



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

X.814

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(11/95)

SERIE X: REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS

Seguridad

**Tecnología de la información –
Interconexión de sistemas abiertos –
Marcos de seguridad para sistemas
abiertos: Marco de confidencialidad**

Recomendación UIT-T X.814

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.º 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.814 se aprobó el 21 de noviembre de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-5.

NOTA

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

© UIT 1996

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

	<i>Página</i>
1 Alcance.....	1
2 Referencias normativas	2
2.1 Recomendaciones Normas Internacionales idénticas.....	2
2.2 Pares de Recomendaciones Normas Internacionales de contenido técnico equivalente	2
3 Definiciones	2
3.1 Definiciones del modelo de referencia básico	2
3.2 Definiciones de arquitectura de seguridad	3
3.3 Definiciones de la visión general de los marcos de seguridad	3
3.4 Definiciones adicionales	3
4 Abreviaturas	4
5 Análisis general de la confidencialidad.....	4
5.1 Conceptos básicos	4
5.1.1 Protección de la información	4
5.1.2 Operaciones de ocultación y revelación.....	5
5.2 Clases de servicios de confidencialidad.....	5
5.3 Tipos de mecanismos de confidencialidad.....	6
5.4 Amenazas a la confidencialidad.....	7
5.4.1 Amenazas cuando la confidencialidad se proporciona impidiendo el acceso.....	7
5.4.2 Amenazas cuando la confidencialidad se proporciona ocultando la información	7
5.5 Tipos de ataques a la confidencialidad.....	7
6 Políticas de confidencialidad.....	8
6.1 Establecimiento de las políticas	8
6.1.1 Caracterización de la información	8
6.1.2 Caracterización de las entidades	8
7 Información y facilidades de confidencialidad.....	8
7.1 Información de confidencialidad	8
7.1.1 Información de confidencialidad de ocultación	9
7.1.2 Información de confidencialidad de revelación	9
7.2 Facilidades de confidencialidad	9
7.2.1 Facilidades relacionadas con el funcionamiento.....	9
7.2.1.1 Ocultación.....	9
7.2.1.2 Revelación.....	9
7.2.2 Facilidades relacionadas con la gestión	10
8 Mecanismos de confidencialidad	10
8.1 Provisión de la confidencialidad mediante la prevención del acceso	10
8.1.1 Protección de la confidencialidad mediante la protección física de los medios.....	10
8.1.2 Protección de la confidencialidad mediante el control del encaminamiento.....	10
8.2 Provisión de la confidencialidad mediante el cifrado	10
8.2.1 Provisión de la confidencialidad mediante el relleno de datos	11
8.2.2 Provisión de la confidencialidad mediante eventos ficticios.....	11
8.2.3 Provisión de la confidencialidad mediante protección del encabezamiento de las PDU	11
8.2.4 Provisión de confidencialidad mediante campos que varían en función del tiempo.....	11
8.3 Provisión de confidencialidad mediante ubicación contextual	12
9 Interacciones con otros servicios y mecanismos de seguridad.....	12
9.1 Control de acceso.....	12

Anexo A – Confidencialidad en el modelo básico de referencia de OSI	13
A.1 Confidencialidad en modo con conexión	13
A.2 Confidencialidad en modo sin conexión	13
A.3 Confidencialidad de campos seleccionados	13
A.4 Confidencialidad del flujo de tráfico	13
A.5 Utilización de la confidencialidad en las capas de OSI	13
A.5.1 Utilización de la confidencialidad en la capa física	13
A.5.2 Utilización de la confidencialidad en la capa de enlace de datos	13
A.5.3 Utilización de la confidencialidad en la capa de red	14
A.5.4 Utilización de la confidencialidad en la capa de transporte	14
A.5.5 Utilización de la confidencialidad en la capa de presentación	14
A.5.6 Utilización de la confidencialidad en la capa de aplicación	14
Anexo B – Ejemplo de secuencia de movimientos a través de diferentes entornos de confidencialidad protegida..	15
Anexo C – Representación de la información	16
Anexo D – Canales protegidos	17
Anexo E – Reseña de facilidades de confidencialidad	18
E.1 Entidades de confidencialidad	18
E.1.1 Iniciador	18
E.1.2 Verificador	18
E.1.3 Tercera parte confiable para facilidades de confidencialidad	18

Resumen

La presente Recomendación | Norma Internacional define un marco general para la prestación de servicios de confidencialidad. La confidencialidad es la propiedad de que una información no esté disponible ni sea divulgada a personas, entidades o procesos no autorizados.

Introducción

Numerosas aplicaciones de sistemas abiertos tienen requisitos de seguridad que dependen de la prevención de la divulgación de la información. Dichos requisitos pueden incluir la protección de la información utilizada en la prestación de otros servicios de seguridad, tales como los de autenticación, control de acceso o integridad, ya que si un atacante pudiera conocerla, podría reducir o anular la eficacia de esos servicios.

Se entiende por confidencialidad la propiedad de que una información no esté disponible ni sea divulgada a personas, entidades o procesos no autorizados.

La presente Recomendación | Norma Internacional define un marco general para la prestación de los servicios de confidencialidad.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

**TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS
ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS:
MARCO DE CONFIDENCIALIDAD**

1 Alcance

La presente Recomendación | Norma Internacional sobre marcos de seguridad para sistemas abiertos trata de la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde se considera que el término «sistema abierto» abarca sectores tales como base de datos, aplicaciones distribuidas, procesamiento distribuido abierto e interconexión de sistemas abiertos. Los marcos de seguridad se relacionan con la definición de los medios para proteger los sistemas y objetos dentro de sistemas y las interacciones entre sistemas. Los marcos de seguridad no están relacionados con la metodología para construir sistemas o mecanismos.

Los marcos de seguridad tratan de los elementos de datos y secuencias de operaciones (pero no de los elementos de protocolo) que se pueden utilizar para obtener servicios de seguridad específicos. Estos servicios de seguridad pueden aplicarse a entidades comunicantes de sistemas así como a datos intercambiados entre sistemas, y a datos gestionados por sistemas.

La presente Recomendación | Norma Internacional trata de la confidencialidad de la información en la extracción, transferencia y gestión, y:

- 1) define los conceptos básicos de confidencialidad;
- 2) identifica posibles clases de mecanismos de confidencialidad;
- 3) clasifica e identifica facilidades para cada clase de mecanismos de confidencialidad;
- 4) identifica la gestión requerida para apoyar las clases de mecanismos de confidencialidad; y
- 5) trata de la interacción de mecanismos de confidencialidad y los servicios sustentadores con otros servicios y mecanismos de seguridad.

Entre los diferentes tipos de normas que pueden utilizar este marco cabe citar:

- 1) las normas que incorporan el concepto de confidencialidad;
- 2) las normas que especifican servicios abstractos que incluyen confidencialidad;
- 3) las normas que especifican usos de un servicio de confidencialidad;
- 4) las normas que especifican medios de proporcionar confidencialidad dentro de una arquitectura de sistema abierto; y
- 5) las normas que especifican mecanismos de confidencialidad.

Dichas normas pueden hacer uso del presente marco como se indica a continuación:

- las normas de tipo 1), 2), 3), 4) y 5) pueden emplear la terminología de este marco;
- las normas de tipo 2), 3), 4) y 5) pueden emplear las facilidades definidas en la cláusula 7 de este marco;
- las normas de tipo 5) pueden basarse en las clases de mecanismos definidas en la cláusula 8 de este marco.

Al igual que ocurre con otros servicios de seguridad, el de confidencialidad sólo puede ser prestado en el contexto de una política de seguridad definida para una aplicación determinada. Las definiciones de políticas de seguridad específicas quedan fuera del alcance de la presente Recomendación | Norma Internacional.

No es materia de esta Recomendación | Norma Internacional la especificación de los detalles de los intercambios de protocolo que es preciso efectuar para lograr la confidencialidad.

Tampoco se especifican en esta Recomendación | Norma Internacional mecanismos concretos de soporte de servicios de confidencialidad ni los detalles pormenorizados de los servicios y protocolos de gestión de la seguridad. Los mecanismos genéricos para sustentar la confidencialidad se describen en la cláusula 8.

Algunos de los procedimientos descritos en este marco de seguridad logran la confidencialidad mediante la aplicación de técnicas criptográficas. Este marco no depende de la utilización de un determinado algoritmo criptográfico o de otro tipo, si bien ciertas clases de mecanismos de confidencialidad pueden depender de las propiedades de algoritmos particulares.

NOTA – Aunque ISO no normaliza algoritmos criptográficos, sí normaliza los procedimientos utilizados para registrarlos en ISO/CEI 9979:1991, *Procedures for the registration of encipherment algorithms* (procedimientos para el registro de algoritmos de cifrado).

El presente marco trata de la provisión de confidencialidad cuando la información está representada por datos a los que los atacantes potenciales pueden acceder por lectura. El alcance de este marco incluye, la confidencialidad del flujo de tráfico.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación UIT-T X.233 (1993) | ISO/CEI 8473-1:1994, *Tecnología de la información – Protocolo para proporcionar el servicio de red sin conexión de interconexión de sistemas abiertos: Especificación del protocolo.*
- Recomendación UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de seguridad de la capa de red.*
- Recomendación UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Tecnología de la información – Intercambio de telecomunicaciones e información entre sistemas – Protocolo de seguridad de la capa de transporte.*
- Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general.*
- Recomendación UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de interconexión de sistemas abiertos para aplicaciones del CCITT.*
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic reference model – Part 2: Security Architecture.*

3 Definiciones

A los efectos de la presente Recomendación | Norma Internacional, se aplican las siguientes definiciones.

3.1 Definiciones del modelo de referencia básico

La presente Recomendación | Norma Internacional utiliza los siguientes términos generales relacionados con la seguridad, definidos en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

- a) conexión (N);
- b) entidad (N);
- c) facilidad (N);
- d) capa (N);

- e) unidad de datos de protocolo (N);
- f) unidad de datos de servicio (N);
- g) servicio (N);
- h) dato unidad (N);
- i) datos de usuario (N);
- j) segmentación.

3.2 Definiciones de arquitectura de seguridad

La presente Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.800 del CCITT | ISO 7498-2:

- a) amenaza activa;
- b) confidencialidad;
- c) descifrado (decipherment);
- d) descifrado (decryption);
- e) cifrado (encipherment);
- f) cifrado (encryption);
- g) política de seguridad basada en la identidad;
- h) clave;
- i) amenaza pasiva;
- j) control de encaminamiento;
- k) política de seguridad basada en reglas;
- l) sensibilidad;
- m) análisis de tráfico;
- n) relleno de tráfico.

3.3 Definiciones de la visión general de los marcos de seguridad

La presente Recomendación | Norma Internacional utiliza los siguientes términos generales relacionados con la seguridad, definidos en la Rec. UIT-T X.810 | ISO/CEI 10181-1:

- a) clave secreta;
- b) clave privada;
- c) clave pública.

3.4 Definiciones adicionales

A los efectos de la presente Recomendación | Norma Internacional se aplican las siguientes definiciones:

3.4.1 entorno de confidencialidad protegida: Entorno que impide la divulgación no autorizada de información ya sea impidiendo la inspección no autorizada de los datos o la obtención no autorizada de información sensible a través de la inspección de datos. La información sensible puede incluir algunos o todos los atributos de datos (por ejemplo, valor, tamaño o existencia).

3.4.2 datos de confidencialidad protegida: Datos dentro de un entorno de confidencialidad protegida.

NOTA – Un entorno de confidencialidad protegida puede proteger también algunos (o todos) los atributos de los datos de confidencialidad protegida.

3.4.3 información de confidencialidad protegida: Información cuyas codificaciones concretas (es decir, datos) son de confidencialidad protegida.

3.4.4 ocultación: Operación que aplica la protección de confidencialidad a datos no protegidos o protección de confidencialidad adicional a datos ya protegidos.

3.4.5 revelación: Operación que suprime parcial o totalmente la protección de confidencialidad aplicada previamente.

3.4.6 información de confidencialidad de ocultación: Información que se utiliza para realizar la operación **ocultación**.

3.4.7 información de confidencialidad de revelación: Información que se utiliza para realizar la operación **revelación**.

3.4.8 ataque directo: Ataque a un sistema basado en deficiencias de los algoritmos, principios o propiedades subyacentes de un mecanismo de seguridad.

3.4.9 ataque indirecto: Ataque a un sistema que no se basa en las deficiencias de un mecanismo de seguridad determinado (por ejemplo, ataques que evitan el mecanismo, o ataques que dependen de la utilización incorrecta del mecanismo por el sistema).

4 Abreviaturas

A los efectos de esta Recomendación | Norma Internacional se aplican las siguientes abreviaturas:

HCI	Información de confidencialidad de ocultación (<i>hiding confidentiality information</i>)
PDU	Unidad de datos de protocolo (<i>protocol data unit</i>)
RCI	Información de confidencialidad de revelación (<i>revealing confidentiality information</i>)
SDU	Unidad de datos de servicio (<i>service data unit</i>)

5 Análisis general de la confidencialidad

5.1 Conceptos básicos

El objetivo del servicio de confidencialidad es asegurar que la información esté a disposición solamente de aquellos que tienen autorización para acceder a la misma. En la medida en que la información se representa mediante datos y en la medida en que los datos pueden originar cambios contextuales (por ejemplo, las manipulaciones de los ficheros pueden resultar en cambios en el directorio o cambios en el número de ubicaciones de almacenamiento disponibles), puede derivarse información a partir de un dato de varias maneras diferentes:

- 1) interpretando la semántica del propio dato;
- 2) utilizando los atributos asociados del dato (por ejemplo, existencia, fecha de creación, tamaño, fecha de la última actualización, etc.) para facilitar las deducciones;
- 3) considerando que el contexto de los datos, es decir, aquellos otros objetos de datos que están asociados con él; y
- 4) observando las variaciones dinámicas de la representación.

La información puede ser protegida asegurando que los datos están limitados a los autorizados o representando los datos de manera que su semántica permanezca accesible solamente a aquellos que poseen alguna información crítica. La protección efectiva de la confidencialidad requiere que se proteja la información de control necesaria (tales como claves y otra RCI). Esta protección puede ser proporcionada por mecanismos que son diferentes de los utilizados para proteger los datos (por ejemplo, las claves criptográficas pueden ser protegidas por medios físicos).

En este marco se utilizan las nociones de entornos protegidos y de entornos protegidos superpuestos. Los datos dentro de entornos protegidos se protegen mediante la aplicación de un determinado mecanismo (o mecanismos) de seguridad. Todos los datos dentro de un entorno protegido se protegen de manera similar. Cuando dos o más entornos se superponen, los datos en la superposición tienen una protección múltiple. Cabe deducir que la protección continua de los datos que son trasladados de un entorno a otro debe entrañar entornos protegidos superpuestos.

5.1.1 Protección de la información

La comunicación o almacenamiento de información se realiza representando la información como ítems de datos. Los mecanismos de confidencialidad protegen contra la divulgación de la información protegiendo algunos o todos los ítems enumerados en 5.1 anterior.

Entre las maneras de lograr la confidencialidad figuran las siguientes:

- 1) prevención del conocimiento de la existencia de los datos o de características de los mismos (por ejemplo, el tamaño de los datos o su fecha de creación);
- 2) prevención del acceso a la lectura de los datos; y
- 3) prevención del conocimiento de la semántica de los datos.

Los mecanismos de confidencialidad protegen contra la divulgación de la información de una de las dos maneras siguientes:

- 1) protegiendo la representación del elemento de información contra su divulgación; o
- 2) protegiendo las reglas de representación contra la divulgación de las mismas.

En el segundo caso, la protección contra la divulgación de la existencia de un elemento de datos o de otros atributos del mismo puede conseguirse combinando varios elementos de datos en un elemento de datos compuesto y protegiendo las reglas de representación del objeto compuesto contra la divulgación de las mismas.

5.1.2 Operaciones de ocultación y revelación

La operación **ocultación** se puede modelar como un movimiento de información de un entorno A a la superposición (B) de A con otro entorno C. La operación **revelación** se puede considerar como la inversa de la operación ocultación. Esto se ilustra en el Anexo B.

Cuando la información es trasladada de un entorno protegido por un mecanismo de confidencialidad a un entorno protegido por otro mecanismo de confidencialidad:

- 1) si la operación **ocultación** del segundo mecanismo precede a la operación **revelación** del primero, la información está protegida continuamente; y
- 2) si la operación **revelación** del primer mecanismo precede a la operación **ocultación** del segundo, la información no está protegida continuamente.

Para que el caso 1) anterior sea posible, debe existir alguna forma de conmutatividad entre la **revelación** del mecanismo antiguo y la **ocultación** del nuevo. Un ejemplo en el que **ocultación** y **revelación** actúan con propiedades conmutativas se produce cuando un entorno está protegido mediante el control de acceso o por medios físicos y el otro está protegido mediante transformaciones criptográficas.

La confidencialidad influye en la extracción, transferencia y gestión de la información como se indica a continuación:

- 1) se proporciona confidencialidad en una transferencia de información que emplea la interconexión de sistemas abiertos cuando se combinan la operación **ocultación**, la transferencia mediante una facilidad (N-1) y la operación **revelación** para formar la parte transmisión de un servicio (N);
- 2) se proporciona confidencialidad en el almacenamiento y la extracción de datos cuando se combinan la operación **ocultación**, el almacenamiento y la extracción y la operación **revelación** para formar un servicio de almacenamiento y extracción de nivel superior;
- 3) pueden proporcionarse otras formas de confidencialidad combinando **ocultación** y **revelación** con otras operaciones (por ejemplo, las utilizadas para la gestión de datos).

Con algunos mecanismos de confidencialidad, la facilidad **ocultación** forma parte de los datos de confidencialidad protegida disponibles al usuario de servicio antes que la facilidad haya completado el procesamiento de todos los datos. De manera similar, con algunos mecanismos, la facilidad **revelación** puede comenzar a trabajar en el procesamiento de parte de un ítem de datos de confidencialidad protegida antes de que esté disponible la totalidad. De este modo, un ítem de datos puede consistir simultáneamente en partes que no están aún **ocultas**, partes que están **ocultas** y partes que han sido **reveladas**.

5.2 Clases de servicios de confidencialidad

Los servicios de confidencialidad se pueden clasificar según el tipo de protección de información que sustentan.

Los tipos de protección de la información son:

- 1) protección de la semántica de los datos;
- 2) protección de la semántica de los datos y de los atributos asociados;
- 3) protección de la semántica de los datos, de sus atributos y de cualquier información que pueda derivarse de los datos en cuestión.

Además, el servicio se puede clasificar según el tipo de amenazas que existen en el entorno en el cual funciona y contra el cual se protege la información. Con este criterio, los servicios se pueden clasificar como sigue:

1) *Protección contra amenazas externas*

En estos servicios se supone que los que tienen legítimo acceso a la información no la divulgarán a los que no están autorizados. Estos servicios no protegen la información divulgada a las partes autorizadas y no constriñen el comportamiento de estas partes mientras poseen la información previamente protegida.

Ejemplo: Los ficheros sensibles de A están protegidos con cifrado, pero los procesos que poseen las claves de descifrado requeridas pueden leer los ficheros protegidos y escribirlos a continuación en ficheros no protegidos.

2) *Protección contra amenazas internas*

En estos servicios se supone que los que están autorizados a acceder a información y datos críticos pueden voluntariamente o no realizar actividades que a la larga comprometan la confidencialidad de la información que se ha de proteger.

Ejemplo: Se asocian etiquetas y permisos de seguridad a los recursos que están protegidos y a las entidades que pueden acceder a los mismos. Los accesos están restringidos de acuerdo con un modelo de control de flujo bien definido e interpretado.

Los servicios que proporcionan protección de confidencialidad contra amenazas internas deben rechazar los canales protegidos (véase el Anexo D) o restringir su velocidad de transferencia de información dentro de niveles admisibles. Además, deben rechazar las deducciones no autorizadas que puedan venir de la utilización imprevista de canales de información legítimos [tales como deducciones basadas en indagaciones a bases de datos construidas cuidadosamente, cada una de las cuales es legítima individualmente, o deducciones basadas en la (in)capacidad de una facilidad del sistema de aplicar una instrucción].

5.3 Tipos de mecanismos de confidencialidad

El objetivo de los mecanismos de confidencialidad es impedir la divulgación no autorizada de información, para lo cual un mecanismo de confidencialidad puede:

1) Impedir el acceso a los datos (por ejemplo, mediante la protección física de un canal).

Se pueden utilizar mecanismos de control de acceso (descritos en la Rec. UIT-T X.812 | ISO/CEI 10181-3) para permitir que sólo las entidades autorizadas tengan acceso a los datos.

Las técnicas para la protección física están fuera del ámbito de esta Recomendación | Norma Internacional, aunque se incluyen en otras, como la ISO 10202 (*Security Architecture of Integrated Circuit Cards*) y ANSI X9.17 / ISO 8734 (*Financial Institution Key Management – Wholesale*).

2) Utilizar técnicas de correspondencia (transformación) que hagan que la información que ha de protegerse sea relativamente inaccesible a todos salvo a los que posean alguna información crítica sobre la técnica de correspondencia. Estas técnicas son:

- a) cifrado;
- b) relleno de datos;
- c) espectro ensanchado.

Se pueden utilizar mecanismos de confidencialidad de cualquier tipo junto con otros mecanismos del mismo tipo o de un tipo diferente.

Con los mecanismos de confidencialidad se puede lograr diferentes clases de protección:

- protección de la semántica de los datos;
- protección de los atributos de los datos (incluida la existencia de los datos); o
- protección contra las inferencias (deducciones).

Ejemplos de estas clases de mecanismo son:

- 1) cifrado para ocultar los datos;
- 2) cifrado junto con segmentación y relleno para ocultar la longitud de las unidades de datos de protocolo (PDU) (véase 8.2);
- 3) técnicas de espectro ensanchado para ocultar la existencia de un canal de comunicación.

5.4 Amenazas a la confidencialidad

Hay una sola amenaza genérica a la información de confidencialidad protegida, a saber, la divulgación de la información protegida. Hay varias amenazas a los datos de confidencialidad protegida que corresponden a las diferentes maneras en la cual la información de confidencialidad protegida se puede deducir a partir de los datos. A continuación se describen algunas de las amenazas a los datos de confidencialidad protegida en diferentes entornos.

5.4.1 Amenazas cuando la confidencialidad se proporciona impidiendo el acceso

Estas amenazas son:

- 1) la penetración del mecanismo que impide el acceso, por ejemplo:
 - a) aprovechando la fragilidad de los canales protegidos físicamente;
 - b) usurpando los certificados o utilizándolos indebidamente;
 - c) aprovechando la fragilidad de la aplicación del mecanismo que impide el acceso (por ejemplo, un usuario podría pedir acceso a un fichero A, y una vez que se le ha concedido el acceso a A, modificar el nombre del fichero presentado para acceder a otro fichero, B);
 - d) insertando «caballos de Troya» en el soporte lógico confiable;
- 2) la penetración de los servicios de los que depende el mecanismo que impide el acceso (por ejemplo, usurpación de identidad cuando el acceso se basa en autenticación de identidad, utilización impropia de certificados, o penetración del mecanismo de integridad utilizado para proteger los certificados);
- 3) la explotación de facilidades del sistema que pueden divulgar, directa o indirectamente, información sobre el mismo;
- 4) canales protegidos.

5.4.2 Amenazas cuando la confidencialidad se proporciona ocultando la información

Estas amenazas son:

- 1) la penetración del mecanismo criptográfico (ya sea mediante criptoanálisis, claves sustraídas, ataques a texto claro elegido, o por otros medios);
- 2) el análisis del tráfico;
- 3) el análisis de los encabezamientos de las PDU;
- 4) los canales protegidos.

5.5 Tipos de ataques a la confidencialidad

A cada una de las amenazas indicadas anteriormente corresponde uno o más ataques, a saber, la materialización de la amenaza en cuestión.

Es posible distinguir entre ataques activos y pasivos, es decir, ataques a la confidencialidad que tienen como resultado un cambio de sistema y ataques que no provocan ningún cambio de sistema.

NOTA – El carácter pasivo o activo de un ataque puede determinarse tanto por las características del sistema atacado como por las acciones llevadas a cabo por el atacante.

Ejemplos de ataques pasivos son:

- 1) las escuchas furtivas y las derivaciones telefónicas;
- 2) el análisis del tráfico.
- 3) el análisis de los encabezamientos de las PDU para fines no autorizados;
- 4) la copia de datos de las PDU no destinados al sistema de copia;
- 5) el criptoanálisis.

Ejemplos de ataques activos son:

- 1) los «caballos de Troya» (códigos cuyas características no documentadas facilitan rupturas de la seguridad);
- 2) los canales protegidos;
- 3) la penetración de los mecanismos que sustentan la confidencialidad, tal como el de autenticación (por ejemplo, usurpando con éxito la identidad de una entidad autorizada), penetración del mecanismo de control de acceso e interceptación de claves;
- 4) las invocaciones espurias de la facilidad criptográfica, tal como los ataques a texto claro elegido.

6 Políticas de confidencialidad

La política de confidencialidad es aquella parte de una política de seguridad que trata de la prestación y utilización del servicio de confidencialidad.

Los datos, que representan información y cuya confidencialidad se protege, están sometidos a control, superado el cual, las entidades pueden leerla. Una política de confidencialidad debe identificar, por consiguiente, la información que está sometida a control e indicar a qué entidades está previsto permitirles su lectura.

Dependiendo de la importancia relativa de la confidencialidad de los diferentes tipos de información, una política de confidencialidad puede indicar también el tipo y la intensidad de los mecanismos que han de utilizarse para prestar los servicios de confidencialidad con cada uno de esos tipos diferentes de información.

La gestión de las políticas de seguridad de confidencialidad no se trata en esta Recomendación | Norma Internacional.

6.1 Establecimiento de las políticas

Al establecer una política de confidencialidad se necesitan medios para identificar la información y las entidades implicadas.

Una política de seguridad se puede considerar como un conjunto de reglas. Cada regla de una política de confidencialidad puede asociar una caracterización de datos y una caracterización de entidades. En algunas políticas, estas reglas no se expresan de manera explícita sino que pueden derivarse de la propia política.

En las subcláusulas que siguen se describen varias maneras de establecer las políticas de confidencialidad. Obsérvese que, aunque algunos mecanismos de confidencialidad tienen un mecanismo paralelo en clases concretas de establecimiento de políticas, la manera de establecer una política no entraña directamente la utilización de un mecanismo específico para aplicarla.

6.1.1 Caracterización de la información

Una política puede identificar la información de diversas maneras. Por ejemplo:

- 1) identificando la entidad que la crea;
- 2) identificando el grupo de entidades que pueden leerla;
- 3) por su ubicación; o
- 4) identificando el contexto en el que se presentan los datos (por ejemplo, su función prevista).

6.1.2 Caracterización de las entidades

Hay muchas maneras de caracterizar las entidades que intervienen en una regla de política de confidencialidad. Dos procedimientos utilizados frecuentemente consisten en la identificación individual y exclusiva de cada entidad y en la asociación de atributos a cada una de ellas. Estas dos maneras de caracterizar las entidades originan otras dos clases de políticas: políticas basadas en la identidad y políticas basadas en reglas, respectivamente. Dichas políticas se analizan detalladamente en el marco de control de acceso (véase la Rec. UIT-T X.812 | ISO/CEI 10181-3).

7 Información y facilidades de confidencialidad

7.1 Información de confidencialidad

En 5.1.2 se examinan las operaciones **ocultación** y **revelación**. El Anexo B muestra, mediante la Figura B.1, el paso de datos de un entorno de confidencialidad protegida a otro utilizando esas operaciones.

Con algunos mecanismos de confidencialidad, las operaciones **ocultación** y **revelación** utilizan información auxiliar. Dicha información se conoce como información de confidencialidad de ocultación (HCI) e información de confidencialidad de revelación (RCI), respectivamente.

7.1.1 Información de confidencialidad de ocultación

La información de confidencialidad de ocultación (HCI) es la información utilizada por la operación **ocultación**.

Ejemplos de la misma son:

- 1) las claves públicas;
- 2) las claves simétricas;
- 3) la ubicación en la que han de almacenarse los datos; y
- 4) las reglas de segmentación.

7.1.2 Información de confidencialidad de revelación

La información de confidencialidad de revelación (RCI) es la información utilizada por la operación **revelación**.

Ejemplos de la misma son:

- 1) las claves privadas;
- 2) las claves simétricas;
- 3) la ubicación en la que estaban almacenados los datos; y
- 4) las reglas de segmentación.

7.2 Facilidades de confidencialidad

En el Anexo E se identifican varias facilidades de confidencialidad. Las facilidades de confidencialidad pueden dividirse en facilidades relacionadas con aspectos del funcionamiento y facilidades relacionadas con aspectos de la gestión.

7.2.1 Facilidades relacionadas con el funcionamiento

7.2.1.1 Ocultación

Esta facilidad protege la confidencialidad de los datos. Las entradas a esta facilidad son:

- 1) datos (posiblemente de confidencialidad protegida);
- 2) HCI;
- 3) identificadores específicos del mecanismo, como los mencionados en el Anexo E.

Las posibles salidas son:

- 1) datos de confidencialidad protegida;
- 2) otros resultados de la operación **ocultación** efectuada;
- 3) el identificador distintivo del entorno de confidencialidad protegida en el cual se han colocado los datos de confidencialidad protegida.

7.2.1.2 Revelación

Esta facilidad suprime la protección dada a los datos mediante una operación **ocultación** previa. Las posibles entradas son:

- 1) datos de confidencialidad protegida;
- 2) RCI;
- 3) identificadores específicos de mecanismo, como los mencionados en el Anexo E.

Las posibles salidas son:

- 1) datos (posiblemente de confidencialidad protegida);
- 2) otros resultados de la operación **revelación** efectuada;
- 3) el identificador distintivo del entorno en el cual se han colocado los datos de salida.

7.2.2 Facilidades relacionadas con la gestión

Las facilidades de gestión de la confidencialidad permiten a un usuario obtener, modificar y eliminar información HCI y RCI (por ejemplo, claves) necesaria para la provisión de la confidencialidad. En términos generales, estas facilidades son:

- 1) instalación de información de gestión;
- 2) modificación de información de gestión;
- 3) supresión de información de gestión;
- 4) listado de información de gestión.

8 Mecanismos de confidencialidad

La confidencialidad de los datos depende del medio en el que residen o por el que transitan. Por consiguiente:

- 1) la confidencialidad de datos almacenados puede asegurarse utilizando mecanismos que oculten la semántica (por ejemplo, el cifrado) o que fragmenten los datos;
- 2) la confidencialidad de datos en tránsito puede asegurarse utilizando mecanismos que impidan el acceso (tales como canales protegidos físicamente o el control del encaminamiento), mecanismos que oculten la semántica de los datos (por ejemplo, el cifrado) o mecanismos que dispersen los datos (por ejemplo, los saltos de frecuencias).

Estos mecanismos pueden utilizarse solos o combinados.

La clasificación anterior muestra que los mecanismos de confidencialidad pueden agruparse como sigue:

- 1) mecanismos que impiden el acceso no autorizado a los datos;
- 2) mecanismos de cifrado que ocultan los datos pero los dejan accesibles; y
- 3) mecanismos contextuales que hacen que los datos sean accesibles sólo parcialmente, de manera que no pueden ser recreados por completo a partir de un volumen limitado de datos acopiados.

8.1 Provisión de la confidencialidad mediante la prevención del acceso

La confidencialidad mediante la prevención del acceso puede conseguirse con el control de acceso, que se describe en la Rec. UIT-T X.812 | ISO/CEI 10181-3 o mediante la protección física de los medios y el control del encaminamiento que se describen a continuación.

8.1.1 Protección de la confidencialidad mediante la protección física de los medios

Pueden tomarse medidas de tipo físico para asegurar que los datos que residen en un determinado medio sólo pueden ser inspeccionados utilizando un conjunto de mecanismos específicos y limitados. La confidencialidad de los datos se consigue garantizando que sólo las entidades autorizadas podrán valerse de tales mecanismos.

8.1.2 Protección de la confidencialidad mediante el control del encaminamiento

La finalidad de este mecanismo es impedir la divulgación no autorizada de la información representada por los elementos de datos transferidos. El mecanismo sustenta la confidencialidad utilizando solamente facilidades fiables y seguras para encaminar los datos.

8.2 Provisión de la confidencialidad mediante el cifrado

La finalidad de estos mecanismos es impedir la divulgación de la semántica de los datos, tanto si están en tránsito como si están almacenados. Puede considerarse que estos mecanismos funcionan entre dos conjuntos de entidades:

- cualquier entidad del primer conjunto puede poseer los datos inicialmente (con acceso a la semántica); y
- cualquier entidad del segundo conjunto es un recipiente autorizado de la información que los datos representan.

Se han de considerar diferentes clases de mecanismos de confidencialidad:

- 1) mecanismos de confidencialidad basados en el cifrado simétrico, en el que se utiliza la misma clave para cifrar (operación **ocultación**) y para descifrar (operación **revelación**) los datos; y
- 2) mecanismos de confidencialidad basados en el cifrado asimétrico en el que se utiliza una clave pública para cifrar (operación **ocultación**) los datos y se utiliza la correspondiente clave privada para descifrarlos (operación **revelación**).

La principal distinción entre estas dos clases básicas de mecanismos es que, en 1), los mecanismos capaces de efectuar la operación **ocultación** son aquellos que pueden efectuar la operación **revelación** y viceversa, mientras que en 2) todos, o casi todos, pueden efectuar la operación **ocultación** y sólo los que tienen acceso a la clave privada pueden efectuar la operación **revelación**.

8.2.1 Provisión de la confidencialidad mediante el relleno de datos

La finalidad de este mecanismo es impedir el conocimiento de la información representada por el tamaño de un elemento de datos. Este mecanismo aumenta el tamaño de los elementos de datos de manera que el tamaño de un elemento de datos con relleno guarde poca relación con su tamaño original. Una manera de hacer esto consiste en añadir datos aleatorios al principio o al final del elemento de datos. Ha de hacerse de forma que el relleno sea reconocible como tal por las entidades autorizadas pero a las entidades no autorizadas les resulte indistinguible de los datos. Puede utilizarse, a tal fin, el relleno de datos junto con las transformaciones criptográficas.

Este mecanismo puede emplearse junto con la segmentación de datos que se describe en la Rec. UIT-T X.273 | ISO/CEI 11577.

El relleno de datos se puede utilizar para impedir que el tamaño de los elementos de datos se emplee como un canal protegido.

8.2.2 Provisión de la confidencialidad mediante eventos ficticios

La finalidad de este mecanismo es impedir las deducciones basadas en la frecuencia con la que se produce un determinado evento. Un ejemplo de este mecanismo se encuentra en los protocolos de seguridad de capa de red que tratan de ocultar el volumen de tráfico intercambiado por enlaces que no son fiables.

Este mecanismo produce seudoeventos (por ejemplo, PDU falsas) que sólo las partes autorizadas pueden identificar como tales. Este mecanismo se puede utilizar para contrarrestar ataques a canales protegidos que efectúan la señalización sobre la base de variaciones de la frecuencia de una actividad.

NOTA – El relleno de datos y de tráfico son ejemplos de este mecanismo. En ambos casos, el mecanismo esconde los atributos de un objeto insertándolo en otro mayor y protegiendo criptográficamente el conjunto.

8.2.3 Provisión de la confidencialidad mediante protección del encabezamiento de las PDU

La finalidad de este mecanismo es impedir deducciones basadas en encabezamientos de PDU durante la comunicación.

Un caso de este mecanismo es la ocultación de direcciones que se describe en la Rec. UIT-T X.273 | ISO/CEI 11577. Un sistema intermedio X puede recibir una PDU, cifrarla e insertarla en una nueva PDU cuyo origen parece ser X y cuyo destino parece ser Y, un sistema par donde los datos son descifrados y se recupera la PDU original. Como el encabezamiento original (incluidas las direcciones) está cifrado, no es posible ninguna deducción basada en la información de encabezamiento que no sea la consiguiente al hecho de que X e Y están intercambiando PDU cifradas.

Otro caso es cuando para cada PDU auténtica enviada por un sistema A, se crean n copias adicionales con direcciones de destino y opciones de encabezamiento diferentes (es decir, el sistema crea un tráfico ficticio; este mecanismo es también un ejemplo de los mecanismos descritos en 8.2.2).

La ocultación de la dirección en la capa de red se describe en la Rec. UIT-T X.273 | ISO/CEI 11577, aunque se puede realizar también en otras capas (véase la UIT-T X.411 | ISO/CEI 10021-4, relativa a sistemas de tratamiento de mensajes, describe la utilización de la ocultación de dirección en la capa de aplicación).

Este mecanismo contiene ideas similares a las expuestas en 8.3.

8.2.4 Provisión de confidencialidad mediante campos que varían en función del tiempo

Este mecanismo utilizado junto con el cifrado, protege contra deducciones basadas en las variaciones dinámicas de los ítems de datos. Para esto, combina los datos que se han de proteger con campos que varían en función del tiempo de modo que los ataques no pueden determinar si los cambios en la representación son causados por cambios de los datos o por cambios de los campos que varían en función del tiempo. Teóricamente, este mecanismo genera una representación de datos diferente para cada observación potencial significativa de los datos protegidos, de modo que se impiden también las deducciones basadas en la ausencia de variación dinámica. Como ejemplos cabe citar:

1) *Transmisión de PDU*

Se coloca un campo que varía en función del tiempo enfrente de la parte protegida de cada PDU; los datos combinados resultantes se cifran utilizando un mecanismo criptográfico con encadenamiento (es decir, el campo que varía afecta la incipción de los datos subsiguientes).

2) *Almacenamiento*

Los campos que varían en función del tiempo se colocan al principio de los ficheros almacenados, de modo que oculten los cambios (o la ausencia de cambios).

Este mecanismo se puede utilizar junto con relleno y segmentación para ocultar las variaciones del tamaño de los datos protegidos.

8.3 Provisión de confidencialidad mediante ubicación contextual

Se puede proporcionar una forma de protección de la confidencialidad impidiendo el acceso a los datos cuando éstos puedan ser encontrados en un gran número de diferentes contextos. Si no es factible (por motivos de cálculo o físicos) examinar todos los contextos posibles en el tiempo que precede al cambio del contexto utilizado, se puede obtener un cierto nivel de confidencialidad.

Como ejemplo de este mecanismo cabe citar:

- 1) la provisión de un gran número de canales físicos o virtuales a través de los cuales se transmite información (por ejemplo, utilización de «espectro ensanchado» de un gran número de radiofrecuencias);
- 2) la provisión de un gran número de ubicaciones para almacenamiento de los datos (por ejemplo, direcciones en un disco magnético);
- 3) la transmisión de información a través de canales de comunicación secundarios escondidos que son ocultados dentro de un canal de comunicación primario (esteganografía).

Esta forma de confidencialidad supone que los destinatarios no autorizados no pueden obtener la información necesaria para identificar el contexto correcto de un momento dado. Por consiguiente, esta información debe ser protegida por un servicio de confidencialidad.

9 Interacciones con otros servicios y mecanismos de seguridad

Esta cláusula describe cómo se pueden utilizar otros servicios y mecanismos de seguridad para sustentar la confidencialidad. No se describe la utilización de la confidencialidad para sustentar otros servicios de seguridad.

9.1 Control de acceso

Se puede utilizar el control de acceso descrito en la Rec. UIT-T X.812 | ISO/CEI 10181-3 para reglamentar el acceso a los datos.

Anexo A

Confidencialidad en el modelo básico de referencia de OSI

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

La relación entre servicios de seguridad y modelo de referencia de OSI se define en la Rec. X.800 del CCITT | ISO 7498-2. En este anexo se hace un resumen de lo que es pertinente en materia de confidencialidad.

Se consideran diferentes servicios de seguridad:

- confidencialidad en modo con conexión;
- confidencialidad en modo sin conexión;
- confidencialidad de campos seleccionados;
- confidencialidad del flujo de tráfico.

A.1 Confidencialidad en modo con conexión

Este servicio proporciona la confidencialidad de todos los datos de usuario (N) en una conexión (N).

A.2 Confidencialidad en modo sin conexión

Este servicio proporciona la confidencialidad de campos seleccionados en los datos de usuario (N) en una conexión (N) en una sola SDU (N) en modo sin conexión.

A.3 Confidencialidad de campos seleccionados

Este servicio proporciona la confidencialidad de campos seleccionados en los datos de usuario (N) en una conexión (N) o en una sola SDU (N) en modo sin conexión.

A.4 Confidencialidad del flujo de tráfico

Este servicio proporciona la protección de la información que pudiera derivarse de la observación de los flujos de tráfico.

A.5 Utilización de la confidencialidad en las capas de OSI

Los servicios de confidencialidad son pertinentes en las siguientes capas de OSI:

- capa física (capa 1);
- capa de enlace de datos (capa 2);
- capa de red (capa 3);
- capa de transporte (capa 4);
- capa de presentación (capa 6);
- capa de aplicación (capa 7).

A.5.1 Utilización de la confidencialidad en la capa física

Los servicios de confidencialidad en modo con conexión y de confidencialidad del flujo de tráfico, ya sea aislados o en combinación, son los únicos servicios de seguridad prestados en la capa física. La confidencialidad del flujo de tráfico adopta dos formas: confidencialidad del flujo de tráfico total, que sólo puede proporcionarse en algunos tipos de transmisión, y confidencialidad del flujo de tráfico limitada, que puede proporcionarse siempre.

A.5.2 Utilización de la confidencialidad en la capa de enlace de datos

Los servicios de confidencialidad en modo con conexión y de confidencialidad en modo sin conexión son los únicos servicios de seguridad prestados en la capa de enlace de datos. Estos servicios utilizan mecanismos de cifrado.

A.5.3 Utilización de la confidencialidad en la capa de red

Los servicios de confidencialidad en modo con conexión, confidencialidad en modo sin conexión y confidencialidad del flujo de tráfico son los únicos servicios prestados en la capa de red. La confidencialidad en modo con conexión y en la confidencialidad en modo sin conexión pueden proporcionarse mediante un mecanismo de cifrado y/o el control del encaminamiento. La confidencialidad del flujo de tráfico puede proporcionarse mediante un mecanismo de relleno de tráfico, en combinación con un servicio de confidencialidad en la capa de red, o por debajo de la misma y/o el control del encaminamiento. Estos servicios permiten la confidencialidad entre nodos de red, nodos de subred o relevadores.

A.5.4 Utilización de la confidencialidad en la capa de transporte

Los servicios de confidencialidad en modo con conexión y de confidencialidad en modo sin conexión son los únicos servicios de confidencialidad prestados en la capa de transporte. La confidencialidad en modo con conexión y la confidencialidad en modo sin conexión pueden proporcionarse mediante un mecanismo de cifrado. Estos servicios permiten la confidencialidad entre sistemas de extremo.

A.5.5 Utilización de la confidencialidad en la capa de presentación

En la capa de presentación pueden prestarse los servicios de confidencialidad en modo con conexión, confidencialidad en modo sin conexión y confidencialidad de campos seleccionados. En el caso de la confidencialidad de campos seleccionados, la indicación de qué campos han de ser de confidencialidad protegida es proporcionada por la capa de aplicación.

A.5.6 Utilización de la confidencialidad en la capa de aplicación

En la capa de aplicación se pueden prestar todos los servicios de confidencialidad, a saber, confidencialidad en modo con conexión, confidencialidad en modo sin conexión, confidencialidad de campos seleccionados y confidencialidad del flujo de tráfico. La confidencialidad en modo con conexión y la confidencialidad en modo sin conexión pueden proporcionarse mediante un mecanismo de cifrado de capa más baja. La confidencialidad de campos seleccionados puede proporcionar mediante un mecanismo de cifrado en la capa de presentación. Es posible apoyar un servicio de confidencialidad de tráfico limitada empleando un mecanismo de relleno de tráfico en la capa de aplicación, en combinación con un servicio de confidencialidad en una capa más baja.

Anexo B

Ejemplo de secuencia de movimientos a través de diferentes entornos de confidencialidad protegida

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

La Figura B.1 muestra un ejemplo de secuencia de operaciones **ocultación/revelación** que preservan la confidencialidad de los datos a medida que se desplazan de un entorno inicial A a un entorno E. En el ejemplo se supone que los entornos A y E sustentan la confidencialidad mediante el control de acceso, mientras que el entorno C protege la confidencialidad mediante el cifrado. Los entornos superpuestos B (A y C) y D (C y E) protegen los datos mediante el cifrado y el control de acceso.

El diagrama ilustra las operaciones que se indican a continuación:

- 1) una operación **ocultación**, t, que cifra los datos y los sitúa, de esa manera, en el entorno B superpuesto;
- 2) una operación **revelación**, u, que traslada los datos de B a C. Esta operación retira los datos del entorno protegido mediante control de acceso pero no afecta a la protección de la confidencialidad aplicada con la operación **ocultación** «t»;
- 3) una operación **ocultación**, v, que aplica de nuevo la protección mediante el control de acceso trasladando los datos al entorno D superpuesto, donde los datos quedan protegidos mediante el cifrado y el control de acceso de E;
- 4) una operación **revelación**, w, que descifra los datos y, de esa manera, los saca de D y los introduce en E.

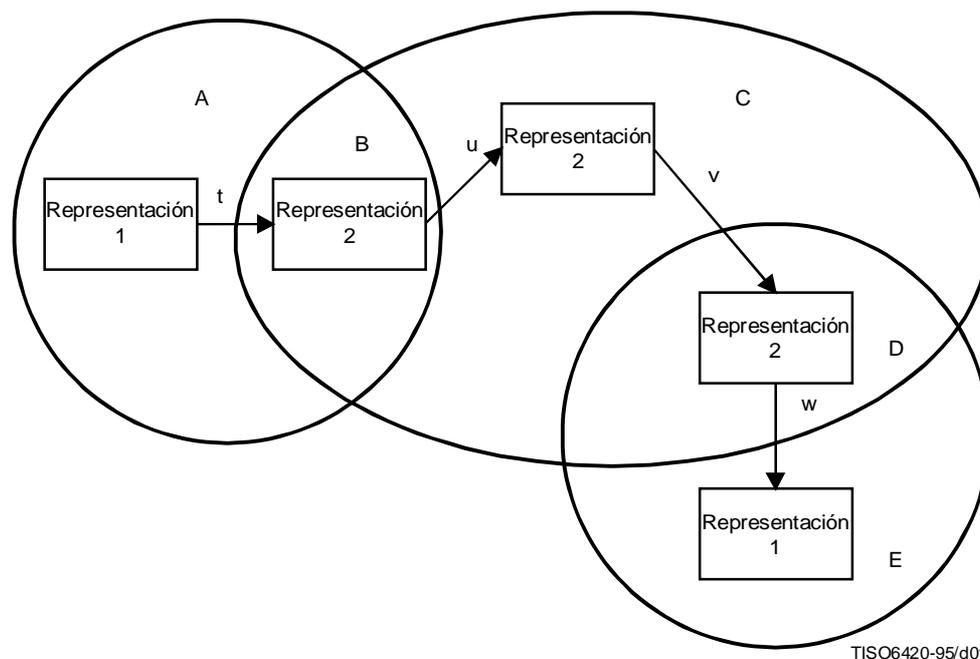


Figura B.1 – Ilustración de regiones protegidas

Anexo C

Representación de la información

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

La comunicación o el almacenamiento de un elemento de información se realiza utilizando una *representación* del elemento de información [por ejemplo, el número diecisiete puede codificarse como 17 decimal, 11 hexadecimal, el noveno entero impar, el séptimo número primo o 289 (17*17)]. La información puede obtenerse a partir de su representación o de los atributos de la misma. Es posible, por tanto, conseguir información de las siguientes maneras:

- 1) inspeccionando un valor de datos cuando se conocen los convenios de representación y la información conexas;
- 2) cerciorándose de si existe o no un elemento de datos;
- 3) por el tamaño de un elemento de datos;
- 4) mediante las variaciones dinámicas de las representaciones.

Por ejemplo, la información de que «el Rey ha muerto» podría deducirse como sigue:

- inspeccionando una expresión booleana cuyo valor es verdadero cuando el rey está muerto y falso en caso contrario;
- cerciorándose de la existencia o no de un fichero llamado «informe de la muerte del Rey» en un directorio de ficheros;
- inspeccionando una lista de monarcas muertos y observando que su longitud ha aumentado;
- estableciendo que se observa el cambio diario de un contador que indica el número total de días en los que el país ha permanecido sin monarca.

La correspondencia entre un elemento de información y alguna forma de representación del mismo se define mediante un conjunto de *reglas de representación*. Dichas reglas describen:

- cómo se codifica la información en datos;
- cómo puede hacerse que los datos restituyan la información que está codificada en los mismos; y
- qué cambios contextuales, explícitos e implícitos, deben introducirse cuando se codifica la información (por ejemplo, la creación de un fichero puede dar lugar a cambios en el directorio).

Los mecanismos de confidencialidad de los que trata el presente marco protegen cualquier elemento de información de una de las dos maneras siguientes:

- 1) protegiendo una representación del elemento de información contra su divulgación al garantizar que se halla dentro de un *entorno* apropiado; o
- 2) protegiendo el conocimiento de las reglas de representación contra la divulgación de las mismas.

Puede considerarse que diferentes entornos tienen diferentes resistencias, dependiendo del grado de protección contra la divulgación proporcionada a las representaciones en esos entornos. También puede considerarse que diferentes conjuntos de reglas de representación tienen diferentes resistencias, dependiendo del grado de dificultad que tiene el que las reglas de representación lleguen a ser conocidas por entidades no autorizadas.

Como base para la descripción de las características de diferentes tipos de mecanismos de confidencialidad se utiliza el concepto de *contexto de protección de la confidencialidad*. Un contexto de protección de la confidencialidad (de cualquier elemento de información) es una representación particular de ese elemento de información existente en un entorno determinado.

El comportamiento de los mecanismos de confidencialidad puede comprenderse reconociendo que la transferencia de la información entraña potencialmente el desplazamiento a través de una secuencia de diferentes contextos de protección de la confidencialidad.

Un cambio de representación o un cambio de entorno constituyen un movimiento de un contexto de protección de la confidencialidad a otro. El cambio de representación se producirá normalmente hacia una representación más fuerte (más protectora) o hacia una representación más débil (menos protectora). De manera similar, el cambio de entorno se producirá normalmente hacia un entorno más fuerte (más protector) o hacia un entorno más débil (menos protector).

En el Anexo B se da un ejemplo de movimiento a través de diferentes contextos de protección de la confidencialidad.

Anexo D

Canales protegidos

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

El término canales protegidos denomina a los mecanismos que no están destinados a ser utilizados para comunicación y que se pueden emplear para transferir información de manera que infringen la política de seguridad.

Los ataques a los canales protegidos son ataques efectuados dentro de un sistema por el emisor de algunos datos. Las agresiones de este tipo no se limitan a utilizar medios particulares de transferencia de la información, como los proporcionados normalmente para ese fin, de manera específica. En un entorno suficientemente complejo hay por lo general uno o más medios de transferencia de la información fuera de los mecanismos proporcionados para comunicar datos, almacenarlos y extraerlos. Esos medios se llaman canales protegidos.

Muchos de los canales protegidos conllevan la modulación autorizada de estados o eventos visible a entidades no autorizadas a recibir información del origen de esa modulación. La información se transfiere mediante un común entendimiento entre el origen y el recipiente del significado que ha de atribuirse a la modulación.

Entre los canales típicos de los mecanismos de comunicación de datos se incluye la atribución de significado:

- a los diferentes tamaños disponibles de PDU (N);
- a las diferentes direcciones de destino que pueden ser recibidas o interceptadas por el recipiente del canal protegido en conexiones (N) o transmisiones en modo sin conexión (N); y
- a las diferentes duraciones disponibles entre las transmisiones de las PDU (N) por la misma conexión (N) o desde la misma entidad (N).

Lo último es un ejemplo de canal protegido de temporización.

Entre los canales típicos de los mecanismos de almacenamiento y extracción de datos se incluye la atribución de significado:

- al nombre dado a una zona de almacenamiento;
- a la presencia o ausencia de datos almacenados con denominación específica;
- al volumen de datos almacenados;
- a la capacidad de aceptar nuevos datos para su almacenamiento;
- al tiempo durante el cual los datos denominados específicamente permanecen (o no permanecen) almacenados.

Los canales como los del primer ejemplo, en los que los datos (un nombre) pueden ser almacenados y recuperados a continuación, se denominan «canales protegidos de almacenamiento».

Los recursos del sistema y los protocolos de comunicación pueden ser especificados y modelados como objetos abstractos definidos para proporcionar un cierto número de operaciones de primitivas específicas. Por ello, de una manera más general, los canales típicos incluyen la atribución de significado:

- a la elección de una de las operaciones disponibles;
- al orden en que se utilizan las primitivas de servicio; y
- al tiempo entre utilizations de una operación, cuando son potencialmente visibles por el recipiente del canal especial.

La confidencialidad de la información sólo se puede garantizar cuando todos los medios de transferir información están identificados (incluidos los canales protegidos) y cada uno es controlado mediante el uso de mecanismos de confidencialidad adecuados.

En muchos casos, no es factible impedir completamente el acceso a canales protegidos (por razones técnicas, de organización, económicas, u otras). Sin embargo, puede ser factible reducir a niveles considerados aceptables la frecuencia a la cual se puede transmitir información a través de estos canales.

Anexo E

Reseña de facilidades de confidencialidad

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

Reseña de facilidades de seguridad		Elemento		Entidad: iniciador, verificador, confidencialidad-TTP	
				Función:	
				Objeto de información: datos de confidencialidad protegida	
		Objetivo del servicio	La información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados		
A C	Entidad	Autoridad del dominio de seguridad (SDA)			
	Función				
T I V	Actividad relacionada con la gestión	<ul style="list-style-type: none"> - Instalación de información de gestión - Modificación de información de gestión - Supresión de información de gestión 	<ul style="list-style-type: none"> - Listado de información de gestión - Inhabilitación de información de gestión - Rehabilitación de información de gestión 		
I D	Entidad	Iniciador	Verificador	Confidencialidad-TTP	
	Función				
A D	Actividad relacionada con el funcionamiento	<ul style="list-style-type: none"> - Ocultación de datos - Etiqueta de seguridad 	<ul style="list-style-type: none"> - Revelación de datos - Etiqueta de seguridad 	- Certificado de entidad	
I N F O	Elemento de datos de entrada/salida gestionado por la SDA	<ul style="list-style-type: none"> - Claves públicas - Claves simétricas - Etiqueta de seguridad 			
R M A	Tipo de información utilizada en la operación	<ul style="list-style-type: none"> - Información de confidencialidad de ocultación (HCI) - Información de confidencialidad de relevación (RCI) 			
C I Ó N	Información de control	<ul style="list-style-type: none"> - Tipo de mecanismo de confidencialidad protegida - Nivel de confidencialidad protegida 			

En este anexo se utilizan los siguientes conceptos.

E.1 Entidades de confidencialidad

La confidencialidad en sistemas abiertos comprende las siguientes entidades:

E.1.1 Iniciador

Entidad que genera datos de confidencialidad protegida para transmisión o almacenamiento.

E.1.2 Verificador

Entidad que extrae información a partir de datos de confidencialidad protegida.

E.1.3 Tercera parte confiable para facilidades de confidencialidad

Entidad que distribuye información de confidencialidad de ocultación o información de confidencialidad de revelación a entidades que intercambian datos de confidencialidad protegida.