Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1352

(09/2022)

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

Aplicaciones y servicios con seguridad (2) – Seguridad en la Internet de las cosas (IoT)

Requisitos de seguridad para los dispositivos y pasarelas de Internet de las cosas

Recomendación UIT-T X.1352

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–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	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	**X.1360–X.1369**
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad en la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD DE LAS IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1352

Requisitos de seguridad para los dispositivos y pasarelas de Internet de las cosas

Resumen

La Recomendación UIT-T X.1352 establece requisitos detallados para cinco dimensiones de seguridad aplicables al dispositivo y pasarela de Internet de las cosas (IoT): autenticación; criptografía; seguridad de los datos; seguridad de plataformas de dispositivos, y la seguridad física, basada en el modelo de referencia IoT especificado en la Recomendación UIT-T Y.4100 y el marco de seguridad IoT de la Recomendación UIT-T X.1361.

La dimensión de la autenticación incluye la autenticación del usuario, la seguridad en la utilización de las credenciales de autenticación y la autenticación de los dispositivos. La dimensión del cifrado incluye la utilización del cifrado seguro, la seguridad en la gestión de claves y la seguridad en la generación de números aleatorios. La dimensión de la seguridad de datos incluye la seguridad en la transmisión y el almacenamiento, el control del flujo de información, la seguridad en la gestión de sesiones y la gestión de la información de identificación personal (PII). La dimensión de la seguridad de plataformas de dispositivos incluye cinco elementos: seguridad del *software*, seguridad en las actualizaciones, gestión de la seguridad, registro y sello de tiempo. De manera análoga, la dimensión de la seguridad física incluye la seguridad de la interfaz física y la protección contra las manipulaciones.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1352	02/09/2022	17	11.1002/1000/14990

Palabras clave

Autenticación, criptografía, evaluación de seguridad IoT, pasarela IoT, seguridad de datos, seguridad de plataformas de dispositivos, seguridad de pasarelas y dispositivos IoT, seguridad física.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1352

Requisitos de seguridad para los dispositivos y pasarelas de Internet de las cosas

1 Cometido

Esta Recomendación establece requisitos detallados para cinco dimensiones de seguridad aplicables al dispositivo y pasarela de Internet de las cosas (IoT): autenticación; criptografía; seguridad de los datos; seguridad de plataformas de dispositivos, y seguridad física. Estos requisitos de seguridad se basan en el modelo de referencia de la IoT especificado en [UIT-T Y.4100] y en el marco de seguridad de la IoT especificado en [UIT-T X.1361].

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión; habida cuenta de ello, se alienta a los usuarios de esta Recomendación a que utilicen la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T X.1361] Recomendación UIT-T X.1361 (2018), *Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela*

[UIT-T Y.4100] Recomendación UIT-T Y.4100/Y.2066 (2014), *Requisitos comunes de la Internet de las cosas*

3 Definiciones

3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 autenticación [b-UIT-T X.1254]: Confirmación de la identidad declarada de una entidad.

3.1.2 capacidad [b-ISO 16100-1]: Conjunto de funciones y servicios con una serie de criterios para evaluar el desempeño de un proveedor de capacidad.

3.1.3 confidencialidad [b-UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.4 credencial [b-UIT-T X.1252]: Conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados.

3.1.5 número aleatorio de calidad criptográfica [b-UIT-T X.667]: Número aleatorio o número seudoaleatorio generado por un mecanismo que garantiza una separación suficiente de valores generados repetidamente para que sean aceptables para su uso en criptografía (y que se utilizan efectivamente).

3.1.6 criptografía [b-UIT-T X.800]: Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado.

3.1.7 integridad de los datos [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.8 dispositivo [b-UIT-T Y.4000]: En el contexto de la Internet de las cosas se trata de una pieza de equipo con las capacidades obligatorias de comunicación y las capacidades opcionales de detección, de accionamiento y de adquisición, almacenamiento y procesamiento de datos.

3.1.9 gestión de claves [b-UIT-T X.800]: Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves, de acuerdo con una política de seguridad.

3.1.10 gestión de parches [UIT-T X.1361]: Proceso que abarca la adquisición, prueba e instalación de múltiples parches en sistemas de información.

NOTA – Podría considerarse la capacidad de gestión de vulnerabilidad.

3.1.11 información de identificación personal (PII) [b-ISO/CEI 29100]: Toda información que a) puede utilizarse para identificar el titular de la información de identificación personal (IIP) con quien está relacionada esa información, o b) está o puede estar relacionada directa o indirectamente con el titular de la PII.

3.1.12 seguridad física [b-UIT-T X.800]: Medidas adoptadas para proporcionar la protección física de los recursos contra amenazas deliberadas o accidentales.

3.1.13 configuración segura [UIT-T X.1361]: Proceso por el que los dispositivos de red deberían configurarse para reducir el nivel de vulnerabilidades inherentes y prestar únicamente los servicios requeridos para desempeñar su función.

3.1.14 pasarela de seguridad [UIT-T X.1361]: Punto de conexión entre redes o entre subgrupos dentro de redes o entre aplicaciones de soporte lógico dentro de diferentes dominios de seguridad destinado a proteger una red según una determinada política de seguridad particular en el entorno IoT.

NOTA – El término figura a veces como pasarela. Adaptación de [b-ISO/CEI 27033-1].

3.1.15 amenaza [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.1.16 vulnerabilidad [b-ISO/CEI 27000]: Debilidad de un activo o control que puede ser aprovechada por una o más amenazas.

3.1.17 gestión de vulnerabilidad [UIT-T X.1361]: Proceso de detección, clasificación, subsanación y reducción de vulnerabilidades.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 dimensión de seguridad: Conjunto de medidas de seguridad diseñadas para solventar un determinado aspecto de la seguridad.

3.2.2 seguridad de plataformas de dispositivos: Equipo de seguridad para *firmware* y su capacidad actualizada y gestión de *software* gestionado por terceros junto con la capacidad de auditoría de que se ha dotado a un dispositivo y una pasarela de IoT.

NOTA – El *firmware* se sustituye por un *software* en un sistema operativo en función de la capacidad del soporte físico.

3.2.3 ofuscación: Efecto de una operación realizada en el código de programa o datos de la aplicación que hace que estas queden ocultas o invisibles de alguna manera sin que eso afecte al resultado del código.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API	Interfaz de programación de aplicaciones
CAPTCHA	Prueba de Turing pública y completamente automática para distinguir a los ordenadores de los humanos (*completely automated public turing test to tell computers and humans apart*)
CoAP	Protocolo de aplicación limitada (*constrained application protocol*)
DoS	Denegación de servicio (*denial of service*)
F/W	*Firmware*
FTP	Protocolo de transferencia de ficheros (*file transfer protocol*)
H/W	Soporte físico (*hardware*)
ID	Identificador
IDS	Sistema de detección de intrusiones (*intrusion detection system*)
IMEI	Identidad internacional de equipo móvil (*international mobile equipment identity*)
IoT	Internet de las cosas (*Internet of things*)
IPS	Sistema de prevención de intrusiones (*intrusion prevention system*)
LwM2M	Máquina a máquina ligeros (*lightweight machine to machine*)
MAC	Control de acceso a medios (*media access control*)
MCU	Unidad de microcontrolador (*microcontroller unit*)
MQTT	Transporte de telemetría de puesta en cola de mensajes (*message queuing telemetry transport*)
OS	Sistema operativo (*operating system*)
PII	Información de identificación personal (*personally identifiable information*)
PIN	Número de identificación personal (*personal identification number*)
S/W	Soporte lógico (*software*)
SD	Digital seguro *(secure digital*)
SHA	Algoritmo de generación numérica seguro (*secure hash algorithm*)
SNMP	Protocolo de gestión simple de red (*simple network management protocol*)
SSA	Apropiación furtiva de datos (*shoulder-surfing attack*)
SWD	Depuración de cables en serie (*serial wire debug*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
UART	Receptor/transmisor asíncrono universal (*universal asynchronous receiver/transmitter*)
UID	Identificador único (*unique identifier*)
UPnP	Disponibilidad universal sin preparativos (*universal plug and play*)
USB	Bus universal en serie (*universal serial bus*)

5 Convenios

En la presente Recomendación, se utilizan los siguientes convenios:

La expresión "se recomienda" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio.

La expresión "se requiere" o "se deberá" indica un requisito que debe cumplirse estrictamente, sin permitir desviación alguna si se va a invocar la conformidad con la presente Recomendación.

En el cuerpo de la presente Recomendación, ocasionalmente puede aparecer la expresión "puede", en cuyo caso debe interpretarse como "es capaz de".

En el Apéndice I aparecen verbos que expresan obligación que no deben interpretarse en sentido normativo.

6 Generalidades

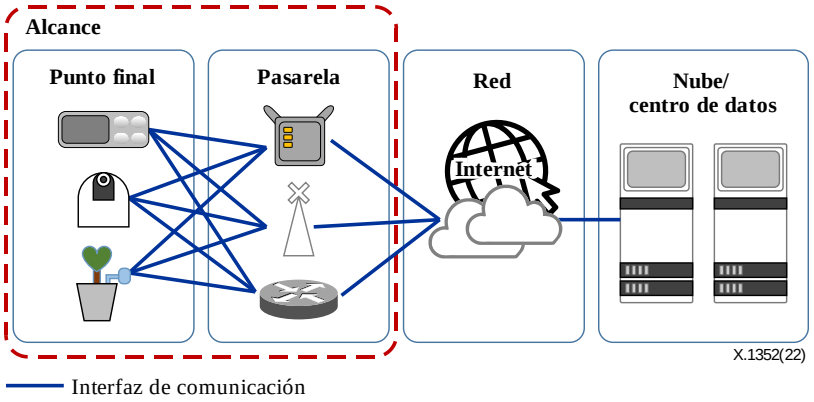

Figura 1 – Alcance de los requisitos de seguridad

Sobre la base de las capacidades de seguridad propuestas en [UIT-T X.1361] y [UIT-T Y.4100], y examinadas en el Apéndice II, se especifican requisitos de seguridad para hacer frente a los retos y amenazas de los dispositivos y pasarelas IoT (excluidos los sistemas y plataformas de red) para cinco dimensiones de seguridad, a saber, autentificación; criptografía; seguridad de los datos; seguridad de plataformas de dispositivos, y seguridad física.

La dimensión de la autenticación consiste en la autenticación del usuario, la seguridad en la utilización de las credenciales de autenticación y la autenticación de los dispositivos.

La dimensión del cifrado incluye la utilización de algoritmos de cifrado seguro, la seguridad en la gestión de claves y la seguridad en la generación de números aleatorios.

La dimensión de la seguridad de datos abarca la protección de los datos de transmisión y la protección de los datos en reposo, el control del flujo de información, la seguridad en la gestión de sesiones y la protección de la PII.

Para la dimensión de seguridad de plataformas de dispositivos, hay cinco elementos, a saber, seguridad de soporte lógico (S/W); seguridad en las actualizaciones; gestión de la seguridad; registro, y sello de tiempo.

De manera análoga, para la dimensión de la seguridad física, se han definido los conceptos de seguridad de la interfaz física y la protección contra las manipulaciones.

En la Figura 2 se muestran los objetivos de las dimensiones de seguridad para los dispositivos y pasarelas de IoT. Los dispositivos y pasarelas de IoT están comúnmente formados por una unidad de microcontrolador (MCU), un módulo de comunicación, una memoria y puertos de entrada/salida. Un

elemento seguro existe como forma de soporte físico (H/W) o S/W. En una MCU hay soporte físico (F/W), interfaces físicas y memoria. En este caso, el S/W con un sistema operativo (OS) puede sustituirse por F/W. El módulo de comunicación requiere criptografía para la seguridad de los datos en la transmisión. Los datos en las memorias flash se almacenan de forma segura para la autenticación, el cifrado y la confidencialidad/integridad de los datos. El acceso a través de interfaces físicas como un receptor/transmisor asíncrono universal (UART) también exige la autenticación del usuario. Las interfaces H/W no utilizadas se suprimirán o desconectarán.

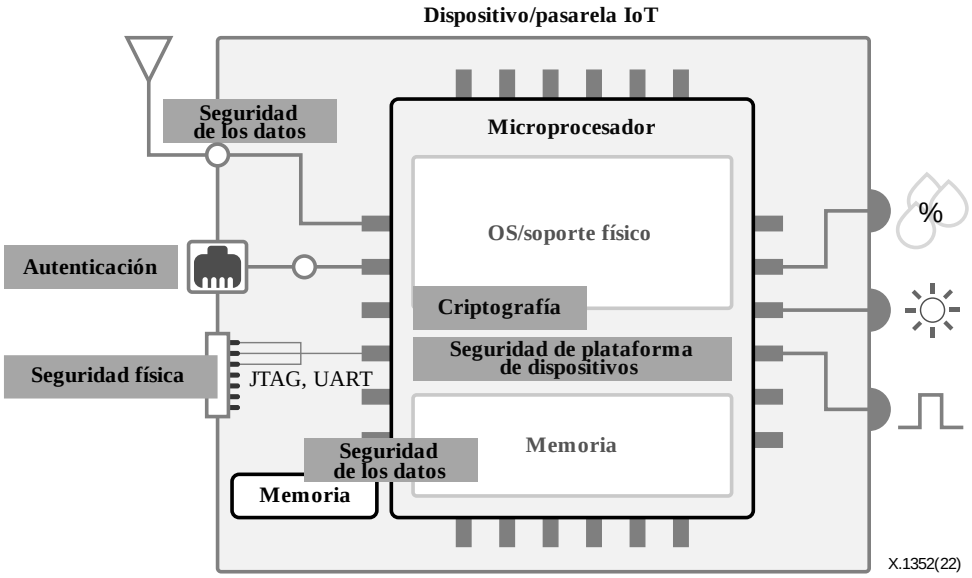

Figura 2 – Ejemplo de dimensiones de seguridad aplicadas a dispositivos y pasarelas de IoT

7 Amenazas de seguridad/vulnerabilidades para los dispositivos y pasarelas de IoT

En las cláusulas 7.1 y 7.2 se describen las amenazas de seguridad/vulnerabilidades a los dispositivos y pasarelas de IoT, que pueden convertir a estos en posibles blancos de ciberataques. Las amenazas de seguridad para las pasarelas incluyen las amenazas para los dispositivos de IoT.

7.1 Amenazas de seguridad/vulnerabilidades para los dispositivos de IoT

Entre las amenazas/vulnerabilidades específicas de que son objeto los dispositivos están las siguientes:

– AS-D-1: Salto del sistema de autenticación: un usuario no autorizado consigue acceder a un dispositivo y también puede acceder a datos críticos, por ejemplo, los datos del usuario y los archivos de configuración almacenados en el dispositivo.

– AS-D-2: Conexión de dispositivo no autorizado: un dispositivo está expuesto a algún dispositivo no autorizado, o sus datos, como los datos de usuario, pueden transmitirse a algún dispositivo no autorizado.

– AS-D-3: Privilegio excesivo: dar privilegios excesivos o innecesarios permite a un atacante acceder a todas las operaciones aceptables y a los datos controlados, en particular los datos de usuario de un dispositivo.

– AS-D-4: Intentos repetidos de autenticación no restringidos: un usuario no autorizado que realiza varios intentos de autenticación puede conseguir acceder a la cuenta de un titular genuino.

– AS-D-5: Error debido a un acceso simultáneo: un acceso simultáneo desde varias cuentas de administrador puede provocar cambios no coordinados en la configuración de funcionalidades críticas.

– AS-D-6: Exposición y adivinación de la información de autenticación: cuando la información de autenticación, como una contraseña, está codificada en firme o almacenada en texto simple, o cuando una contraseña de autenticación o número de identificación personal (PIN) se exponen en texto simple (lo que se conoce también como apropiación furtiva de datos o "SSA"), la información de autenticación puede exponerse a un atacante o ser adivinada por este.

– AS-D-7: Contraseña débil: es posible que un atacante obtenga una combinación insegura, por ejemplo con una contraseña incorrecta o débil que le permita hacerse pasar por un usuario genuino.

– AS-D-8: Número aleatorio/clave de cifrado débil: una clave criptográfica insuficiente o un número aleatorio predecible puede que no sean capaces de proteger los datos críticos.

– AS-D-9: Algoritmo criptográfico débil: un atacante puede predecir datos importantes o descubrir el texto simple de un mensaje cifrado (texto cifrado) analizando el tráfico que utilice un algoritmo criptográfico débil.

– AS-D-10: Ausencia de validación de la entrada: la ausencia de validación de la entrada puede hacer que un dispositivo funcione incorrectamente.

– AS-D-11: Exposición de datos y manipulación de datos: los datos críticos, como los datos de usuario, la configuración de dispositivos y las claves criptográficas, que se transmiten mediante un dispositivo o se almacenan en este pueden estar expuestos a un atacante o ser explotados o manipulados por este.

– AS-D-12: Pirateo de sesión de usuario: un atacante puede obtener un acceso no autorizado a la cuenta de un usuario genuino cuya sesión se ha cerrado de manera anormal o explotar sesiones válidas de varios dispositivos que utilizan la misma clave criptográfica.

– AS-D-13: Actualización insegura: cuando el archivo previsto para la actualización no es descargable o existe la posibilidad de ejecutar un archivo de actualización manipulado cuyo origen no ha sido autorizado/autentificado.

– AS-D-14: Fallo de la actualización: un error producido durante la actualización puede causar un funcionamiento anormal de los dispositivos.

– AS-D-15: Error de integridad: una manipulación no intencionada de los códigos ejecutables o los valores de configuración puede provocar errores de funcionamiento de un dispositivo.

– ST-D-16: Código malicioso S/W: un código que tiene funciones no intencionadas puede utilizarse con fines maliciosos.

– AS-D-17: Explotación de información de memoria residual: la clave criptográfica, la contraseña y los datos sensibles utilizados para las operaciones criptológicas, las autenticaciones y las transmisiones de datos permanecen en la memoria y pueden ser explotados.

– AS-D-18: Modificación no intencionada de las configuraciones críticas: la ausencia de controles de seguridad de los dispositivos puede provocar cambios no intencionados de las configuraciones críticas y prestaciones de servicios no seguras.

– AS-D-19: Respuesta de error insegura: la no detección adecuada de errores y comportamientos maliciosos y la ausencia de respuesta a estos pueden provocar prestaciones de servicios no seguras.

– AS-D-20: Desarrollo no seguro: las posibles vulnerabilidades de seguridad pueden proceder del diseño y la implementación de un dispositivo, y es posible que no se haya realizado o se haya realizado de manera inadecuada la evaluación de dichas vulnerabilidades o que no se haya dado respuesta a ellas o se haya hecho de manera inadecuada.

– AS-D-21: Sistema operativo vulnerable: las funcionalidades de un dispositivo pueden resultar comprometidas o eludidas en el entorno de un sistema operativo vulnerable.

– AS-D-22: módulos o bibliotecas vulnerables de terceros: los módulos o bibliotecas vulnerables de terceros pueden permitir a un atacante acceder a los que estén en peligro.
– AS-D-23: Registro de información sensible insegura en el registro del sistema: la información sensible inscrita en el registro de un sistema puede estar expuesta a un atacante y ser utilizada por este.
– AS-D-24: Exposición de información crítica mediante el proceso de depuración: es posible que se exponga información crítica a un atacante o que este la utilice a través del proceso de generación de registro y depuración cuando se desbloquea y distribuye un dispositivo.
– AS-D-25: Acceso físico no autorizado: cuando un dispositivo se expone a un acceso físico no autorizado y a cambios no intencionados en su configuración.

7.2 Amenazas de seguridad/vulnerabilidades para las pasarelas de IoT

Entre las amenazas/vulnerabilidades específicas de que son objeto las pasarelas están las siguientes:

– AS-P-1: Transmisión de datos no fiables: la transmisión de datos no fiables puede hacer que un dispositivo funcione de manera incorrecta o que se distribuyan códigos maliciosos.
– AS-P-2: Denegación de servicio (DoS) o denegación de servicio distribuida (DoS): un ataque DoS puede hacer que un dispositivo deje de estar disponible.

8 Requisitos de seguridad

En esta Recomendación se especifican los requisitos de seguridad para los dispositivos y pasarelas IoT basados en las cinco dimensiones de seguridad definidas en la cláusula 6, y se establece un conjunto de requisitos de seguridad basado en las disposiciones del modelo de amenaza y las propiedades funcionales específicas de la IoT, etc. La capacidad de seguridad se basa en [UIT-T X.1361], como se indica en el Apéndice II.

8.1 Autenticación

La dimensión de la autenticación consiste en la autenticación del usuario, la seguridad en la utilización de las credenciales de autenticación y la autenticación de los dispositivos.

8.1.1 Autenticación del usuario

Se requiere modificar la contraseña por defecto del fabricante (AU-1-1).

– Habrá que definir una contraseña en el momento de la autenticación inicial o cuando deba modificarse tras ella.
– Hay que velar por que la contraseña no coincida con el valor inicial u otro valor anterior.

El usuario deberá primeramente ser identificado y autentificado cuando se acceda a la gestión de seguridad o a datos sensibles (AU-1-2).

– Al acceder a la gestión de la seguridad, como la configuración de un dispositivo de IoT, la cuenta de usuario o los privilegios, el usuario deberá ser identificado y autentificado.
– Los usuarios con acceso privilegiado a la gestión de seguridad o a los datos sensibles deberán gestionarse separadamente de los usuarios normales.

El número de intentos de autenticación deberá ser limitado (AU-1-3).

– Un dispositivo de IoT puede ser vulnerable a los ataques de fuerza bruta si se permiten los intentos de autenticación repetidos. Por consiguiente, deberá ofrecer una función para responder adecuadamente a los continuos intentos de autenticación.

– Esta función puede proporcionarse mediante uno de los métodos siguientes:

  a) limitando el número de intentos de autenticación para bloquear la cuenta o desactivar la función de autenticación durante un periodo de tiempo determinado (se recomienda limitar el número de intentos de autenticación a cinco como máximo y desactivar la función de autenticación durante cinco minutos como mínimo);

  b) cuando se supere el número indicado de intentos de autenticación, habrá que considerar que hay un tráfico de red no autorizado y agregar al usuario a la lista de bloqueo automático (se recomienda limitar el número de intentos de autenticación a diez como máximo);

  c) aplicación de prueba de Turing pública y completamente automática para distinguir a los ordenadores de los humanos (Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA).

La contraseña preinstalada del dispositivo debe ser única (AU-1-4).

Se debe proporcionar una función para gestionar las cuentas y privilegios de los usuarios (AU-1-5).

– Debe ser posible gestionar todas las cuentas de usuario (incluidas la cuenta de administrador) utilizadas en un dispositivo de IoT, por ejemplo, añadirlas y suprimirlas, así como asignar privilegios.

– Si se utiliza un modelo de control de acceso basado en roles, se deben especificar claramente los privilegios de acceso para todas las funciones del dispositivo de IoT y asignar los privilegios en consecuencia.

Se debe aplicar el principio de privilegio mínimo a todas las cuentas de usuario (AU-1-6).

– Se deben asignar los privilegios basados en roles a todas las cuentas de usuario.

Se debe restringir el acceso simultáneo a la cuenta de administrador (AU-1-7).

– El acceso simultáneo de los servicios de gestión debe limitarse a la misma cuenta de administrador y se debe proporcionar una función para desconectar los accesos anteriores o limitar los intentos de nuevos accesos.

Se debe proporcionar una contraseña segura en cuanto a su longitud, ciclo y complejidad (AU-1-8).

– Los dispositivos de IoT deben proporcionar una función para que el usuario defina una contraseña segura teniendo en cuenta su longitud, ciclo y complejidad.

8.1.2 Seguridad en la utilización de credenciales

No se deben utilizar credenciales codificadas en firme (AU-2-1).

– Las contraseñas (PIN, código secreto, etc.) no se deben codificar en firme ni guardarse en texto simple.

Durante la autenticación mediante contraseña, la contraseña debe enmascararse (AU-2-2).

– Si una contraseña se muestra en texto simple, podrá ser vulnerable a un ataque de tipo SSA. Por tanto, para evitar esta visualización en la entrada de la contraseña, los caracteres de los componentes de la contraseña deberían enmascararse, por ejemplo, utilizando asteriscos ("*").

No se debería proporcionar información específica sobre el fallo de la autenticación (AU-2-3).

8.1.3 Autenticación de dispositivos

Se deberá mantener el identificador único (UID) de cada dispositivo H/W (AU-3-1). Véase el Cuadro 1.

– El dispositivo de IoT deberá tener un identificador (ID) único y fijo.

Cuadro 1 – UID de dispositivos de IoT

ID	Descripción
Dirección de control de acceso a los medios (MAC)	Identificador único asignado a la interfaz de red para establecer la comunicación en la capa de enlace de datos del segmento de red (48 bits).
Identidad internacional de equipo móvil (IMEI), número de autenticación de terminal móvil internacional	Número único asignado a los teléfonos inteligentes. Lo asigna el fabricante en el momento de la comercialización de los teléfonos móviles. Consta de 15 cifras en total, a saber: un código de aprobación (ocho cifras); un número de serie de modelo (seis cifras); y un número de verificación (una cifra).

Los dispositivos deben autenticarse mutuamente antes de que se transmitan datos sensibles o estarán interconectados a efectos de control (AU-3-2).

– Algunos ejemplos de autenticación mutua son:

a) la utilización de una clave privada basada en el método de cifrado de clave pública;

b) la utilización de atributos de seguridad (UID, clave, etc.) y chips de seguridad;

c) la aplicación de la seguridad de la capa de transporte (TLS) (o la TLS de datagramas) al protocolo ligero de comunicación, es decir, el protocolo de aplicación limitada (CoAP), protocolo máquina a máquina ligeros (LwM2M), o el transporte de telemetría de puesta en cola de mensajes (MQTT).

8.2 Criptografía

– Si es difícil utilizar algoritmos criptográficos generales debido a la limitada capacidad de memoria y almacenamiento, se utilizarán algoritmos criptográficos ligeros.

– Deberían utilizarse algoritmos criptográficos para la protección contra ataques de canal secundario.

Las claves criptográficas deberán gestionarse de manera segura a lo largo de todo su ciclo de vida (CR-1-2).

– Las claves se deben generar, actualizar, distribuir, utilizar, almacenar y destruir de manera segura.

Debería generarse un número aleatorio dentro de un algoritmo con aleatoriedad demostrada (CR-1-3).

8.3 Seguridad de los datos

La dimensión de la seguridad de datos abarca la protección de los datos de transmisión y la protección de los datos en reposo, el control del flujo de información, la seguridad en la gestión de sesiones y la protección de la PII.

8.3.1 Seguridad en la transmisión y el almacenamiento

Deberán cifrarse los datos transmitidos (DS-1-1).

– Los datos transmitidos deberán cifrarse utilizando un algoritmo criptográfico seguro (véase CR-1-1).

Se debe aplicar un modo seguro cuando se cree un canal de control o datos (DS-1-2).

– Cuando se transmiten datos, debería utilizarse un protocolo de seguridad que garantice la confidencialidad e integridad de los datos transmitidos, así como la autenticación de las partes origen y destino.

Se deberán cifrar los datos almacenados en los dispositivos (DS-1-3).

– Los datos almacenados en dispositivos deberán cifrarse utilizando un algoritmo criptográfico seguro (véase CR-1-1).

Los datos suprimidos no serán restablecidos (DS-1-4).

– Si es necesario deshacerse de un dispositivo, actualizarlo o sustituirlo, se debe proporcionar una función de supresión (por ejemplo, la inicialización de fábrica) para que no puedan recuperarse los datos.

8.3.2 Control del flujo de información

No debe permitirse el tráfico de red no autorizado (DS-2-1).

8.3.3 Seguridad en la gestión de sesiones

La sesión debe cerrarse después de la terminación del temporizador de reposo (DS-3-1).

– Si se accede de nuevo tras el cierre de la sesión, se debe realizar otra vez la autenticación.

El ID de sesión debe ser un valor impredecible (DS-3-2).

– Se debe aplicar un algoritmo numérico aleatorio seguro a la generación del ID de sesión.

– En cada autentificación de sesión, se debe cambiar el ID de sesión y se deben suprimir los ID de sesión que se hayan utilizado.

8.3.4 Gestión de PII

La PII debe gestionarse de manera segura a lo largo del ciclo de vida de la clave (DS-4-1).

– Las PII se deben recopilar, utilizar, almacenar y destruir de manera segura.

8.4 Seguridad de plataformas de dispositivos

Para la dimensión de seguridad de plataformas de dispositivos, hay cinco elementos, a saber, seguridad de S/W; seguridad en las actualizaciones; gestión de la seguridad; registro, y sello de tiempo.

8.4.1 Seguridad de soporte lógico

Se debe aplicar la codificación segura (PL-1-1).

– El S/W se debe diseñar e implementar teniendo en cuenta la seguridad.

Se deben comprobar y suprimir las vulnerabilidades de seguridad conocidas (PL-1-2).

– Si el S/W se desarrolló utilizando protocolos y bibliotecas, interfaces de programación de aplicaciones (API), paquetes o programas informáticos de código abierto que contengan vulnerabilidades de seguridad conocidas, es posible que el F/W y el sistema operativo también las tengan.

– Se deberá utilizar el dominio público de las vulnerabilidades de seguridad conocidas (p. ej., [b-CVE]), para comprobar las vulnerabilidades de seguridad del dispositivo y suprimirlas.

Se debe aplicar la ofuscación (PL-1-3).

– Estos requisitos pueden aplicarse principalmente a las aplicaciones desarrolladas (aplicaciones), lo que facilita la restauración del código fuente.

– Dado que las herramientas de ingeniería inversa de código abierto pueden utilizarse para extraer información lógica o clave importante, es necesario contar con un nivel apropiado de protección.

Debe soportarse una función de verificación de la integridad para los parámetros de configuración y los códigos ejecutables (PL-1-4).

– A fin de garantizar la validez del dispositivo de IoT, se debe comprobar la integridad de los parámetros de configuración y los códigos ejecutables en el momento de su arranque, de manera periódica automática o manualmente.

Se implementa una acción de respuesta apropiada en caso de que haya un error de integridad.

8.4.2 Seguridad en las actualizaciones

Las actualizaciones deberán ser realizadas por usuarios autorizados (PL-2-1).

Debe soportarse la función de restitución por si fallase la actualización (PL-2-2).

La integridad y la autenticación deben comprobarse antes de una actualización (PL-2-3).

– La autenticación se debería realizar con respecto al usuario que realiza la actualización, las verificaciones de integridad se deberían comparar con la dirección del servidor de actualización y ambas deberían compararse con el fichero de actualización.
– La autenticidad de un usuario puede ser confirmada mediante la reautenticación del usuario inmediatamente antes del procedimiento de actualización.
– Un usuario autorizado puede verificar la integridad de la dirección del servidor de actualización mediante una inspección visual.
– La verificación de la integridad y autenticidad de los ficheros de actualización puede efectuarse verificando una firma digital criptográfica.

8.4.3 Gestión de la seguridad

Se deben desactivar los servicios innecesarios (PL-3-1).

– Se deben desactivar los servicios innecesarios (Telnet, el protocolo de transferencia de ficheros (FTP), la disponibilidad universal sin preparativos (UPnP), el protocolo de gestión simple de red (SNMP), etc.) y se deben especificar los servicios necesarios prestados por el dispositivo.

La gestión a distancia se debe realizar en un entorno fiable (PL-3-2).

Se debe aplicar una biblioteca segura de terceros (PL-3-3).

– La biblioteca de terceros y el módulo utilizado para el desarrollo deben corresponder a la versión más reciente, y carecer de vulnerabilidades o defectos de seguridad conocidos.

Se debe proporcionar una autoprueba (PL-3-4).

– Se debe proporcionar una función de autoprueba para detectar los errores del H/W y el S/W principal cuando se inicia (enciende) un dispositivo de IoT o después de su inicio.

8.4.4 Registro

Se debe generar el registro para los eventos relacionados con la seguridad (PL-4-1).

– El registro debe implementarse y debe ser posible detectar y rastrear todo comportamiento anormal del dispositivo.

Debe proporcionarse un mecanismo de registro seguro (PL-4-2).

– A fin de hacer frente a su pérdida y sus cambios no autorizados (incluida la supresión), debe haber un mecanismo para proteger los registros.

8.4.5 Sello de tiempo

Se debe proporcionar un sello de tiempo fiable (PL-5-1).

8.5 Seguridad física

La dimensión de seguridad física implica proteger las interfaces físicas y los dispositivos IoT contra la alteración.

8.5.1 Interfaz física segura

Se debe desactivar toda interfaz externa innecesaria (PH-1-1).

– Se deben especificar las dimensiones y funciones de todas las interfaces externas (red de área local, bus universal en serie (USB), puerto de la tarjeta Secure Digital (SD), etc.) expuestas al exterior.

– Si es necesario, se debe controlar el acceso para prevenir el acceso no autorizado.

Se deberá prevenir el acceso no autorizado a la interfaz interna (PH-1-2).

– Se deben especificar las dimensiones y funciones de todas las interfaces internas (Grupo de acción de prueba conjunta (JTAG), depuración de cables en serie (SWD), UART, etc.) expuestas al exterior.

– Si es necesario, se debe realizar un control de acceso para prevenir el acceso no autorizado.

8.5.2 Protección contra las manipulaciones

Se debe soportar una función para la detección de manipulaciones físicas no autorizadas y para la respuesta a dichas manipulaciones (por ejemplo, sellos a prueba de manipulaciones, cerraduras, sistema de reacción en caso de manipulación, interruptores y alarmas de reseteo) (PH-2-1).

Anexo A

Lista de correspondencias entre los requisitos de seguridad de la Internet de las cosas y las amenazas de seguridad/vulnerabilidades

(El presente anexo es parte integrante de la Recomendación.)

Los requisitos de seguridad de la IoT se enumeran y describen en la cláusula 8 y las amenazas de seguridad/vulnerabilidades se especifican en la cláusula 7. En el Cuadro A.1 se muestra la correspondencia entre los requisitos de seguridad de la IoT y las amenazas de seguridad/vulnerabilidades.

Cuadro A.1 – Lista de correspondencias entre requisitos de seguridad de IoT y amenazas de seguridad/vulnerabilidades

Número del requisito	Dimensión del requisito	Descripción del requisito	Amenazas de seguridad/vulnerabilidades
AU-1-1	Autenticación	Se requiere modificar la contraseña por defecto del fabricante.	AS-D-6
AU-1-2	Autenticación	El usuario deberá primeramente ser identificado y autentificado cuando se acceda a la gestión de seguridad o a datos sensibles.	AS-D-1
AU-1-3	Autenticación	El número de intentos de autenticación deberá ser limitado.	AS-D-4 AS-D-5
AU-1-4	Autenticación	La contraseña preinstalada del dispositivo debe ser única.	AS-D-1
AU-1-5	Autenticación	Se debe proporcionar una función para gestionar las cuentas y privilegios de los usuarios.	AS-D-3
AU-1-6	Autenticación	Se debe aplicar el principio de privilegio mínimo a todas las cuentas de usuario.	AS-D-3
AU-1-7	Autenticación	Se debe restringir el acceso simultáneo a la cuenta de administrador.	AS-D-1
AU-1-8	Autenticación	Se debe proporcionar una contraseña segura en cuanto a su longitud, ciclo y complejidad.	AS-D-7
AU-2-1	Autenticación	No se deben utilizar credenciales codificadas en firme.	AS-D-6
AU-2-2	Autenticación	Durante la autenticación mediante contraseña, la contraseña debe enmascararse.	AS-D-6
AU-2-3	Autenticación	No se debería proporcionar información específica sobre el fallo de la autenticación.	AS-D-6
AU-3-1	Autenticación	Se debe conservar el ID único de cada dispositivo *hardware*.	AS-D-2

Cuadro A.1 – Lista de correspondencias entre requisitos de seguridad de IoT y amenazas de seguridad/vulnerabilidades

Número del requisito	Dimensión del requisito	Descripción del requisito	Amenazas de seguridad/vulnerabilidades
AU-3-2	Autenticación	Los dispositivos deben autenticarse mutuamente antes de que se transmitan o controlen datos antes de la interconexión.	AS-D-2
CR-1-1	Criptografía	Se utilizarán algoritmos de cifrado seguros cuando se transmitan o almacenen datos.	AS-D-8 AS-D-9
CR-1-2	Criptografía	Las claves criptográficas deberán gestionarse de manera segura a lo largo de todo su ciclo de vida.	AS-D-8
CR-1-3	Criptografía	Debería generarse un número aleatorio dentro de un algoritmo con aleatoriedad demostrada.	AS-D-8
DS-1-1	Seguridad de los datos	Deberán cifrarse los datos transmitidos.	AS-D-11
DS-1-2	Seguridad de los datos	Se debe aplicar un modo seguro cuando se cree un canal de control o datos.	AS-D-11
DS-1-3	Seguridad de los datos	Se deberán cifrar los datos almacenados en el dispositivo.	AS-D-11
DS-1-4	Seguridad de los datos	Los datos suprimidos no serán restablecidos.	AS-D-17
DS-2-1	Seguridad de los datos	No debe permitirse el tráfico de red no autorizado.	AS-G-1
DS-3-1	Seguridad de los datos	La sesión debe cerrarse después de la terminación del temporizador de reposo.	AS-D-12
DS-3-2	Seguridad de los datos	El ID de sesión debe ser un valor impredecible.	AS-D-12
DS-4-1	Seguridad de los datos	La PII debe gestionarse de manera segura a lo largo del ciclo de vida de la clave.	AS-D-11
PL-1-1	Seguridad de plataformas de dispositivos	Se debe aplicar la codificación segura.	AS-D-10 AS-D-20 AS-D-23 AS-D-24
PL-1-2	Seguridad de plataformas de dispositivos	Se deben comprobar y suprimir las vulnerabilidades de seguridad conocidas.	AS-D-16 AS-D-21
PL-1-3	Seguridad de plataformas de dispositivos	Se debe aplicar la ofuscación.	AS-D-16

Cuadro A.1 – Lista de correspondencias entre requisitos de seguridad de IoT y amenazas de seguridad/vulnerabilidades

Número del requisito	Dimensión del requisito	Descripción del requisito	Amenazas de seguridad/vulnerabilidades
PL-1-4	Seguridad de plataformas de dispositivos	Debe soportarse una función de verificación de la integridad para los parámetros de configuración y los códigos ejecutables.	AS-D-15
PL-2-1	Seguridad de plataformas de dispositivos	Las actualizaciones deberán ser realizadas por un usuario autorizado.	AS-D-13
PL-2-2	Seguridad de plataformas de dispositivos	Debe soportarse la función de restitución por si fallase la actualización.	AS-D-14
PL-2-3	Seguridad de plataformas de dispositivos	La integridad y la autenticación deben comprobarse antes de una actualización.	AS-D-15
PL-3-1	Seguridad de plataformas de dispositivos	Se deben desactivar los servicios innecesarios.	AS-D-16
PL-3-2	Seguridad de plataformas de dispositivos	La gestión a distancia se debe realizar en un entorno fiable.	AS-D-18
PL-3-3	Seguridad de plataformas de dispositivos	Se debe aplicar una biblioteca segura de terceros.	AS-D-22
PL-3-4	Seguridad de plataformas de dispositivos	Se debe proporcionar una autoprueba.	AS-D-19
PL-4-1	Seguridad de plataformas de dispositivos	Se debe generar el registro para los eventos relacionados con la seguridad.	AS-D-23
PL-4-2	Seguridad de plataformas de dispositivos	Debe proporcionarse un mecanismo de registro seguro.	AS-D-23
PL-5-1	Seguridad de plataformas de dispositivos	Se debe proporcionar un sello de tiempo fiable.	AS-D-18
PH-1-1	Seguridad física	Se debe desactivar toda interfaz externa innecesaria.	AS-D-24 AS-D-25
PH-1-2	Seguridad física	Se deberá prevenir el acceso no autorizado a la interfaz interna.	AS-D-24 AS-D-25

Cuadro A.1 – Lista de correspondencias entre requisitos de seguridad de IoT y amenazas de seguridad/vulnerabilidades

Número del requisito	Dimensión del requisito	Descripción del requisito	Amenazas de seguridad/vulnerabilidades
PH-2-1	Seguridad física	Se debe soportar una función para la detección de manipulaciones físicas no autorizadas y para la respuesta a dichas manipulaciones (por ejemplo, sellos a prueba de manipulaciones, cerraduras, sistema de reacción en caso de manipulación e interruptores y alarmas de reseteo).	AS-D-24 AS-D-25

Apéndice I

Capacidades de seguridad de la Internet de las cosas

(Este apéndice no forma parte integrante de esta Recomendación.)

I.1 Generalidades

En la presente Recomendación sólo se estudian requisitos de seguridad y se tiene en cuenta la fiabilidad y la calidad de los servicios. Se amplían las capacidades de seguridad de la IoT respecto de las descritas en [UIT-T X.1361]. La arquitectura de la IoT debe incluir las capacidades generales enumeradas en el Cuadro I.1.

Cuadro I.1 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad

Capacidades	Requisitos relacionados
Capacidad de comunicación segura para soportar comunicaciones seguras, fiables y con protección de la privacidad	DP-1-1, DS-1-2
Capacidad de gestión de claves segura para soportar comunicaciones seguras	CR-2-1
Capacidad de gestión de datos segura para proporcionar una gestión de datos segura, fiable y con protección de privacidad	DS-2-1, DS-1-4
Capacidad de autenticación para la autenticación de dispositivos	AU-1-1, AU-1-2, AU-1-3, AU-1-4, AU-1-8
Capacidad de autorización (control de acceso) para autorizar dispositivos	AU-3-1, AU-3-2
Capacidad de auditoría para monitorizar el acceso a datos o los intentos de acceder a las aplicaciones de IoT de manera totalmente transparente, rastreable y reproducible, basándose en reglamentos y leyes apropiados	PL-4-1, PL-4-2
Capacidad de prestación de servicios segura para prestar servicios de modo seguro, fiable y con protección de privacidad	DS-4-1, DS-3-2
Capacidad de integración segura para integrar diferentes políticas y técnicas de seguridad relativas a la variedad de componentes funcionales IoT	–
Capacidad de implementar protocolos seguros utilizando algoritmos criptográficos normalizados y a disposición del público	CR-1-1
Capacidad de implementar protocolos seguros basándose en criptografía ligera	CR-1-1
Capacidad de actualización de soporte lógico segura y estructurada para actualizar módulos de soporte lógico o aplicaciones	PL-2-1, PL-2-2, PL-2-3
Capacidad de gestión de identidades para dispositivos/sensores de IoT, pasarelas y plataformas/servicios	AU-2-1, AU-2-2, AU-2-3, DS-3-2, DS-4-1
Capacidad de análisis de la vulnerabilidad	–
Capacidad de monitorizar el acceso a datos o los intentos de acceder a las aplicaciones de IoT de manera totalmente transparente, rastreable y reproducible	PL-4-1, PL-4-2
Capacidad de seguridad de soporte físico (por ejemplo, módulo de plataforma de confianza) para evitar los riesgos de seguridad física que acompañan la virtualización de la pasarela y red	PH-1-1, PH-1-2, PH-2-1
Capacidad de encaminamiento multitrayecto para evitar ataques de retransmisión selectiva	–

Cuadro I.1 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad

Capacidades	Requisitos relacionados
Capacidad de protección de la PII contra ataques PII a lo largo de todo el ciclo de vida PII	DS-4-1
Capacidad de configuración segura	–
Capacidad mediante criptografía ligera	CR-1-1
Capacidad de encriptación simple con encriptación con datos de máscara asociados (EAMD) [b-UIT-T X.1362] para comunicar con otras entidades, incluida la pasarela	–

La arquitectura de la IoT debe incluir las capacidades relacionadas con los algoritmos criptográficos enumeradas en el Cuadro I.2.

Cuadro I.2 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para los algoritmos criptográficos

Capacidades	Requisitos relacionados
Capacidad de producción de un número aleatorio de calidad criptográfica para soportar la gestión de claves [b-IETF RFC 4086]	CR-3-1
Capacidad de actualización periódica de las claves criptográficas necesarias para trenes de radiodifusión	–
Capacidad de utilizar algoritmos criptográficos normalizados	CR-1-1

La arquitectura de la IoT debe incluir las capacidades relacionadas con el contexto enumeradas en el Cuadro I.3.

Cuadro I.3 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para el contexto

Capacidades	Requisitos relacionados
Capacidad de resistir a ataques de canal paralelo	–
Capacidad de soportar prácticas de codificación segura para que se aplique una validación rigurosa de datos en sistemas y servicios, aplicaciones de bases de datos y servicios web	PL-1-1, PL-1-3, PL-1-4
Capacidad de realizar una evaluación del riesgo planificado para determinar riesgos en contextos operativos	PL-1-4

I.2 Capacidades de seguridad de sensores/dispositivos

Los sensores/dispositivos de la IoT deberían incluir las capacidades generales enumeradas en el Cuadro I.4.

Cuadro I.4 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para los sensores/dispositivos de la IoT

Capacidades	Requisitos relacionados
Capacidad de gestión de claves	CR-2-1
Capacidad de negociación de algoritmo criptográfico	CR-1-1
Capacidad de encriptación de datos y, en algunos casos, de datos de plano de señalización, control y gestión para reducir los problemas de seguridad relativos a la confidencialidad de los datos transmitidos por redes inalámbricas	CR-1-1, DS-1-1, DS-1-2
Capacidad de integridad de datos para datos transmitidos por redes inalámbricas utilizando programas de protección de integridad adecuados que ofrecen garantías de que los datos de usuario o de señalización, control o gestión no han sido manipulados ni alterados	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Capacidad de autenticación del origen de los datos o de las identidades de los sensores/dispositivos de IoT y de los administradores y personal de mantenimiento de las redes de sensores	AU-1-2, AU-1-6, PL-2-1
Capacidad de gestión de parches, incluidos los módulos de soporte lógico seguros de actualización y transformación	PL-2-1, PL-2-2, PL-2-3
Capacidad de implementar protocolos seguros sobre la base de criptografía ligera	CR-1-1
Capacidad de control de acceso para que sólo los usuarios o dispositivos autorizados puedan acceder a elementos de red, información almacenada, flujos de información, servicios y aplicaciones	AU-1-2, AU-3-1, AU-3-2
Capacidad de prevención o detección de manipulaciones	PH-2-1
Capacidad de producir números aleatorios de calidad criptográfica para soportar la gestión de claves	CR-3-1
Capacidad de resistir a ataques de canal paralelo	–
Capacidad de protección y detección de *software* malintencionado	–
Capacidad de protección de la PII contra las violaciones de PII	DS-4-1

Los dispositivos de la IoT deberían incluir las capacidades generales enumeradas en el Cuadro I.5.

Cuadro I.5 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para los dispositivos de la IoT

Capacidades	Requisitos relacionados
Capacidad de verificar la autenticidad e integridad del soporte lógico en un dispositivo utilizando firmas digitales generadas criptográficamente [b-ISO/CEI 9796-3]	PL-1-4
Capacidad de cortafuego, detección de intrusiones, protección contra intrusiones o inspección detallada de paquetes para controlar el tráfico destinado a terminar en un dispositivo	DS-2-1
Capacidad de realizar configuraciones seguras	PL-1-4

I.3 Capacidades de seguridad de pasarelas

La plataforma/servicio debería incluir las capacidades generales enumeradas en el Cuadro I.6.

Cuadro I.6 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para la pasarela

Capacidades	Requisitos relacionados
Capacidad de sistema de detección de intrusiones (IDS)/de sistema de prevención de intrusiones (IPS)	DS-2-1
Capacidad de gestión de claves	CR-2-1
Capacidad de realizar configuraciones seguras	PL-1-4
Capacidad de negociación de algoritmo criptográfico	CR1-1
Capacidad de encriptar datos y, en algunos casos, datos de plano de señalización, control y gestión con dispositivos y componentes IoT en el centro de datos para reducir los problemas de seguridad relativos a la confidencialidad de los datos transmitidos por redes inalámbricas	CR-1-1, DS-1-1, DS-1-2
Capacidad de integridad para datos transmitidos por redes inalámbricas utilizando programas de protección de integridad adecuados que ofrecen garantías de que los datos de usuario o de señalización, control o gestión no han sido manipulados ni alterados	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Capacidad de disponibilidad para gestionar ataques de negación de servicio, desde el uso de técnicas de codificación de fuente seguras, pruebas de análisis de código de fuente y pruebas de vulnerabilidad hasta el uso de IDS/IPS basados en red o huésped	PL-1-1
Capacidad de autenticación del origen de los datos o de las identidades de los sensores/dispositivos de IoT y de los administradores y personal de mantenimiento de las redes de sensores	AU-1-2, AU-1-6, PL-2-1
Capacidad de control de acceso para que sólo los usuarios o dispositivos autorizados puedan acceder a elementos de red, información almacenada, flujos de información, servicios y aplicaciones	AU-1-2, AU-3-1, AU-3-2
Capacidad de responsabilización de dispositivo IoT para que toda infracción en materia de políticas pueda rastrearse hasta un dispositivo en concreto	PL-4-1
Capacidad de actualizar módulos de soporte lógico seguros	PL-2-1, PL-2-2, PL-2-3

I.4 Capacidades de seguridad de red

De conformidad con la [b-UIT-T X.805], las redes deben incluir las capacidades de seguridad enumeradas en el Cuadro I.7.

Cuadro I.7 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para la red

Temas	Capacidades	Requisitos relacionados
C_NT.1 [b-UIT-T X.805]	La dimensión de seguridad de la comunicación garantiza que la información sólo circule entre los puntos extremo autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremo)	PL-3-1

I.5 Capacidades de seguridad de plataformas/servicio

La plataforma/servicio debería incluir las capacidades generales enumeradas en el Cuadro I.8.

Cuadro I.8 – Cuadro de correspondencias entre los requisitos de seguridad y las funciones de seguridad para plataforma/servicio

Capacidades	Requisitos relacionados
Capacidad de proteger una credencial de operaciones criptográficas, que es un grupo de datos presentados como prueba de títulos y/o identidades alegados	DS-2-1
Capacidad de modificar nombres de usuarios y contraseñas por defecto durante la configuración inicial	AU-1-1, AU-1-2
Capacidad de aplicar contraseñas seguras y políticas de control de acceso granular	AU-1-4, AU-1-6
Capacidad de poner a disposición puertos no necesarios	PL-3-1, PH-1-1, PH-1-2
Capacidad de soportar una configuración segura, por ejemplo, para eliminar servicios y soportes lógicos innecesarios	AU-1-5, PL-3-1
Capacidad de protección contra infecciones de *software* maligno utilizando un soporte lógico de protección contra esas amenazas	PL-3-4
Capacidad de aplicar políticas de gestión de parches	PL-2-1, PL-2-2, PL-2-3
Capacidad de gestionar vulnerabilidades	PL-1-1, PL-1-2
Capacidad de actualizar módulos y aplicaciones de soporte lógico seguros	PL-2-1, PL-2-3
Capacidad de gestionar claves para transferir mensajes de forma segura entre una pasarela y una plataforma/servicio	CR-1-2
Capacidad de negociación de algoritmo criptográfico para establecer una tunelización segura entre la pasarela y la plataforma/servicio en caso de que se necesite una transferencia de mensajes segura entre ambas; capacidad de disponibilidad para gestionar ataques de negación de servicio	AU-1-5, DS-1-1, DS-1-2
Capacidad de monitorizar la red	–
Capacidad de proteger la PII en reposo	DS-4-1
Capacidad de seguridad de nivel de aplicación para prevenir los ataques y amenazas de nivel de aplicación descritos en la cláusula 8.4 de [UIT-T X.1361]	–
Capacidad de ofrecer apoyo para reducir los ataques de inferencia	–

Apéndice II

Casos prácticos sobre la aplicación de requisitos de seguridad para dispositivos y pasarelas de la Internet de las cosas

(Este apéndice no forma parte integrante de esta Recomendación.)

Muchos dispositivos de IoT tienen vulnerabilidades y deficiencias de seguridad respecto de la autenticación, la criptografía y la protección de datos. Además, la mayoría de ellos son vulnerables a las interfaces físicas y las plataformas de desarrollo de dispositivos. En este apéndice se describen casos relativos al desarrollo de la seguridad en relación con los requisitos propuestos.

II.1 Caso práctico de autenticación – Vulnerabilidad a los ataques de intermediario

Hay vulnerabilidad en el procedimiento de autenticación entre el servidor y la cámara de red. La cámara de red no deniega los certificados inválidos durante la toma de contacto TLS. Un atacante roba una clave importante. Véase la Figura II.1.

Algunas contramedidas son:

– denegar el certificado inválido de capa de conexión segura;

– utilizar la fijación de clave pública del protocolo de transporte de hipertexto.

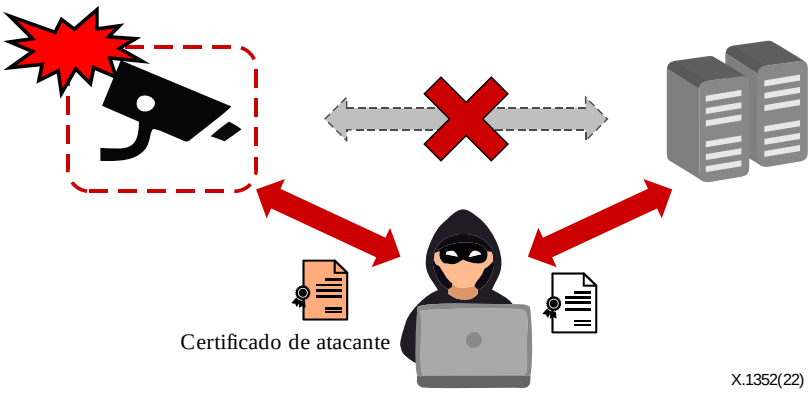

Figura II.1 – Caso práctico de autenticación

II.2 Caso práctico de dominio de criptografía – Algoritmo criptográfico débil

Véase la Figura II.2.

Algunas vulnerabilidades son:

– algoritmo de cifrado débil: Base64;

– metodología de comprobación de datos: algoritmo de generación numérica seguro 1 (SHA1).

Algunas contramedidas son:

– un nivel de seguridad mayor que el de un algoritmo de cifrado de 128 bits (véase [b-ISO/CEI 19790]);

– metodología de verificación de datos SHA256 [b-ISO/CEI 10118-3].

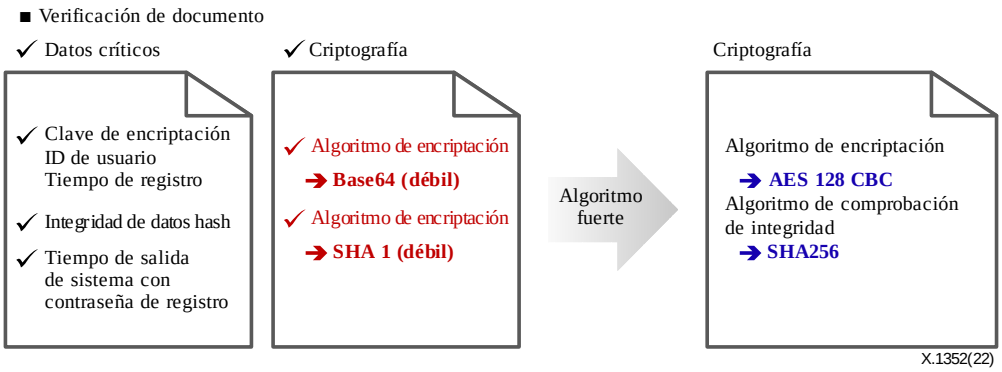

Figura II.2 – Caso práctico de dominio de criptografía

II.3 Caso práctico sobre la seguridad de datos y el dominio de criptografía – Débil comprobación de integridad en el envío de datos

Véase la Figura II.3.

La vulnerabilidad consiste en:

– la comprobación débil de la integridad en el envío de datos (metodología de comprobación de integridad de datos: verificación por redundancia cíclica).

Algunas contramedidas son:

– metodología de verificación de datos: datos hash SHA256 [b-ISO/CEI 10118-3];

– divisiones totales de datos y marco reunidos.

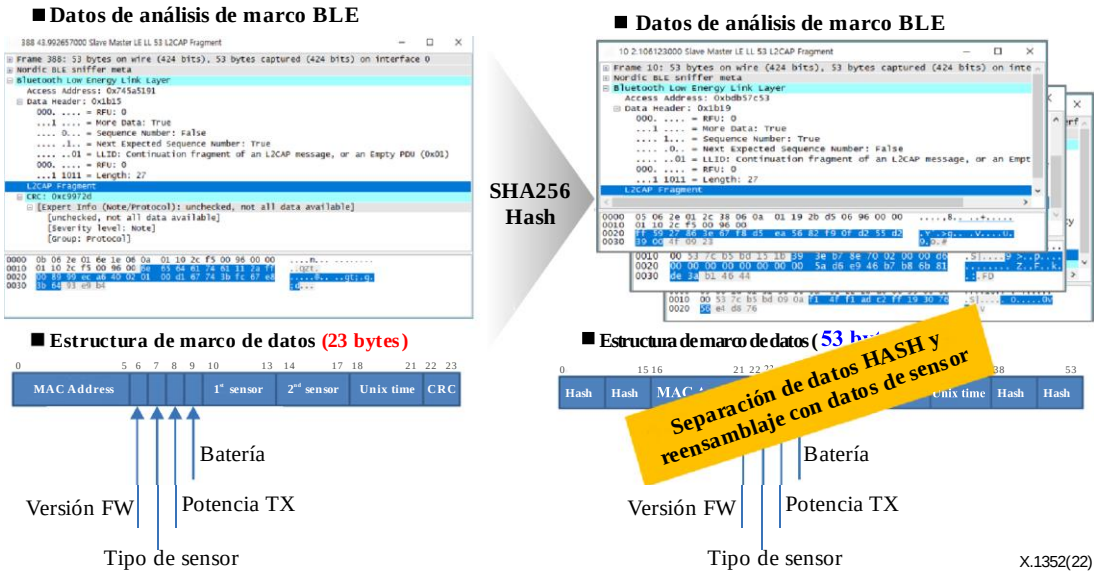

Figura II.3 – Caso práctico de dominio de seguridad de datos y criptografía

II.4 Caso práctico de dominio de seguridad de las plataformas de dispositivos – Codificación débil contra explotación

Véase la Figura II.4.

La vulnerabilidad consiste en:

– desbordamiento de la memoria y API débil.

La contramedida consiste en:

– comprobar la codificación segura y proponer la supresión de códigos débiles mediante herramientas de análisis estático.

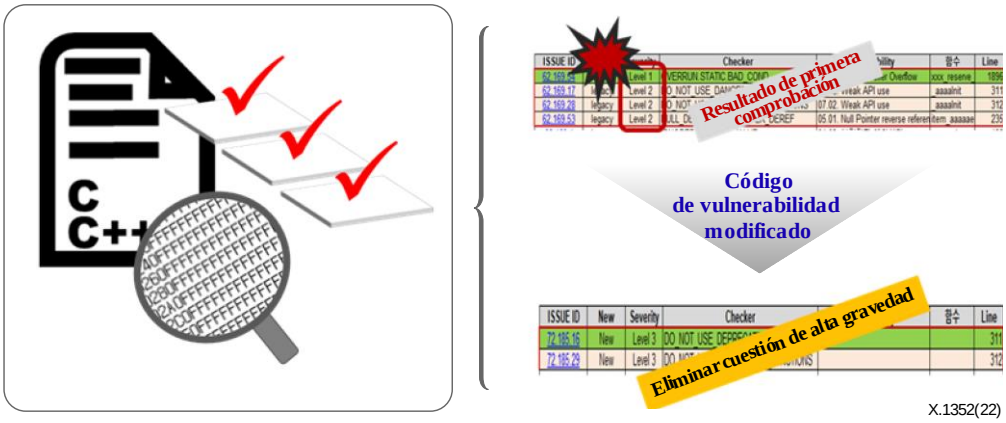

Figura II.4 – Caso práctico de dominio de seguridad de las plataformas de dispositivos

II.5 Caso práctico sobre el dominio de seguridad física – Vulnerabilidad de la interfaz interior en una tarjeta de circuito impreso

Véase la Figura II.5.

La vulnerabilidad consiste en:

– la disponibilidad del puerto JTAG en un producto de masa.

La contramedida consiste en:

– activar la protección del acceso a la memoria en la MCU.

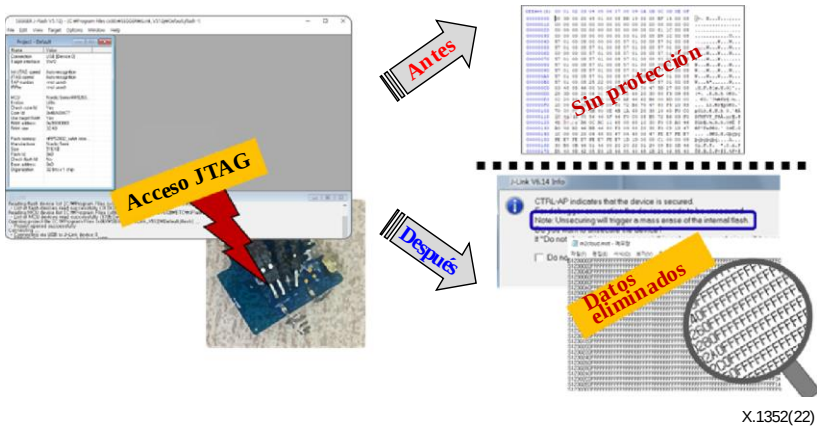

Figura II.5 – Caso práctico de dominio de seguridad física

Bibliografía

[b-UIT-T X.667] Recomendación UIT-T X.667 (2012), *Tecnología de la información – Procedimientos para el funcionamiento de las autoridades de registro de los identificadores de objeto: Generación de identificadores únicos universales y su utilización como componentes de identificador de objetos*

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*

[b-UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2021), *Términos y definiciones de referencia para la gestión de la identidad*

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2020), *Marco de garantía de autentificación de entidad*

[b-UIT-T X.1362] Recomendación UIT-T X.1362 (2017), *Procedimiento de encriptación simple para la Internet de las cosas (IoT)*

[b-UIT-T Y.4000] Recomendación UIT-T Y.4000/Y.2060 (2012), *Visión general de la Internet de las cosas*

[b-ISO 16100-1] ISO 16100-1 (2009), *Sistemas de automatización industrial e integración – Elaboración de perfiles de capacidades para software de fabricación a efectos de interoperabilidad – Parte 1: Marco*

[b-ISO/CEI 10118-3] ISO/CEI 10118-3 (2018), *IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

[b-ISO/CEI 19790] ISO/CEI 19790 (2012), *Tecnología de la información – Técnicas de seguridad – Requisitos de seguridad para módulos criptográficos*

[b-ISO/CEI 27000] ISO/CEI 27000 (2018), *Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Sinopsis y vocabulario*

[b-ISO/CEI 27033-1] ISO/CEI 27033-1 (2015), *Information technology – Security techniques – Network security – Part 1: Overview and concepts*

[b-ISO/CEI 29100] ISO/CEI 29100 (2011), *Information technology –Security techniques – Privacy framework*

[b-ISO/CEI 9796-3] ISO/CEI 9796-3 (2006), *Tecnología de la información – Técnicas de seguridad – Esquemas de firma digital que reestablecen los mensajes – Parte 3: Mecanismos discretos basados en logaritmos*

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Requisitos de aleatoriedad para la seguridad*

[b-CVE] Mitre Corporation (Internet). *Vulnerabilidades y riesgos comunes.* Bedford, MA: Mitre Corporation. Disponible [visto el 29/10/2022] en https://cve.mitre.org/

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás 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 la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
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
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2023