridad definidos en el estandar *ISO 7498:*

El estandar ISO 7498-2 define un *servicio de seguridad* como el servicio proporcionado por un nivel de un sistema abierto que garantiza la seguridad de los sistemas abiertos o a las transferencias de datos en dichos sistemas. Estos servicios están divididos en cinco categorías y 14 servicios específicos. Las categorías son :

1. Autenticación.

2. Control de acceso.

3. Confidencialidad.

4. Integridad.

5. No repudio.

### *1.2.2.1 Autenticación*

El servicio de *autenticación* asegura que las entidades que se comunican son quién reclaman ser. El estandar ISO 7498-2 define dos servicios de autenticación específicos:

1. ***Autenticación del origen de los datos***: Este servicio se aplica a comunicaciones no orientadas a conexión donde las unidades de datos son independientes y por lo tanto en este caso lo más que se puede garantizar es que el origen de cada unidad de datos correxponde con la indicada en su cabecera. Este servicio puede ofrecerse en aplicaciones como el correo electrónico, donde no hay una comunicación previa entre entidades finales. (Este servicio esta asociado con el servicio de integridad dedatos no orientado a conexión; no parece muy útil asegurar la identidad del origen de los datos si no se puede garantizar su integridad).

2. ***Autenticación de entidades pares***: Este servicio se aplica a comunicaciones orientadas a conexión. Al establecerse la conexión de nivel (N) este servicio asegura la identidad de las dos entidades que se comunican, es decir, se asegura que cada una es quién dice ser. Posteriormente en la fase de transferencia debe garantizar que un intruso no pueda suplantar a cualquiera de las dos entidades legítimas que se comunican a efectos de transmisiones o recepciones no autorizadas.

### *1.2.2.2 Control de acceso*

El servicio de control de acceso evita el uso no autorizado de los recursos. Este servicio controla quien puede tener acceso a un recurso, bajo que condiciones puede tener lugar el acceso y que se le permite hecer a aquel que accede a un recurso.

### *1.2.2.3 Confidencialidad*

El servicio de *confidencialidad* asegura que la información o no va a ser revelada ni va a estar disponible a individuos no autorizados, entidades o procesos. Este aspecto tiene especial importancia cuando las redes de comunicaciones que transportan la información presentan puntos vulnerables respecto de la seguridad. Se han descrito cuatro versiones de este servicio:

1. ***Confidencialidad orientada a conexión***: Consiste en la protección de todos los datos de usuario en una comunicación orientada a conexión de nivel *N*.

2. ***Confidencialidad no orientada a conexión:*** Consiste en la protección de todos los datos de usuario contenidos en una sóla unidad de datos del servicio (UDS) en una comunicación no orientada a conexión de nivel *N*.

3. ***Confidencialidad selectiva***: Consiste en la protección de campos específicos de todas las unidades de datos de usuario de una comunicación orientada a conexión de nivel *N* o de una sóla unidad de datos del servicio (UDS) en una comunicación no orientada a conexión de nivel *N*.

4. ***Confidencialidad aplicada al analisis del tráfico:*** Este servicio sirve para la protección de los datos frente a un análisis del tráfico originado por una comunicación entre entidades pares. Así un intruso podría analizar las direcciones origen y destino de las unidades de datos intercambiadas, la cantidad de datos transmitidos y la frecuencia con que tiene lugar la comunicación entre entidades pares.

### *1.2.2.4 Integridad*

El servicio de integridad asegura que datos son recibidos exactamente a como han sido enviados por una entidad autorizada, es decir sin duplicaciones, retransmisiones, modificaciones o inserciones.

Cuando se detecta una violación en la integridad de los datos el servicio de integridad puede o bien avisar de que se ha producido este hecho o utilizar mecanismos

para la recuperación de la perdida de integridad de los datos. Así se han definido las siguientes modalidades del servicio.

1. ***Integridad orientada a conexión con mecanismos de recuperación***: Proporciona la integridad de todos las unidades de datos de usuario de una comunicación orientada a conexión de nivel *N* y detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos dentro de una secuencia entera de unidad de datos del servicio (UDS) haciendo uso de mecanismos de recuperación de la integridad si fuera necesario. El uso de este servicio junto con el servicio de autenticación de entidad par proporciona un alto grado de protección frente a la mayoría de ataques activos.

2. ***Integridad orientada a conexión sin mecanismos de recuperación:*** Este servicio es semejante al anterior con la diferencia de que en este caso sólo se detecta las violaciones en la integridad de los datos pero no se articulan mecanismos de recuperación de la integridad.

3. ***Integridad orientada a conexión sobre campos selectivos:*** Este servicio asegura la integridad de campos específicos dentro de las unidades de datos de usuario de nivel *N* en una comunicación orientada a una conexión y toma una determinación de si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.

4. ***Integridad no orientada a conexión:*** Este servicio asegura la integridad de una sóla unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión teniendo alguna forma de detección de la modificación de una UDS. Adicionalmente también pueden existir algunos mecanismos que garanticen la detección de retransmisiones.

5. ***Integridad no orientada a conexión sobre campos selectivos:*** Este servicio asegura la integridad de campos específicos dentro de una sóla unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión. Este servicio toma alguna determinación si los campos seleccionados han sido modificados.

#### *1.2.2.5 No repudio*

El servicio de no repudio evita que las entidades pares que se comunican puedan denegar el haber participado en parte o en toda la comunicación. Se han definido dos modalidades del servicio:

1. ***No repudio con prueba de origen***: Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue enviado por la entidad especificada.

2. ***No repudio con prueba de entrega***: Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue recibido por la entidad especificada.

## 1.2.3 Mecanismos de seguridad

Los servicios de seguridad son implementados utilizando mecanismos de seguridad. Un servicio de seguridad puede utilizar uno o varios mecanismos de seguridad. En la arquitectura de seguridad definida para el modelo ISA se han definido los siguientes mecanismos de seguridad:

### *1.2.3.1 Encriptación*

La *encriptación* es un mecanismo que utiliza la *criptografía* para transformar las unidades de datos intercambiadas por las entidades pares. El mecanismo de *encriptación* contempla dos funciones a realizar sobre las unidades de datos: *la función de encriptado y la función de desencriptado*. El mecanismo de *encriptación* protege a los datos de usuario frente a la revelación de los contenidos (estos serán denominados ataques activos).

Antes de realizar la función de encriptado las unidades de datos a intercambiar se denominan ***texto en claro***. Para la transmisión de las unidades de datos una entidad par aplicará la *función de encriptado* sobre el texto en claro transformándolo a datos ininteligibles, tambien llamado ***texto cifrado***. La entidad receptora de las unidades de datos cifradas deberá realizar la función inversa denominada *desencriptado* para poder recuperar *el texto en claro.*

El mecanismo de encriptación se utiliza típicamente para proporcionar el *servicio de confidencialidad*, aunque también puede soportar otros servicios de seguridad como los *servicios de integridad y de autenticación*. Se han definido dos modalidades del mecanismo de encriptado: la encriptación convencional y la encriptación de clave pública.

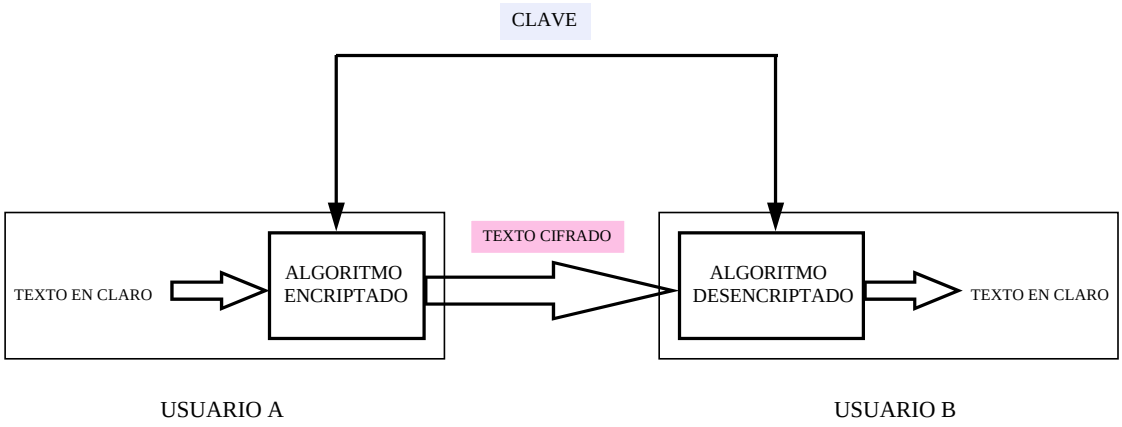
#### *1.2.3.1.1 Encriptación conveccional*

En la encriptación convencional las unidades de datos a intercambiar por las entidades pares (*texto en claro*) se transforman en un texto ininteligible (*texto cifrado*) al aplicar una función de encriptado. En la encriptación convencional la función de encriptado tiene dos elementos: el ***algoritmo de encriptado*** y una ***clave*** que controla dicho algoritmo. El algoritmo de encriptado se aplicará sobre las unidadesde datos y obtendrá diferentes resultados al aplicarse sobre las mismas unidades de datos dependiendo de la clave utilizada en cada momento. Cambiando la *clave* se cambia el texto cifrado obtenido.

En la figura se ilustra el proceso de la encriptación convencional. El usuario A genera a partir de un *texto en claro* un *texto cifrado* después de aplicar la función de encriptado (con un algoritmo de encriptado y una clave). El usuario B una vez recibido el texto cifrado puede transformarlo a texto en claro usando la función de desencriptado lo que implica el uso de un algoritmo de desencriptado y la misma clave que fue usada en la encriptación.

La seguridad de la encriptación convencional depende de varios factores. Primero el algoritmo de encriptación debe ser capaz de hacer inviable desencriptar los datos a partir sólo del texto encriptado. La seguridad de la encriptación convencional depende de la seguridad en el conocimiento de la clave no de la seguridad en el conocimiento del algoritmo. Es decir se asume que es inviable desencriptar un mensaje con sólo el mensaje y el algoritmo criptográfico. En otras palabras no necesitamos conservar secreto el algoritmo; sólo necesitamos conservar secreta la clave.

La encriptación convencional es quizas el mecanismo de seguridad más difundido. El hecho que el algoritmo de encriptado/desencriptado no necesite ser secreto significa que los fabricantes pueden y han desarrollado implementaciones harware para algoritmos de encriptación de datos. Estas implementaciones harware están ampliamente disponibles e incorporados a un número de productos. Con el uso de la encriptación convencional, el principal problema de la seguriad es mantener secreta la clave.




En resumen se puede decir que la *encriptación convencional* para su funcionamiento requiere:

1. Un algoritmo para realizar las funciones de encriptado/desencriptado y una clave.

2. El emisor y receptor deben compartir el algoritmo y la clave.

y por requerimientos de seguridad :

1. Que la *clave* se conserve secreta.

2. Debe ser imposible o impracticable desencriptar un mensaje si no hay otra información disponible.

3. El conocimiento del mensaje cifrado y el algoritmo debe ser insuficiente para conocer la clave.

Los algoritmos de encriptado utilizados más comúnmente son los encriptadores de bloque. Un encriptador de bloque procesa una entrada de texto en claro en bloques de tamaño fijo, y produce un bloque de texto cifrado de igual tamaño para cada bloque de texto en claro. Los dos algoritmos conveccionales más importantes que además son encriptadores de bloque son el DES y el DES tripe

El esquema de encriptado más utilizado comúnmente es el estándar de encriptado de datos (DES, “Data Encryption Standar”), adoptado en 1977 por el Buró Nacional de Estándares, ahora el Instituto Nacional de Estándares y tecnología (NIST, “National Institute of Standars and Technology”) como el estándar Federal de Procesamiento de la Información número 46 (FIPS PUB 46). El DES Triple fue propuesto por primera vez por Tuchman [TUCH79] y constituyo la primera normalización para aplicaciones comerciales. El DES Triple es una variante del DES convencional que utiliza dos claves y tres ejecuciones del algoritmo DES.

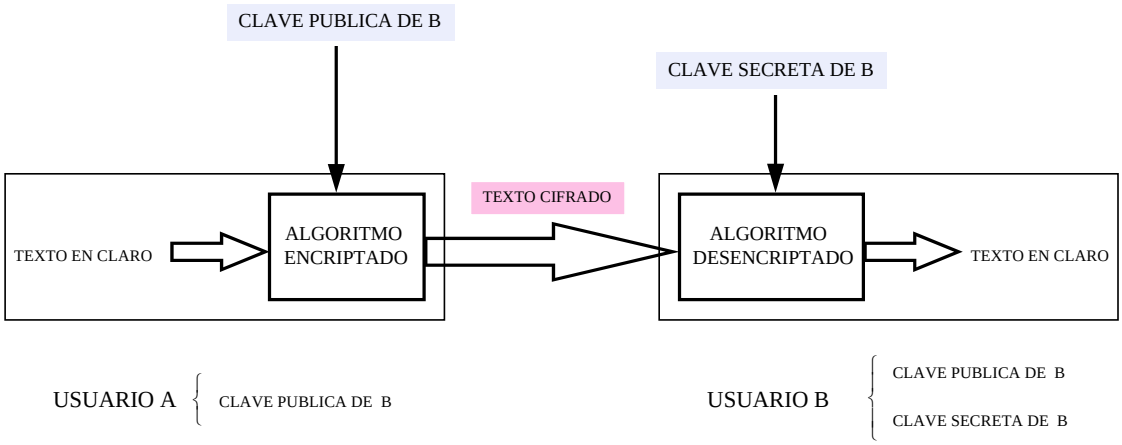
#### *1.2.3.1.2 Encriptación de clave pública*

En la encriptación convencional la clave usada para las funciones de encriptado y desencriptado es la misma. Esta no es una condición estrictamente necesaria en los modelos de encriptación. Así es posible desarrollar un algoritmo criptográfico que utilice una clave para las funciones de encriptado y otra clave para las funciones de desencriptado. Además estos algoritmos tienen dos importantes características:

- Es inviable determinar la clave de desencriptado con sólo el conocimiento del algoritmo de encriptado y la clave de encriptado.

- En algunos algoritmos (como RSA) cualquier clave puede usarse para el encriptado y la otra para el desencriptado.

Este modelo de encriptación conocido como *encriptación de clave pública* se ilustra en la figura.




En la encriptación de clave pública son esenciales los siguientes pasos:

1. Cada entidad par del sistema final en la red genera un par de claves para ser utilizadas en las funciones de encriptado y desencriptado de datos.

2. Cada entidad par publica su clave de encriptado situándola en un registro público o fichero. Esta es la *clave pública*. La clave asociada es la *clave privada.*

3. Si una entidad A desea enviar un mensaje a otra entidad B, encripta el mensaje usando la clave pública de la entidad B.

*4.* Cuando la entidad B recibe el mensaje, lo desencripta usando la clave privada de la entidad B. Ningún otra entidad puede desencriptar el mensaje, ya que sólo la entidad B conoce su *clave privada.*

Con este modelo todos los participantes tienen acceso a las claves públicas. Las claves privadas son generadas localmente a cada participante y por lo tanto no necesitan ser distribuidas. En la medida que un sistema controla su clave privada la comunicación es segura. En cualquier momento un sistema puede cambiar su clave privada y publicar la clave pública asociada para reemplazar su vieja clave pública.

Puede ser necesario sin embargo un refinamiento. Ya que cualquiera puede transmitir un mensaje a la entidad *A* usando su *clave pública* se necesita un medio para evitar intrusos.Así se puede considerar el siguiente escenario: La entidad A prepara una unidad de datos, la encripta con su propia clave privada y luego encripta el resultado con la clave pública de la entidad B. Del otro lado la entidad B usa primero su clave privada y luego la clave pública de la entidad A en una doble función de desencriptado. Ya que la unidad de datos viene encriptada con la clave secreta de la entidad A sólo podría venir de la propia entidad A. Ya que fue encriptado con la clave pública de la entidad B sólo puede ser leeido por dicha entidad (B). Con esta técnica cualquiera dos estaciones puede en cualquier momento establecer una comunicación segura sin tener que realizar una distribución de claves y asegurando además con este mecanismo un servicio de confidencialidad y autenticación. Volveremos a este esquema al hablar de los *mecanismos de firma digital*.

La principal desventaja de la encriptación de clave pública comparada con la encriptación convencional es que los algoritmos son mucho más complejos.

En resumen se puede decir que la encriptación de clave pública para su funcionamiento requiere:

1. Un algoritmo para realizar las funciones de encriptado/desencriptado y un par de claves, una para el encriptado y otra para el desencriptado.

2. El emisor y receptor deben tener cada uno dicho algoritmo y una de las claves del par

y por requerimientos de seguridad :

1. Que una de las claves se conserve secreta.

2. Debe ser imposible o inviable desencriptar un mensaje si no hay otra información disponible.

3. El conocimiento del mensaje cifrado y el algoritmo de encriptado/desencriptado debe ser insuficiente para conocer la otra clave del par.

La generación, distribución y almacenamiento de las claves criptográficas usadas en la encriptación convencional o de clave pública implicará en la mayoría de los casos un intercambio de información de control entre entidades pares. A estos procedimientos los denominaremos ***protocolos de distribución de claves*** o protocolos de seguridad.

Uno de los primeros esquemas de clave pública fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT y publicado por primera vez en 1978 [RIVE78]. El esquema Rivest-Shamir-Adleman (RSA) ha sido considerado desde entonces como la única técnica aceptada mundialmente e implementada de algoritmo de encriptado de clave pública. RSA es un cifrador de bloque en el que el texto en claro y el texto cifrado son enteros entre *0* y *n-1* para algún *n*.

#### *1.2.3.1.3 Localización de los mecanismos de encriptación*

Cuando se habla de un entorno de red formado por la interconexión de redes de diferentes tecnologías necesitamos decidir que unidades de datos hay que encriptar (a que nivel de la arquitectura ISA aplicar los mecanismos de seguridad) y donde deberíamos fisicamente situar los mecanismos de encriptación. Si consideramos por ejemplo una red de conmutación de paquetes podemos determinar dos alternativas a la hora de situar los mecanismos de encriptación.

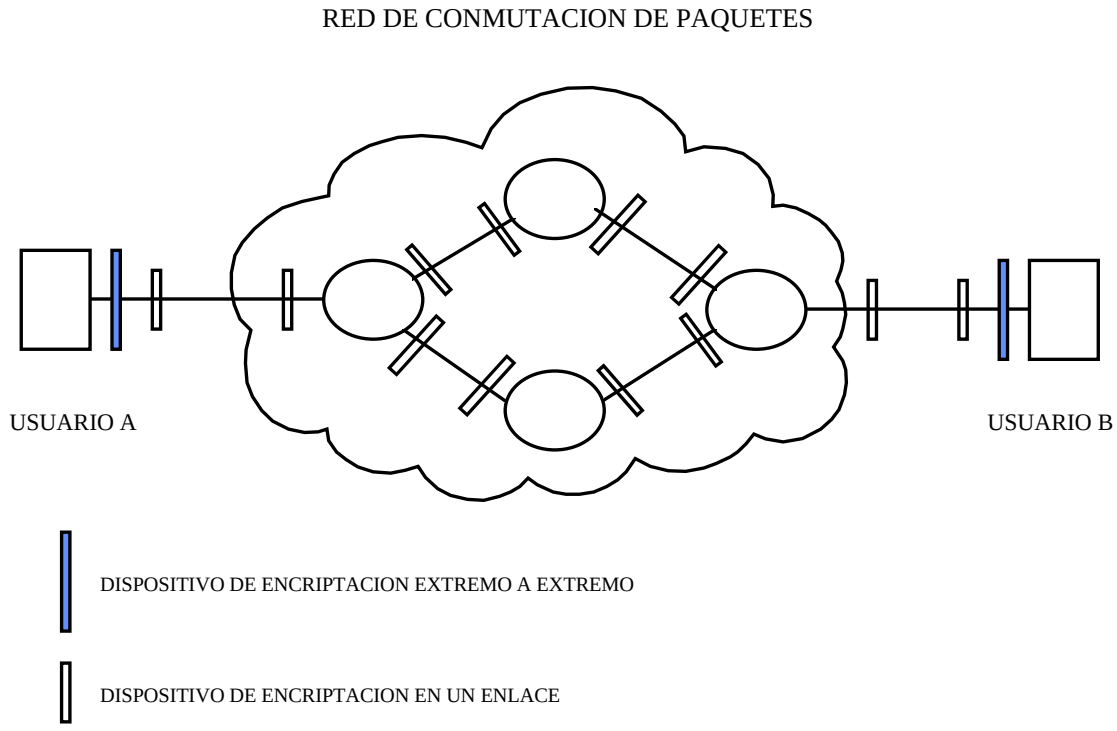
Si se sitúan los mecanismos de encriptación en los extremos de los enlaces entre cada par de nodos se va a conseguir que todo el tráfico entre todos los enlaces sea seguro. Ahora bién esta idea implica lógicamente una gran cantidad de dispositivos de encriptado a situar en la red. Una desventaja de esta alternativa es que los datos deberían ser desencriptados cada vez que llegan a un nodo de la red de conmutación de paquetes; esto es debido a que cada nodo necesita leer el número de circuito virtual de la cabecera de cada paquete para encaminar dicho paquete. Por lo tanto el mensaje es vulnerable en cada nodo. Si es una red pública de conmutación de paquetes, el usuario no no va a tener control de la seguridad de los nodos.

Otra posibilidad sería situar los mecanismos de encriptación en los sistemas informáticos de los usuarios. En este caso las funciones de encriptado/desencriptado se llevan a cabo en los sistemas finales. La estación origen encripta los datos y a continuación estos datos son transmitidos inalterados a través de la red hasta llegar a la estación destino. La estación destino que comparte una clave con la estación origen es por tanto capaz de desencriptar los datos.

Utilizando los mecanismos de encriptación en los sistemas finales hay que tener en cuenta una serie de aspectos. Si tenemos una red de conmutación de paquetes sólo podremos encriptar el campo de datos de un paquete. No podríamos encriptar la

cabecera que incluye el número de canal lógico del paquete puesto que los nodos de la red de conmutación de paquetes no podrían leer la cabecera ya que se supone que sólo los usuarios finales pueden desencriptar los datos.

Por lo tanto utilizando los mecanismos de encriptación en los sistemas finales los datos de usuario se conservan seguros aunque las cabeceras de los paquetes de datos siempre se transmiten en claro siendo por tanto vulnerable el patrón de tráfico. Una manera de conseguir una mayor seguridad sería combinar ambos tipos de encriptado, es decir, se situarían mecanismos de encriptación entre cada par de nodos de manera que en los enlaces irían encriptados tanto los datos como las cabeceras de los paquetes protegiendo así el control de tráfico y además se seguirían utilizando los mecanismos de encriptación en los sistemas finales con el fin de proteger los datos de usuario

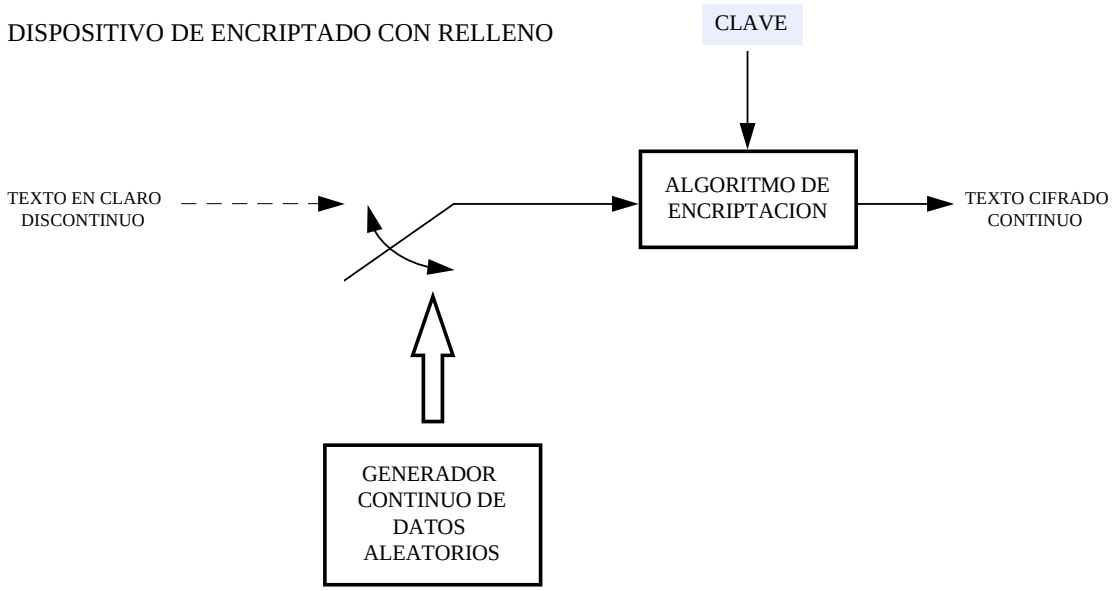



### *1.2.3.2 Tráfico de relleno*

Los usuarios de las redes de datos y especialmente de las redes públicas deben siempre considerar la posibilidad de que un intruso pueda realizar un análisis del tráfico en la red. Este análisis puede contemplar el estudio de las cabeceras de las unidades de datos (números de secuencia, direcciones origen y destino, números de circuito virtual etc) o la cantidad de tráfico que entra o sale de un determinado sistema informático.

El tráfico de ***relleno*** es un mecanismo de seguridad que consiste en producir una salida de *texto cifrado* continuamente incluso en ausencia de *texto en claro*. Cuando hay texto en claro disponible este se encripta y transmite. Cuando no hay *texto en claro*

presente se generan datos aleatorios que son a continuación encriptados y transmitidos. Esto hace imposible para un intruso el distinguir entre el flujo de datos válidos y el ruido y por lo tanto es imposible deducir la cantidad de tráfico. El receptor debería discriminar entre datos válidos e inválidos (simplemente aquellos patrones de bits que se ajunten al formato de un paquete serán válidos y el resto inválidos; en cualquier caso se perderá un tiempo en analizar estas estructuras).




### *1.2.3.3 Mecanismos de intercambio de Autenticación*

La *autenticación* de unidades de datos es un mecanismo que permite que las partes que se comunican verifiquen que los mensajes recibidos son *auténticos*. Una unidad de datos, un mensaje, fichero, documento u otra colección de datos se dice que son *auténticos* cuando son genuinos (no han sido alterados) y vienen de la fuente que alegan venir. El *mecanismo de autenticación* protege a las unidades de datos intercambiadas de los denominados *ataques activos* por parte de los intrusos, es decir de las posibles alteraciones o modificaciones.

La *autenticación* puede contemplar dos aspectos: por un lado que los contenidos de los mensajes no han sido alterados y por otro que el origen de las unidades de datos es auténtica y por lo tanto no ha sido alterada o falsificada. También se puede desear verificar que las unidades de datos no han sido retardadas artificialmente (para ello se pueen utilizar los denominados de sellos de tiempo o identificadores de uso único) y la secuencia de la unidad de datos considerada relativa a las otras unidades de datos intercambiadas. En definitiva los mecanismos de autenticación van a implicar el intercambio de una serie de una serie de información de control entre las entidades pares implicadas constituyendo un auténtico protocolo, el denominado ***protocolo de autenticación.***

Se pueden considerar dos funciones implicadas en los mecanismos de autenticación: el denominado *código de autenticación de mensajes* y la *encriptación*.

#### *1.2.3.3.1 Código de autenticación de mensajes*

Esta técnica de *autenticación* supone el uso de una clave secreta para generar un pequeño bloque de datos conocido como código de autenticación de mensajes y que se incorpora al propio mensaje. Esta técnica supone que dos entidades que se comunican (sean Ay B)comparten una clave secreta común $K_{AB}$. Cuando A tiene un mensaje que enviar a B, calcula el código de autenticación del mensaje como función del mensaje y la clave : $CAM = F(K_{AB}, M)$. Luego se transmite el mensaje y el código al destino. El receptor realiza los mismos cálculos en el mensaje recibido, utilizando la misma clave secreta, para generar el nuevo código de autenticación. El coódigo recibido se compara con el código calculado. Si asumimos que sólo el receptor y el emisor conocen la identidad de la clave secreta y el código recibido coincide con el código calculado entonces se cumple que:

1. La entidad destinataria se asegura que la unidad de datos intercambiada no ha sido alterada. Si un intruso alterara el mensaje, pero no altera el código entonces el cálculo del código de la receptor diferirá del código recibido. Ya que se asume que el intruso no conoce la clave secreta, el intruso no puede alterar el código que corresponde al mensaje alterado

2. La entidad destinataria se asegura que la unidad de datos intercambiada proviene de la entidad emisora alegada. Puesto que nadie conoce la clave secreta, nadie puede confeccionar un mensaje con el código apropiado.

3. Si se trata de comunicaciones orientadas a conexión la unidad de datos intercambiada puede incluir un número de secuencia (X.25, HDLC e ISO nivel de transporte) que la entidad destinataria puede utilizar para asegurar que esa unidad de datos está en secuencia. Puesto que el intruso no conoce la clave secreta no podría introducir el número de secuencia adecuado.

Se pueden usar un gran número de algoritmos para generar el código de autenticación. Téngase en cuenta que el mecanismo de código de autenticación es similar a la encriptación. Sin embargo una diferencia clara es que el algoritmo de autenticación no necesita ser reversible como debe ser para la desemcriptación. Ello es debido a que las propiedades matemáticas de la función de autenticación es menos vulnerable a ser roto que la encriptación.

#### *1.2.3.3.2 Encriptacion como mecanismo de autenticación*

La *encriptación* se puede convertir en un mecanismo de autenticación. Así en un modelo de *encriptación convencional* donde sólo las entidades emisora y receptora comparten la clave secreta únicamente la *auténtica* entidad emisora podría encriptar con éxito una unidad de datos dirigida a otra entidad. Si además las unidades de datos intercambiadas incluyen un código de detección de errores y un número de secuencia la entidad receptora estará segura de que no se han producido alteraciones y que el número de secuencia es el adecuado

Un modelo de *encriptación de clave pública* sin embargo no proporciona siempre un mecanismo de autenticación. Encriptando sólo con la clave pública de la entidad receptora sólo se garantiza la confidencialidad de los datos pero no la autenticidad puesto que cualquiera puede conocer la clave pública de la entidad receptora.

Puesto que la encriptación convencional puede proporcionar autenticación y ya que ésta es ampliamente implementada en productos comerciales habría que determinar en que casos tendría sentido emplear un código de autenticación:

El código de autenticación puede tener sentido en determinadas aplicaciones en las que hay que difundir una unidad de datos a muchos destinos y no es reconmendable por motivos de coste realizar multiples funciones de encriptado. También puede ser suficiente para determinadas aplicaciones en la que no es tan importante la confidencialidad de los datos como que esos datos provengan de una entidad específica.

### *1.2.3.4 Firma digital*

Los mecanismos de autenticación protegen los datos de usuario intercambiados por las entidades pares de los ataques de un intruso externo pero pueden no protegerlos de las propias entidades pares. Así por ejemplo una entidad receptora podría inventarse una unidad de datos añadir un código de autenticación y decir que viene de la entidad emisora con la que comparte la clave secreta

En estas situaciones es necesario algo más que los mecanismos de autenticación, es por ello que surgen los mecanismos de firma digital. Estos tienen las siguientes propiedades:

1. Debe ser posible verificar al autor y los datos y el tiempo de la firma

2. Debe ser posible autentificar los contenidos de los mensajes en el tiempo de la firma

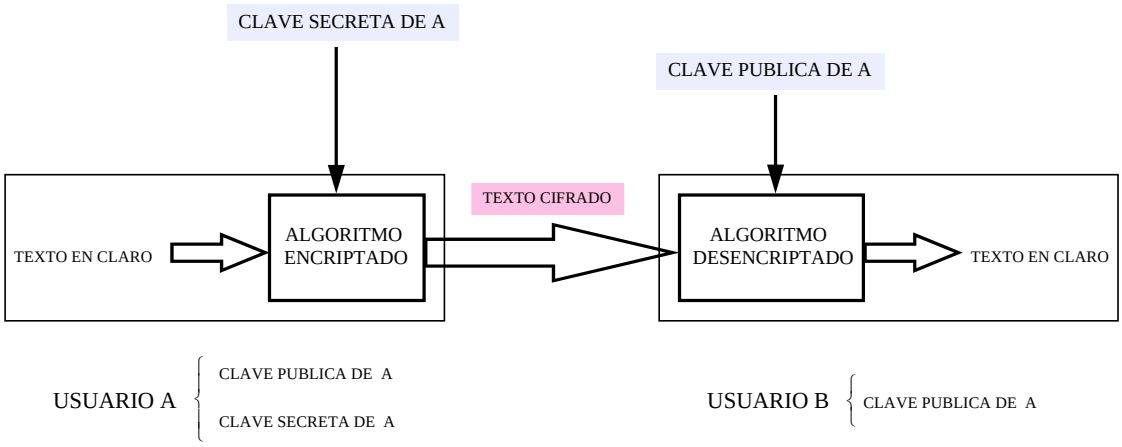
3. La firma debe estar disponible por las tres parte para resolver disputas

Se dedece por lo tanto la función de firma digital incluye la función de autenticación. Se han definido varias modalidades del mecanismo de firma digital. Así se van a considerar dos categorías denominadas frima digital directa y arbitraria:

#### *1.2.3.4.1 Firma digital directa*

Ya se ha comentado que el modelo de encriptación de clave pública no siempre es útil para porporcionar la autenticación de los datos. Sin embargo hay un método de usar la encriptación de clave pública para proporcionar un *mecanismo de firma digital* la cual incluye autenticación.

La figura ilustra un ejemplo de uso del modelo de encriptación de clave pública para proporcionar el mecanismo de *firma digital*. Hay que tener en cuenta que los algoritmos de encriptación de clave pública pueden ser empleados en cualquier orden. Es decir una entidad puede encriptar con la clave pública y desencriptar con la clave privada o encriptar con la privada y desencriptar con la pública. Este segundo caso sería el representado en la figura : la entidad A encripta una unidad de datos con la clave privada de A y se lo manda a la entidad B. La entidad B puede desencriptar el mensaje utilizando la clave pública de A. Puesto que la unidad de datos fue encriptada usando la clave privada de A (y sólo A la conoce) esto quiere decir que la encriptación del mensaje entero sirve de mecanismo de firma digital. Además es imposible alterar la unidad de datos sin acceder a la clave privada de A con lo cual la unidad de datos es a la vez autenticada.

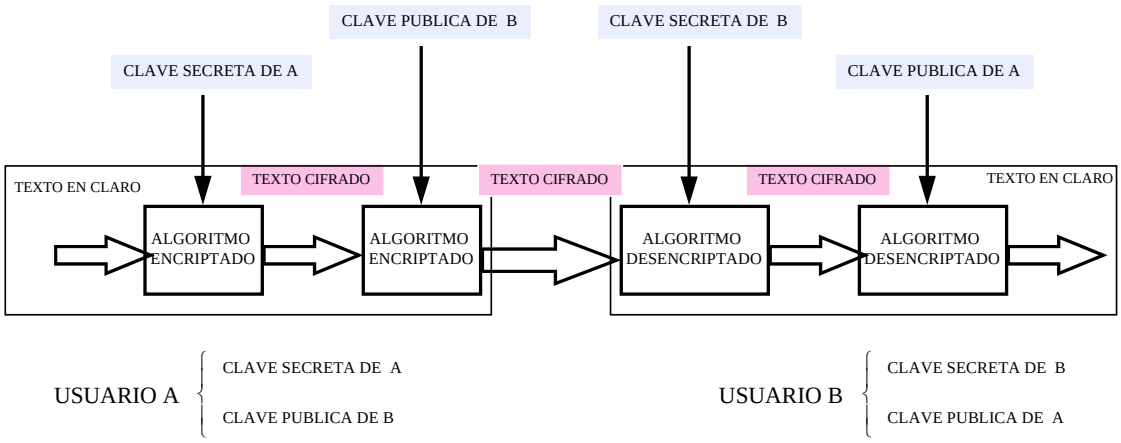



En el modelo anterior la unidad de datos completa es encriptada. Otras opciones serían encriptar una porción mínima de la unidad de datos que podría incluir la dirección origen y destino, un número de secuencia y un código de redundancia. Si una

porción de la unidad de datos es encriptada con la clave secreta del emisor, sirve como firma que verifica el origen, contenido y secuenciamiento.

Este modelo sin embargo no garantiza que cualquier intruso no pueda aceder a los contenidos de las unidades de datos. Esto es obvio en el caso de la encriptación aplicada a una parte de la unidad de datos, ya que el resto de la unidad de datos es transmitido en claro, aunque también ocurre en el caso de la encriptación completa ya que cualquier observador puede desencriptar el mensaje usando la clave pública de la entidad emisora.

Es sin embargo posible desarrollar otro modelo que constituye un mecanismo de firma digital untilizando la encriptación de clave pública, que incluya autenticación y la confidencialidad de las unidades de datos. En este modelo la entidad emisora A encripta una unidad de datos con la clave privada del emisor (lo que sirve de mecanismo de firma)y a continuación encriptamos el resultado anterior usando la clave pública de la entidad receptora. El texto final cifrado sólo puede ser desencriptado por la entidad receptora correspondiente lo que garantiza la confidencialidad. La desventaja de este modelo es que el algoritmo de clave pública que suele ser complejo debe ser realizado cuatro veces en vez de dos como en el caso anterior.




### *1.2.3.4.2 Firma digital arbitrada*

Todos los modelos descritos hasta ahora respecto a la firma digital tienen un punto en común: la seguridad del modelo depende de la clave privada del emisor. Ahora bien la entidad emisora puede denegar una unidad de datos alegando que la clave privada se perdió o alguien la robó. Para solventar este problema se pueden emplear controles administrativos relativos a la seguridad de las claves secretas con la presencia de un árbitro. Estos son los denominados mecanismos de firma digital arbitrados.

Existen una gran variedad de modelos de firma arbitrada al igual que modelos de firma directa. En términos generales ellos operan de la siguiente forma: Cada unidad de datos firmado por una entidad emisora S dirigido a una entidad receptora R debe pasar

primero por una *entidad A* que opera como arbitro que verifica la unidad de datos y su firma (verifica el origen y el contenido). La unidad de datos es entonces fechada y enviada a la entidad receptora R con la indicación de que ha sido verificada por una entidad que opera como arbitro. La presencia de la *entidad A* resuelve el problema inherente en modelos de firma directa en los que una entidad S puede negar haber enviado el mensaje.

La entidad que opera como árbitro juega un papel crucial en este tipo de modelo ya que todas las partes deben tener un grado de fiabilidad respecto a que el mecanismo de arbitraje funciona correctamente.

#### *1.2.3.4.3 Firma digital versus autenticación*

Todos los mecanismos de firma digital descritos proporcionan *autenticación* más la capacidad de resolver disputas entre las entidades que se comunican. Por lo tanto estos mecanismos podrían ser superiores a los simples modelos de autenticación dicutidos antes. Sin embargo aunque la autenticación es muy frecuente los modelos de firma digital son todavía raros. La principales razones son las siguientes:

1. Los mecanismos de firma digital son más complejos y por tanto más costosos.

2. Todos los mecanismos de firma digital pueden ser vulnerables en algún modo y siempre requieren algunos procedimientos de control extra o administartivos

3. En algunas circunstancias sólo se requieren mecanismos de autenticación simples y cualquier función adicional es superflua.

### *1.2.3.5 Mecanismos de Integridad de datos*

En el estandar ISO 7498 se hace una marcada distinción entre los mecanismos de *autenticación* e *integridad*. Los mecanismos de autenticación hacen referencia a las funciones que permiten confirmar la identidad (*integridad*) de la entidad o entidades pares que se comunican. Sin embargo los mecanismos de *integridad* hacen referencia a las funciones que permiten confirmar la corrección de los *datos* intercambiados entre las entidades pares. Los mecanismos de integridad pueden estar basados o utilizar técnicas similares al control de errores.

La integridad de datos es un aspecto central en todos los protocolos de comunicaciones. Tanto en comunicaciones orientadas a conexión como no orientadas a conexión es comun el uso de un *código de redundancia* para la protección de la cabecera o la unidad de datos del protocolo (PDU) completa intercambiada entre

entidades pares. Además en las comunicaciones orientadas a conexión se suelen usar números de secuencia para asegurar que las unidades de datos no sufren pérdidas, duplicaciones o desórdenes.

Estos mecanismos intrinsecos a los propios protocolos de comunicaciones pueden ser utilizados como mecanismos de integridad. Por ejemplo, si el código de redundancia de una unidad de datos del protocolo (UDP) es encriptada entonces un intruso podría modificar la UDP pero no podría modificar el código de redundancia para hacerlo conforme a los cambios. La entidad receptora podría detectar el error entre el código de redundancia recibido y el calculado y concluir que hubo una violación de la integridad de los datos. Igualmente el uso de números de secuencia encriptados protege a las unidades de intercambiadas de las retransmisiones, borrado o desorden. Otras técnicas a considerar serían el uso de sellos de tiempo e identificadores de uso único.

### *1.2.3.6 Mecanismos de Control de Acceso*

Los mecanismos de control de acceso permiten asegurar que sólo usuarios autorizados van a tener acceso a un sistema particular y a sus recursos individuales y que el acceso o modificación de una parte de los datos sólo estará también sólo permitido a individuos autorizados y programas. Los mecanismos de control de acceso están más relacionados con los mecanismos de seguridad propios de un sistema informático que con la seguridad en la distribución de la información en la red de datos. Es decir en la mayoría de los casos los mecanismos de control de acceso están implementados dentro de un sólo sistema informático para controlar el acceso a sus recursos. Sin embargo ya que el acceso a un sistema informático es por medio de una red de datos el *control de acceso* es una de las areas de interes de la arquitectura de seguridad ISA.

#### *1.2.3.6.1 Control de acceso orientado a usuario*

Los mecanismos de control de acceso orientados a usuario tratan de limitar los usuarios que acceden a los recursos del sistema. Estos mecanismos están evaluados sobre una red de datos e implican un dialogo o protocolo entre el potencial usuario del sistema y el propio sistema que puede incluir encriptación de palabras clave, gestión de claves etc.

El control de acceso de usuario en un entorno distribuido tal como una Red de Area Local (RAL) puede ser centralizado o distribuido. En modelo centralizado y en combinación con la técnica de acceso al medio de la RAL se determina que usuario puede utilizar la red de datos y a que sistemas se puede conectar. En un modelo

descentralizado el acceso a la red de datos pude ser transparente y sería en este caso el sistema informático final quien arbitraría los mecanismos de acceso de los usuarios.

#### *1.2.3.6.2 Control de acceso orientado a datos*

Una vez que un usuario ha conseguido acceder a un sistema informático debe haber establecidos una serie de mecanismos de control que afecten a los datos sensibles almacenados en la Base de Datos del sistema informático. Es decir asociado con cada usuario puede haber establecido un perfil que especifica las operaciones permitidas y los ficheros accesibles. El sistema de gestión de la Base de Datos debe controlar el acceso a elementos específicos y campos dentro de dichos elementos.

Las consideraciones de los mecanismos de control de acceso orientado a los datos en un entorno de red son semejantes a las consideraciones respecto de los mecanismos de control de acceso orientado a usuario. Si sólo se permiten que ciertos usuarios accedan a determinados campos de la unidades de datos almacenadas debe de ser necesario proteger esos campos durante su transmisión por la red. Típicamente el control de acceso a los datos es descentralizado, es decir está controlado por el propio sistema de gestión de la Base de Datos.

### *1.2.3.7 Control de encaminamiento*

Los funciones de encaminamiento realizadas por el nivel de red de la arquitectura ISA distribuidas en los distintos sistemas informáticos que constituyen la red de datos pueden ser utilizadas como mecanismos de seguridad. Así se podrían utilizar técnicas de encaminamiento dinámico o rutas alternativas para encaminar las unidades de datos etiquetas con un cierto grado de seguridad. O por ejemplo se podría utilizar una ruta alternativa si se detectan manipulaciones de la unidades de datos.

### *1.2.3.8 Mecanismos de arbitaje por una tercera entidad*

La seguridad en la comunicación entre dos entidades pares es proporcionada por una tercera entidad la cual tiene la garantía de las entidades pares que se comunican. Esta tercera entidad maneja la información necesaria para proporcionar esa garantía.

### *1.2.3.9 Etiqueta de seguridad*

Los recursos del sistema incluyendo las unidades de datos del protocolo (UDP´s) pueden tener estiquetas de seguridad asociadas a ellas para indicar un nivel de

seguridad. Una etiqueta de seguridad puede ser un campo distinto en una UDP o puede estar implícito (por ejemplo por el uso de una clave específica para encriptar datos o implicito por el contexto de los datos tales como origen o ruta).

#### *1.2.3.10 Detección de eventos*

La detección de eventos relativos a la seguridad es un mecanismo definido como parte de gestión del sistema ISA, específicamente denominado *gestión de manejo de eventos*. Ejemplos de eventos relativos a la seguridad son :una violación de seguridad específica, un evento específico seleccionado etc.

La detección de un evento relativo a la seguridad podría originar alguna de las siguientes acciones: notificación local o remota del evento, finalización de una sesión de usuario o diferentes acciones de recuperación.

#### *1.2.3.11 Fichero de auditorías*

El *fichero de auditorías* es un fichero de información de seguridad, con la notificación de eventos relativos a la seguridad. Tal fichero permite la detección e investigación de posibles deficiencias en la seguridad del sistema permitiendo acciones posteriores. El estudio de este fichero será la base para testear los sistemas de control y asegurar que los servicios y mecanismos de seguridad implementados se adecuan a la politica de seguridad establecida

La generación de este fichero con información relativa a la seguridad se puede considerar como un *mecanismo de seguridad* aunque las funciones posteriores a realizar en base a dicho fichero se pueden considerar que son parte de las funciones de gestión de seguridad del sistema.

#### *1.2.3.12 Mecanismos de restauración*

Los mecanismos de restauración manejan peticiones de otros mecanismos tales como los mecanismos de detección de eventos y lleva a cabo acciones de recuperación aplicando un conjunto de reglas. Las acciones de recuperación pueden ser: inmediatas (produciendo la interrupción de operaciones) o temporales(ocasionando la invalidación temporal de una entidad). También se puede incluir una entidad en una “lista negra” o cambiar la clave en uso.

## 1.2.4 Relación entre servicios y mecanismos de seguridad

Una vez definidos los servicios y mecanimos de seguridad resulta imprescindible determinar para cada servicio qué mecanismo o mecanismos son los apropiados para proporcionar dichos servicios. En las tabla siguientes se desciben que mecanismos son utilizados para implementar los distintos servicios de seguridad.

| MECANISMOS / SERVICIOS | ENCRIPTADO | FIRMA DIGITAL | INTEGRIDAD | AUTENTICACIÓN | TRAFICO DE RELLENO | CONTROL ENCAMINAMIENTO | ARBITRAJE |
|---|---|---|---|---|---|---|---|
| AUTENTICACIÓN ENTIDADES PARES | X | X | | X | | | |
| AUTENTICACIÓN DATOS DE ORIGEN | X | X | | | | | |
| CONFIDENCIALIDAD ORIENTADA A CONEXIÓN | X | | | | | X | |
| CONFIDENCIALIDAD NO ORIENTADA A CONEXIÓN | X | | | | | X | |
| CONFIDENCIALIDAD DE CAMPOS SELECTIVOS | X | | | | | | |
| CONFIDENCIALIDAD DE CONTROL DE TRAFICO | X | | | | X | X | |

| MECANISMOS / SERVICIOS | ENCRIPTADO | FIRMA DIGITAL | INTEGRIDAD | AUTENTICACIÓN | TRAFICO DE RELLENO | CONTROL ENCAMINAMIENTO | ARBITRAJE |
|---|---|---|---|---|---|---|---|
| INTEGRIDAD ORIENTADA A CONEXION CON MECANISMOS DE RECUPERACION | X | | X | | | | |
| INTEGRIDAD NO ORIENTADA A CONEXION CON MECANISMOS DE RECUPERACION | X | | X | | | | |
| INTEGRIDAD ORIENTADA A CONEXION SOBRE CAMPOS SELECTIVOS | X | | X | | | | |
| INTEGRIDAD NO ORIENTADA A CONEXION | X | X | X | | | | |
| INTEGRIDAD NO ORIENTADA A CONEXION SOBRE CAMPOS SELECTIVOS | X | X | X | | | | |
| NO REPUDIO EN ORIGEN | | | X | | | | |
| NO REPUDIO EN DESTINO | | | X | | | | |

### *1.2.4.1 Servicio de Autenticación*

El mecanismo fundamental para proporcionar el *servicio de autenticación* es la ***encriptación.*** Si las entidades pares que se comunican comparten la información necesaria para el intercambio de unidades de datos encriptadas ninguna otra tercera entidad puede reclamar una falsa identidad. Otro mecanismo más explicito es la ***firma digital.*** En este caso una entidad emisora debe firmar las unidades de datos de forma que la firma puede ser autenticada.

Otro grupo de mecanismos que pueden ser utilizados para implementar el servicio de autenticación son los denominador en ISA como mecanismos de ***intercambio de autenticación***. Estos mecanismos constituyen en si mismos un auténtico protocolo que incluyen el uso de palabras clave u otros medios de identificación de una entidad, el uso del código de autenticación de mensajes, el intercambio de unidades de datos de asentimiento etc. Estos mecanismos pueden utilizarse para proporcionar el servicio de autenticación de entidades pares.

### *1.2.4.2 Servicio de Confidencialidad*

El mecanismo fundamental para proporcionar el *servicio de confidencialidad* es también la ***encriptación.*** La *encriptación* puede ser usada para la protección de las unidades de datos frente a la revelación de sus contenidos localizando los mecanismos de encriptación en los sistemas finales. Si los mecanismos de encriptación se sitúan en los enlaces entre cada par de nodos (siempre considerando una red de conmutación de paquetes) se puede además proporcionar el *servicio de confidencialidad aplicada al análisis de trafico.* Este último servicio de confidencialidad también puede ser proporcionado con el mecanismo de ***tráfico de relleno*** de tal manera que a un intruso le sea imposible interpretar ningun elemento de las unidades de datos encriptadas intercambiadas

Otro mecanismo que puede ser utilizado para proporcionar el servicio de confidencialidad es el ***control de encaminamiento***. Para unidades de datos especialmente sensibles pueden elegirse rutas específicas que incluyan redes seguras. Por ejemplo si una organización puede emplear tanto redes privadas como públicas para interconectar sus sucursales y dispone de una red privada equipada con mecanismos de encriptado los datos sensibles se deberían encaminar sólo a través de dicha red privada.

### *1.2.4.3 Servicio de Integridad*

El principal mecanismo para proporcional el servicio de integridad de las unidades de datos es la ***encriptación***. Si un intruso no puede desencriptar las unidades de datos entonces e imposible que el éste modifique con éxito sus contenidos. Las alteraciones en las unidades de datos serán detectadas por la entidad receptora al realizar la función de desencriptado. También son útiles los mecanismos de ***firma digital*** para comunicaciones no orientadas a comunicación.

La *encriptación* proporciona un medio para detectar la alteración de un mensaje, pero por si misma no permite contemplar otros aspectos de la integridad tales como retransmisiones, reordenamientos o destrucción de unidades de datos. Para este propósito se necesitan mecanismos que el modelo ISA define como ***mecanismos de integridad de datos***. En general se usan mecanismos diferentes para proporcionar integridad de campos selectivos o de unidades de datos individuales en comunicaciones no orientadas a conexión y para proporcionar integridad de las unidades de datos en una comunicación orientada a conexión. Estos mecanismos están basados en los mecanismos de control de errores presentes en el protocolo de intercambio de unidades de datos.

### *1.2.4.4 Servicio de No Repudio*

El principal mecanismo para proporcionar el *servicio de no repudio* es la ***firma digital***, la cual invoca el uso de una *clave privada* aplicada a una parte de los datos. Para evitar el repudio de los contenidos de las unidades de datos, más que la unidad de datos misma se usan mecanismos de ***integridad de datos*** tales como la encriptación de un código de detección de error como parte de la firma digital. Finalmente se pueden utilizar los mecanismos de ***arbitarje por una tercera entidad*** con el fin de proporcionar el servicio de no repudio

## 1.2.5 Provisión de Servicios de Seguridad en un nivel del modelo ISA

Los servicios de seguridad en un nivel particular de la arquitectura ISA deben ser invocados por petición. En el primer caso una entidad de nivel *N+1* hace una petición de seguridad para el servicio del nivel ***N***. En el caso de comunicación orientada a conexión, los servicios de seguridad son pedidos en la fase de establecimiento de la conexión. La provisión de un servicio de seguridad puede originar una negociación entre las entidades pares que se comunican de nivel *N+1* y el servicio de nivel *N*. Esto

puede ser realizado como un procedimiento separado o como parte integral del protocolo de establecimiento orientado a conexión. En el caso de comunicación no orientada a comunicación el servicio de seguridad es pedido para cada unidad de datos.

En el caso de que una entidad de nivel *N+1* no especifique un objetivos de de seguridad, el nivel *N* seguirá una política de seguridad de acuerdo con la información presente en una base de datos de gestión del sistema.

Una vez que se ha decidido el servicio de seguridad que debe proporcionar el nivel *N* este tratará de alcanzar esos objetivos de seguridad de una de las siguientes formas:

- Activando los mecanismos de seguridad directamente dentro del nivel *N*
- Invocando los servicios de seguridad del nivel *N-1*

#### *1.2.5.1 Establecimiento de una conexión segura de nivel* **N**

Si se van a proporcionar servicios de seguridad en una comunicación orientada a conexión el primer paso es proporcionar esos servicios en la fase de establecimiento de la conexión. Para alcanzar los objetivos de seguridad es a veces fundamental la secuencia de acciones a realizar. A continuación se describen un conjunto de operaciones en la secuencia apropiada:

1. ***Control de acceso al servicio***: El nivel N debe determinar si a la entidad de nivel N+1 que hace la petición se la permite la petición de conexión segura de nivel N

2. ***Autenticación de entidades pares:*** Si la entidad de nivel *N+1* pide un servicio de autenticación entonces se activarán los mecanismos de intercambio de autenticación con el fin de proporcionar el servicio de autenticación unilateral o mutua. Estos mecanismos se materializarán en forma de un *protocolo de autenticación.*

3. ***Control de acceso(entidad destino):*** La entidad destino de nivel ***N*** o los sistemas intermedios pueden imponer restricciones de control de acceso.

4. ***Confidencialidad***: Si la entidad de nivel *N+1* ha pedido un servicio de confidencialidad total o selectiva para la conexión de nivel *N* esto implica el establecimiento de un modelo de encriptación y distribución de claves. Esto puede ser realizado en el *protocolo de autenticación* o realizado por un protocolo independiente.

5. ***Integridad de datos***: Si la entidad de nivel *N+1* ha pedido un servicio de integridad para todos los datos de usuario o para campos selectivos de dichos datos en la conexión de nivel *N* esto implica que en la fase de transferencia se activaran los mecanismos de integridad necesarios (por ejemplo números de secuencia, códigos de redundancia etc).

6. ***Servicios de no repudio***: Si la entidad de nivel *N+1* ha pedido un servicio de no repudio el nivel *N* deberá proporcionar los mecanismos adecuados.

### *1.2.5.2 Fase transferencia en una conexión segura de nivel* N

En la fase de transferencia de una conexión segura de nivel N pueden tener lugar las siguientes funciones o mecanismos de seguridad:

1. Autenticación de entidad par (a intervalos).

2. Protección de campos seleccionados.

3. Funcionamiento de los mecanismos de integridad.

4. Notificación de de ataques activos

Además lo siguiente puede ser necesitado

- Grabación del security audit trail

- Manejo y detección de eventos de seguridad.

### *1.2.5.3 Servicios de seguridad en una comunicación no orientada a conexión*

La petición de tales servicios de seguridad deberá hacerse por cada unidad de datos de protocolo (UDP) intercambiada entre entidades pares. No todos los servicios disponibles en los protocolos orientados a conexión están disponibles en comunicaciones no orientados a conexión. Algunos de estos servicios son:

- Autenticación de entidad par.

- Autenticación de datos de origen.

- Servicio de control de acceso.

- Confidencialidad no orientada a conexión.
- Confidencialidad de campos selectivos.
- Integridad no orientada a conexión.
- Integridad no orientada a conexión de campos selectivos.
- No repudio de origen.

### 1.2.6 Localización de los servicios y mecanismos de seguridad en los niveles ISA

El estandar ISO 7498-2 ha establecido una serie de criterios para situar los servicios y mecanismos de seguridad en los niveles ISA. Algunos de estos criterios son:

- Debe minimizarse el número de formas alternativas para alcanzar un servicio.
- Es aceptable confeccionar sistemas seguros ofreciendo servicios de seguridad en más de un nivel.
- No deberían implementarse inecesariamente funciones requeridas en los mecanismos de seguridad duplicando las funciones ya existentes en la arquitectura ISA.
- Se debería evitar la violación de la independencia de un nivel.
- La cantidad de funcionalidad relativa a servicios de seguridad debería ser minimizada
- La arquitectura de seguridad ISA se asume que se aplica a sistemas finales conteniendo los 7 niveles.

A continuación en una tabla se describen qué servicios de seguridad pueden ser ofrecidos en los distintos niveles de la arquitectura ISA y los mecanismos que se deberían implementar en cada nivel de acuerdo a los principios definidos en el estandar ISO 7498-2.

| NIVEL ISA / SERVICIOS | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| AUTENTICACIÓN ENTIDADES PARES | | | X | X | | | X |
| AUTENTICACIÓN DATOS DE ORIGEN | | | X | X | | | X |
| CONFIDENCIALIDAD ORIENTADA A CONEXIÓN | X | X | X | X | | | X |
| CONFIDENCIALIDAD NO ORIENTADA A CONEXIÓN | | X | X | X | | | X |
| CONFIDENCIALIDAD DE CAMPOS SELECTIVOS | | | | | | | X |
| CONFIDENCIALIDAD DE CONTROL DE TRAFICO | X | | X | | | | X |

| NIVEL ISA / SERVICIOS | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| INTEGRIDAD ORIENTADA A CONEXION CON MECANISMOS DE RECUPERACION | | | | X | | | X |
| INTEGRIDAD NO ORIENTADA A CONEXION CON MECANISMOS DE RECUPERACION | | | X | X | | | X |
| INTEGRIDAD ORIENTADA A CONEXION SOBRE CAMPOS SELECTIVOS | | | | | | | X |
| INTEGRIDAD NO ORIENTADA A CONEXION | | | X | X | | | X |
| INTEGRIDAD NO ORIENTADA A CONEXION SOBRE CAMPOS SELECTIVOS | | | | | | | X |
| NO REPUDIO EN ORIGEN | | | | | | | X |
| NO REPUDIO EN DESTINO | | | | | | | X |

| NIVEL ISA / MECANISMOS | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| ENCRIPTADO | X | X | X | X | | X | |
| FIRMA DIGITAL | | | X | X | | X | X |
| INTEGRIDAD | | | X | X | | X | |
| AUTENTICACION | | | X | X | | | X |
| TRAFICO DE RELLENO | | | X | | | | X |
| CONTROL DE ENCAMINAMIENTO | | | X | | | | |
| AUDITORIAS | | | | | | X | X |

### *1.2.6.1 Nivel físico*

Los únicos servicios proporcionados en el nivel físico son la *confidencialidad en comunicaciones orientadas a conexión y la confidencialidad aplicada al control de tráfico***.** La *encriptación* total de los datos es el principal mecanismo de seguridad en el nivel físico. Otros servicios como la *integridad* y la *autenticación* no se pueden manejados a este nivel puesto que se requiere del manejo de información adicional que a nivel de bit no puede procesar. Sin embargo el uso de las funciones de encriptación en este nivel puede permitir soportar estos servicios en niveles superiores.

Los servicios de seguridad ofrecidos en el nivel físico típicamente proporcionan seguridad en enlaces punto a punto. Por ejemplo la seguridad puede ser aplicada entre un terminal y un sistema final, entre un sistema final y un sistema intermedio o entre dos sistemas intermedios. La mayor ventaja de los servicios ofrecidos en este nivel es que la protección puede ser independiente de los protocolos de niveles superiores. Sin embargo los dispositivos y mecanismos que proporcionan seguridad en este nivel están orientados a un tecnología específica. (por ejemplo los dispositivos que proporcionan confidencilidad en comunicaciones por radio no serán adecuados en comunicaciones que utilizan par trenzado).

La utilidad de los servicios en este nivel es limitada cuando se atraviesan redes de conmutación de paquetes puesto que los nodos intermedios deben procesar las cabeceras de las unidades de datos. Sin embargo cuando se requiera *confidencialidad aplicada al control de tráfico* es claramente el mejor nivel en el que implementar dicho servicio.

### *1.2.6.2 Nivel de enlace*

Los servicios de seguridad de nivel de enlace se proporcionan típicamente en un enlace punto a punto al igual que los servicios de nivel físico. De nuevo los servicios deben terminar en los puntos donde residen las entidades pares de nivel de enlace, por ejemplo sistemas finales y nodos conmutadores. En un entorno de Redes de Area Local los servicios de seguridad pueden ser ofrecidos basados en la propia tecnología de acceso al medio.

Una ventaja de los servicios ofrecidos en este nivel es la independencia de los niveles superiores haciendo posible utilizar dispositivos de seguridad de nivel de enlace con una gran variedad de familias de protocolos. Los dispositivos que implementan servicios de seguridad en el nivel de enlace son específicos tanto a la propia tecnología de nivel de enlace como a la tecnología de nivel físico.

De acuerdo al estandar ISO 7498-2 los servicios ofrecidos en el nivel de enlace son *la confidencialidad orientada a conexión y la confidencialidad no orientada a conexión.* Debido a que la mayoría de los protocolos de nivel de enlace incorporan números de secuencia y un código de detección de errores podría parecer que es una oportunidad para proporcionar el *servicio de integridad orientada a conexión con mecanismos de recuperación.* Sin embargo en estos protocolos el campo de número de secuencia es relativamente pequeño y el código de detección de errores no ha sido seleccionado para propósitos de seguridad. Por lo tanto puede no ser posible proporcionar un servicio de integridad no orientada a conexión de “alta calidad” en este nivel sin introducir un protocolo específico.

En entornos de Redes de Area Local los protocolos de nivel de enlace no proporcionan servicios orientados a conexión pero si proporcionan mecanismos de detección de errores. Esto sugiere que se podría ofrecer un servicio de integridad no orientada a conexión (sin mecanismos de recuperación). El comite IEEE 802.10 Secure Interoperable LAN Standars (SILS) ha definido un protocolo denominado Secure Data Exchange (SDE) que opera entre el subnivel LLC y el subnivel MAC. El protocolo SDE podría ser usado en un entorno de Red de Area Local en el cual no todas las estaciones podrían tenerlo implementado. Por lo tanto la capacidad de detección de errores nativa en este nivel no está explotada en el protocolo SDE, en su lugar este

protocolo introduce sus propios mecanismos de integridad orientados a dar un servicio de seguridad. El protocolo SDE proporciona además del servicio de *integridad no orientada a conexión el servicio de autenticación del origen de los datos e incluso el servicio de control de acceso*. Todos estos servicios están omitidos sin embargo en las recomendaciones del estandar ISO 7498-2 respecto a los servicios ofrecidos en el nivel de enlace.

En resumen hay significativas diferencias respecto de los servicios de seguridad que pueden ser ofrecidos en el nivel de enlace según se tenga un enlace punto a punto o una Red de Area Local. La diferencia fundamental es que la *confidencialidad* puede ser ofrecida en una linea punto a punto de manera totalmente transparente. En contraste en entornos de Red de Area Local la riqueza de servicios ofrecidos por el protocolo SDE pueden no sen transparentes para los sistemas finales.

Aunque el estandar ISO 7498 cita la confidencialidad orientada a conexión y no orientada a conexión como potenciales servicios de nivel de enlace, un anexo al estandar establece que la encriptación a nivel de enlace no es recomendable. La encriptación puede ser hecha a nivel físico o a nivel de red dependiendo de los requerimientos. Por lo tanto la provisión de este servicio en el nivel de enlace es una duplicación del esfuerzo.

### *1.2.6.3 Nivel de red*

La implantación de servicios de seguridad en el nivel de red permite que a las entidades finales se las pueda ofrecer un servicio de seguridad independientemente de la tecnología de las distintas redes que separan a las entidades pares. El estandar ISO 7498-2 cita varios servicios de seguridad apropiados en este nivel: *confidencialidad orientada y no orientada a conexión, confidencialidad aplicada al análisis de tráfico, integridad (orientada a conexión sin recuperación y no orientada a conexión), autenticación de entidades pares y de origen de datos y control de acceso.*

Si se tiene una red de conmutación de paquetes X.25 y por lo tanto un nivel de red orientado a conexión los servicios de seguridad van a ser independientes de los niveles superiores. Así se pueden ofrecer servicios de seguridad específicos que pueden proporcionar protección transparente para protocolos ISA, TCP/IP o protocolos propietarios en niveles superiores. Tales servicios necesariamente finales son ofrecidos en el extremo de un circuito virtual X.25 aunque ese circuito virtual atraviese multiples redes X.25 interconectadas a través de pasarelas X.75.

El estandar ISO 7498-2 argumenta que los servicios de seguridad deberían ser consistentes con los servicios de seguridad proporcionados en ese nivel. En el caso de

redes X.25 el protocolo de nivel de red utiliza números de secuencia en las unidades de datos (paquetes) pero no tiene mecanismos de integridad. En tales circunstancias puede ser más apropiado por ejemplo proporcionar servicios de *confidencialidad, autenticación de entidad par y control de acceso* para circuitos X.25 y utilizar los mecanismos que implementan la integridad orientada a conexión y autenticación en el nivel de transporte.

Si en la arquitectura de comunicaciones de los sistemas finales se dispone de un nivel de red no orientado a conexión (IP,CLNS) los servicios de seguridad son ofertados indenpendientemente de la tecnología y el número de redes atravesadas siempre y cuando se disponga de los elemneto de interconexión adecuados (puentes, pasarela o encaminadores IP) Así en conjunción con CLNP o IP se puede ofertar los servicios de *autenticación de origen de datos, integridad no orientada a conexión, confidencialidad no orientada a conexión y control de acceso.* En este subnivel se pueden implementar servicios y mecanismos de modo que sean independientes de la tecnología de las distintas redes atravesadas. Los mismos protocolos y mecanismos podrían ser usados para proporcionar comunicaciones seguras entre dos estaciones de RAL de distintas tecnologías y separadas por una red de conmutación de paquetes. Los dispositivos que proporcionan estos servicios pueden ser específicos según el tipo de tecnología empleada en los niveles inferiores (nivel físico y de enlace).

Históricamente los servicios de seguridad de nivel físico y de enlace estaban normalmente implementados en hardware externo. Es mucho más adecuado implementar la seguridad de nivel de red internamente en un sistema final o intermedio. Implementaciones externas del nivel de red también son posibles pero pueden presentar algunos problemas como la falta de transparencia pudiendo interferir en la gestión de red.

Los servicios de seguridad proporcionados en el subnivel CLNP o IP puede ser empleado para proporcionar seguridad entre un sistema final y un sistema intermedio (por ejemplo un encaminador). Puede tener algunas ventajas el ofrecer servicios de seguridad en sistemas intermedios. En muchas topologías de red un sistema intermedio a menudo actúa como elemento de interconexión entre una RAL y una red de Area Extendida o como límite entre una entidad administrativa “local” y otras entidades administrativas. Proporcionar servicios de seguridad en el elemento intermedio es especialmente atractivo desde la prespectiva de la gestión de seguridad cuando sólo se quiere que un pequeño grupo de sistemas se vean afectados en vez de todos los sistemas finales.

Como conclusión se puede decir que la mayoría de los servicios de seguridad definidos se pueden ofrecer en el nivel de red. El estandar ISO 7498-2 contempla los siguientes servicios de seguridad en el nivel de red:

1. ***Autenticación de entidad par***: Este servicio puede ser implementado con los mecanismos de *intercambio de autenticación o de firma digital*

2. ***Autenticación de datos de origen***: Este servicio puede ser implementado con los mecanismos de *encriptación o de firma digital.*

3. ***Servicio de control de acceso***: Este servicio proporciona los mecanismos apropiados de control de acceso. El control de acceso permite a los sistemas finales controlar el establecimiento de conexiones de red y para rechazar llamadas no deseadas. También permite que una o más subredes controlen el uso de los recurso de nivel de red.

4. ***Confidencialidad orientada a conexión***: Este servicio puede ser implementado con los mecanismos de *encriptación* y *control de encaminamiento*.

5. ***Confidencialidad aplicada al control de tráfico:*** Este servicio puede ser implementado con un mecanismo de *tráfico de relleno* en conjunción con un servicio de confidencialidad rn capas inferiores al nivel de red y con mecanismos de control de encaminamiento.

6. ***Integridad orientada a conexión sin recuperación***: Este servicio puede ser implementado con un mecanismo de *integridad de datos* algunas veces en conexión con un mecanismo de *encriptado*

7. ***Integridad no orientada a conexión***: Este servicio puede ser implementado con un mecanismo de *integridad de datos* algunas veces en conexión con un mecanismo de *encriptado*.

La implementación de servicios de seguridad en el nivel de red en sistemas finales tiende a requerir la modificación del nucleo del sistema operativo puesto que frecuentemente el nivel de red suele estar implementado en el nucleo del sistema operativo. Por lo tanto la provisión de servicios de seguridad en el nivel de red requiere la cooperación de los vendedores de los sistemas finales e intermedios.

### *1.2.6.4 Nivel de transporte*

Los servicios que pueden ser ofrecidos en el nivel de transporte son prácticamente los mismos que los ofrecidos en el nivel de red. La principal diferencia es que el nivel de red cumple las funciones de transporte de las unidades entre sistemas finales, mientras que el nivel de transporte soporta el dialogo entre entidades pares de los sistemas finales. Por lo tanto el servicio de *inegridad orientada a conexión con*

*mecanismos de recuperación* es más adecuada de implementar en el nivel de transporte, que gestiona la conexión de usuario extremo a extremo. Por contra el servicio de *confidencialidad aplicada al control de tráfico* si se aplica a todas las conexiones entre entidades de sistemas finales se deberían ofrecer en el nivel de red.

Sólo hay una diferencia entre los servicios de seguridad ofrecidos en el nivel de red y los ofrecidos en el nivel de transporte: la capacidad de proporcionar seguridad en los sistemas intermedios (caso del nivel de red) o sólo entre los sistemas finales (caso del nivel de transporte). Los servicios de seguridad de nivel de transporte en comunicaciones orientadas a conexión ofrecen en principio una protección no disponible en el nivel de red. Esto es debido a la naturaleza de la comunicación orientada a conexión frente a la comunicación no orientada a conexión de los niveles inferiores. Sin embargo en la práctica una buena implmentación de un protocolo de nivel de transporte orientado a conexión puede hacer uso de los servicios de *integridad no orientada a conexión y autenticación de origen de datos* proporcionados en el nivel de red.

Los mecanismos de seguridad de nivel de transporte pueden ser implementados dentro del sistema operativo. De aquí que la introducción de mecanismos de seguridad en el nivel de transporte requiera la cooperación con los vendedores de sistemas finales.

#### *1.2.6.5 Nivel de sesión*

El estandar ISO 7498-2 no permite ofrecer servicios de seguridad en el nivel de sesión. Es el nivel de transporte quien en la comunicación entre entidades pares debe ser capaz de proporcionar esos servicios. Además si se utilizan mecanismos de encriptación en el nivel de transporte la cabecera de nivel de sesión es protegida.

#### *1.2.6.6 Nivel de presentación*

El nivel de presentación no proporciona específicamente servicios de seguridad, ya que estos pueden ser ofrecidos en el nivel de aplicación Sin embargo el nivel de presentación debe proprocionar funcionalidades y mecanismos que operan sobre la sintaxis de codificación de los datos; estas facilidades son proporcionadas en beneficio del nivel de aplicación

En particular, para servicios de nivel de aplicación que descansan en mecanismos de encriptación, estos mecanismos pueden ser realizados en el nivel de presentación.

El único servicio de nivel de aplicación que no requiere los mecanismos del nivel de presentación es el *control de acceso*. Aquellos servicios de aplicación que utilizan los mecanismos de nivel de preserntación son

- Confidencialidad orientada a conexión
- Confidencialidad no orientada a conexión
- Confidencialidad de campos selectivos

Cualquier otro servicios de seguridad de nivel de aplicación puede ser soportado por los mecanismos del nivel de presentación o por los mecanismos en el nivel de aplicación.

### *1.2.6.7 Nivel de aplicación*

Cualquiera de los servicios de seguridad definidos para el modelo ISA puede ser ofrecido en el nivel de aplicación, además el estandar ISO 7498-2 establece que el servicio de *no repudio* debe ser ofrecido sólo en este nivel.. A través del interfaz de servicio de nivel de aplicación un usario puede pedir servicios de seguridad independientemente del nivel de la arquitectura en la cual se encuentran los mecanismos que implementan dichos servicios.

Una de las razones más atractiva de proporcionar servicios de seguridad en este nivel es la capacidad de implementar estos servicios fuera del sistema operativo. Por lo tanto los usuarios pueden implementar servicios de seguridad en sus aplicaciones ni necesidad de dependen de los vendedores de los sistemas finales.