



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.1121**

(04/2004)

SERIE X: REDES DE DATOS, COMUNICACIONES DE  
SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las telecomunicaciones

---

**Marco general de tecnologías de seguridad para  
las comunicaciones móviles de datos de  
extremo a extremo**

Recomendación UIT-T X.1121

---

RECOMENDACIONES UIT-T DE LA SERIE X

**REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD**

<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 declaraciones 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 de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.379
<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.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–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>	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
<b>SEGURIDAD</b>	
	X.800–X.849
<b>APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS</b>	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
<b>PROCESAMIENTO DISTRIBUIDO ABIERTO</b>	
	X.900–X.999
<b>SEGURIDAD DE LAS TELECOMUNICACIONES</b>	
	<b>X.1000–</b>

Para más información, véase la Lista de Recomendaciones del UIT-T.

## **Recomendación UIT-T X.1121**

### **Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo**

#### **Resumen**

Esta Recomendación describe las amenazas contra la seguridad en las comunicaciones móviles de datos de extremo a extremo y los requisitos de seguridad con relación al usuario móvil y al proveedor de servicio de aplicación (ASP, *application service provider*). Asimismo, esta Recomendación indica cuándo aplicar tecnologías de seguridad que realizan funciones de seguridad en los modelos de comunicaciones móviles de datos de extremo a extremo.

#### **Orígenes**

La Recomendación UIT-T X.1121 fue aprobada el 29 de abril de 2004 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

## 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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

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.

## 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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2005

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	1
3.1 Definiciones de arquitectura de seguridad del modelo de referencia OSI .....	1
3.2 Definiciones adicionales.....	2
4 Abreviaturas, siglas acrónimos .....	3
5 Visión de conjunto.....	3
6 Modelos de comunicación móvil de datos de extremo a extremo.....	3
6.1 Modelo general de comunicación móvil de datos de extremo a extremo entre el usuario móvil y el ASP .....	4
6.2 Modelo de pasarela de comunicación móvil de datos de extremo a extremo entre un usuario móvil y el ASP.....	4
7 Características de la comunicación móvil de datos de extremo a extremo .....	4
8 Amenazas contra la seguridad en el entorno móvil .....	5
8.1 Amenazas generales contra la seguridad .....	5
8.2 Amenazas contra la seguridad en servicios móviles .....	6
8.3 Relación entre amenazas contra la seguridad y modelos de comunicación de extremo a extremo .....	7
9 Requisitos de seguridad para comunicaciones móviles de datos de extremo a extremo .....	8
9.1 Requisitos de seguridad desde el punto de vista del usuario móvil .....	8
9.2 Requisitos de seguridad desde el punto de vista del ASP.....	12
9.3 Relación entre los requisitos de seguridad y las amenazas contra la seguridad.....	15
10 Funciones de seguridad para satisfacer los requisitos de seguridad en sistemas móviles.....	16
11 Tecnologías de seguridad para comunicaciones móviles de datos de extremo a extremo .....	20



# Recomendación UIT-T X.1121

## Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo

### 1 Alcance

Esta Recomendación proporciona requisitos de seguridad para el usuario móvil y para el proveedor de servicio de aplicación en la capa superior del modelo de referencia OSI para las comunicaciones móviles de datos de extremo a extremo entre un terminal móvil en una red móvil y un servidor de aplicación en una red abierta.

La presente Recomendación proporciona un marco de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo.

Esta Recomendación no proporciona los detalles de componentes de red móvil salvo para el acceso de red inalámbrica a un terminal móvil cuando se conecta a una red abierta.

### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

- Recomendación UIT-T Q.1701 (1999), *Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- Recomendación UIT-T Q.1711 (1999), *Modelo funcional de red para las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- Recomendación UIT-T Q.1761 (2004), *Principios y requisitos para la convergencia de sistemas fijos e IMT-2000 existentes*.
- Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.
- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*.
- 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*.

### 3 Definiciones

#### 3.1 Definiciones de arquitectura de seguridad del modelo de referencia OSI

Los siguientes términos se definen en la Rec. UIT-T X.800:

- a) control de acceso;
- b) autenticación;
- c) información de autenticación;
- d) intercambio de autenticación;

- e) autorización;
- f) disponibilidad;
- g) confidencialidad;
- h) criptografía;
- i) integridad de los datos;
- j) autenticación del origen de los datos;
- k) cifrado;
- l) integridad;
- m) clave;
- n) intercambio de claves;
- o) gestión de claves;
- p) no repudio;
- q) notarización;
- r) contraseña;
- s) privacidad

## 3.2 Definiciones adicionales

En esta Recomendación se definen los siguientes términos:

**3.2.1 anonimato:** Posibilidad que permite el acceso anónimo a servicios con el objeto de no descubrir la información personal y comportamiento del usuario, tales como su localización, frecuencia de utilización de un servicio, etc.

**3.2.2 apropiación furtiva de datos:** Amenaza contra la seguridad por la cual una persona recoge información en lugares públicos mediante la observación furtiva del teclado, lectura de la pantalla o escucha de un terminal móvil.

**3.2.3 terminal móvil:** Entidad que tiene una función de acceso de red inalámbrica y conecta una red móvil para comunicación de datos con servidores de aplicación u otros terminales móviles.

**3.2.4 red móvil:** Red que proporciona puntos de acceso de red inalámbrica a terminales móviles.

**3.2.5 usuario móvil:** Entidad (o persona) que utiliza y opera el terminal móvil para la recepción de diversos servicios procedentes de proveedores de servicios de aplicación.

**3.2.6 servicio de aplicación:** Servicios tales como banca móvil, comercio móvil, etc.

**3.2.7 servidor de aplicación:** Entidad que se conecta a una red abierta para comunicaciones de datos con terminales móviles.

**3.2.8 proveedor de servicio de aplicación (ASP):** Entidad (persona o grupo) que suministra servicios de aplicación a usuarios móviles a través de un servidor de aplicación.

**3.2.9 pasarela de seguridad móvil:** Entidad que encamina comunicaciones de datos entre un terminal móvil y un servidor de aplicación, modifica los parámetros de seguridad o del protocolo de comunicación de una red móvil a una red abierta, o viceversa, y que puede realizar funciones de gestión de normativa de seguridad para comunicaciones móviles de datos de extremo a extremo.

**3.2.10 gestión de normativas de seguridad:** Función para gestionar o negociar un conjunto de normas destinadas a proporcionar servicios de seguridad clasificados que se pueden aplicar en la pasarela de seguridad móvil u otro servidor.

#### **4 Abreviaturas, siglas o acrónimos**

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

ASP	Proveedor de servicio de aplicación ( <i>application service provider</i> )
DoS	Denegación de servicio ( <i>denial of service</i> )
IMT-2000	Telecomunicaciones móviles internacionales-2000 ( <i>international mobile telecommunications-2000</i> )
LAN	Red de área local ( <i>local area network</i> )
OSI	Interconexión de sistemas abiertos ( <i>open systems interconnection</i> )
PC	Computador personal ( <i>personal computer</i> )
PDA	Asistente personal de datos ( <i>personal data assistant</i> )
PIN	Número de identificación personal ( <i>personal identification number</i> )

#### **5 Visión de conjunto**

Los terminales móviles con capacidad de comunicación de datos (como teléfonos móviles IMT-2000, computador portátil o agenda personal de datos con tarjeta de radiocomunicación) se han difundido ampliamente y diversos servicios de aplicación (por ejemplo, comercio electrónico móvil) se suministran a través de la red móvil. En aplicaciones de comercio electrónico, la seguridad es necesaria e indispensable.

Hay muchos temas en estudio relacionados con el operador móvil (por ejemplo, arquitectura de seguridad en la red telefónica móvil IMT-2000). Sin embargo, es también importante investigar desde la óptica del usuario móvil y del ASP.

Cuando se estudia la seguridad de una comunicación móvil desde el punto de vista del usuario móvil o del ASP, la seguridad de una comunicación móvil de datos de extremo a extremo entre un terminal móvil y un servidor de aplicación es uno de los aspectos más importantes.

Además, para el sistema móvil que conecta una red móvil a una red abierta, es necesario estudiar la seguridad en las capas superiores (capas de aplicación, presentación y sesión) del modelo de referencia OSI pues hay diversas aplicaciones de red móvil (por ejemplo, red telefónica móvil IMT-2000, LAN inalámbrica, tecnología Bluetooth) o red abierta.

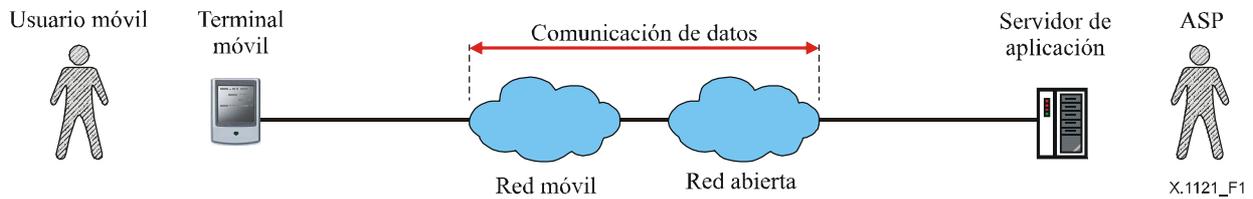
Esta Recomendación describe las amenazas contra la seguridad que pueden afectar a las comunicaciones móviles de datos de extremo a extremo y los requisitos de seguridad desde el punto de vista del usuario móvil y del ASP. Asimismo, esta Recomendación indica cuándo se presentan las tecnologías de seguridad que efectúan algunas funciones de seguridad en los modelos de comunicación móvil de datos de extremo a extremo.

#### **6 Modelos de comunicación móvil de datos de extremo a extremo**

Antes de describir las tecnologías de seguridad en comunicaciones móviles, se deben definir los modelos de comunicación móvil de datos de extremo a extremo. Los modelos de comunicación móvil de datos de extremo a extremo clarifican la relación entre entidades en modelos y los puntos a los cuales se deben adaptar las tecnologías de seguridad.

## 6.1 Modelo general de comunicación móvil de datos de extremo a extremo entre el usuario móvil y el ASP

El modelo general de comunicación móvil de datos de extremo a extremo y el ASP se ilustra en la figura 1.



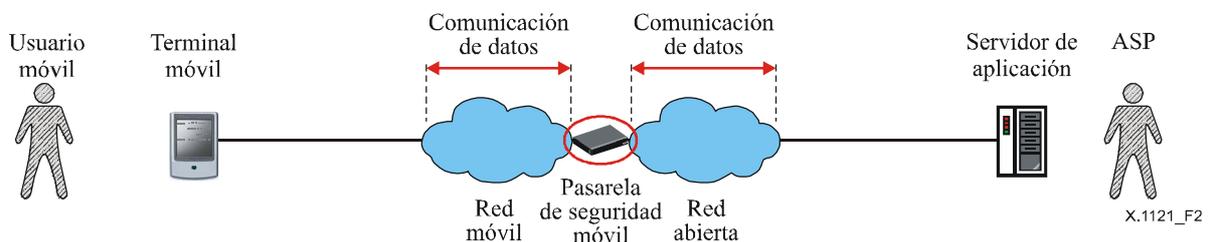
**Figura 1/X.1121 – Modelo general de comunicación móvil de datos de extremo a extremo entre un usuario móvil y el ASP**

En este modelo hay seis entidades: usuario móvil, terminal móvil, red móvil, red abierta, servidor de aplicación y ASP.

Asimismo, hay cinco relaciones entre: usuario móvil y terminal móvil, terminal móvil y red móvil, red móvil y red abierta, red abierta y servidor de aplicación, y terminal móvil y servidor de aplicación.

## 6.2 Modelo de pasarela de comunicación móvil de datos de extremo a extremo entre un usuario móvil y el ASP

En la figura 2 se muestra otro modelo (modelo de pasarela) de comunicación móvil de datos de extremo a extremo entre usuario móvil y ASP.



**Figura 2/X.1121 – Modelo de pasarela de comunicación móvil de extremo a extremo entre un usuario móvil y el ASP**

En este modelo hay siete entidades: usuario móvil, terminal móvil, red móvil, red abierta, servidor de aplicación, ASP y pasarela de seguridad móvil.

Asimismo, hay siete relaciones entre: usuario móvil y terminal móvil, terminal móvil y red móvil, red móvil y pasarela de seguridad móvil, pasarela de seguridad móvil y red abierta, red abierta y servidor de aplicación, terminal móvil y pasarela de seguridad móvil, y pasarela de seguridad móvil y servidor de aplicación.

## 7 Características de la comunicación móvil de datos de extremo a extremo

La comunicación móvil de datos de extremo a extremo posee diversas características comparadas con la comunicación general de datos de extremo a extremo en una red abierta. Estas características son:

## **La comunicación móvil está basada en la comunicación inalámbrica**

En razón que la comunicación móvil de datos de extremo a extremo se basa en la comunicación inalámbrica, es más inestable que una comunicación de datos por cable de extremo a extremo en una red abierta. Además, el movimiento del usuario durante la comunicación móvil de datos de extremo a extremo añade mayor inestabilidad.

La comunicación inalámbrica se puede basar en una comunicación de difusión entre un terminal móvil y una red móvil.

## **Los terminales móviles son, en general, terminales pequeños**

Los terminales móviles que se utilizan para comunicaciones móviles de datos de extremo a extremo son, por lo general, más pequeños que los terminales típicos existentes (por ejemplo, PC de escritorio) que se utilizan para comunicaciones de datos de extremo a extremo en una red abierta. Las consecuencias son las siguientes:

- dificultad en la entrada o salida de datos;  
Es difícil ingresar datos a través del teclado y visualizar muchos datos en la pantalla en razón del espacio limitado de la misma (en especial, el caso de un terminal portátil de tamaño reducido);
- menor calidad de procesamiento que el PC de escritorio;
- limitación de la capacidad de aplicación correspondiente (tamaño de la memoria, alimentación de energía, etc.).

## **Los terminales móviles son llevados por usuarios móviles**

### **8 Amenazas contra la seguridad en el entorno móvil**

Hay dos tipos de riesgos que afectan a la seguridad. Uno de ellos se refiere a amenazas generales contra la seguridad que pudieran existir en cualquier red abierta. El otro tipo se refiere a las amenazas contra la seguridad en una red móvil que pudieran existir debido a las características de las comunicaciones móviles.

#### **8.1 Amenazas generales contra la seguridad**

Como un subgrupo de comunicaciones de datos de extremo a extremo, las comunicaciones móviles de datos de extremo a extremo son también vulnerables a las amenazas generales contra la seguridad que están presentes en las redes abiertas.

##### **8.1.1 Escucha clandestina**

El mayor problema identificado en redes abiertas es la susceptibilidad a la escucha clandestina por parte de intrusos anónimos que pueden interceptar activamente los datos transmitidos, provocando así una fuga de la información.

##### **8.1.2 Perturbación deliberada de la comunicación**

Esto tiene lugar cuando una interferencia intencional o no intencional perturba al emisor o receptor de un enlace de comunicación, haciendo que éste sea inutilizable. Esto puede producir una denegación de servicio.

##### **8.1.3 Inyección y modificación de datos**

Esto ocurre cuando una entidad no autorizada inserta, modifica o suprime información transmitida entre un terminal móvil y un servidor de aplicación. La entidad no autorizada puede ser una persona, un programa o un ordenador. Estos ataques se producen cuando un intruso añade datos a una conexión existente con el objeto de apoderarse de la misma o de introducir datos con intención maliciosa. Esta amenaza puede producir una denegación de servicio.

#### **8.1.4 Interrupción**

Este tipo de ataque produce la destrucción de un componente de un terminal móvil o un elemento de red, como la destrucción de una pieza de soporte lógico, por ejemplo el disco duro; el corte de una línea de comunicación; o la inhabilitación del sistema de gestión de fichero en un terminal móvil o un elemento de red en la infraestructura de red móvil.

#### **8.1.5 Acceso no autorizado**

El control de acceso es la capacidad para limitar y controlar el acceso a un servidor de aplicación a través de un enlace de comunicación. Esta amenaza ocurre cuando una entidad ilegal tiene acceso a un servidor de aplicación mediante la usurpación de la identidad del usuario móvil real. Se debe identificar o autenticar la entidad que intenta tener acceso no autorizado.

#### **8.1.6 Repudio**

Este ataque ocurre cuando el emisor o el receptor niega el hecho de haber transmitido o recibido un mensaje, respectivamente.

### **8.2 Amenazas contra la seguridad en servicios móviles**

Hay amenazas contra la seguridad en servicios móviles que resultan de las características de las comunicaciones móviles, especialmente en el caso de comunicaciones inalámbricas y comunicaciones de difusión entre un terminal móvil y una red móvil. El problema más identificado en una red inalámbrica es la susceptibilidad a ataques anónimos.

Las amenazas contra la seguridad en servicios móviles son las siguientes:

#### **8.2.1 Escucha clandestina**

En comunicaciones móviles, se puede efectuar mediante la interceptación de las señales radioeléctricas y la decodificación de los datos transmitidos, provocando así una fuga de la información.

#### **8.2.2 Perturbación deliberada de la comunicación**

En comunicaciones móviles esto se puede producir muy probablemente entre un terminal móvil y una red móvil. Hay dos tipos de ataques: interferencia deliberada contra un terminal móvil e interferencia deliberada contra un elemento de red. En el primero el terminal móvil falso finge ser el terminal móvil legal. En el segundo se sustituye indebidamente el elemento de red legítimo interconectándolo con el terminal móvil a través de la interfaz inalámbrica.

#### **8.2.3 Apropiación furtiva de datos**

Ocurre cuando un intruso recoge información en lugares públicos mediante la observación furtiva del teclado, lectura de la pantalla o escucha de un terminal móvil. Esto produce fuga de la información.

#### **8.2.4 Terminal móvil perdido**

Esta amenaza contra la seguridad puede ocurrir mientras que el terminal móvil es transportado por el usuario móvil. Esto puede producir la pérdida o destrucción de la información almacenada en el terminal móvil.

#### **8.2.5 Terminal móvil robado**

Esta amenaza también puede ocurrir mientras que el terminal móvil es transportado por el usuario móvil. Puede producir fuga en la información almacenada en el terminal móvil, supresión de datos como resultado del acceso no autorizado del terminal móvil robado, así como la pérdida de la información almacenada en el terminal móvil.

### 8.2.6 Interrupción no premeditada de la comunicación

Es una amenaza contra la seguridad causada por la comunicación inestable o la limitación de la fuente de alimentación. Esto puede producir supresión de datos.

### 8.2.7 Lectura incorrecta

Este es un riesgo que afecta la seguridad del sistema por una indicación visual pequeña del terminal móvil. Puede producir supresión de datos por suplantación del ASP.

### 8.2.8 Error de entrada

Es un riesgo que afecta la seguridad producido por la dificultad de ingresar datos a través del teclado o botonera de un terminal móvil. Esto puede producir la falta de autenticación del usuario.

## 8.3 Relación entre amenazas contra la seguridad y modelos de comunicación de extremo a extremo

Estas amenazas contra la seguridad aparecen en lugares determinados del modelo. La relación de las amenazas contra la seguridad y las entidades funcionales en los modelos se ilustra en los cuadros 1 y 2.

Estos cuadros indican que en un servidor de aplicación y en una pasarela de seguridad móvil aparecen las mismas amenazas contra la seguridad. Asimismo, muestran que en la relación entre: terminal móvil y servidor de aplicación; terminal móvil y pasarela de seguridad móvil; servidor de aplicación y pasarela de seguridad móvil, hay amenazas similares contra la seguridad.

**Cuadro 1/X.1121 – Relación entre amenazas generales contra la seguridad y modelos**

Entidad, relación	Amenaza	Escucha clandestina	Perturbación de la comunicación	Inyección/modificación	Interrupción	Acceso no autorizado	Repudio
Terminal móvil					X	X	
Servidor de aplicación			X		X	X	
Relación entre usuario móvil y terminal móvil							
Relación entre terminal móvil y servidor de aplicación	X	X	X	X	X		X
Pasarela de seguridad móvil					X	X	
Relación entre terminal móvil y pasarela de seguridad móvil	X	X	X	X	X		X
Relación entre servidor de aplicación y pasarela de seguridad móvil	X	X	X	X	X		X

**Cuadro 2/X.1121 – Relación entre amenazas de seguridad en sistemas móviles y modelos**

Entidad, relación \ Amenaza	Escucha clandestina	Perturbación de la comunicación	Apropiación furtiva de datos	Terminal perdido/robado	Interrupción no premeditada	Lectura errónea/error de entrada
Terminal móvil		X		X		
Servidor de aplicación						
Relación entre usuario móvil y terminal móvil			X			X
Relación entre terminal móvil y servidor de aplicación	X	X			X	
Pasarela de seguridad móvil		X				
Relación entre terminal móvil y pasarela de seguridad móvil	X	X			X	
Relación entre servidor de aplicación y pasarela de seguridad móvil	X	X			X	

## 9 Requisitos de seguridad para comunicaciones móviles de datos de extremo a extremo

Hay dos tipos de requisitos de seguridad para comunicaciones móviles de datos de extremo a extremo. Uno de ellos está considerado desde el punto de vista del usuario móvil y el otro desde el punto de vista del ASP.

### 9.1 Requisitos de seguridad desde el punto de vista del usuario móvil

Hay muchas expectativas y necesidades de usuario diferentes cuando se aplica el requisito de seguridad. Un hecho común a todos los usuarios móviles es su expectativa a que la aplicación funcione y sea sencilla de utilizar. Muchas personas esperan que los proveedores de servicio y de aplicación gestionen sus datos personales de manera segura y respetando su privacidad. Para lograr esta expectativa, el usuario móvil establece condiciones en las siguientes cuestiones de seguridad de la información:

- gestión de la identidad;
- confidencialidad de los datos;
- integridad de los datos;
- autenticación;
- control de acceso;
- no repudio;
- anonimato;
- privacidad;
- aptitud para el uso;
- disponibilidad.

### **9.1.1 Gestión de la identidad**

La gestión de la identidad se refiere generalmente a la protección de la información de identidad del usuario. Por consiguiente, la gestión de identidad es un aspecto muy importante de privacidad del usuario. Durante la comunicación se pueden utilizar seudónimos. El requisito de gestión de la identidad del usuario móvil es crear (o petición para crear), mantener, suprimir (o petición para suprimir), y aplicar claves conforme a la política de seguridad del usuario móvil.

### **9.1.2 Confidencialidad de los datos**

Los requisitos de confidencialidad de los datos del usuario móvil son los siguientes:

#### **Confidencialidad de la comunicación de datos entre el terminal móvil y el servidor de aplicación**

Proporciona confidencialidad de todos los datos o de la información sensible transmitida entre el terminal móvil y un servidor de aplicación.

#### **Confidencialidad de los datos almacenados en un terminal móvil**

Proporciona confidencialidad de todos los datos o de la información sensible almacenada en un terminal móvil.

#### **Confidencialidad de los datos almacenados en el servidor de aplicación**

Proporciona confidencialidad de todos los datos o de la información sensible en un servidor de aplicación que está asociado con un usuario móvil.

En el "modelo de pasarela", los requisitos de confidencialidad de los datos del usuario móvil también abarcan:

#### **Confidencialidad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o de la información sensible transmitida entre el terminal móvil y una pasarela de seguridad móvil.

#### **Confidencialidad de la comunicación de datos entre el servidor de aplicación y la pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o de la información sensible transmitida entre un servidor de aplicación y una pasarela de seguridad móvil.

#### **Confidencialidad de los datos almacenados en una pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o de la información sensible almacenada en una pasarela de seguridad móvil.

### **9.1.3 Integridad de los datos**

Los requisitos de integridad de los datos del usuario móvil están constituidos por:

#### **Integridad de la comunicación de datos entre el terminal móvil y el servidor de aplicación**

Proporciona integridad de todos los datos transmitidos entre el terminal móvil y un servidor de aplicación.

#### **Integridad de los datos almacenados en el terminal móvil**

Proporciona integridad de todos los datos almacenados en el terminal móvil.

### **Integridad de los datos almacenados en un servidor de aplicación**

Proporciona integridad de todos los datos almacenados en un servidor de aplicación que está asociado con el usuario móvil (Por ejemplo, información personal del usuario móvil).

En el "modelo de pasarela", los requisitos de integridad de los datos del usuario móvil abarcan también:

### **Integridad de la comunicación de datos entre el terminal móvil y una pasarela de seguridad móvil**

Proporciona integridad de todos los datos transmitidos entre el terminal móvil y una pasarela de seguridad móvil.

### **Integridad de la comunicación de datos entre un servidor de aplicación y una pasarela de seguridad móvil**

Proporciona integridad de todos los datos transmitidos entre un servidor de aplicación y una pasarela de seguridad móvil.

### **Integridad de los datos almacenados en una pasarela de seguridad móvil**

Proporciona integridad de todos los datos almacenados en una pasarela de seguridad móvil que está asociada con un usuario móvil.

#### **9.1.4 Autenticación**

Hay dos tipos de autenticación: autenticación de entidad y autenticación de mensaje. La autenticación de entidad es para probar la identidad de ésta a una entidad correspondiente. La autenticación de mensaje es para probar el origen o la recepción de los datos. Los requisitos de autenticación del usuario móvil constan de lo siguiente:

#### **Autenticación del ASP**

Este es un tipo de autenticación de entidad utilizado para confirmar la identidad de un ASP y asegurar que no haya usurpación de identidad o que el ASP intente efectuar una repetición no autorizada de una conexión previa.

#### **Autenticación del usuario móvil**

Este es un tipo de autenticación de entidad empleado para verificar la identidad del usuario de un terminal móvil mediante la aplicación de diversos esquemas de autenticación de usuario tales como huella digital, contraseña o número de identificación personal (PIN) para suministrar protección contra el acceso no autorizado desde un terminal móvil perdido o robado.

#### **Autenticación de los datos recibidos**

Este es un tipo de autenticación de mensaje utilizado para corroborar el origen de un dato de comunicación. En esta autenticación no se dispone la protección contra duplicación o modificación de datos.

#### **9.1.5 Control de acceso**

Los requisitos de control de acceso del usuario móvil son los siguientes:

#### **Control de acceso en un terminal móvil**

Proporciona protección contra el acceso no autorizado de un terminal móvil o la utilización no autorizada del mismo.

El control de acceso estará de acuerdo con las políticas de seguridad del usuario móvil.

## **Control de acceso en un servidor de aplicación**

Proporciona protección contra el acceso no autorizado de un servidor de aplicación a los datos enviados por un usuario móvil tal como la información personal del usuario móvil.

El control de acceso estará de acuerdo con las políticas de seguridad del usuario móvil.

En el "modelo de pasarela", los requisitos de control de acceso del usuario móvil abarcan también:

### **Control de acceso en la pasarela de seguridad móvil**

Proporciona protección en una pasarela de seguridad móvil contra el acceso no autorizado a los datos enviados por un usuario móvil tal como la información personal del usuario móvil.

El control de acceso estará de acuerdo con las políticas de seguridad del usuario móvil.

#### **9.1.6 No repudio**

Existe en una o en las dos variantes siguientes:

##### **No repudio con prueba de origen**

Se utiliza para comprobar el origen de los datos recibidos en un ASP determinado. Esto se requiere como medida de protección contra cualquier intento por parte del ASP de negar falsamente el envío de los datos.

##### **No repudio con prueba de entrega**

Se utiliza para proporcionar la prueba de la entrega de datos a un ASP. Esto se requiere como medida de protección contra cualquier intento subsiguiente por parte del ASP para negar falsamente la recepción de los datos.

Los requisitos de no repudio están vinculados con los requisitos siguientes: confidencialidad de la comunicación de datos entre el terminal móvil y el servidor de aplicación, integridad de la comunicación de datos entre el terminal móvil y el servidor de aplicación, integridad de los datos almacenados en el terminal móvil, autenticación del usuario móvil y control de acceso en el terminal móvil.

El "modelo de pasarela", está vinculado con los siguientes requisitos: confidencialidad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil, confidencialidad de la comunicación de datos entre la pasarela de seguridad móvil y el servidor de aplicación, integridad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil, integridad de la comunicación de datos entre la pasarela de seguridad móvil y el servidor de aplicación, integridad de los datos almacenados en la pasarela de seguridad móvil.

#### **9.1.7 Anonimato**

Permite el envío de un mensaje de modo tal que el ASP no pueda identificar el usuario móvil (y terminal móvil).

#### **9.1.8 Privacidad**

Se utiliza para evitar fugas de la información e impedir que una persona no autorizada obtenga la información.

Los requisitos de privacidad están vinculados con los siguientes requisitos: confidencialidad de la comunicación de datos entre el terminal móvil y el servidor de aplicación, confidencialidad de los datos almacenados en el terminal móvil, confidencialidad de los datos almacenados en el servidor de aplicación, control de acceso en el terminal móvil y control de acceso en el servidor de aplicación.

El "modelo de pasarela", está vinculado con los siguientes requisitos: confidencialidad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil, confidencialidad de la comunicación de datos entre la pasarela de seguridad móvil y el servidor de aplicación, confidencialidad de los datos almacenados en la pasarela de seguridad móvil y control de acceso en la pasarela de seguridad móvil.

### **9.1.9 Facilidad de utilización**

Permite la utilización simple de una aplicación y evita la mala lectura o la introducción con errores.

### **9.1.10 Disponibilidad**

Proporciona al usuario móvil la posibilidad de recibir un servicio de aplicación en cualquier lugar y en cualquier momento.

## **9.2 Requisitos de seguridad desde el punto de vista del ASP**

Las empresas comerciales que ofrecen sus servicios a los usuarios móviles deben proteger sus sistemas contra fraudes. Debido a las características específicas del equipo móvil, la autenticación del abonado y los mecanismos de pago se deben manejar con mucho cuidado. Asimismo, si un servicio se entrega a los usuarios móviles no se puede evitar la verificación y no repudio del servicio. Por tanto, el ASP tiene requisitos en los aspectos siguientes:

- confidencialidad de los datos;
- integridad de los datos;
- autenticación;
- control de acceso;
- no repudio;
- disponibilidad.

### **9.2.1 Confidencialidad de los datos**

Los requisitos de confidencialidad de los datos del ASP constan de lo siguiente:

#### **Confidencialidad de la comunicación de datos entre un terminal móvil y un servidor de aplicación**

Proporciona confidencialidad de toda la información sensible transmitida entre un terminal móvil y el servidor de aplicación.

#### **Confidencialidad de los datos almacenados en el terminal móvil**

Proporciona confidencialidad de todos los datos o del contenido sensible enviado por el ASP y almacenados en un terminal móvil.

#### **Confidencialidad de los datos almacenados en el servidor de aplicación**

Proporciona confidencialidad de todos los datos almacenados en el servidor de aplicación.

En el "modelo de pasarela", los requisitos de confidencialidad de los datos del ASP abarcan también:

#### **Confidencialidad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o información sensible transmitida entre un terminal móvil y una pasarela de seguridad móvil.

### **Confidencialidad de la comunicación de datos entre el servidor de aplicación y la pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o información sensible transmitida entre el servidor de aplicación y una pasarela de seguridad móvil.

### **Confidencialidad de los datos almacenados en una pasarela de seguridad móvil**

Proporciona confidencialidad de todos los datos o contenidos sensibles enviados por el ASP y almacenados en una pasarela de seguridad móvil.

## **9.2.2 Integridad de los datos**

Los requisitos de integridad de los datos del ASP son los siguientes:

### **Integridad de la comunicación de datos entre el terminal móvil y el servidor de aplicación**

Proporciona integridad de todos los datos transmitidos entre un terminal móvil y el servidor de aplicación.

### **Integridad de los datos almacenados en el terminal móvil**

Proporciona integridad de todos los datos o contenidos enviados por el ASP y almacenados en un terminal móvil.

### **Integridad de los datos almacenados en el servidor de aplicación**

Proporciona integridad de todos los datos almacenados en el servidor de aplicación.

En el "modelo de pasarela", los requisitos de integridad de los datos del ASP abarcan también:

### **Integridad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil**

Proporciona integridad de todos los datos (o parte de ellos) entre un terminal móvil y una pasarela de seguridad móvil.

### **Integridad de la comunicación de datos entre el servidor de aplicación y una pasarela de seguridad móvil**

Esto proporciona integridad de todos los datos transmitidos entre el servidor de aplicación y una pasarela de seguridad móvil.

### **Integridad de los datos almacenados en la pasarela de seguridad móvil**

Proporciona integridad de todos los datos o contenidos enviados por el ASP y almacenados en una pasarela de seguridad móvil.

## **9.2.3 Autenticación**

El requisito de autenticación del ASP consiste también en la autenticación de entidad (usuario móvil y terminal móvil) y autenticación de mensaje (datos recibidos).

### **Autenticación del usuario móvil**

Este es un tipo de autenticación de entidad utilizado para confirmar la identidad de un usuario móvil con el objeto de asegurar que el usuario móvil no intenta efectuar una simulación de identidad o repetición no autorizada de una conexión previa.

### **Autenticación del terminal móvil**

Este es un tipo de autenticación de entidad utilizado para confirmar la identidad de un terminal móvil con el objeto de asegurar que el terminal móvil posee la funcionalidad necesaria para tener acceso a un servicio de aplicación.

## **Autenticación de los datos recibidos**

Este es un tipo de autenticación de mensaje utilizado para corroborar el origen de los datos de comunicación. No es un requisito de protección contra duplicación o modificación de datos.

### **9.2.4 Control de acceso**

El requisito de control de acceso del ASP está constituido por el control de acceso en el servidor de aplicación y el control de acceso en el terminal móvil.

#### **Control de acceso en el servidor de aplicación**

Proporciona protección contra el acceso no autorizado o la utilización no autorizada de un servidor de aplicación.

El control de acceso estará de acuerdo con las políticas de seguridad del ASP.

#### **Control de acceso en el terminal móvil**

Proporciona protección contra el acceso no autorizado a los datos o contenidos enviados por el ASP en el terminal móvil.

El control de acceso estará de acuerdo con las políticas de seguridad del ASP.

En el "modelo de pasarela", los requisitos de control de acceso del ASP incluyen también:

#### **Control de acceso en la pasarela de seguridad móvil**

Proporciona protección contra el acceso no autorizado a los datos o contenidos enviados por el ASP en la pasarela de seguridad móvil.

El acceso de control estará de acuerdo con las políticas de seguridad del ASP.

### **9.2.5 No repudio**

Existe en una o en las dos variantes siguientes:

#### **No repudio con prueba de origen**

Se utiliza para comprobar que el origen de los datos recibidos es un usuario móvil determinado. Esto también se requiere como protección contra cualquier intento del usuario móvil de negar falsamente el envío de los datos o de su contenido.

#### **No repudio con prueba de entrega**

Se utiliza para proporcionar la prueba de la entrega de datos a un usuario móvil. Esto también se requiere como medida de protección contra cualquier intento subsiguiente del usuario móvil de negar falsamente la recepción de los datos o de su contenido.

Los requisitos de no repudio del ASP están vinculados con los siguientes requisitos: confidencialidad de la comunicación de datos entre el terminal móvil y el servidor de aplicación, integridad de la comunicación de datos entre el terminal móvil y el servidor de aplicación, integridad de los datos almacenados en el terminal móvil, autenticación del usuario móvil y control de acceso en el terminal móvil.

El "modelo de pasarela" está vinculado con los siguientes requisitos: confidencialidad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil, confidencialidad de la comunicación de datos entre la pasarela de seguridad móvil y el servidor de aplicación, integridad de la comunicación de datos entre el terminal móvil y la pasarela de seguridad móvil, integridad de la comunicación de datos entre la pasarela de seguridad móvil y el servidor de aplicación, integridad de los datos almacenados en la pasarela de seguridad móvil.

### 9.2.6 Disponibilidad

Permite al usuario móvil autorizado la posibilidad de recibir un servicio de aplicación en cualquier momento en el lugar que se encuentre.

### 9.3 Relación entre los requisitos de seguridad y las amenazas contra la seguridad

Cada requisito de seguridad constituye una medida preventiva contra determinadas amenazas de la seguridad. La relación entre los requisitos de seguridad y las amenazas contra la seguridad figuran en los cuadros 3 y 4.

**Cuadro 3/X.1121 – Relación entre los requisitos de seguridad y las amenazas generales contra la seguridad**

Requisito \ Amenaza	Escucha clandestina	Perturbación de la comunicación	Inyección/modificación	Interrupción	Acceso no autorizado	Repudio
Gestión de la identidad	X				X	X
Confidencialidad de la comunicación de datos	X					
Confidencialidad de los datos almacenados					X	
Integridad de la comunicación de datos			X			
Integridad de los datos almacenados					X	
Autenticación de la identidad			X		X	X
Autenticación del mensaje			X			
Control de acceso			X		X	
No repudio						X
Anonimato					X	
Privacidad	X				X	
Facilidad de utilización						
Disponibilidad		X		X		

**Cuadro 4/X.1121 – Relación entre los requisitos de seguridad y las amenazas contra la seguridad en sistemas móviles**

Requisito \ Amenaza	Escucha clandestina	Perturbación de la comunicación	Apropiación furtiva de datos	Terminal perdido/ robado	Interrupción no deliberada	Lectura errónea/introducción errónea
Gestión de la identidad	X					
Confidencialidad de la comunicación de datos	X					
Confidencialidad de los datos almacenados				X		
Integridad de la comunicación de datos						
Integridad de los datos almacenados				X		
Autenticación de la identidad				X		
Autenticación del mensaje						
Control de acceso				X		
No repudio						
Anonimato				X		
Privacidad	X		X	X		
Facilidad de utilización						X
Disponibilidad		X			X	

### 10 Funciones de seguridad para satisfacer los requisitos de seguridad en sistemas móviles

Para llevar a cabo los requisitos de seguridad en comunicaciones móviles de datos de extremo a extremo, se pueden utilizar las siguientes funciones de seguridad:

- cifrado;
- intercambio de claves;
- firma digital;
- control de acceso;
- integridad de los datos;
- intercambio de autenticación;
- notarización.

#### Cifrado

La función cifrado puede proporcionar confidencialidad en la comunicación de datos o bien en los datos almacenados.

Los algoritmos de cifrado pueden ser reversibles o irreversibles. Hay dos clasificaciones generales de algoritmos de cifrado reversibles:

- a) Cifrado simétrico (es decir, clave secreta), en el cual el conocimiento de la clave de cifrado implica el conocimiento de la clave de descifrado y viceversa; y

- b) Cifrado asimétrico (es decir, cifrado público), en el cual el conocimiento de la clave de cifrado no implica el conocimiento de la clave de descifrado, o viceversa. Las dos claves de dichos sistemas se denominan a menudo como "clave pública" y "clave privada".

Los algoritmos de cifrado irreversibles pueden utilizar o no una clave. Cuando utilizan una clave, ésta puede ser pública o secreta.

En razón de la baja capacidad de procesamiento o pequeña capacidad de la memoria de los terminales móviles, existen algunas dificultades en aplicar las funciones de cifrado existentes, en especial los algoritmos asimétricos, utilizadas en redes abiertas existentes. En el caso de la utilización continua de las funciones de cifrado existentes en un servidor en redes abiertas, se utiliza habitualmente el modelo de pasarela.

### **Intercambio de claves**

La función intercambio de claves permite la compartición de claves en aplicaciones de cifrado, en especial la del algoritmo cifrado simétrico.

### **Firma digital**

La función firma digital define dos procesos:

- a) firma de un dato, y
- b) verificación de un dato firmado.

El primer proceso utiliza información que es propia (es decir, única y confidencial) del firmante. El segundo proceso utiliza procedimientos e información que se dispone públicamente pero no se puede deducir de la misma la información privada del firmante.

El proceso de firmado comprende el cifrado de los datos o bien la producción de un valor de comprobación criptográfica de los datos empleando la información privada del firmante como clave privada.

El proceso de verificación entraña el uso de procedimientos e información pública para determinar si la firma se presentó correctamente con la información privada del firmante.

Las características esenciales de la función firma digital es que ésta sólo se puede producir utilizando la información privada del firmante. Así, cuando se verifica la firma, se puede probar en todo momento a un tercero (por ejemplo, juez o árbitro) que sólo el poseedor legítimo de la información privada puede realizar la firma digital.

Con relación a la función cifrado, existen algunas dificultades en aplicar las funciones de firma digital existentes utilizadas en redes abiertas existentes debido a la baja eficacia de procesamiento o pequeña capacidad de la memoria de los terminales móviles.

### **Control de acceso**

La función control de acceso puede utilizar la identidad autenticada de una entidad o información acerca de la entidad (tal como condición de miembro en un conjunto de entidades conocido) o capacidades de la entidad, a fin de determinar y poner en vigor los derechos de acceso de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo de acceso inadecuado, la función control de acceso rechazará entonces el intento y, además, puede comunicar el incidente con el propósito de generar una alarma así, como grabarlo como parte de un registro de auditoría de seguridad.

La función control de acceso se puede basar en la utilización de los siguientes elementos:

- a) bases de información de control de acceso, donde se mantiene en una base de datos el derecho de acceso de las entidades pares;
- b) información de autenticación tal como contraseñas, posesión y presentación subsiguiente de la prueba de autorización de la entidad de acceso;

- c) capacidades, posesión y presentación subsiguiente de la prueba que da derecho al acceso a la entidad o recurso definido por la capacidad;
- d) etiquetas de seguridad, las que se pueden utilizar asociadas con una entidad para acordar o denegar acceso, generalmente con arreglo a la política de seguridad en vigor;
- e) tiempo de tentativa de acceso;
- f) ruta de tentativa de acceso;
- g) duración del acceso; y
- h) ubicación física de la tentativa de acceso.

La función control de acceso se puede aplicar en cualquier entidad par de una asociación de comunicación y/o en una pasarela de seguridad móvil.

El control de acceso que afecta a la entidad de origen o pasarela de seguridad móvil se utiliza para determinar si el emisor está autorizado para comunicarse con el receptor y/o utilizar los recursos de comunicación requeridos.

### **Integridad de los datos**

Se consideran dos aspectos de integridad de los datos: la integridad de una unidad o campo de datos simple y la integridad de un tren de unidades o campos de datos. En general, se utilizan diversas tecnologías para proporcionar estos dos tipos de función de integridad, si bien el suministro del segundo tipo sin el primero no es práctico.

La determinación de la integridad de una unidad de datos simple implica dos procesos, uno en la entidad emisora y el otro en la entidad receptora. La entidad emisora añade a los datos una cantidad que es función de los datos propiamente dichos. Esta cantidad puede ser una información suplementaria tal como un código de verificación de bloque o un valor de comprobación criptográfica, y puede ser cifrado. La entidad receptora genera una cantidad correspondiente y compara su resultado con la cantidad recibida para determinar si los datos han sido modificados en el tránsito. Este proceso por sí mismo no prestará protección contra la reproducción de una unidad de datos simple.

La protección de la integridad de una secuencia de unidades de datos (es decir, protección contra desorden, pérdida, repetición e inserción o modificación de los datos) requiere añadir alguna forma de orden explícito tal como numeración secuencial, indicación de tiempo, o encadenamiento criptográfico.

### **Intercambio de autenticación**

Algunas tecnologías de seguridad que se pueden aplicar al intercambio de autenticación son:

- a) empleo de información de autenticación, tal como contraseñas proporcionadas por una entidad emisora y verificada por la entidad receptora;
- b) tecnologías criptográficas; y
- c) utilización de características y/o posesiones de la entidad.

Se puede incorporar la función intercambio de autenticación para proporcionar autenticación de entidad par. Si la función no permite autenticar la entidad, se producirá el rechazo o la terminación de la conexión y puede generar una inserción en el registro de auditoría de seguridad y/o un informe a un centro de gestión de seguridad.

Cuando se utilizan técnicas criptográficas, se pueden combinar con protocolos de iniciación de diálogo para la protección contra repetición (es decir, asegurar el contacto activo).

La elección de la tecnología de seguridad que realiza el intercambio de autenticación, dependerá de las circunstancias en las cuales han de ser utilizadas con:

- a) indicación de tiempo y relojes sincronizados;
- b) tomas de contacto de dos o tres instancias (para autenticación unilateral y mutua, respectivamente); y
- c) funciones de no repudio obtenidas por firma digital y/o mecanismos de notarización.

### Notarización

Las propiedades de los datos comunicados entre dos o más entidades, tales como su integridad, origen, tiempo y destino, se pueden asegurar mediante una función de notarización. El mecanismo de seguridad es proporcionado por una tercera parte de confianza (notario), que se constituye en custodio de las entidades comunicantes, y que dispone de la información necesaria para prestar la seguridad requerida de manera verificable. Cada instancia de comunicación puede utilizar firma digital, cifrado, y funciones de integridad según sea apropiado al servicio proporcionado por el notario. Cuando se invoca la función notarización, los datos entre las entidades comunicantes se efectúan a través de las instancias de comunicación protegidas y el notario.

Estas funciones de seguridad se utilizan para satisfacer algunos de los requisitos de seguridad. En el cuadro 5 se muestra la relación entre los requisitos de seguridad y las funciones.

**Cuadro 5/X.1121 – Ilustración de la relación entre los requisitos de seguridad y las funciones**

Requisito \ Función	Cifrado	Intercambio de claves	Firma digital	Control de acceso	Integridad de los datos	Intercambio de autenticación	Notarización
Gestión de la identidad	X	X	X			X	
Confidencialidad de la comunicación de datos	X	X		X		X	
Confidencialidad de los datos almacenados	X			X			
Integridad de la comunicación de datos	X	X	X	X	X	X	
Integridad de los datos almacenados	X		X	X	X		
Autenticación de entidad	X		X			X	
Autenticación de mensaje	X	X	X		X	X	
Control de acceso				X		X	
No repudio			X			X	X
Anonimato	X						
Facilidad de utilización				X			
Privacidad	X			X		X	
Disponibilidad				X		X	

## 11 Tecnologías de seguridad para comunicaciones móviles de datos de extremo a extremo

Para llevar a cabo las funciones de seguridad como se describe en la cláusula 10, se utilizan diversas tecnologías de seguridad para comunicaciones móviles de datos de extremo a extremo (es decir, tecnologías de seguridad en comunicaciones móviles). Éstas se clasifican según la función de seguridad efectuada por la tecnología de seguridad y dónde se aplica dicha tecnología. En razón que una tecnología de seguridad se aplica a una entidad o una relación entre entidades en modelos de comunicación móvil de datos de extremo a extremo, los lugares en los que se aplican dichas tecnologías de seguridad señalan entidades o relaciones entre entidades. Los cuadros 1 y 2 indican dónde aparecen las amenazas de seguridad en modelos de comunicaciones móviles de datos de extremo a extremo. Los cuadros 3 y 4 muestran qué requisito de seguridad se aplica como medida preventiva para una determinada amenaza de seguridad, y el cuadro 5 indica las funciones de seguridad que satisfacen los requisitos de seguridad. En el cuadro 6 se puede ver la relación entre las funciones de seguridad y los lugares para aplicar estas funciones de seguridad y los modelos. En otras palabras, el cuadro 6 muestra dónde se aplican las tecnologías de seguridad móviles, que efectúan determinadas funciones de seguridad, en los modelos.

Una determinada tecnología de seguridad móvil puede ejecutar sólo una parte de las funciones de seguridad o ser aplicada a un lugar específico. Por ejemplo, se puede utilizar el algoritmo criptográfico de curva elíptica para efectuar una función de intercambio de claves en la relación entre el usuario y un terminal móvil. La tecnología de autenticación biométrica se puede utilizar para realizar la función de intercambio de autenticación en la relación entre el usuario y un terminal móvil. La tecnología PKI (infraestructura de clave pública) se puede utilizar para efectuar todas las funciones de seguridad en las relaciones entre terminal móvil y servidor, terminal móvil y pasarela de seguridad móvil, y servidor y pasarela de seguridad móvil.

**Cuadro 6/X.1121 – Relación entre tecnologías de seguridad en comunicaciones móviles y modelo**

Funciones realizadas por tecnologías	Lugares en los cuales se aplican tecnologías	Terminal móvil	Servidor de aplicación /Pasarela de seguridad móvil	Relación entre usuario móvil y terminal móvil	Relación entre terminal móvil y servidor de aplicación u otras relaciones
Cifrado		X	X	X	X
Intercambio de claves					X
Firma digital		X	X		X
Control de acceso		X	X	X	X
Integridad de los datos		X	X		X
Intercambio de autenticación		X	X	X	X
Notarización					X



## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación