



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.815

(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: MARCO DE INTEGRIDAD**

Recomendación UIT-T X.815

(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.815 se aprobó el 21 noviembre de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-6.

NOTA

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

© UIT 1996

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

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

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

ÍNDICE

	<i>Página</i>
1 Alcance.....	1
2 Referencia normativas.....	2
2.1 Recomendaciones Normas Internacionales idénticas.....	2
2.2 Pares de Recomendaciones Normas Internacionales de contenido técnico equivalente	2
2.3 Referencias adicionales.....	2
3 Definiciones	3
4 Abreviaturas	4
5 Análisis general de la integridad	4
5.1 Conceptos básicos	5
5.2 Tipos de servicios de integridad.....	5
5.3 Tipos de mecanismo de integridad.....	5
5.4 Amenazas a la integridad	6
5.5 Tipos de ataques a la integridad	7
6 Políticas de integridad	7
6.1 Establecimiento de políticas.....	7
6.1.1 Caracterización de los datos.....	8
6.1.2 Caracterización de las entidades	8
6.1.2.1 Políticas basadas en la identidad	8
6.1.2.2 Políticas basadas en reglas	8
7 Información y facilidades de integridad.....	8
7.1 Información de integridad.....	8
7.1.1 Información de integridad de blindaje	8
7.1.2 Información de integridad de detección de modificación	8
7.1.3 Información de integridad de desblindaje	8
7.2 Facilidades de integridad	9
7.2.1 Facilidades relacionadas con el funcionamiento.....	9
7.2.2 Facilidades relacionadas con la gestión	9
8 Clasificación de los mecanismos de integridad.....	10
8.1 Provisión de la integridad mediante la criptografía	10
8.1.1 Provisión de la integridad mediante el sellado.....	10
8.1.2 Provisión de integridad mediante firmas digitales	10
8.1.3 Provisión de integridad mediante el cifrado de datos redundantes	11
8.2 Provisión de integridad mediante el contexto	11
8.2.1 Repetición de los datos	11
8.2.2 Contexto acordado previamente.....	12
8.3 Provisión de la integridad mediante la detección y acuse de recibo	12
8.4 Provisión de integridad mediante la prevención	12
9 Interacciones con otros servicios y mecanismos de seguridad.....	12
9.1 Control de acceso	12
9.2 Autenticación del origen de los datos	12
9.3 Confidencialidad.....	13
Anexo A – Integridad en el modelo básico de referencia de OSI	14
Anexo B – Coherencia externa de datos.....	16
Anexo C – Reseña de facilidades de integridad	18

Resumen

La presente Recomendación | Norma Internacional define un marco general para la prestación de servicios de seguridad. La propiedad que garantiza que los datos no han sido alterados ni destruidos de una manera no autorizada se denomina integridad.

Introducción

Numerosas aplicaciones de sistemas abiertos tienen requisitos de seguridad que dependen de la integridad de los datos. Dichos requisitos pueden incluir la protección de los datos utilizados en la prestación de otros servicios de seguridad, tales como los de autenticación, control de acceso, confidencialidad, auditoría y no repudio, ya que, si un atacante pudiera modificarlos, podría reducir o anular la eficacia de estos servicios.

Se llama integridad a la propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada. La presente Recomendación | Norma Internacional define un marco general para la prestación de los servicios de integridad.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

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

1 Alcance

La Recomendación | Norma Internacional sobre marcos de seguridad para sistemas abiertos trata de la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde el término «sistema abierto» se considera que abarca campos tales como los relativos a bases de datos, aplicaciones distribuidas, procesamiento distribuido abierto e interconexión de sistemas abiertos. Corresponde a los marcos de seguridad la definición de medios para proporcionar protección a sistemas y a objetos dentro de los sistemas, así como en las interacciones entre sistemas. La metodología de la construcción de sistemas o mecanismos queda fuera del alcance de los marcos de seguridad.

Los marcos de seguridad tratan tanto de elementos de datos como de secuencias de operaciones (pero no de elementos de protocolo) que pueden ser utilizados para obtener servicios de seguridad específicos. Dichos servicios pueden aplicarse a las entidades comunicantes de sistemas y a datos intercambiados entre sistemas, así como a datos gestionados por sistemas.

La presente Recomendación | Norma Internacional trata de la integridad de los datos en las operaciones de extracción, transferencia y gestión de información, y:

- 1) define el concepto básico de integridad de datos;
- 2) identifica posibles clases de mecanismos de integridad;
- 3) define facilidades para cada clase de mecanismo de integridad;
- 4) identifica la gestión necesaria para sustentar las clases de mecanismos de integridad;
- 5) trata de la interacción de los mecanismos de integridad y los servicios de soporte con otros servicios y mecanismo de seguridad.

Este marco puede ser utilizado por varios tipos de normas diferentes, entre ellas:

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

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

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

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

NOTA – Aunque ISO no normaliza algoritmos criptográficos, si normaliza los procedimientos utilizados para registrarlos en ISO/CEI 9979.

La integridad tratada en esta Recomendación | Norma Internacional es la definida por la constancia de un valor de datos. Esta noción (constancia de un valor de datos) abarca todos los casos en los que representaciones diferentes de un valor de datos se consideran equivalentes (por ejemplo, diferentes codificaciones ASN.1 del mismo valor). Otras formas de invariabilidad quedan excluidas.

La utilización del término datos en esta Recomendación | Norma Internacional incluye todos los tipos de estructura de datos (tales como conjuntos o recopilaciones de datos, secuencias de datos, sistemas de ficheros y bases de datos).

Este marco trata de la provisión de integridad a datos a los que se considera que los posibles atacantes pueden acceder por escritura. Por consiguiente, se centra en la provisión de integridad mediante mecanismos, criptográficos y no criptográficos, que no dependen exclusivamente de la regulación del acceso.

2 Referencia normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones 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 – Modelo de referencia básico: El modelo básico*.
- Recomendación UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de seguridad de la capa de red*.
- Recomendación UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Tecnología de la información – Intercambio de telecomunicaciones e información entre sistemas – Protocolo de seguridad de la capa de transporte*.
- Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.
- Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de atenuación*.
- Recomendación UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*.

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación UIT-T X.224 (1993), *Protocolo para proporcionar el servicio de transporte en modo conexión para la interconexión de sistemas abiertos*.
ISO/CEI 8073:1992, *Telecommunications and information exchange between Systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service*.
- 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*.

2.3 Referencias adicionales

- ISO/CEI 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

3 Definiciones

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

3.1 Esta Recomendación | Norma Internacional se basa en los conceptos desarrollados en la Rec. UIT-T X.200 | ISO 7498-1 y utiliza los siguientes términos definidos en ella:

- 1) conexión (N);
- 2) entidad (N);
- 3) facilidad (N);
- 4) capa (N);
- 5) unidad de datos de servicio (N), SDU (N);
- 6) servicio (N);
- 7) datos de usuario (N).

3.2 Esta Recomendación | Norma Internacional se basa en los conceptos desarrollados en la Rec. X.800 del CCITT | ISO 7498-2 y utiliza los siguientes términos definidos en ella:

- a) control de acceso;
- b) integridad de la conexión;
- c) integridad de los datos;
- d) descifrado;
- e) decripción;
- f) firma digital;
- g) cifrado;
- h) encripción;
- i) política de seguridad basada en la identidad;
- j) integridad;
- k) clave;
- l) control de encaminamiento;
- m) política de seguridad basada en reglas.

NOTA – Cuando no se indica otra cosa, en esta norma el término «integridad» significa integridad de los datos.

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

- a) huella dactilar digital;
- b) función de cálculo de claves;
- c) función unidireccional;
- d) clave privada;
- e) clave pública;
- f) sello;
- g) clave secreta;
- h) tercera parte confiable.

3.4 La presente Recomendación | Norma Internacional se basa en conceptos desarrollados en la Rec. UIT-T X.811 | ISO/CEI 10181-2 y utiliza el siguiente término definido en ella:

- parámetro que varía en función del tiempo.

3.5 A los efectos de esta Recomendación | Internacional se aplican las siguientes definiciones:

3.5.1 canal de integridad protegida: Canal de comunicaciones al cual se ha aplicado un servicio de integridad.

NOTA – En la Rec. X.800 del CCITT | ISO 7498-2 se hace referencia a dos formas de servicios de integridad para canales de comunicación. Dichas formas (integridad en modo con conexión y en modo sin conexión) se describen en el Anexo A.

3.5.2 entorno de integridad protegida: Entorno en el cual se impiden o pueden detectarse las alteraciones no autorizadas de los datos (incluida la creación y supresión).

3.5.3 datos de integridad protegida: Los datos y todos los atributos pertinentes dentro de un entorno de integridad protegida.

3.5.4 blindaje: Conversión de datos en datos de integridad protegida.

3.5.5 desblindaje: Conversión de datos de integridad protegida en los datos blindados originalmente.

3.5.6 validación: Comprobación de los datos de integridad protegida para detectar pérdida de integridad.

4 Abreviaturas

PDU	Unidad de datos de protocolo (<i>protocol data unit</i>)
SDU	Unidad de datos de servicio (<i>service data unit</i>)
SII	Información de integridad de blindaje (<i>shield integrity information</i>)
MDII	Información de integridad de detección de modificación (<i>modification detection integrity information</i>)
UII	Información de integridad de desblindaje (<i>unshield integrity information</i>)

5 Análisis general de la integridad

El objetivo del servicio de integridad es proteger la integridad de los datos y de sus atributos pertinentes que pudiera estar comprometida de diferentes maneras:

- 1) modificación de datos no autorizada;
- 2) supresión de datos no autorizada;
- 3) creación de datos no autorizada;
- 4) inserción de datos no autorizada;
- 5) reproducción de datos no autorizada.

El servicio de integridad protege contra estas amenazas mediante la prevención o la detección con o sin recuperación. La protección efectiva de la integridad puede no ser posible si la información de control necesaria (como claves y SII) no tiene integridad y/o confidencialidad protegidas; esta protección depende a menudo, implícita o explícitamente, de principios diferentes de los contenidos en el mecanismo que protege los datos.

La noción de entornos protegidos se utiliza explícitamente en este marco para captar la idea de que la protección de la integridad incluye la protección contra la creación y/o supresión no autorizadas. De este modo, la creación/supresión no autorizadas de datos se puede considerar como modificaciones no autorizadas de algún entorno protegido. De manera similar, la inserción y reproducción se pueden considerar como modificaciones de un conjunto de datos estructurados (por ejemplo, una secuencia o una estructura de datos).

Se señala que algunas alteraciones de los datos no repercuten en su integridad. Por ejemplo, si una descripción ASN.1 contiene un tipo de datos **SET OF** (CONJUNTO DE), no se infringe la integridad si los miembros del tipo de datos son reordenados. Los mecanismos de integridad complejos pueden reconocer que algunas transformaciones de datos estructurados no comprometen la integridad de los datos. Estos mecanismos permiten transformaciones de datos firmados o sellados sin que sea necesario calcular de nuevo la firma o el sello digital, respectivamente.

El objetivo del servicio de integridad es proteger contra las modificaciones no autorizadas de los datos, o detectarlas, incluidas la creación y supresión no autorizadas de los datos. La prestación del servicio de integridad se realiza mediante las siguientes actividades:

- 1) **blindaje:** generación de datos de integridad protegida a partir de datos;
- 2) **validación:** comprobación de los datos de integridad protegida para detectar fallos de integridad;
- 3) **desblindaje:** regeneración de datos a partir de datos de integridad protegida.

Estas actividades no emplean necesariamente técnicas criptográficas, y cuando las emplean, éstas no transforman necesariamente los datos. Por ejemplo, la operación **blindaje** se puede proporcionar anexando un sello o una firma digital a los datos. En este caso, después de la **validación** satisfactoria, se efectúa el **desblindaje** a través de la supresión del sello o de la firma digital.

El servicio de integridad se aplica a la extracción, transferencia y gestión de la información como sigue:

- 1) Para la información que se transfiere en un entorno de OSI, el servicio de integridad se proporciona combinando el **blindaje**, la transferencia mediante una facilidad (N-1), y el **desblindaje** para formar la parte transmisión de un servicio (N).
- 2) Para el almacenamiento y extracción de los datos, el servicio de integridad se proporciona combinando el **blindaje** y almacenamiento y la extracción y **desblindaje**.

Tanto la operación **blindaje** como la operación **desblindaje** pueden proporcionarse como operaciones paralelas de tal manera que los mismos datos (por ejemplo, todos los datos de una conexión (N), puedan constar al mismo tiempo de partes que todavía no han sido **blindadas**, partes que son retenidas como datos de integridad protegida y partes que han sido **desblindadas**.

Los mecanismos de integridad proporcionan entornos protegidos y, por ello, tanto la etapa de **blindaje** como la de **desblindaje** pueden conllevar la transferencia de datos entre entornos protegidos. Cuando los datos de integridad protegida son transferidos de un entorno protegido por un mecanismo de integridad a otro, el **blindaje** del segundo mecanismo debe preceder al **desblindaje** del primero para que los datos permanezcan protegidos de manera continua.

5.1 Conceptos básicos

Cabe distinguir varios tipos de servicios de integridad, dependiendo de la actividad relacionada con los datos de que se trate (creación, supresión, modificación, inserción y/o reproducción), de si se requiere la prevención o sólo la detección de una violación y de si se sustenta la recuperación de los datos en caso de violación de la integridad. En 5.2 se describen los diferentes tipos de servicios de integridad.

Los mecanismos que pueden utilizarse para prestar estos servicios pueden dividirse en dos amplias categorías que dependen del nivel de actividad sistemática supuesta en una tentativa de violación de integridad. En 5.3 se describen estos diferentes tipos de mecanismos.

5.2 Tipos de servicios de integridad

Los servicios de integridad se clasifican de acuerdo con los siguientes criterios:

- 1) Por el tipo de violación contra la que protegen. Los tipos de violación son:
 - a) modificación de datos no autorizada;
 - b) creación de datos no autorizada;
 - c) supresión de datos no autorizada;
 - d) inserción de datos no autorizada;
 - e) reproducción de datos no autorizada.
- 2) Por el tipo de protección que sustentan. Los tipos de protección son:
 - a) prevención de compromisos de la integridad;
 - b) detección de compromisos de la integridad.
- 3) En función de si incluyen o no mecanismos de recuperación:

en el primer caso (con recuperación), la operación **desblindaje** puede recuperar los datos originales (y posiblemente señalar una acción de recuperación o un error a efectos de auditoría, por ejemplo) cuando la operación **validación** indica alteración;

en el segundo caso (sin recuperación), la operación **desblindaje** es incapaz de recuperar los datos originales cuando la operación **validación** indica alteración.

5.3 Tipos de mecanismo de integridad

Por regla general, la capacidad de proteger datos depende del medio utilizado. Algunos medios son, por su propia naturaleza, difíciles de proteger (por ejemplo, medios de almacenamiento o medios de comunicación que se pueden eliminar) y, en consecuencia, partes no autorizadas pueden acceder a los datos y manipularlos a voluntad. En estos

medios, la finalidad del mecanismo de integridad es detectar la modificación y, posiblemente, restablecer los datos afectados. Por consiguiente se distinguen los siguientes casos de mecanismos de integridad:

- 1) Los que impiden el acceso al medio:
 - a) canales aislados físicamente y sin ruido;
 - b) control de encaminamiento;
 - c) control de acceso.
- 2) Los que detectan modificaciones no autorizadas de los datos o secuencias de ítems de datos, incluidos los casos de creación, supresión y repetición no autorizadas de los datos:
 - a) sellos;
 - b) firmas digitales;
 - c) repetición de datos (utilizada como un medio de combatir otros tipos de violación);
 - d) huellas dactilares digitales junto con transformaciones criptográficas;
 - e) números de secuencia de mensajes.

Desde el punto de vista de la solidez de la protección, estos mecanismos se pueden clasificar como sigue:

- 1) sin ninguna protección;
- 2) con detección de modificación y de creación;
- 3) con detección de modificación, creación, supresión y repetición;
- 4) con detección de modificación y de creación con recuperación; y
- 5) con detección de modificación, creación, supresión y repetición con recuperación.

5.4 Amenazas a la integridad

Desde el punto de vista de los servicios prestados, las amenazas pueden clasificarse como sigue:

- 1) Creación/modificación/supresión/inserción/reproducción no autorizadas en entornos que sustentan la integridad de los datos mediante la prevención.
Ejemplo: derivaciones de un canal seguro.
- 2) Creación/modificación/supresión/inserción/reproducción no autorizadas y no detectadas en entornos que sustentan la integridad mediante la detección.

Ejemplo: la integridad de los datos se puede garantizar cifrando los datos protegidos y las sumas de control asociadas como se describe en la Rec. UIT-T X.274 | ISO/CEI 10736. Si las entidades comunicantes A y B están utilizando la misma clave para apoyar el cifrado y la integridad de los datos no está protegida en el origen, los datos de integridad protegida que se enviaron de A a B pueden presentarse ulteriormente a A como si fuera originados en B (un ataque por reflexión).

Desde el punto de vista del medio en el que residen los datos, las amenazas pueden clasificarse como sigue:

- 1) amenazas propias del medio en el que los datos están almacenados;
- 2) amenazas propias del medio por el que se transmiten los datos;
- 3) amenazas independientes del medio.

En la medida en que esta Recomendación | Norma Internacional considera las violaciones de la integridad como acciones no autorizadas, no trata del tema de las modificaciones autorizadas que pudieran vulnerar la coherencia externa de los datos que se describe en el Anexo B (por ejemplo, falsa contabilidad). En consecuencia, la presente Recomendación | Norma Internacional, a diferencia del marco de confidencialidad, no se ocupa del tema de los ataques procedentes del interior (este último marco trata temas relacionados con la protección continua de la información, tales como la posibilidad de que un acceso autorizado vaya seguido de una liberación no autorizada, intencionada o no, de la información de confidencialidad protegida).

5.5 Tipos de ataques a la integridad

A cada una de las amenazas enumeradas anteriormente corresponden uno o más ataques, es decir, la materialización de la amenaza en cuestión. La finalidad de los ataques es hacer fallar el mecanismo o los mecanismos utilizados para proporcionar la integridad y se pueden clasificar como sigue:

- 1) Ataques destinados a corromper los mecanismos criptográficos o a explotar la fragilidad de dichos mecanismos. Estos ataques son:
 - a) penetración del mecanismo criptográfico;
 - b) supresión y repetición (selectivas).
- 2) Ataques destinados a hacer fallar el mecanismo contextual utilizado (los mecanismos contextuales intercambian datos a horas y/o en ubicaciones específicas). Estos ataques son:
 - a) cambios masivos y coordinados de reproducciones de ítems de datos;
 - b) penetración del mecanismo que establece el contexto.
- 3) Ataques destinados a hacer fallar los mecanismos de detección y de acuse de recibo. Estos ataques son:
 - a) acuses de recibo falsos;
 - b) aprovechamiento de una secuenciación defectuosa entre el mecanismo de acuse de recibo y el tratamiento de los datos recibidos.
- 4) Ataques destinados a hacer fallar, subvertir o sobornar los mecanismos de prevención. Estos ataques son:
 - a) ataques al propio mecanismo;
 - b) penetración de los servicios de los que depende el mecanismo;
 - c) aprovechamiento de facilidades con efectos secundarios no intencionales.

6 Políticas de integridad

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

Los datos, cuya integridad se protege, están sometidos a control, superando el cual, las entidades pueden crearlos, alterarlos y suprimirlos. Una política de integridad debe identificar, por consiguiente, los datos que están sometidos a control e indicar qué entidades están autorizadas a crear, alterar o suprimir datos.

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

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

6.1 Establecimiento de políticas

Para establecer una política de seguridad se necesitan medios con los que identificar la información y las entidades que intervienen.

Una política de seguridad puede considerarse como un conjunto de reglas. Cada regla de una política de integridad puede asociar una caracterización de datos, una caracterización de entidades y un conjunto de actividades de datos permitidas (por ejemplo, creación, alteración y supresión). En algunas políticas, estas reglas no se expresan explícitamente sino que pueden derivarse del establecimiento de la política.

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

6.1.1 Caracterización de los datos

Una política puede identificar los datos de diversas maneras. Por ejemplo:

- 1) identificando a las entidades autorizadas a crear/alterar/suprimir dichos datos;
- 2) por su ubicación; o
- 3) identificando el contexto en el que se presentan los datos (por ejemplo, la función prevista para los mismos).

6.1.2 Caracterización de las entidades

Hay muchas maneras de caracterizar las entidades a las que se aplica una política de integridad. A continuación se dan dos ejemplos principales.

6.1.2.1 Políticas basadas en la identidad

En esta forma de establecimiento de políticas, las entidades son identificadas individualmente, identificadas como parte de un grupo de entidades equivalentes (a los efectos de la política de integridad) o identificadas por el cometido que desempeñan. Así pues, cada una de las entidades autorizadas a participar satisfactoriamente en una actividad de datos poseerá una identidad individual, un identidad de grupo o una identidad de cometido, utilizada para caracterizarla.

En el caso de los cometidos, una política de integridad puede especificar grupos exclusivos de cometidos a disposición de cada entidad, con lo que los cometidos de grupos diferentes no se puede alegar que se realizan simultáneamente.

6.1.2.2 Políticas basadas en reglas

En esta forma de establecimiento de políticas, los atributos están asociados con cada entidad y con cada ítem de datos de integridad protegida. Las reglas globales que se aplican a los atributos de las entidades y de los datos determinan las acciones permitidas. Las políticas basadas en reglas se analizan con más detalle en la visión general del marco de seguridad (Rec. UIT-T X.810 | ISO/CEI 10181-1).

7 Información y facilidades de integridad

En esta cláusula se clasifica la información necesaria para el correcto funcionamiento de un servicio de integridad, así como las facilidades que utilizan o generan la información en cuestión.

7.1 Información de integridad

Para **blindar**, **validar** o **desblindar** los datos pueden emplear información auxiliar. Dicha información se conoce como información de integridad y se clasifica como sigue.

7.1.1 Información de integridad de blindaje

La información de integridad de blindaje (SII) es la información utilizada para **blindar** datos. Ejemplos de la misma son:

- 1) las claves privadas;
- 2) las claves secretas;
- 3) el identificador de algoritmo y los parámetros criptográficos pertinentes;
- 4) parámetros que varían en función de tiempo (por ejemplo, sellos de fecha y hora).

7.1.2 Información de integridad de detección de modificación

La información de integridad de detección de modificación (MDII), es la información utilizada para **validar** datos de integridad protegida. Ejemplos de la misma son:

- 1) las claves públicas;
- 2) las claves secretas.

7.1.3 Información de integridad de desblindaje

La información de integridad de desblindaje (UII), es la información utilizada para **desblindar** datos de integridad protegida. Ejemplos de la misma son:

- 1) las claves públicas;
- 2) las claves secretas.

7.2 Facilidades de integridad

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

7.2.1 Facilidades relacionadas con el funcionamiento

Estas facilidades son:

1) **blindaje**

Esta facilidad aplica la protección de integridad a los datos. Las posibles entradas son:

- los datos que se han de proteger;
- SII;
- identificadores específicos del mecanismo, tales como los mencionados en el Anexo C,

y las posibles salidas son:

- datos de integridad protegida;
- códigos de compleción/devolución.

2) **validar**

Esta facilidad comprueba los datos con integridad protegida para las modificaciones. Las posibles entradas son:

- datos de integridad protegida;
- MDII;
- identificadores específicos del mecanismo, tales como los mencionados en el Anexo C,

y las posibles salidas son:

- una indicación de si se ha violado o no la integridad de los datos.

3) **desblindaje**

Esta facilidad convierte los datos de integridad protegida en los datos originalmente **blindados**.

Las posibles entradas son:

- datos de integridad protegida;
- UII;
- identificadores específicos del mecanismo, tales como los mencionados en el Anexo C,

y las posibles salidas son:

- datos;
- códigos de compleción/devolución.

7.2.2 Facilidades relacionadas con la gestión

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

- 1) instalación de información de gestión;
- 2) modificación de información de gestión;
- 3) supresión de información de gestión;
- 4) listado de información de gestión;
- 5) inhabilitación de información de gestión;
- 6) rehabilitación de información de gestión.

8 Clasificación de los mecanismos de integridad

En esta cláusula se clasifican los mecanismos de integridad según los medios que utilizan para prestar un servicio de integridad.

8.1 Provisión de la integridad mediante la criptografía

Se han de considerar dos clases de mecanismos de integridad criptográficos:

- 1) mecanismos de integridad basados en técnicas criptográficas simétricas, en los que la validación de datos de integridad protegida es posible mediante el conocimiento de la clave secreta que se utilizó para blindar los datos; y
- 2) mecanismos de integridad basados en técnicas criptográficas asimétricas, en los que la validación de datos de integridad protegida es posible mediante el conocimiento de la clave pública correspondiente a la clave privada que se utilizó para blindar los datos.

Los mecanismos del primer tipo corresponden a los sellos mientras que los mecanismos del segundo tipo corresponden a las firmas digitales.

Los parámetros que varían en función del tiempo se pueden utilizar junto con mecanismos de integridad basados en técnicas criptográficas para la protección contra la reproducción.

8.1.1 Provisión de la integridad mediante el sellado

El sellado proporciona integridad anexando un valor de comprobación criptográfico a los datos que han de ser protegidos. En el sellado se utiliza la misma clave secreta para proteger y para validar la integridad de los datos. Cuando se utiliza esta clase de mecanismo, se conocen por adelantado todos los validadores potenciales o dichos validadores han de tener los medios de acceder a la clave secreta.

El conjunto de entidades capaces de sellar los datos y el conjunto de entidades capaces de validarlos son coincidentes, por la propia definición del mecanismo.

Este mecanismo sustenta la detección de modificaciones como sigue:

- **Blindaje** se logra adjuntando un valor de comprobación criptográfico a los datos cuya integridad se ha de proteger (por ejemplo, se calcula una función unidireccional en los datos que se han de proteger y este valor se transforma mediante un mecanismo de cifrado).
- **Validación** se logra utilizando los datos, el valor de comprobación criptográfico y la clave secreta para determinar si los datos concuerdan con el sello (por ejemplo, la facilidad podría presentar los datos y la clave secreta para la facilidad de blindaje y comparar el sello resultante con el valor que se fijó realmente a los datos). Cuando es así, se considera que los datos no han sido modificados.
- **Desblindaje** se realiza suprimiendo el valor de comprobación criptográfico, una vez que los datos han sido validados.

8.1.2 Provisión de integridad mediante firmas digitales

Las firmas digitales se calculan utilizando una clave privada y un algoritmo criptográfico asimétrico. Los datos blindados (los datos más la firma digital anexada) se pueden validar utilizando la clave pública correspondiente. En general, la clave pública puede estar disponible públicamente.

Las firmas digitales permiten que el conjunto de entidades que pueden **validar** los datos sea arbitrario en cuanto a su tamaño y composición.

Este mecanismo sustenta la detección de las modificaciones como sigue:

- **Blindaje** se logra adjuntando valores de comprobación criptográficos a los datos cuya integridad se ha de proteger (por ejemplo, se calcula una huella dactilar digital de los datos que se han de proteger y este valor se combina con la clave privada y, posiblemente, con otros parámetros para generar uno o más valores que forman colectivamente la firma digital).
- **Validación** se logra utilizando una huella dactilar digital de los datos recibidos, la firma digital y la clave pública con un algoritmo que verifica la firma digital. Si fracasa la verificación de la firma digital, se considera que los datos han sido alterados.
- **Desblindaje** se efectúa suprimiendo el valor de comprobación criptográfico, una vez que los datos han sido validados.

Este mecanismo puede sustentar también la autenticación del origen de los datos y el no repudio.

8.1.3 Provisión de integridad mediante el cifrado de datos redundantes

La integridad de los datos redundantes (por ejemplo, lenguaje natural) se puede apoyar mediante el cifrado. Los datos que incluyen códigos de detección de errores y huellas dactilares digitales son redundantes y su integridad se puede proteger mediante el cifrado (a condición de que el algoritmo de cifrado utilizado haga imposible la predicción de cómo los cambios de los datos cifrados se reflejarán en los datos originales después del descifrado).

Los protocolos de seguridad de capa más baja (Recs. UIT-T X.273 | ISO/CEI 11577 y X.274 | ISO/CEI 10736) utilizan este tipo de mecanismo para proporcionar la protección de la integridad a datos de confidencialidad protegida.

Este mecanismo sustenta la detección de modificaciones como sigue:

- **Blindaje** se logra cifrando los datos redundantes.
- **Validación** se logra descifrando los datos blindados y determinando si satisfacen las invarianzas de los datos originales satisfechos. Como ejemplo cabe citar:
 - 1) si los datos originales eran una secuencia de caracteres ASCII, los datos recuperados tienen que tener la misma propiedad;
 - 2) si los datos originales eran una locución humana en un lenguaje dado, los datos recuperados deben ser (o se debe hacer que sean con pequeñas modificaciones) una locución humana comúnmente aceptada en el mismo idioma;
 - 3) si los datos originales contenían sumas de control, se pueden calcular las mismas sumas de control en las porciones pertinentes de los datos protegidos y ver si los resultados concuerdan con los valores de suma de control insertados en los datos descifrados.
- **Desblindaje** se realiza descifrando los datos cifrados.

NOTA – Se sabe que este mecanismo no es adecuado para varias formas comunes de redundancia (por ejemplo, los datos con códigos de detección de errores) utilizados junto con formas comunes de cifrado (por ejemplo, cifrados de bloque, tales como DES, con o sin encadenamiento). Un ejemplo relativamente sencillo de posibles trampas es el siguiente:

Si hubiese que proteger un texto ACCII (por ejemplo, correo electrónico corriente) mediante cifrado DES, el mensaje podría ser modificado de manera no detectable mediante truncación (a menos naturalmente que el encabezamiento del correo contenga un indicador de longitud, como suele hacerse).

8.2 Provisión de integridad mediante el contexto

La integridad puede ser apoyada por mecanismos que almacenan o transmiten los datos en uno o más contextos acordados previamente. Estos mecanismos pueden proteger los datos así como las estructuras de datos (por ejemplo, secuencias de unidades de datos) y comprenden los siguientes:

8.2.1 Repetición de los datos

Esta clase de mecanismo de integridad se basa en la repetición de los datos en el espacio (por ejemplo, en varias zonas de almacenamiento) o en el tiempo (en diferentes momentos). Se supone que los posibles atacantes no pueden comprometer simultáneamente más que un número limitado de repeticiones y que cuando se detectan los ataques, los datos pueden ser reconstruidos a partir de las copias auténticas.

Un mecanismo de este tipo puede ser utilizado, por ejemplo, por bases de datos resistentes a los ataques de penetración.

Estos mecanismos proporcionan detección de la supresión de la integridad con recuperación y se puede utilizar junto con otros mecanismos de seguridad. Proporciona la integridad como sigue:

- El **blindaje** se efectúa proporcionando muchas copias de los mismos datos sucesivamente en el tiempo o en ubicaciones diferentes.
- La **validación** se efectúa recogiendo una copia de los datos en cada uno de los momentos o ubicaciones determinados. Las copias se comparan y si no son idénticas, se considera que se ha producido una violación de la integridad.
- El **desblindaje** (con recuperación) puede efectuarse cuando se satisface algún criterio establecido previamente (por ejemplo, el «90% o más de los valores concuerdan») eligiendo como el valor correcto el que minimiza alguna medida preasignada (por ejemplo, la probabilidad de recuperación errónea).

Se debe señalar que el criterio de recuperación se debe satisfacer cuando todos los valores concuerdan y que en estas circunstancias el valor que minimiza la medida deber ser el valor común.

8.2.2 Contexto acordado previamente

Estos mecanismos proporcionan la detección de la supresión de los datos de integridad protegida y se utilizan a menudo junto con otros mecanismos de integridad:

- El **blindaje** se efectúa proporcionando los datos en un momento y/o ubicación específicos dentro de un nivel determinado de variación.
- La **validación** se efectúa previendo los datos en un momento y/o ubicación determinados. Si no están presentes, se considera que se ha producido una violación de la integridad.

Para evitar la sustitución de datos alternativos, como se ha señalado anteriormente, este mecanismo debe combinarse con otros mecanismos de integridad.

8.3 Provisión de la integridad mediante la detección y acuse de recibo

Estos mecanismos utilizan detección de integridad cuando se efectúan operaciones equipotentes con realimentación positiva (se considera que una operación es equipotente cuando múltiples ejecuciones sucesivas de la operación dan el mismo resultado que una sola de ellas). Ejemplos de tales mecanismos son las transmisiones con acuse positivo (por ejemplo, el transporte de clase 4 que se describe en la Rec. UIT-T X.224 | ISO/CEI 8073) y las operaciones distantes con realimentación. En estos mecanismos se supone que las operaciones **blindaje** y **validación/desblindaje** tienen la misma duración y, por regla general, no son adecuadas para el almacenamiento de datos:

- **Blindaje** se realiza repitiendo la misma acción hasta que la política de integridad indique otra cosa o hasta que se reciba un acuse positivo.
- **Validación** se efectúa en cada ejemplar de datos blindados (a menos que la política de integridad indique otra cosa); las validaciones satisfactorias dan lugar a acuses positivos de señalización a la entidad que efectúa la operación de blindaje.

Si se puede hacer una corrección para entregar información correcta a partir de la operación **desblindaje** del mecanismo de protección de modificación de integridad utilizado, el desblindaje de este mecanismo puede señalar un acuse positivo.

Puede ser eficaz si, cuando la **validación** indica un resultado negativo (que ha producido una modificación o una supresión) se indica un acuse negativo a la operación de **blindaje**.

Estos mecanismos suponen que se pueden detectar las modificaciones de los datos por otros medios y, por consiguiente, se pueden considerar como mecanismos que mejoran la protección contra la modificación de los datos.

8.4 Provisión de integridad mediante la prevención

La integridad se puede proporcionar impidiendo el acceso físico a los medios de almacenamiento o transmisión de los datos y mediante el control de acceso.

La especificación de los medios para impedir el acceso físico está fuera del ámbito de este marco.

El control de acceso se describe en el marco de control de acceso.

9 Interacciones con otros servicios y mecanismos de seguridad

Esta cláusula describe cómo se pueden utilizar otros servicios y mecanismos de seguridad para la integridad, pero no se describe la utilización de la integridad para apoyar otros servicios de seguridad.

9.1 Control de acceso

Se puede utilizar el control de acceso para crear entornos con integridad protegida.

9.2 Autenticación del origen de los datos

La autenticación del origen de los datos se puede utilizar para sustentar la integridad. Por ejemplo, si no es posible autenticar el origen de una PDU, puede considerarse que la PDU está comprometida. De manera similar, si la fuente supuesta de una PDU no está autorizada para crear la PDU, se ha producido una violación de la integridad.

9.3 Confidencialidad

En algunos casos la redundancia se puede combinar con el cifrado para obtener datos que no pueden ser modificados sin detección.

En realidad, los datos redundantes (tales como idioma natural y datos que incluyen sumas de control y valores de cálculo de claves) tienen propiedades que no varían. Por regla general, los cambios de los datos cifrados no preservarán con alta probabilidad estas propiedades una vez que los datos alterados están «descifrados».

(Otra manera de decir esto es cuando k bits de información se codifican en $k + m$ secuencias de bits, las codificaciones válidas constituyen un subconjunto aislado de todas las posibles secuencias de bits; si se producen cambios en los datos cifrados, después del descifrado, cambios que desde el punto de vista del atacante se consideran aleatorios, la probabilidad de que los datos alterados sean descifrados como una codificación válida es del orden de 2^{-m} .)

Esta redundancia (incluidas las sumas de control y las funciones de cálculo de claves) junto con la confidencialidad basada en la criptografía pueden sustentar la integridad.

Anexo A

Integridad en el modelo básico de referencia de OSI

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

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

Se consideran diferentes servicios de seguridad:

- integridad en modo con conexión con recuperación;
- integridad en modo con conexión sin recuperación;
- integridad de campos seleccionados en modo con conexión;
- integridad en modo sin conexión;
- integridad de campos seleccionados en modo sin conexión.

A.1 Integridad en modo con conexión con recuperación

Este servicio proporciona la integridad de todos los datos de usuario (N) en una conexión (N) y detecta cualquier modificación, inserción, supresión o reproducción de cualquier dato dentro de una secuencia completa de SDU (con tentativa de recuperación).

A.2 Integridad en modo con conexión sin recuperación

Este servicio proporciona la integridad de todos los datos de usuario (N) en una conexión (N) y detecta cualquier modificación, inserción, supresión o reproducción de cualquier dato en una secuencia completa de SDU (sin tentativa de recuperación).

A.3 Integridad de campos seleccionados en modo con conexión

Este servicio proporciona la integridad de campos seleccionados en los datos de usuario (N) en una SDU (N) transferida por una conexión y adopta la forma de determinar si los campos seleccionados han sido modificados, insertados, suprimidos o reproducidos.

A.4 Integridad en modo sin conexión

Cuando este servicio es prestado por la capa (N), proporciona la seguridad de la integridad a la entidad (N + 1) solicitante.

A.5 Integridad de campos seleccionados en modo sin conexión

Este servicio proporciona la integridad de campos seleccionados dentro de una sola SDU y en modo sin conexión adopta la forma de una indicación que permite saber si los campos seleccionados han sido modificados.

A.6 Utilización de la integridad en las capas OSI

Los servicios de integridad son pertinentes a las siguientes capas OSI:

- capa de enlace de datos;
- capa de red (capa 3);
- capa de transporte (capa 4);
- capa de aplicación (capa 7).

A.6.1 Utilización de la integridad en la capa de enlace de datos

Los servicios de integridad pueden ser sustentados en la capa de enlace de datos como se describe en IEEE 802.10.

A.6.2 Utilización de la integridad en la capa de red

Los servicios de integridad en modo con conexión sin recuperación y de integridad en modo sin conexión son los únicos servicios de integridad prestados en la capa de red. La integridad en modo con conexión sin recuperación y la integridad en modo sin conexión pueden proporcionarse mediante un mecanismo de integridad de datos en conexión con un mecanismo de cifrado. Estos servicios permiten la integridad entre nodos de red, nodos de subred o relevadores.

A.6.3 Utilización de la integridad en la capa de transporte

Los servicios de integridad en modo con conexión con recuperación, integridad en modo con conexión sin recuperación e integridad en modo sin conexión son los únicos servicios de integridad prestados en la capa de red. La integridad en modo con conexión con o sin recuperación y la integridad en modo sin conexión pueden proporcionarse mediante un mecanismo de integridad de datos en conexión con un mecanismo de cifrado. Estos servicios permiten la integridad entre sistemas de extremo.

A.6.4 Utilización de la integridad en la capa de aplicación

En la capa de aplicación se pueden prestar todos los servicios de integridad, a saber, integridad en modo con conexión con recuperación, integridad en modo con conexión sin recuperación, integridad de campos seleccionados en modo con conexión, integridad en modo sin conexión e integridad de campos seleccionados en modos sin conexión. La integridad en modo con conexión con o sin recuperación y la integridad en modo sin conexión pueden sustentarse mediante un mecanismo de integridad de datos de capa más baja (en combinación a veces con un mecanismo de cifrado). La integridad de campos seleccionados puede sustentarse mediante un mecanismo de integridad de datos de capa más baja (en combinación a veces con un mecanismo de cifrado) en la capa de presentación.

Anexo B

Coherencia externa de datos

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

NOTA – El texto que sigue trata el tema de la integridad interna/externa (desarrollado en el documento original de Clark y Wilson y otros trabajos subsiguientes) y explora la repercusión que estas nociones podrían tener en el marco de la integridad. Cuando es posible, y con miras a limitar la reproducción literal a un mínimo, se citan frases de las publicaciones que se indican.

Las referencias no normativas 1, 2 y 3 indicadas más adelante contienen varias referencias a un modelo de integridad propuesto por D.D. Clark y D.R. Wilson. Lo que sigue es un intento de resumir el modelo y de resaltar los puntos del mismo que pueden repercutir en el marco presente.

Este marco considera la integridad en el sentido del mantenimiento de un invariante específico en los datos (su valor constante). El modelo de Clark y Wilson tiene en cuenta invariantes adicionales. De manera específica, supone que un sistema de computador refleja y emula los datos y procesos que son externos al computador. Por consiguiente, la prueba final de integridad consiste en asegurar que los datos que se hallan dentro del computador son coherentes con los del mundo que se pretende que representen. De ello se sigue que los controles de integridad nunca pueden ser un asunto estrictamente interno al computador.

Como resultado, la integridad de datos del modelo Clark-Wilson puede ser considerado como un planteamiento en dos etapas:

- 1) han de existir mecanismos adecuados para iniciar los cambios, cuando los cambios sean necesarios, de modo que se mantenga la coherencia externa de los datos; y
- 2) han de existir los mecanismos adecuados que aseguren que, cuando se inician los cambios, se llevan a cabo como una operación atómica de una transacción bien constituida.

En el supuesto que los puntos anteriores reflejan con exactitud nuestra comprensión intuitiva de la integridad, nos vemos inducidos a establecer la siguiente distinción semántica:

- **Coherencia interna de datos:** Un dato es coherente internamente si todas las modificaciones de ese elemento satisfacen las políticas pertinentes de seguridad de la integridad.
- **Coherencia externa de datos:** Un dato es coherente externamente cuando su valor es conforme a la situación del mundo real que describe.

Si se acepta la distinción anterior, puede combinarse con la siguiente clasificación de la intensidad de la protección de la integridad:

- Protección fuerte es la que mantiene la coherencia interna y externa de los datos. Protección débil es la que detecta la violación de la coherencia interna y/o externa de los datos.

Por otra parte, y en la medida en que los cambios en los datos son efectuados como operaciones atómicas por procesos fiables, es posible que se desee analizar las propiedades de estas operaciones. Por ejemplo:

- 1) ¿Puede violarse la atomicidad de la operación?; y
- 2) ¿Existe la seguridad de que la operación se llevará a cabo efectivamente?

Por último, es posible que se desee clasificar los mecanismos de integridad con respecto al mantenimiento de las siguientes propiedades:

- coherencia interna/externa;
- protección débil/fuerte;
- atomicidad/seguridad de las operaciones en los datos protegidos.

Así pues, cuando se especifique un mecanismo de integridad deberá considerarse lo siguiente:

- 1) ¿Qué forma de coherencia (interna, externa, ambas) tiene el mecanismo?
- 2) ¿Proporciona el mecanismo una protección débil o fuerte de la integridad de los datos? ¿Es resistente a ataques preparados técnicamente, a cambios aleatorios, o a ambos? ¿Proporciona recuperación?
- 3) ¿Protege el mecanismo la atomicidad de las operaciones o proporciona la seguridad (también) de que la operación se llevará a cabo?

Referencias

- 1) CLARK, David y WILSON, David: A Comparison of Commercial and Military Computer Security Policies, *Proceedings of 1987 IEEE Symposium on Security and Privacy*.
- 2) NIST Special Publication 500-160: Report on the Invitational Workshop on Integrity Policy in Computer Information Systems (WIPCIS); edited by Stuart W. Katzke and Zella G. Ruthberg.
- 3) NIST Special Publication 500-168: Report on the Invitational Workshop on Data Integrity; edited by Zella Ruthberg and William T. Polk.

Anexo C

Reseña de facilidades de integridad

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

Reseña de facilidades de seguridad			Elemento	Entidad: Iniciador, verificador, integridad-TTP		
				Función:		
				Objeto de información: Datos de integridad protegida		
			Objetivo del servicio	Proteger los datos contra modificación/supresión/creación/inserción/repetición no autorizadas		
A C T I V I D A D E S		Entidad	Autoridad del dominio de seguridad (SDA)			
		Función				
		Actividad relacionada con la gestión	– Instalación de información de gestión – Modificación de información de gestión – Supresión de información de gestión		– Listado de información de gestión – Inhabilitación de información de gestión – Rehabilitación de información de gestión	
			Entidad	Iniciador	Verificador	Integridad-TTP
		Función				
		Actividad relacionada con el funcionamiento	– Blindaje de datos Etiqueta ACL Suma de control Valor de comprobación criptográfico Firma digital	– Validación de integridad Etiqueta ACL Suma de control Valor de comprobación criptográfico Firma digital – Desblindar (recuperar datos) Valor de comprobación criptográfico Firma digital	– Emisión de ACL Valor de comprobación criptográfico Suma de control Certificado	
I N F O R M A C I Ó N	Elemento de datos de entrada/salida gestionado por la SDA		– Identificadores (iniciador, verificador, integridad-TTP) – Claves criptográficas – Valor variable con el tiempo			
	Tipo de información utilizada en la operación		– Información de integridad de blindaje (SII) – Información de integridad de detección de modificación (MDII) – Información de integridad de desblindaje (UII)			
	Información de control		– Periodo de tiempo – Ruta – Ubicación – Situación del sistema			

En este anexo se utilizan los siguientes conceptos:

C.1 Entidades de integridad

La integridad en sistemas abiertos entraña algunas entidades básicas:

- iniciador;
- verificador;
- tercera parte confiable.

C.1.1 Iniciador

Entidad que genera datos de integridad protegida blindando los datos y enviándolos o almacenándolos.

C.1.2 Verificador

Entidad que recibe o extrae datos del iniciador, comprueba su valor después de validarlos para detectar fallos de integridad y, cuando es necesario, regenera el valor de los datos.

C.1.3 Tercera parte confiable para facilidades de integridad

Entidad que distribuye SII o MDI y/o realiza operaciones pertinentes a la seguridad en nombre del iniciador o del verificador.