



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

**X.810**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

(11/95)

**REDES DE DATOS Y COMUNICACIÓN  
ENTRE SISTEMAS ABIERTOS  
SEGURIDAD**

---

**TECNOLOGÍA DE LA INFORMACIÓN –  
INTERCONEXIÓN DE SISTEMAS ABIERTOS –  
MARCOS DE SEGURIDAD PARA SISTEMAS  
ABIERTOS: VISIÓN GENERAL**

**Recomendación UIT-T X.810**

(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.810 se aprobó el 21 de noviembre de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-1.

---

### 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
<b>REDES PÚBLICAS DE DATOS</b>	
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
<b>INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
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
<b>INTERFUNCIONAMIENTO ENTRE REDES</b>	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
<b>SISTEMAS DE TRATAMIENTO DE MENSAJES</b>	X.400-X.499
<b>DIRECTORIO</b>	X.500-X.599
<b>GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS</b>	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
<b>GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	X.700-X.799
<b>SEGURIDAD</b>	X.800-X.849
<b>APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
<b>TRATAMIENTO ABIERTO DISTRIBUIDO</b>	X.900-X.999



## ÍNDICE

		<i>Página</i>
1	Alcance.....	1
2	Referencias normativas .....	1
	2.1 Recomendaciones   Normas Internacionales idénticas.....	1
	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 la arquitectura de seguridad .....	2
	3.3 Definiciones adicionales .....	2
4	Abreviaturas .....	4
5	Notación .....	4
6	Organización .....	4
	6.1 Parte 1 – Visión general .....	5
	6.2 Parte 2 – Autenticación.....	5
	6.3 Parte 3 – Control de acceso.....	5
	6.4 Parte 4 – No repudio .....	5
	6.5 Parte 5 – Confidencialidad.....	6
	6.6 Parte 6 – Integridad.....	6
	6.7 Parte 7 – Alarmas y auditoría de seguridad .....	6
	6.8 Gestión de claves .....	7
7	Conceptos comunes.....	7
	7.1 Información de seguridad .....	7
	7.2 Dominio de seguridad .....	7
	7.2.1 Política de seguridad y reglas de política de seguridad.....	8
	7.2.2 Autoridad de dominio de seguridad .....	8
	7.2.3 Interrelación entre dominios de seguridad .....	8
	7.2.4 Establecimiento de las reglas de interacción seguras.....	9
	7.2.5 Transferencia de información de seguridad entre dominios .....	9
	7.3 Consideraciones relativas a la política de seguridad para servicios de seguridad específicos .....	10
	7.4 Entidades confiables .....	10
	7.5 Confianza .....	10
	7.6 Terceras partes confiables.....	11
8	Información de seguridad genérica .....	11
	8.1 Etiquetas de seguridad .....	11
	8.2 Valores de comprobación criptográficos .....	12
	8.3 Certificados de seguridad.....	12
	8.3.1 Presentación de certificados de seguridad.....	12
	8.3.2 Verificación y encadenamiento de certificados de seguridad .....	13
	8.3.3 Revocación de certificados de seguridad .....	13
	8.3.4 Reutilización de certificados de seguridad.....	13
	8.3.5 Estructura de los certificados de seguridad.....	13
	8.4 Testigo de seguridad .....	14
9	Facilidades de seguridad genéricas .....	14
	9.1 Facilidades relacionadas con la gestión .....	14
	9.1.1 Instalar SI.....	15
	9.1.2 Desinstalar SI.....	15
	9.1.3 Cambiar SI .....	15

	<i>Página</i>
9.1.4 Validar SI.....	15
9.1.5 Invalidar SI.....	15
9.1.6 Inhabilitar/rehabilitar un servicio de seguridad.....	15
9.1.7 Registrar.....	15
9.1.8 Desregistrar.....	15
9.1.9 Distribuir SI.....	15
9.1.10 Hacer lista de SI.....	15
9.2 Facilidades operacionales conexas.....	15
9.2.1 Identificar autoridades de seguridad confiables.....	15
9.2.2 Identificar reglas de interacción seguras.....	15
9.2.3 Adquirir SI.....	15
9.2.4 Generar SI.....	16
9.2.5 Verificar SI.....	16
10 Interacciones entre mecanismos de seguridad.....	16
11 Denegación de servicio y disponibilidad.....	17
12 Otros requisitos.....	17
Anexo A – Algunos ejemplos de mecanismos de protección para certificados de seguridad.....	18
A.1 Protección con un servicio de seguridad de las comunicaciones de OSI.....	18
A.2 Protección con un parámetro dentro del certificado de seguridad.....	18
A.2.1 Método de autenticación.....	18
A.2.2 Método de clave secreta.....	19
A.2.3 Método de la clave pública.....	19
A.2.4 Método de función unidireccional.....	19
A.3 Protección de los parámetros internos y externos durante el tránsito.....	19
A.3.1 Transferencia de los parámetros internos a la autoridad de seguridad expedidora.....	19
A.3.2 Transferencia de los parámetros externos entre entidades.....	19
A.4 Uso de los certificados de seguridad por una entidad o por grupos de entidades.....	20
A.5 Vinculación de un certificado de seguridad con accesos.....	20
Anexo B – Bibliografía.....	21

## **Resumen**

La presente Recomendación | Norma Internacional define el marco en el que se especifican los servicios de seguridad para los sistemas abiertos. Esta parte de los marcos de seguridad describe la organización del marco de seguridad, define los conceptos de seguridad que se requieren en más de una parte del marco de seguridad y describe la interrelación de los servicios y mecanismos identificados en otras partes del marco.

## **Introducción**

Muchas aplicaciones tienen necesidades de seguridad para proteger la comunicación de la información contra diversas amenazas. Algunas de las amenazas más conocidas, así como los servicios y mecanismos de seguridad que se pueden usar para protegerse contra ellas se describen en la Rec. X.800 del CCITT | ISO 7498-2.

Esta Recomendación | Norma Internacional define el marco en el que se especifican los servicios de seguridad para los sistemas abiertos.



## NORMA INTERNACIONAL

## RECOMENDACIÓN UIT-T

## TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: VISIÓN GENERAL

### 1 Alcance

Los marcos de seguridad tratan de la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde el término *sistemas abiertos* se considera que comprende sectores tales como bases de datos, aplicaciones distribuidas, procesamiento distribuido abierto e interconexión de sistemas abiertos. La finalidad de los marcos de seguridad es definir los medios para proporcionar protección a los sistemas y a los objetos dentro de los sistemas y así como a 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 elementos de datos y secuencias de operaciones (pero no de elementos de protocolo) que se utilizan para obtener servicios de seguridad específicos. Estos servicios de seguridad pueden aplicarse a las entidades comunicantes de sistemas, a los datos intercambiados entre sistemas y a los datos gestionados por sistemas.

Los marcos de seguridad sientan la base para futuras normalizaciones, puesto que proporciona terminología y definiciones coherentes de interfaces de servicios abstractos para requisitos de seguridad específicos y clasifican también los mecanismos que se pueden utilizar para satisfacer estos requisitos.

A menudo un servicio de seguridad depende de otros servicios de seguridad, lo que dificulta aislar una parte de seguridad de las otras. Los marcos de seguridad se relacionan con servicios de seguridad particulares, describen la gama de mecanismos que se puede utilizar para proporcionar los servicios de seguridad e identifican las interdependencias entre los servicios y los mecanismos. Para describir estos mecanismos puede ser necesario recurrir a un servicio de seguridad diferente y es de esta manera que los marcos de seguridad describen el resguardo de un servicio de seguridad con respecto a otro.

Esta parte de los marcos de seguridad:

- describe la organización de los marcos de seguridad;
- define los conceptos de seguridad que se necesitan en más de una parte de los marcos de seguridad;
- describe la interrelación entre los servicios y mecanismos identificados en otras partes de los marcos.

### 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 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 de la UIT 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.*

## 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

Las definiciones siguientes se utilizan en la visión general o son comunes a dos o más de las partes subsiguientes de los marcos de seguridad.

A los efectos de esta Recomendación | Norma Internacional son aplicables las siguientes definiciones.

### 3.1 Definiciones del modelo de referencia básico

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

- capa (N);
- entidad (N);
- unidad de datos de protocolo (N);
- proceso de aplicación;
- sistema abierto real;
- sistema real.

### 3.2 Definiciones de la arquitectura de seguridad

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

- control de acceso;
- disponibilidad;
- texto cifrado;
- valor de comprobación criptográfico;
- descifrado;
- denegación de servicio;
- firma digital;
- cifrado;
- amenaza interna;
- clave;
- gestión de claves;
- texto claro;
- amenaza externa;
- auditoría de seguridad;
- etiqueta de seguridad;
- política de seguridad;
- sensibilidad;
- amenaza.

### 3.3 Definiciones adicionales

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

**3.3.1 algoritmo criptográfico asimétrico:** Algoritmo para ejecutar el cifrado o el descifrado correspondiente, cuyas claves para el cifrado y el descifrado son diferentes.

NOTA – Con algunos algoritmos criptográficos asimétricos, el descifrado del texto cifrado o la generación de una firma digital requiere la utilización de más de una clave privada.

**3.3.2 autoridad de certificación:** Una autoridad que es confiable (en el contexto de una política de seguridad) para crear certificados de seguridad que contienen una o más clases de datos pertinentes a la seguridad.

**3.3.3 entidad condicionalmente confiable:** Una entidad que es confiable en el contexto de una política de seguridad, pero que no puede infringir la política de seguridad sin ser detectada.

**3.3.4 encadenamiento criptográfico:** Modo de utilización de un algoritmo criptográfico en el cual la transformación realizada por el algoritmo depende de los valores de las entradas o salidas previas.

**3.3.5 huella dactilar digital:** Característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características.

**3.3.6 identificador de distintivo:** Datos que identifican de manera única a una entidad.

**3.3.7 función de cálculo de clave:** Función (matemática) que transforma los valores de un conjunto de valores (posiblemente muy) grande en una gama de valores más pequeña.

**3.3.8 función unidireccional:** Función (matemática) cuyo cálculo es fácil pero que, cuando se conoce un resultado, no es factible, mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrados para obtenerlo.

**3.3.9 función de cálculo de clave unidireccional:** Función (matemática) que es a la vez una función unidireccional y una función de cálculo de clave.

**3.3.10 clave privada:** Clave que se utiliza con un algoritmo criptográfico asimétrico y cuya posesión está restringida (usualmente a una sola entidad).

**3.3.11 clave pública:** Clave que se utiliza con un algoritmo criptográfico asimétrico y que puede estar disponible públicamente.

**3.3.12 certificado de revocación:** Certificado de seguridad expedido por una autoridad de seguridad para indicar que un determinado certificado de seguridad ha sido revocado.

**3.3.13 certificado de lista de revocaciones:** Certificado de seguridad que contiene una lista de certificados de seguridad que han sido revocados.

**3.3.14 sello:** Valor de comprobación criptográfico que sustenta la integridad pero que no protege contra falsificaciones hechas por el destinatario (es decir, no proporciona servicios de no repudio). Cuando un sello está asociado con un elemento de datos, se dice que el elemento de datos está *sellado*.

NOTA – Aunque un sello por sí mismo no proporciona el no repudio, algunos mecanismos de no repudio utilizan el servicio de integridad proporcionado por los sellos, por ejemplo, para proteger las comunicaciones con terceras partes confiables.

**3.3.15 clave secreta:** Clave que se utiliza con un algoritmo criptográfico simétrico. La posesión de una clave secreta está restringida (usualmente a dos entidades).

**3.3.16 administrador de seguridad:** Persona que es responsable de la definición o aplicación de una o más partes de una política de seguridad.

**3.3.17 autoridad de seguridad:** Entidad que es responsable de la definición, aplicación o cumplimiento de la política de seguridad.

**3.3.18 certificado de seguridad:** Conjunto de datos pertinentes a la seguridad expedida por una autoridad de seguridad o tercera parte confiable, junto con información de seguridad que se utiliza para proporcionar servicios de integridad y autenticación de origen de los datos para los datos.

NOTA – Se considera que todos los certificados son certificados de seguridad (véanse las definiciones pertinentes en ISO 7498-2). Se adopta el término *certificado de seguridad* para evitar conflictos de terminología con la Rec. UIT-T X.509 | ISO/CEI 9594-8 (es decir, la norma de autenticación del directorio).

**3.3.19 cadena de certificados de seguridad:** Secuencia ordenada de certificados de seguridad, en la cual el primer certificado de seguridad contiene información pertinente a la seguridad y cada certificado de seguridad subsiguiente contiene información de seguridad que se puede utilizar para verificar certificados de seguridad previos.

**3.3.20 dominio de seguridad:** Un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad, donde el conjunto de elementos está sujeto a la política de seguridad, para las actividades especificadas y la política de seguridad es administrada por la autoridad de seguridad para el dominio de seguridad.

**3.3.21 autoridad de dominio de seguridad:** Autoridad de seguridad que es responsable de la aplicación de una política de seguridad para un dominio de seguridad.

**3.3.22 información de seguridad:** Información necesaria para prestar los servicios de seguridad.

**3.3.23 restablecimiento de seguridad:** Acciones que se ejecutan y procedimientos que se aplican cuando se detecta o se sospecha que se ha producido una infracción de la seguridad.

**3.3.24 reglas de interacción seguras:** Reglas de política de seguridad que reglamentan las interacciones entre dominios de seguridad.

**3.3.25 reglas de política de seguridad:** Una representación de una política de seguridad para un dominio de seguridad dentro de un sistema real.

**3.3.26 testigo de seguridad:** Conjunto de datos protegido por uno o más servicios de seguridad, junto con la información de seguridad utilizada para prestar esos servicios de seguridad, que se transfiere entre entidades comunicantes.

**3.3.27 algoritmo criptográfico simétrico:** Algoritmo para realizar el cifrado o el algoritmo correspondiente para realizar el descifrado en el cual se requiere la misma clave para el cifrado y el descifrado.

**3.3.28 confianza:** Se dice que la entidad X *confía* en la entidad Y para un conjunto de actividades solamente si la entidad X puede confiar en que la entidad Y se comporta de una manera particular con respecto a las actividades.

**3.3.29 entidad confiable:** Entidad que puede infringir una política de seguridad, ya sea porque ejecuta acciones indebidas o porque no ejecuta las acciones debidas.

**3.3.30 tercera parte confiable:** Autoridad de seguridad o su agente en la que se confía con respecto a algunas actividades pertinentes a la seguridad (en el contexto de una política de seguridad).

**3.3.31 entidad incondicionalmente confiable:** Entidad confiable que puede infringir una política de seguridad sin ser detectada.

## 4 Abreviaturas

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

ACI	Información de control de acceso ( <i>access control information</i> )
OSI	Interconexión de sistemas abiertos ( <i>open systems interconnection</i> )
ODP	Procesamiento distribuido abierto ( <i>open distributed processing</i> )
SI	Información de seguridad ( <i>security information</i> )
TTP	Tercera parte confiable ( <i>trusted third party</i> )

## 5 Notación

La notación de capa utilizada es igual a la definida en la Rec. UIT-T X.200 | ISO/CEI 7498-1.

El término *servicio* se utiliza para indicar un servicio de seguridad, cuando no se indica otro significado.

El término *certificado* se utiliza para indicar un certificado de seguridad, cuando no indica otro significado.

## 6 Organización

El marco de seguridad forma parte de una Norma Internacional (ISO/CEI 10181) que consta de múltiples partes y de una serie de Recomendaciones de la UIT. Los marcos de seguridad se describen a continuación. En el futuro se podrán identificar marcos de seguridad adicionales. El marco de gestión de claves no forma parte de ISO/CEI 10181, pero tiene un alcance similar y se incluye su descripción para que la norma sea completa.

## 6.1 Parte 1 – Visión general

Véase la cláusula 1.

## 6.2 Parte 2 – Autenticación

Este marco describe todos los aspectos de la autenticación aplicables a sistemas abiertos, la relación entre la autenticación y otras funciones de seguridad, como el control de acceso, y los requisitos de gestión de autenticación.

Este marco:

- a) define los conceptos básicos de la autenticación;
- b) identifica las clases posibles de mecanismos de autenticación;
- c) define los servicios de esas clases de mecanismo de autenticación;
- d) identifica los requisitos funcionales de los protocolos para el soporte de esas clases de mecanismo de autenticación; y
- e) identifica los requisitos de gestión generales de la autenticación.

El marco de autenticación ocupa la posición superior de la jerarquía de normas de autenticación que proporcionan los conceptos, la nomenclatura y una clasificación de los métodos de autenticación. Directamente por debajo, normas como ISO/CEI 9798 (mecanismos de autenticación de entidad) ofrecen un conjunto particular de esos métodos con más detalle. Por último, al final de la jerarquía, las normas como la Rec. UIT-T X. 509 | ISO/CEI 9594-8 (marco de autenticación de directorios) emplean esos conceptos y métodos en el contexto de una aplicación o requisito específico.

El marco de autenticación describe un modelo de autenticación, un número de fases que sirven para clasificar las actividades de autenticación, el uso de una tercera parte confiable, el uso de los certificados de autenticación para intercambiar información de autenticación, un servicio genérico de autenticación basado en esas fases, y por lo menos cinco clases de mecanismo de autenticación que prestan ese servicio. Se trata de mecanismos que ofrecen protección contra la divulgación de información de autenticación, y divulgación y reproducción en los mismos (y/o diferentes) verificadores.

## 6.3 Parte 3 – Control de acceso

Este marco describe todos los aspectos de control de acceso (por ejemplo, de usuario a procesos, de usuario a datos, de proceso a proceso, de proceso a datos) de los sistemas abiertos, la relación con otras funciones de seguridad, como la autenticación y la auditoría, y los requisitos de gestión de control de acceso.

Este marco:

- a) define los conceptos básicos de control de acceso;
- b) muestra la manera en que se pueden especializar los conceptos básicos de control de acceso para el apoyar algunos de los mecanismos y servicios comúnmente reconocidos;
- c) define esos servicios y los mecanismos correspondientes de control de acceso;
- d) identifica los requisitos funcionales para que los protocolos sustenten esos servicios y mecanismos de control de acceso;
- e) identifica los requisitos de gestión para sustentar esos servicios y mecanismos de control de acceso;
- f) trata de la interacción de los servicios y mecanismos de control de acceso con otros servicios y mecanismos de seguridad.

Este marco de seguridad describe un modelo de control de acceso, un número de fases que sirven para clasificar las actividades de control de acceso, un servicio genérico de control de acceso basado en esas fases, y por lo menos tres clases de mecanismos de control de acceso que proporcionan ese servicio. Esos mecanismos consisten en listas, capacidades y etiquetas de control de acceso.

## 6.4 Parte 4 – No repudio

Este marco refina y amplía los conceptos de los servicios de seguridad de no repudio descritos en la Rec. X.800 del CCITT | ISO 7498-2 y proporciona un marco para el desarrollo y la prestación de esos servicios.

## ISO/CEI 10181-1 : 1996 (S)

Este marco:

- a) define los conceptos básicos de no repudio;
- b) define los servicios generales de no repudio;
- c) identifica los posibles mecanismos de prestación de los servicios de no repudio;
- d) identifica los requisitos generales de gestión de los servicios y mecanismos de no repudio.

### 6.5 Parte 5 – Confidencialidad

La finalidad del servicio de confidencialidad es proteger la información contra divulgación no autorizada. Este marco trata de la confidencialidad de la información en la extracción, transferencia y gestión.

Este marco:

- a) define los conceptos básicos de confidencialidad;
- b) identifica posibles clases de mecanismos de confidencialidad;
- c) define las facilidades de cada clase de mecanismo de confidencialidad;
- d) identifica la gestión requerida para sustentar las clases de mecanismos de confidencialidad; y
- e) trata de la interacción del mecanismo de confidencialidad y de los servicios sustentadores con otros servicios y mecanismos.

Algunos de los procedimientos descritos en este marco de seguridad logran la confidencialidad mediante la aplicación de técnicas criptográficas. La utilización de este marco no depende de la utilización de uno u otro algoritmo criptográfico determinado, aunque determinadas clases de mecanismos de confidencialidad pueden depender de un algoritmo particular.

### 6.6 Parte 6 – Integridad

La propiedad de que los datos no han sido alterados o destruidos de una manera no autorizada se denomina integridad. Este marco trata de la integridad de los datos en la extracción, transferencia y gestión de la información.

Este marco:

- a) define el concepto básico de integridad;
- b) identifica posibles clases de mecanismos de integridad;
- c) define facilidades para cada clase de mecanismo de integridad;
- d) identifica la gestión requerida para sustentar las clases de mecanismos de integridad;
- e) trata de la interacción del mecanismo de integridad y de los servicios sustentadores con otros servicios y mecanismos.

Algunos de los procedimientos descritos en este marco de seguridad logran la integridad mediante la aplicación de técnicas criptográficas. La utilización de este marco no depende del uso de uno u otro algoritmo criptográfico particular, aunque determinadas clases de mecanismos de integridad pueden depender de las propiedades de un algoritmo particular.

La integridad tratada por este marco es la definida por la constancia de un valor de datos, y no por la constancia de la información que se considera representan los datos. Se excluyen otras formas de invarianza.

### 6.7 Parte 7 – Alarmas y auditoría de seguridad

Este marco:

- a) define los conceptos básicos de auditoría y alarmas de seguridad;
- b) proporciona un modelo general de auditoría y alarmas de seguridad;
- c) identifica la relación entre el servicio de auditoría y alarmas de seguridad y otros servicios de seguridad.

Al igual que en otros servicios de seguridad, la auditoría de seguridad sólo se puede proporcionar en el contexto de una política de seguridad definida. Las autoridades de seguridad son las que definen la política de seguridad dentro de su dominio de seguridad. Toda norma (o normas) que especifiquen mecanismos basados en este marco debe ser capaz de sustentar varias políticas de seguridad.

## 6.8 Gestión de claves

El marco de gestión de claves, que es la parte 1 de ISO/CEI 11770, tiene una relación especial con otros marcos de seguridad porque trata de funciones que no están relacionadas directamente con los servicios de seguridad identificados en la Rec. X.800 del CCITT | ISO 7498-2. Dichas funciones son aplicables en cualquier entorno de tecnología de la información donde sea apropiado el cifrado o la firma digital.

Este marco:

- a) identifica objetivos de gestión de claves;
- b) describe modelos generales en los cuales se basan los mecanismos de gestión de claves;
- c) define los conceptos básicos de gestión de claves comunes a todas las partes que componen esta norma;
- d) define servicios de gestión de claves;
- e) identifica las características de los mecanismos de gestión de claves;
- f) especifica los requisitos para la gestión del material de claves durante su ciclo de vida;
- g) describe un marco para la gestión de material de claves durante su ciclo de vida.

## 7 Conceptos comunes

Se necesitan muchos conceptos en más de una parte de los marcos de seguridad. Esta norma define estos conceptos para su utilización dentro de las partes restantes de esta Recomendación | Norma Internacional.

### 7.1 Información de seguridad

La información de seguridad (SI) es la información necesaria para prestar servicios de seguridad. Como ejemplos de información de seguridad cabe citar:

- reglas de política de seguridad;
- información para prestar servicios de seguridad específicos, tales como información de autenticación (AI, *authentication information*) e información de control de acceso (ACI, *access control information*);
- información pertinente a los mecanismos de seguridad, tales como etiquetas de seguridad, valores de comprobación criptográficos, certificados de seguridad y testigos de seguridad.

Los tipos de SI comunes a más de uno de los marcos de seguridad se examinan en la cláusula 8.

### 7.2 Dominio de seguridad

Un dominio de seguridad es un conjunto de elementos bajo una política de seguridad determinada, administrado por una sola autoridad de seguridad para algunas actividades específicas pertinentes a la seguridad. En las actividades de un dominio de seguridad intervienen uno o más elementos de ese dominio de seguridad y, quizás, elementos de otros dominios de seguridad.

Son ejemplos de actividades:

- el acceso a los elementos;
- el establecimiento o uso de conexiones de capa (N) de OSI;
- las operaciones relacionadas con una función de gestión específica;
- las operaciones de no repudio en las que interviene un notario.

Una actividad puede ser pertinente a la seguridad aunque en ese momento no esté bajo mecanismos que podrían ocasionar la aplicación de una política arbitraria relativa a su uso. En particular, son pertinentes a la seguridad aquellas actividades cuya realización entre cualquier grupo de elementos no se puede impedir y que pueden convertirse en objeto de mecanismos de control en el futuro.

Son ejemplos de elementos de un dominio de seguridad en un entorno de sistemas abiertos los elementos lógicos o físicos, como los sistemas abiertos reales, procesos de aplicación, entidades (N), unidades de datos de protocolo (N), retransmisores y personas que utilizan sistemas abiertos reales. Hay ocasiones en las que es preciso distinguir las personas de los demás elementos de un dominio de seguridad. En esos casos, se utiliza el término *objetos de datos* para los elementos no humanos.

### 7.2.1 Política de seguridad y reglas de política de seguridad

La política de seguridad expresa los requisitos de seguridad de un dominio de seguridad en términos generales. Por ejemplo, una política de seguridad puede identificar los requisitos aplicables a todos los miembros de un dominio de seguridad cuando funciona en condiciones especiales, o los aplicables a toda la información del dominio de seguridad. La aplicación de una política de seguridad resultará en la identificación de los servicios de seguridad que cumplen las prescripciones de la política de seguridad, y se elegirán los mecanismos de seguridad correspondientes para poner en marcha los servicios de seguridad. La decisión sobre los mecanismos que se han de elegir es determinada por las amenazas previstas y el valor de los recursos que hay que proteger.

Generalmente, las políticas de seguridad se formulan como principios generales en lenguaje natural. Estos principios reflejan los requisitos de seguridad de una organización particular o de los miembros de un dominio de seguridad. Antes de que estos requisitos se plasmen en sistemas abiertos reales, hay que perfeccionar la política de seguridad de forma que se pueda derivar de ella un conjunto de reglas de política de seguridad. La interpretación de estos requisitos como reglas de política de seguridad es una actividad de ingeniería. La política de seguridad restringe las actividades de los elementos sujetos a ella, ya sea porque exige ciertas actuaciones o porque prohíbe ciertas actividades. Una política de seguridad también puede autorizar a los elementos a que participen en ciertas actividades. Esta interpretación de la política de seguridad es más amplia que la de la Rec. X.800 del CCITT | ISO 7498-2, que sólo trata de la OSI. Los aspectos de política de seguridad que son específicos de un servicio de seguridad particular se analizan en el marco de seguridad correspondiente a ese servicio.

Hay dos tipos de reglas de política de seguridad para un dominio de seguridad: para actividades dentro de un dominio de seguridad y para actividades entre dominios de seguridad. Este último tipo de regla se llama «regla de interacción segura». La política de seguridad también define qué reglas son aplicables a las relaciones con todos los dominios de seguridad, y cuáles son aplicables a las relaciones con dominios de seguridad particulares.

Las reglas de política de seguridad mantendrán su validez a pesar de los cambios del sistema o de que se modifiquen las actividades y la política de seguridad del dominio de seguridad.

NOTA – Este marco no aborda los siguientes aspectos de política de seguridad:

- la parte que establece o mantiene una política de seguridad;
- los procedimientos para establecer o mantener una política de seguridad;
- el contenido de una política de seguridad;
- los procedimientos para vincular una política de seguridad a un dominio de seguridad.

### 7.2.2 Autoridad de dominio de seguridad

Una autoridad de dominio de seguridad es una autoridad de seguridad responsable de la aplicación de una política de seguridad en un dominio de seguridad.

Una autoridad de dominio de seguridad:

- puede ser una entidad compuesta; esa entidad debe ser identificable;
- según la política de seguridad a la que pueda estar sometida la autoridad de dominio de seguridad, puede delegar la responsabilidad de aplicar la política de seguridad en una o más entidades;
- tiene autoridad sobre los elementos del dominio de seguridad.

NOTA – Una política de seguridad puede ser nula si la autoridad de dominio de seguridad decide no imponer ninguna restricción.

Se dice que dos dominios de seguridad están vinculados cuando están obligados a coordinar sus políticas de seguridad.

### 7.2.3 Interrelación entre dominios de seguridad

Se considera que el concepto de dominio de seguridad es importante por dos razones:

- porque se puede utilizar para describir cómo se administra y gestiona la seguridad, y
- porque se puede utilizar como bloque de construcción para modelar las actividades pertinentes a seguridad que comprende elementos sujetos a autoridades de seguridad diferentes.

Los dominios de seguridad pueden estar relacionados de una o de varias maneras. A continuación se analizan algunas relaciones posibles de dominios de seguridad. Las relaciones entre dominios de seguridad se deben recoger en las políticas de seguridad de los dominios de seguridad tal como son convenidas por las autoridades de seguridad. Esas relaciones se expresan en forma de elementos y actividades de los dominios de seguridad y se reflejan en las reglas de interacción seguras correspondientes a cada uno de los dominios de seguridad. En el resto de esta cláusula se describen algunas relaciones de dominio de seguridad particulares. Pueden existir muchas relaciones de dominio de seguridad diferentes.

- a) Se dice que dos dominios de seguridad están *aislados* el uno del otro cuando no tienen objetos de datos y actividades en común y, por consiguiente, no pueden interactuar.
- b) Se dice que dos dominios de seguridad son *independientes* entre sí, si:
  - no tienen objetos de datos en común; y
  - las actividades dentro de cada dominio de seguridad están restringidas sólo por sus propias políticas de seguridad (y los conjuntos correspondientes de reglas de política de seguridad); y
  - las autoridades de seguridad de los dominios de seguridad no están obligadas a coordinar sus políticas de seguridad.

Dos o más dominios de seguridad independientes pueden concertar un acuerdo para coordinar la compartición de información entre ellos (véase 7.2.4).

- c) Se dice que el dominio de seguridad A es un *subdominio de seguridad* de otro dominio de seguridad B sólo si,
  - el conjunto de elementos de A es un subconjunto del conjunto de elementos de B, o si es igual a éste;
  - el conjunto de actividades de A es un subconjunto del conjunto de actividades de B, o si es igual a éste;
  - la autoridad de seguridad B delega en la autoridad de seguridad A la jurisdicción sobre A; y
  - la política de seguridad de A no está en conflicto con la política de seguridad de B. El dominio de seguridad A puede introducir políticas de seguridad adicionales en caso necesario y si se lo permite la política de seguridad de B.

NOTA 1 – Un subconjunto puede ser igual al conjunto completo. Un subdominio de seguridad puede estar formado, en un extremo, por el conjunto completo de elementos del superdominio de seguridad para algunas clases de actividades o, en el otro extremo, por todas las clases de actividades para algún subconjunto del conjunto de elementos del superdominio de seguridad. Entre estos dos extremos, pueden existir muchas variaciones.

- d) Se dice que el dominio de seguridad A es un *superdominio de seguridad* de otro dominio de seguridad B, sólo si B es un subdominio de seguridad de A.

NOTA 2 – Los marcos de seguridad no requieren que los conceptos de subdominio o superdominio aislados o independientes sean sustentados por cualquier protocolo, especificación o realización particular.

#### 7.2.4 Establecimiento de las reglas de interacción seguras

Para realizar el intercambio de información entre dominios de seguridad tiene que haber un conjunto acordado de reglas de política de seguridad. A esas reglas de política de seguridad se las llama «reglas de interacción seguras». Son parte de las reglas de política de seguridad de cada dominio de seguridad. Las reglas de interacción seguras permiten seleccionar mecanismos y servicios de seguridad comunes, quizás mediante negociación, y que los ítems de información de seguridad de cada dominio de seguridad estén relacionados entre sí, quizás mediante correspondencia. Los dominios de seguridad pueden intercambiar la información de gestión de seguridad necesaria para sustentar las reglas de interacción seguras. Según las relaciones entre dominios de seguridad, las reglas de interacción seguras se pueden determinar de maneras diferentes.

Para las interacciones seguras entre dominios de seguridad independientes, las autoridades de seguridad de esos dominios de seguridad tienen que concertar un acuerdo sobre las reglas de interacción seguras.

Para las interacciones seguras entre subdominios de seguridad, la autoridad de seguridad establecerá las reglas de interacción seguras correspondientes al superdominio de seguridad. Si la política de seguridad del superdominio de seguridad lo permite, los subdominios de seguridad podrán establecer sus propias reglas de interacción seguras.

#### 7.2.5 Transferencia de información de seguridad entre dominios

Las reglas de interacción seguras pueden ser por sí mismas información de seguridad, y puede que sea necesario transferir esa información de seguridad entre dominios de seguridad. Se consideran los casos siguientes:

- La semántica y la representación de la información de seguridad de cada dominio de seguridad son idénticas. Esto significa que la traducción es innecesaria.

- La semántica de la información de seguridad de cada dominio de seguridad es idéntica, pero las representaciones son diferentes. Esto significa que el método utilizado para describir la información de seguridad es diferente y, por ello, se necesita la traducción de sintaxis.
- Tanto la semántica como la representación de la información de seguridad de los dominios de seguridad son diferentes. Esto significa que las reglas de interacción seguras especificarán cómo se traducirá la información de seguridad de un dominio a la información de seguridad del otro dominio. Quizás también se necesite la traducción de sintaxis.

### 7.3 Consideraciones relativas a la política de seguridad para servicios de seguridad específicos

Se pueden utilizar mecanismos de control de acceso en algunas implementaciones de un servicio de integridad o de un servicio de confidencialidad. En estos casos, las reglas de política de seguridad relacionadas con la prestación de un servicio de integridad o de un servicio de confidencialidad deben describir cómo se utilizarán los mecanismos de control de acceso. Estos mecanismos se describen desde el punto de vista de los iniciadores y objetivos (en la Rec. UIT-T X.812 | ISO/CEI 10181-3). Las reglas de política de seguridad definen cómo las entidades, los elementos de información y de datos en las políticas de integridad y de confidencialidad están relacionados con los iniciadores y objetivos en los mecanismos de control de acceso.

Las políticas de confidencialidad se formulan desde el punto de vista de las entidades que pueden examinar ítems de información. Una acción ejecutada por un iniciador en un objetivo puede revelar información a una entidad de dos maneras. En primer lugar, el resultado de la acción puede proporcionar al iniciador alguna información sobre el objetivo. En segundo lugar, la petición de acción puede proporcionar al objetivo alguna información sobre el iniciador. Cuando se utilizan mecanismos de control de acceso para proporcionar un servicio de confidencialidad, se considera que las entidades que intentan obtener información son los iniciadores y los ítems de información son los objetivos.

Las políticas de integridad se formulan desde el punto de vista de las entidades que pueden modificar ítems de datos. Una acción realizada por un iniciador en un objetivo puede originar la modificación de datos de dos maneras. Primeramente, la acción puede hacer que se modifiquen directamente los datos contenidos dentro del objetivo. En segundo lugar, el resultado de la acción puede hacer que se modifique el contenido dentro del iniciador. Cuando se utilizan mecanismos de control de acceso para proporcionar un servicio de integridad, se considera que las entidades que intentan modificar los datos son los iniciadores y los ítems de datos son los objetivos.

### 7.4 Entidades confiables

Se dice que una entidad es *confiable* para algunas clases de actividad, en el contexto de una política de seguridad, si la entidad puede infringir la política de seguridad, ya sea ejecutando acciones que no debe ejecutar o dejando de ejecutar acciones que debe ejecutar. La política de seguridad define las entidades que son confiables y para cada entidad confiable define el conjunto de actividades para las cuales la entidad es confiable. Una entidad que es confiable para un determinado conjunto de actividades no es necesariamente confiable para todas las actividades dentro de un dominio de seguridad.

La declaración de una política de seguridad de que una entidad se comportará de una manera específica no asegura necesariamente que la entidad vaya a comportarse de esa manera. Por ello, la política de seguridad necesitará un medio para detectar las infracciones de la política de seguridad causadas por el mal comportamiento de una entidad confiable. Una entidad confiable que puede comportarse mal sin ser detectada se llama *entidad incondicionalmente confiable*. Una entidad confiable que puede infringir la política de seguridad, pero que no puede hacerlo sin ser detectada, se llama *entidad condicionalmente confiable*.

Una entidad confiable puede ser incondicionalmente confiable para un subconjunto de sus actividades y, al mismo tiempo, condicionalmente confiable para un subconjunto diferente de sus actividades. Esa entidad puede infringir algunos aspectos de la política de seguridad sin ser detectada, pero no puede infringir otros sin ser detectada.

Una política de seguridad de un dominio de seguridad puede declarar que un elemento que no está en el dominio de seguridad es confiable para algunos aspectos del dominio de seguridad. Las reglas de interacción seguras (analizadas en 7.2.4) definen la interacción entre las entidades del dominio de seguridad y las entidades confiables que están fuera del dominio de seguridad.

### 7.5 Confianza

Se dice que la entidad X *confía* en la entidad Y (para un conjunto de actividades) solamente si X confía en que Y se comporta de una manera determinada con respecto a las actividades.

La confianza no es necesariamente mútua. Una entidad en la que no se confía puede utilizar servicios proporcionados por una entidad confiable. Un ejemplo de una situación en la cual la confianza es mútua es cuando dos entidades confiables cooperan para realizar una actividad y cada una de ellas confía en que la otra la ayudará a aplicar la política de seguridad.

La confianza no es necesariamente transitiva. Una política de seguridad puede definir la transitividad de la relación de confianza en casos específicos. Si la entidad A confía en los servicios que proporciona la entidad B y la entidad confiable B confía en los servicios proporcionados por la entidad confiable C, A puede estar confiando indirectamente en que C se comporta de una manera determinada. Cuando esto es así, la confianza es transitiva. Sin embargo, en otras circunstancias B pudiera tomar medidas para asegurar que el comportamiento indebido de C no pueda afectar a las actividades de A. En este caso, la confianza no es transitiva.

## 7.6 Terceras partes confiables

Una tercera parte confiable es una autoridad de seguridad o su agente que es confiable (en el contexto de una política de seguridad) con respecto a algunas actividades pertinentes a la seguridad.

Como ejemplos de terceras partes confiables cabe citar:

- una tercera parte confiable en la autenticación;
- un notario o un servicio de sello fechador en el caso de no repudio;
- un centro de distribución de claves en la gestión de claves.

## 8 Información de seguridad genérica

Algunos tipos de información de seguridad se requieren en más de un marco de seguridad. A continuación se describen estos tipos de información de seguridad.

Los mecanismos de seguridad descritos en estos marcos de seguridad normalmente conllevan el intercambio de información de seguridad entre entidades que requieren servicios de seguridad para una interacción o entre una autoridad de seguridad y las entidades que interactúan. Los mecanismos descritos en estos marcos utilizan cuatro formas comunes de información de seguridad:

- etiquetas de seguridad para indicar la política de seguridad aplicable a un elemento, un canal de comunicación o un ítem de datos;
- valores de comprobación criptográficos para detectar las modificaciones de un ítem de datos;
- certificados de seguridad para proteger la información de seguridad obtenida de una autoridad de seguridad o de una tercera parte confiable, que usarán una o más partes que interactúan;
- testigos de seguridad para proteger la información de seguridad que se transmite entre las partes que interactúan.

NOTA – La información de seguridad se puede proteger mediante diferentes mecanismos de seguridad. Algunos mecanismos de seguridad se basan en la criptografía, y otros utilizan medios físicos.

### 8.1 Etiquetas de seguridad

Una etiqueta de seguridad es un conjunto de atributos de seguridad vinculado a un elemento, canal de comunicación o ítem de datos. La etiqueta de seguridad también indica, explícita o implícitamente, la autoridad de seguridad encargada de crear la vinculación y la política de seguridad aplicable al uso de la etiqueta. La etiqueta de seguridad se utiliza para apoyar una combinación de servicios de seguridad.

Son ejemplos de uso de la etiqueta de seguridad:

- apoyar un mecanismo de control de acceso basado en etiqueta de seguridad, incluida la aplicación del control de acceso para proporcionar integridad y/o confidencialidad;
- indicar el grado de confianza que se puede otorgar al dato, y sus requisitos de tratamiento;
- indicar la sensibilidad del dato y sus requisitos de tratamiento;
- indicar los requisitos de protección, eliminación y otros requisitos de tratamiento.

## 8.2 Valores de comprobación criptográficos

Un valor de comprobación criptográfico es la información que se obtiene realizando una transformación criptográfica en una unidad de datos. Los sellos, firmas digitales y huellas dactilares son tres ejemplos de valores de comprobación criptográficos.

Un sello es una forma de valor de comprobación criptográfico que se calcula utilizando un algoritmo criptográfico simétrico y una clave secreta compartida por las entidades comunicantes. Los sellos se utilizan para detectar la modificación de los datos durante la transferencia.

Una firma digital es un valor de comprobación criptográfico que protege contra las falsificaciones por el destinatario y se calcula utilizando una clave privada y un algoritmo criptográfico asimétrico. La validación de la firma digital requiere el mismo algoritmo criptográfico y la clave pública correspondiente.

NOTA 1 – Aunque hay otros medios de impedir que el destinatario falsifique un valor de comprobación criptográfico (por ejemplo, utilizando módulos criptográficos resistentes a las alteraciones), los marcos de seguridad utilizan el término firma digital para indicar un valor de comprobación criptográfico elaborado mediante un algoritmo criptográfico asimétrico.

NOTA 2 – Con algunos algoritmos criptográficos asimétricos, el cálculo de una firma digital requiere la utilización de más de una clave privada. Cuando se utilizan estos algoritmos, la posesión de cada una de las claves privadas puede estar restringida a diferentes entidades. Esto garantiza que las entidades deben cooperar para generar una firma digital.

Una huella dactilar digital es una característica de un ítem de datos que es suficientemente peculiar del ítem de datos de modo que no sea factible, mediante cálculo, encontrar otro ítem de datos con la misma huella dactilar digital. Es posible utilizar algunas formas de valor de comprobación criptográfico (por ejemplo, el resultado de la aplicación de una función unidireccional a los datos) para proporcionar una huella dactilar digital. Las huellas dactilares digitales pueden ser proporcionadas por medios distintos de los algoritmos criptográficos. Por ejemplo, una copia de un ítem de datos es una huella dactilar digital.

NOTA 3 – Las funciones unidireccionales no son equivalentes a huellas dactilares digitales. Algunas funciones unidireccionales no son adecuadas para crear huellas dactilares digitales, y algunas huellas dactilares digitales no se crean utilizando funciones unidireccionales.

NOTA 4 – El cálculo de una firma digital mediante un algoritmo asimétrico puede tomar mucho tiempo porque en general, los algoritmos asimétricos requieren mucho tiempo de cálculo. Una firma digital se puede calcular a partir de una huella dactilar digital de los datos en vez de los propios datos. Esto puede resultar mejor, pues puede ser más rápido calcular una firma digital de una huella dactilar digital corta que calcular una firma digital de un mensaje largo.

Un valor de comprobación criptográfico no protege necesariamente contra la reproducción de una unidad de datos. La protección contra la reproducción se puede lograr incluyendo en los datos alguna información que puede ser utilizada para detectar reproducciones, tales como número de secuencia o sello fechador, o utilizando encadenamiento criptográfico. Para la protección contra la reproducción, esta información debe ser comprobada por el destinatario de la unidad de datos protegida.

## 8.3 Certificados de seguridad

### 8.3.1 Presentación de certificados de seguridad

Un certificado de seguridad es un conjunto de datos pertinentes a la seguridad expedido por una autoridad de seguridad o una tercera parte confiable, junto con información de seguridad que se utiliza para proporcionar los servicios de integridad y autenticación de origen de los datos para los datos. Un certificado de seguridad contiene una indicación de los periodos de tiempo en los cuales los datos son válidos.

Los certificados de seguridad se utilizan para transportar información de seguridad de una autoridad de seguridad (o de una tercera parte confiable) a entidades que requieren esta información para ejecutar funciones de seguridad. Un certificado de seguridad puede contener información de seguridad para más de un servicio de seguridad.

Como se ha descrito en los otros marcos de seguridad, un certificado de seguridad puede contener información de seguridad (SI) para los siguientes fines:

- control de acceso;
- autenticación;
- integridad;
- confidencialidad;
- no repudio;
- auditoría;
- gestión de claves.

### 8.3.2 Verificación y encadenamiento de certificados de seguridad

La verificación de un certificado de seguridad consiste en validar su integridad mediante la verificación de la identidad alegada por el expedidor del certificado de seguridad y la comprobación de que el expedidor está autorizado a crear el certificado de seguridad. Estas operaciones pueden exigir la presencia de más SI.

Si el verificador de un certificado de seguridad no tiene toda la SI necesaria para verificarlo, puede obtener la SI que necesita de un certificado de seguridad de otra autoridad de seguridad. Este proceso se puede repetir para brindar una cadena de certificados de seguridad. Esta cadena contiene SI que suministra un camino seguro desde una autoridad de seguridad conocida (por ejemplo, una para la que ya se ha establecido SI) hasta la entidad que precisa la SI certificada.

Se utilizará una cadena de certificados de seguridad sólo cuando ésta cumple las restricciones impuestas por todas las políticas de seguridad correspondientes. La existencia de una cadena no es suficiente. Una cadena se utilizará sólo si ese uso está permitido por la relación de confianza entre el verificador de la cadena y las autoridades de seguridad que crearon los certificados de la cadena, y si también está permitido por la relación de confianza entre esas autoridades de seguridad. Esas relaciones las define la política de seguridad del verificador de la cadena de certificados y las políticas de seguridad de las autoridades de seguridad. En particular, a algunas autoridades de seguridad se les confía la expedición de certificados de seguridad para otras autoridades de seguridad, mientras que a otras se les confía la expedición de certificados de seguridad únicamente para las entidades que administran.

### 8.3.3 Revocación de certificados de seguridad

La SI contenida en un certificado de seguridad puede dejar de ser válida. Por ejemplo, si una clave privada está comprometida, entonces no se podrá utilizar la clave pública correspondiente y, por ello, habrá que revocar los certificados de seguridad que contienen esa clave pública.

El mecanismo para revocar los certificados de seguridad incluye la revocación de certificados y la revocación de la lista de certificados. Un *certificado de revocación* es un certificado de seguridad que indica que un certificado particular ha sido revocado. Un *certificado de lista de revocaciones* es un certificado de seguridad que identifica una lista de certificados de seguridad revocados.

### 8.3.4 Reutilización de certificados de seguridad

Algunos certificados de seguridad se pueden utilizar en apoyo de más de un caso de comunicación, mientras otros están destinados a ser utilizados solamente una vez. Un ejemplo de un certificado de seguridad que se puede utilizar más de una vez es el certificado de autenticación definido en la Rec. UIT-T X.509 | ISO/CEI 9594-8. Un ejemplo de un certificado de seguridad que sólo se puede utilizar una vez es un certificado de control de acceso que autoriza un solo acceso. Los certificados de seguridad que se han de utilizar solamente una vez pueden contener información para impedir su reutilización (por ejemplo, un número único).

### 8.3.5 Estructura de los certificados de seguridad

El formato general de un certificado de seguridad tiene tres componentes:

- información requerida en todos los certificados de seguridad;
- información de seguridad específica de uno o más servicios de seguridad;
- información para controlar o limitar el uso de la información de seguridad.

En todos los certificados de seguridad se requieren dos categorías de información:

- a) Información que proporciona la integridad y autenticación de origen de los datos (por ejemplo, un valor de comprobación criptográfico e indicaciones de la información que se ha de utilizar para verificarlo). Cuando se proporciona el servicio de autenticación de origen de los datos, se debe proporcionar también una indicación de la identidad de la fuente declarada del certificado de seguridad (es decir, la autoridad expedidora).
- b) Información que permite identificar un periodo de validez (por ejemplo, un periodo de validez explícito) u obtenerlo (por ejemplo, el tiempo de creación y un periodo de validez implícito). Esto impide la reutilización indefinida del certificado de seguridad, a pesar de que el certificado de seguridad se puede utilizar muchas veces dentro del periodo de validez.

La información empleada para controlar o limitar el uso de la información de seguridad se clasifica en tres categorías:

- a) *Información que protege el certificado de seguridad contra usos no autorizados*

Como ejemplos cabe citar:

- la información (por ejemplo, un identificador distintivo) que identifica a la entidad o entidades cuya SI está incluida en el certificado de seguridad;

- la información que identifica las entidades que están autorizadas a utilizar la SI contenida dentro del certificado de seguridad;
- la información que controla el número de veces que se puede emplear el certificado;
- la información que identifica la política de seguridad que rige el uso del certificado de seguridad;
- los métodos de protección y los parámetros asociados para proteger el certificado de seguridad contra robos (véanse más ejemplos en el Anexo A);
- la información utilizada para protección contra la reproducción (por ejemplo, un número único o una pregunta).

b) *Información que se puede utilizar para ayudar a una auditoría de seguridad*

Son ejemplos:

- un identificador de referencia de certificado de seguridad (por ejemplo, un número de serie) que es único para el certificado de seguridad con respecto a todos los certificados de seguridad expedidos por la misma autoridad o agente de seguridad;
- la identidad (a efectos de auditoría) de la entidad para la cual se expidió originalmente el certificado de seguridad.

c) *Información que se puede utilizar para ayudar a la recuperación de la seguridad*

Son ejemplos:

- un identificador de referencia de certificado de seguridad que se puede emplear para revocar un certificado de seguridad específico;
- un identificador de grupo de certificados de seguridad que se puede emplear para revocar un grupo de certificados de seguridad.

## 8.4 Testigo de seguridad

Un testigo de seguridad es un conjunto de datos protegidos por uno o más servicios de seguridad, junto con información de seguridad que se utiliza en la prestación de estos servicios de seguridad, que se transfiere entre entidades comunicantes. Los testigos de seguridad se pueden clasificar según el creador y según los servicios de seguridad que se utilizan para proteger su contenido.

Un testigo de seguridad expedido por una autoridad de seguridad y protegidos por los servicios de integridad y autenticación de origen de datos se llama «certificado de seguridad» (véase 8.3).

Muchos mecanismos de seguridad precisan un intercambio con integridad protegida de la información de seguridad entre dos entidades comunicantes, ninguna de las cuales es una autoridad de seguridad. Los testigos de seguridad empleados para conseguir esos intercambios con integridad protegida no son certificados de seguridad porque las entidades que los generaron no son autoridades de seguridad. Esos testigos de seguridad se llaman *testigos de seguridad con integridad protegida*.

Todos los testigos de seguridad con integridad protegida contienen la información siguiente:

- información que proporciona la integridad y la autenticación de origen de los datos (por ejemplo, un valor de comprobación criptográfico y una indicación de la información que se empleará para verificarlo).

Un testigo de seguridad con integridad protegida puede contener uno o más de los siguientes ítems de información adicional:

- información que permite identificar un periodo de validez;
- información empleada para la protección contra la reproducción (por ejemplo, un número único).

## 9 Facilidades de seguridad genéricos

Muchas facilidades son necesarias en más de un marco de seguridad. Esta cláusula define los medios que se emplearán en otros marcos de seguridad.

### 9.1 Facilidades relacionadas con la gestión

Esta subcláusula identifica los tipos genéricos de medios de gestión. Puede haber subclases de estos medios de gestión, que son específicas de un mecanismo de seguridad particular.

**9.1.1 Instalar SI**

Esta facilidad establece un conjunto inicial de SI vinculada a un elemento.

**9.1.2 Desinstalar SI**

Esta facilidad hace que se excluya una entidad de un dominio de seguridad mediante la revocación de la SI que declara que la entidad es un miembro del dominio de seguridad.

**9.1.3 Cambiar SI**

Esta facilidad se invoca para modificar la SI asociada a un elemento.

**9.1.4 Validar SI**

Esta facilidad vincula un conjunto de SI con un elemento. Puede invocarla una autoridad de seguridad o su agente.

**9.1.5 Invalidar SI**

Esta facilidad inhabilita cualquier uso de SI asociada a un elemento. Puede invocarla una autoridad de seguridad o su agente. La SI inhabilitada mediante invalidar SI puede permanecer almacenada dentro del sistema a efectos de auditoría y para asegurar que la SI se mantiene inhabilitada.

**9.1.6 Inhabilitar/rehabilitar un servicio de seguridad**

Estas facilidades inhabilitan y rehabilitan aspectos identificados de un servicio de seguridad.

**9.1.7 Registrar**

Esta facilidad hace que una autoridad de seguridad registre alguna información de seguridad asociada a una entidad. Puede invocarla una entidad diferente de la autoridad de seguridad. Por ejemplo, una entidad que desea incorporarse a un dominio de seguridad puede emplear la facilidad de registrar para notificar a una autoridad de seguridad que quiere incorporarse al dominio de seguridad.

**9.1.8 Desregistrar**

Esta facilidad hace que se excluya un elemento de un dominio de seguridad y que se revoque la SI asociada. Puede invocarla una autoridad de seguridad o su agente. Una política de seguridad puede requerir que ciertos tipos de SI no se destruyan nunca.

**9.1.9 Distribuir SI**

Esta facilidad es utilizada por una autoridad de seguridad o su agente para poner ítems de SI a disposición de otras entidades.

**9.1.10 Hacer lista de SI**

Esta facilidad hace una lista de la SI vinculada a un elemento determinado.

**9.2 Facilidades operacionales conexas****9.2.1 Identificar autoridades de seguridad confiables**

Esta facilidad identifica a las autoridades de seguridad que son confiables en el contexto de una política de seguridad para elementos específicos y para determinadas actividades de seguridad (por ejemplo, proporcionar claves de cifrado, proporcionar certificados de seguridad de control de acceso, o proporcionar certificados de seguridad de autenticación).

**9.2.2 Identificar reglas de interacción seguras**

Esta facilidad identifica las reglas de interacción seguras que se utilizarán. Esto puede realizarse a través de información establecida previamente o mediante negociación entre elementos de dominios relacionados entre sí, como se describe en 7.2.4.

NOTA – Las reglas de interacción seguras se establecen mediante acuerdo entre dominios de seguridad, y no mediante el uso de esta facilidad. Esta facilidad identifica las reglas de interacción seguras ya establecidas que son aplicables a una actividad determinada.

**9.2.3 Adquirir SI**

Esta facilidad adquiere SI antes de una actividad.

## ISO/CEI 10181-1 : 1996 (S)

Ejemplos de subclases de esta facilidad son:

- control de acceso: obtener iniciador ACI, obtener objetivo ACI;
- autenticación: adquirir.

### 9.2.4 Generar SI

Esta facilidad genera SI para una actividad conexas de seguridad específica. La SI puede estar vinculada a datos.

Ejemplos de subclases de esta facilidad son:

- control de acceso: vincular acción ACI;
- autenticación: generar;
- no repudio: generar pruebas.

### 9.2.5 Verificar SI

Esta facilidad verifica la validez de la SI producida por una invocación de la facilidad *generar SI*. La facilidad *verificar SI* puede producir por sí misma SI que ha de ser transferida a otra invocación de la facilidad *verificar SI*.

Ejemplos de subclases de esta facilidad son:

- control de acceso: verificar acción ACI;
- autenticación: verificar;
- no repudio: validar pruebas.

Un ejemplo de una situación en la cual la salida de la facilidad *verificar SI* se devuelve para ulterior verificación es un protocolo bidireccional para autenticación mutua. Se supone que las entidades A y B desean autenticarse entre sí, y A inicia el intercambio de protocolos. A invoca la facilidad *generar* para crear información de autenticación que contiene una prueba de la identidad de A y una pregunta a la que B tiene que responder. B invoca la facilidad *verificar* para comprobar que la pregunta vino de A y crea también un nuevo ítem de información de autenticación que contiene una prueba de la identidad de B y una respuesta a la pregunta de A. Seguidamente A invoca la facilidad *verificar* para procesar la respuesta de B. La facilidad *verificar* comprueba que la respuesta vino de B y que concuerda con la pregunta original.

## 10 Interacciones entre mecanismos de seguridad

A menudo sucede que se necesitan varios servicios de seguridad diferentes para un solo caso de comunicación. Esta necesidad se puede satisfacer utilizando un solo mecanismo de seguridad que proporciona múltiples servicios de seguridad, o utilizando simultáneamente varios mecanismos de seguridad diferentes.

Cuando se utilizan simultáneamente mecanismos de seguridad diferentes, a veces los mecanismos interactúan de manera adversa, lo cual puede ser aprovechado por un atacante. Es decir, los mecanismos que proporcionan un nivel de seguridad aceptable cuando se utilizan aisladamente pueden ser más vulnerables cuando se utilizan en combinación con otros mecanismos. A menudo sucede que dos mecanismos de seguridad se pueden combinar de maneras diferentes; las vulnerabilidades de los mecanismos combinados pueden diferir de acuerdo con la manera en la cual se combinan.

Un caso particularmente importante de una interacción entre mecanismos se produce cuando se combinan dos mecanismos criptográficos (por ejemplo, un mecanismo de integridad con un mecanismo de confidencialidad; o un mecanismo de no repudio con un mecanismo de confidencialidad). Las propiedades de seguridad de los mecanismos combinados depende del orden en el cual se aplican las dos transformaciones criptográficas.

En general, cuando se utilizan algoritmos criptográficos asimétricos, se debe aplicar una transformación de integridad o de no repudio al texto claro, y se deben cifrar después los datos firmados o sellados resultantes.

Un ejemplo de un caso en que es necesario aplicar dos servicios en el orden inverso (es decir, confidencialidad primero) es cuando los servicios se aplican entre diferentes entidades, y una entidad tiene que ser capaz de verificar la integridad del texto cifrado sin que se le permita conocer el texto claro. Esta situación puede producirse en sistemas de tratamiento de mensajes, donde un agente de transferencia de mensajes puede tener que verificar la integridad y el origen del mensaje sin que se le permita conocer el texto claro del mensaje.

La utilización de servicios de confidencialidad y de integridad en este orden inverso tiene el riesgo de que el servicio de integridad no pueda apoyar el no repudio. Si se desean los tres servicios, y es necesario el orden inverso de integridad y confidencialidad, es posible aplicar dos mecanismos de integridad, uno antes del mecanismo de confidencialidad y otro después. Un ejemplo de esta situación se produce en sistemas de tratamiento de mensajes. Si se proporciona confidencialidad, se pueden colocar dos firmas digitales diferentes en el mensaje (una calculada en el texto cifrado para consumo del agente de transferencia de mensajes y otra calculada en el texto claro para proporcionar al destinatario el no repudio de origen).

## 11 Denegación de servicio y disponibilidad

La denegación de servicio se produce cuando un servicio se encuentra por debajo del nivel requerido, incluso cuando se torna no disponible. Esa denegación de servicio puede obedecer a un ataque intencionado o a condiciones accidentales, como una tormenta o un terremoto. La disponibilidad es una condición en la que no hay denegación de servicio o empeoramiento de la calidad de las comunicaciones.

No siempre resulta posible prevenir una condición de denegación de servicio. Los servicios de seguridad se pueden emplear para detectar una denegación de servicio y tomar las medidas correctivas adecuadas. Esa detección puede no ser capaz de determinar si la condición es resultado de un ataque o de una condición accidental. Una política de seguridad particular puede requerir que cuando se identifica una denegación de servicio, se registre (a efectos de auditoría) y se envíe una alarma al procesador de alarmas.

Una vez identificada la denegación de servicio, los servicios de seguridad también se pueden emplear para corregirla y volver así a un nivel de servicio aceptable. Esta identificación y las medidas correctivas pueden implicar el uso de servicios de seguridad y de servicios de no seguridad (por ejemplo, reencaminar el tráfico por otros enlaces, pasar a medios de almacenamiento de reserva, o arrancar los procesadores de reserva).

Muchos tipos de servicio diferentes están sujetos a ataques de servicio, y los mecanismos que se emplean para prevenirlos varían según el tipo de aplicación que se protege. Esto significa que es imposible clasificar de forma general los mecanismos de protección contra la denegación de servicio y, por consiguiente, los marcos de seguridad individuales no los describen.

## 12 Otros requisitos

Se puede necesitar otras medidas de seguridad además de las descritas en estos marcos (por ejemplo, medidas de seguridad física y personal). La definición de los servicios de seguridad para sustentar esas medidas está fuera del alcance de esta Recomendación | Norma Internacional. La aplicación de esas medidas de seguridad adicionales puede incluso obviar la necesidad de emplear algunos servicios de seguridad descritos en estos marcos.

## Anexo A

### Algunos ejemplos de mecanismos de protección para certificados de seguridad

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

Un certificado de seguridad está expuesto a la posible amenaza de que un atacante alegue falsamente que es la entidad a la que se refiere ese certificado de seguridad. A este tipo de uso no autorizado de un certificado de seguridad se llama «robo del certificado de seguridad».

Esta amenaza puede provenir tanto del exterior como del interior. La amenaza externa consiste en que un atacante obtenga un certificado de seguridad al espiar las comunicaciones en las que no participa. La amenaza interna consiste en que una entidad que tiene la necesidad legítima de obtener un certificado (por ejemplo, para establecer la SI de una entidad con la que está comunicando), alegue falsamente que es la entidad a la que se refiere ese certificado de seguridad.

Una forma de proteger los certificados de seguridad contra robos es utilizar directamente los servicios de seguridad de las comunicaciones de OSI; otra consiste en emplear métodos de protección alternativos que necesitan parámetros adicionales, internos y externos, con relación al certificado de seguridad.

Se dice que un mecanismo de protección para certificados de seguridad apoya la delegación si una entidad que tiene el derecho a utilizar el certificado de seguridad puede transferir este derecho a otra entidad. Algunos de los mecanismos descritos en este anexo apoyan la delegación.

#### A.1 Protección con un servicio de seguridad de las comunicaciones de OSI

La amenaza de robo cometido por alguien ajeno al sistema se puede solucionar empleando un servicio de confidencialidad durante la transferencia del certificado de seguridad entre entidades comunicantes.

#### A.2 Protección con un parámetro dentro del certificado de seguridad

Hay varios métodos que se pueden utilizar para proteger los certificados de seguridad contra robos. Cada uno de esos métodos emplea parámetros internos contenidos en el certificado y asociados a parámetros externos. Los métodos específicos usados se indican en el certificado de seguridad.

Esos métodos son:

- autenticación;
- clave secreta;
- clave pública;
- función unidireccional.

Un certificado de seguridad puede usar una combinación de estos métodos.

##### A.2.1 Método de autenticación

En este método, el parámetro interno consiste en los identificadores que distinguen las entidades autorizadas a usar el certificado. El parámetro externo es el identificador distintivo de la entidad que trata de usar el certificado. Este parámetro externo es proporcionado por un servicio de autenticación. Facultativamente, el certificado puede contener parámetros internos adicionales, como el número de serie del certificado de autenticación que se utilizará en el proceso de autenticación.

El método de autenticación brinda la siguiente protección al certificado de seguridad:

- restringe el uso del certificado de seguridad a las entidades cuyos identificadores están incluidos en el certificado de seguridad.

Este método no permite a un usuario autorizado del certificado pasar su derecho a otra entidad, puesto que las entidades que pueden usar el certificado están fijadas en el momento en que se crea el certificado. Es decir que este método no admite la delegación.

**A.2.2 Método de clave secreta**

En este método, todo el certificado está cifrado mediante un algoritmo criptográfico simétrico. El parámetro externo de este método es la clave externa utilizada para cifrar el certificado.

El método de clave secreta brinda la protección siguiente al certificado de seguridad:

- restringe el uso del certificado de seguridad a las entidades que conocen el valor de la clave secreta (y que por tanto, pueden descifrar el certificado cifrado).

Este método admite la delegación, puesto que un usuario autorizado del certificado puede pasar su derecho a otra entidad dándole la clave secreta o el certificado descifrado.

**A.2.3 Método de la clave pública**

En este método, el parámetro interno es la clave pública. El parámetro externo es la clave privada correspondiente.

El método de clave pública brinda la protección siguiente al certificado de seguridad:

- restringe el uso del certificado de seguridad a las entidades que conocen el valor de la clave privada (y que por tanto, pueden calcular las firmas digitales mediante la clave privada).

Este método admite la delegación, puesto que un usuario autorizado del certificado puede pasar su derecho a otra entidad dándole la clave privada.

**A.2.4 Método de función unidireccional**

En este método, el parámetro interno es el resultado de aplicar una función unidireccional al parámetro externo. El parámetro interno se llama *clave de protección*, mientras que el parámetro externo se llama *clave de control*.

El método de función unidireccional brinda la protección siguiente al certificado de seguridad:

- restringe el uso del certificado de seguridad a las entidades que conocen el valor de la clave de control (y que por tanto, pueden probar que conocen el valor de la clave de control revelando su valor).

Este método admite la delegación, puesto que un usuario autorizado del certificado puede pasar su derecho a otra entidad dándole la clave de control.

**A.3 Protección de los parámetros internos y externos durante el tránsito**

Hay que considerar cuatro casos:

- Transferencia del parámetro interno a la autoridad expedidora antes de la creación del certificado. Este caso sólo es necesario cuando la autoridad expedidora no genera los parámetros interno y externo.
- Transferencia del parámetro externo de la autoridad expedidora después de la creación del certificado. Este caso sólo es necesario cuando la autoridad expedidora genera los parámetros interno y externo.
- Transferencia del parámetro externo entre entidades cuando se afirma el derecho a usar el certificado.
- Transferencia del parámetro externo entre entidades cuando se delega el derecho a usar el certificado.

**A.3.1 Transferencia de los parámetros internos a la autoridad de seguridad expedidora**

En el método de autenticación, el método de clave pública y el método de función unidireccional, el parámetro interno se puede comunicar a la autoridad de seguridad antes de colocarlo en el certificado de seguridad. La integridad del parámetro interno debe estar protegida durante la transferencia a la autoridad de seguridad.

En el método de clave secreta, el parámetro externo (o sea, la clave secreta) se puede comunicar a la autoridad de seguridad antes de la creación del certificado. Esta transferencia necesita protección de la integridad y de la confidencialidad.

**A.3.2 Transferencia de los parámetros externos entre entidades**

En el método de autenticación, el parámetro externo (o sea, la identidad del usuario del certificado) lo proporciona un mecanismo de autenticación.

En los métodos de clave secreta y función unidireccional, el parámetro externo debe ser transferido cuando se utiliza el certificado. Esto limita el uso del certificado de seguridad a aquellas entidades que conocen el valor correcto de la clave secreta o de la clave de control. La confidencialidad del parámetro externo debe estar protegida durante la transferencia entre entidades.

## ISO/CEI 10181-1 : 1996 (S)

Una diferencia entre estos dos métodos consiste en que con el método de clave secreta es necesario revelar el valor del parámetro externo antes de la verificación del valor de comprobación criptográfico del certificado de seguridad, mientras que en el método de función unidireccional, el valor de comprobación criptográfico se puede verificar antes de revelar el parámetro externo.

En el método de clave privada, no es necesario que el parámetro externo sea transferido entre entidades cuando se utiliza el certificado, puesto que una entidad puede probar que conoce la clave privada sin revelarla (mediante la creación de una firma digital). Con este método, el parámetro externo (la clave privada) sólo necesita ser transferido cuando se delega el derecho a usar el certificado. La confidencialidad de la clave privada debe estar protegida cuando se la transfiere entre entidades.

### A.4 Uso de los certificados de seguridad por una entidad o por grupos de entidades

Los métodos de protección descritos más arriba se pueden utilizar para restringir el uso de un certificado de seguridad a una sola entidad denominada o a un grupo de entidades denominadas:

- Un certificado de seguridad puede estar vinculado a una entidad especificada; la clave secreta, la clave privada o la clave de control se comunica a la entidad única en forma cifrada, y el identificador distintivo o los atributos de seguridad de la entidad aparecen en el certificado de seguridad.
- Un certificado de seguridad puede estar vinculado a un grupo de entidades; la clave secreta, la clave privada o la clave de control se comunica a los miembros en forma cifrada, y el identificador distintivo o los atributos de seguridad del grupo aparecen en el certificado de seguridad. Así, cualquier miembro del grupo puede utilizar el certificado de seguridad.

### A.5 Vinculación de un certificado de seguridad con accesos

Los certificados de seguridad se pueden usar para el control de acceso. En este caso, es importante establecer un vínculo seguro entre un certificado de seguridad y las peticiones de acceso que soporta. Cuando ese vínculo seguro no existe, el certificado de seguridad es vulnerable ante un ataque de reproducción, en el que un atacante transmite una copia de un certificado de seguridad genuino seguida de una petición de acceso falsificada.

Este ataque se puede impedir mediante un servicio de integridad que vincula el certificado de seguridad con el parámetro externo y la petición de acceso.

Cuando se utiliza el método de autenticación, esta vinculación se puede conseguir vinculando el intercambio de autenticación con el mecanismo de integridad; como se describe en el marco de autenticación (véase la Rec. UIT-T X.811 | ISO/CEI 10181-2).

Cuando se utiliza el método de clave secreta, esta vinculación se puede lograr incluyendo una clave para un mecanismo de integridad dentro del cuerpo del certificado de seguridad y utilizando esta clave para sellar la petición de acceso. Como otra posibilidad, la clave secreta (o una variante de la misma) se puede utilizar como la clave para un mecanismo de integridad.

NOTA – Si se usa la misma clave criptográfica con el mecanismo de integridad y el mecanismo de confidencialidad, se puede dar pie a que se produzcan ataques. Para protegerse contra esta amenaza se puede utilizar *variantes de clave*. Una variante de una clave criptográfica es otra clave criptográfica derivada de la original, pero que no es la misma.

Cuando se utiliza el método de función unidireccional, esta vinculación se puede lograr empleando la clave de control como clave del mecanismo de integridad basado en funciones unidireccionales.

Cuando se utiliza el método de la clave pública, esta vinculación se puede lograr empleando la clave privada para firmar las peticiones de acceso.

Con todos estos métodos, la vinculación del certificado de seguridad con el parámetro externo y la petición de acceso también se puede conseguir empleando un servicio de integridad prestado como parte de un servicio de comunicaciones de OSI.

## Anexo B

### Bibliografía

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

- Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación.*
- 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.*
- Recomendación UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio – Marco de autenticación.*
- ISO/CEI 11770-1<sup>1)</sup>, *Information technology – Security techniques – Key management Part 1: Key management framework.*
- ISO/CEI 9798-1:1991, *Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model.*

---

<sup>1)</sup> Se publicará.