Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1367

(09/2020)

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)

Formato normalizado para los registros de errores de Internet de las cosas (IoT) utilizado en las operaciones de incidentes de seguridad

Recomendación UIT-T X.1367

Unión Internacional de Telecomunicaciones

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	X.1140–X.1149
Protocolos de seguridad (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.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
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
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
SEGURIDAD DE 5G	X.1800–X.1819

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

Recomendación UIT-T X.1367

Formato normalizado para los registros de errores de Internet de las cosas (IoT) utilizado en las operaciones de incidentes de seguridad

Resumen

Se plantean dos problemas al tratar de gestionar los incidentes de seguridad del ecosistema de la Internet de las cosas (IoT). El primero es la incompatibilidad de los protocolos entre las redes informáticas que utilizan el protocolo de control de transmisión/protocolo de Internet (TCP/IP) y los dispositivos de borde de la IoT. El segundo es la falta de compatibilidad de los códigos de error entre los fabricantes de dispositivos de borde.

En la Recomendación X.1367 se especifica un formato normalizado de registro de errores que puede colocarse en una carga útil de protocolo, como el syslog (véase IETF RFC 5424), que se utilizará para convertir la información de un registro de errores emitida por un dispositivo de borde al formato normalizado de registro de errores.

En esta Recomendación se especifica también un cuadro de códigos de error normalizados, lo que permite resolver el segundo problema. Gracias a este enfoque normalizado, se pueden gestionar de manera integral los incidentes de seguridad en las redes informáticas y en las redes de dispositivos de borde de la IoT.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1367	2020-09-03	17	11.1002/1000/14263

Palabras clave

Código de error, dispositivo periférico, formato de registro de error, Internet de las cosas (IoT), intervención en caso de incidentes, operación de seguridad.

* 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 adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

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

© UIT 2021

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

ÍNDICE

Recomendación UIT-T X.1367

Formato normalizado para los registros de errores de Internet de las cosas (IoT) utilizado en las operaciones de incidentes de seguridad

1 Alcance

En la presente Recomendación se especifica un formato normalizado de registro de errores que puede colocarse en una carga útil de protocolo, como el syslog [b-IETF RFC 5424], a fin de convertir la información de un registro de errores emitida por un dispositivo de borde al formato normalizado de registro de errores.

Se especifica también en la Recomendación un cuadro de códigos de error normalizados, lo que permite resolver la falta de compatibilidad de los códigos de error entre los fabricantes de dispositivos de borde. Gracias a este enfoque normalizado, se pueden gestionar de manera integral los incidentes de seguridad en las redes informáticas y en las redes de dispositivos de borde de la IoT.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 accionador [b-UIT-T Y.4109]: Dispositivo que activa una acción física tras recibir el estímulo de una señal de entrada.

3.1.2 ataque [b-ISO 13491-1]: Intento de intrusión realizado por un adversario en el dispositivo a fin de obtener o modificar información sensible o un servicio que no está autorizado a obtener o modificar.

3.1.3 autentificación [b-UIT-T X.1277]: La autenticación es el proceso por el que un usuario emplea su autentificador FIDO para demostrar la posesión de una clave registrada a una parte confiante.

3.1.4 autorización [b-UIT-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.5 dispositivo [b-UIT-T Y.4000]: En el contexto de 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.

3.1.6 Internet de las cosas (IoT) [b-UIT-T Y.4000]: Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.

3.1.7 interfaz hombre-máquina (HMI, *human-machine interface*) [b-UIT-T H.320]: Interfaz hombre-máquina entre el usuario y el terminal/sistema que consiste en una sección física (transductor electroacústico, electro-óptico, teclas, etc.) y una sección lógica que trata los estados de operaciones funcionales.

3.1.8 software maligno [b-ISO/CEI 27033-1]: Software maligno diseñado específicamente para dañar o interrumpir un sistema atacando su confidencialidad, integridad y/o disponibilidad.

3.1.9 sensor [b-UIT-T Y.4105]: Dispositivo electrónico que detecta una condición física o un componente químico y transmite una señal electrónica proporcional a la característica observada.

3.1.10 objeto [b-UIT-T Y.4000]: En el contexto de Internet de las cosas se trata de un objeto del mundo físico (objetos físicos) o del mundo de la información (objetos virtuales) que se puede identificar e integrar en las redes de comunicaciones.

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

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 certificación: La certificación es la atestación de un tercero relativa a productos, procesos, sistemas o personas.

NOTA – Sobre la base de la definición que figura en [b-ISO/CEI 17000].

3.2.2 servidor de instrucción y control (C&C): Servidor que envía instrucciones y controla ordenadores (*botnets*) que se han convertido en *bots* tras infectarse con software maligno.

3.2.3 encriptado: Transformación criptográfica de datos para producir un texto cifrado.

NOTA – Sobre la base de la definición de cifrado que figura en [b-UIT-T X.800], que trata el encriptado como su sinónimo.

3.2.4 Dispositivo de borde de la Internet de las cosas: Dispositivo terminal del ecosistema de IoT que recoge datos del mundo real con sensores o incide en el mundo real mediante accionadores.

3.2.5 Pasarela de Internet de las cosas (IoTGW): Dispositivo que conecta una red para dispositivos de borde de IoT con redes informáticas de amplia disponibilidad, como Internet.

3.2.6 unidad de microcontrolador (MCU): Microprocesador incorporado que integra unidades aritméticas, unidades de memoria y puertos de entrada/salida en un circuito integrado.

3.2.7 equipo de intervención en caso de incidentes de seguridad (SIRT): Equipo que recibe los informes sobre "incidentes de seguridad", investiga el problema e interviene para resolverlo.

3.2.8 centro de operaciones de seguridad (SOC): División que vigila el estado de los ordenadores y las redes de la organización y responde después de detectar señales de actividades maliciosas.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

C&C Instrucción y control

FW Cortafuegos

HMI Interfaz hombre-máquina

ID Identificador

IDS Sistema de detección de intrusiones

IoT Internet de las cosas

IoTGW Pasarela de Internet de las cosas

IP Protocolo Internet

JSON Notación de objeto JavaScript

LAN Red de área local

MCU Unidad de microcontrolador

PC Ordenador personal

SIRT Equipo de intervención en caso de incidentes de seguridad

SOC Centro de operaciones de seguridad

TCP Protocolo de control de transmisión

5 Convenios

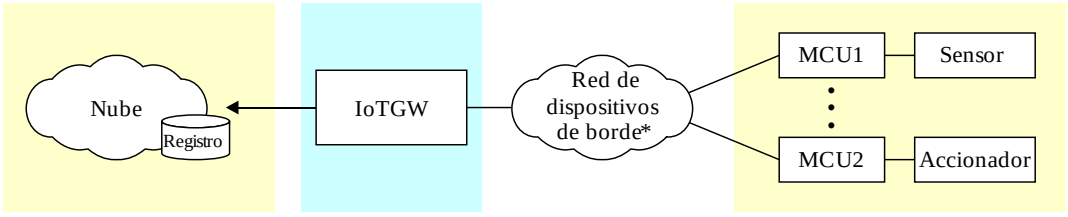
Ninguno.

6 Generalidades

6.1 Procedimiento actual de gestión de errores en un ecosistema de IoT

En el contexto de la gestión de errores en un ecosistema de IoT, si uno de los componentes del sistema de IoT, como el sensor o el accionador, se estropea, se emitirá un código de error que quedará inscrito en un registro de errores. Si el error se produce en raras ocasiones, no es necesario corregirlo. En cambio, si el error persiste, deberá reemplazarse el componente para solucionar el problema.

La Figura 1 representa un ecosistema típico de IoT que consta de componentes de IoT como unidades de microcontroladores (MCU) asociadas con sensores y accionadores, una pasarela de Internet de las cosas (IoTGW) y una nube.



* En esta red se utiliza un protocolo específico

Figura 1 – Ecosistema típico de IoT

La comunicación entre la IoTGW, la MCU1 y la MCU2 en la Figura 1 se basa en un protocolo específico (véase la nota) para el sistema. El sensor MCU1 y el accionador MCU2 son ejemplos de dispositivos de borde de IoT. En este caso, la IoTGW transmite una petición a las MCU y estas responden a la IoTGW con información de registro. La IoTGW también se comunica con la nube (un sistema de soporte o *back-end*).

NOTA – Puede tratarse de un protocolo específico para grandes redes, como oneM2M [b-oneM2M], ECHONET Lite [b-ISO/CEI 14543-4-3], o para pequeñas redes como SPI [b-SPI], I^2C [b-UM10204], Bluetooth [b-IEEE 802.15.1], Zigbee [b-IEEE 802.15.4], o de un protocolo propietario diseñado exclusivamente para este sistema de IoT.

La adecuada gestión de un ecosistema de IoT requiere que este sea capaz de tratar los errores, dado que los dispositivos de borde de IoT a veces se estropean. Estos sistemas procesan los registros de errores con códigos de error e inician las correcciones. Por otra parte, algunos sistemas desglosan los registros de error almacenados con códigos de error que permiten cotejar la información estadística con la finalidad de introducir mejoras en el propio sistema y de gestionar los incidentes de seguridad. Sin embargo, resulta difícil unificar los registros de error de todos los ecosistemas y syslog [b-IETF RFC 5424].

6.2 Descripción general

A fin de intervenir con eficacia en caso de incidente, es fundamental prever las capacidades adecuadas para recopilar y analizar la información de registro de errores de los componentes del ecosistema de IoT. Sin embargo, se reconocen los siguientes problemas específicos por lo que se refiere al ecosistema de IoT.

1) Existe un procedimiento normalizado que incluye el proceso de gestión de incidentes, mediante el uso de syslog [b-IETF RFC 5424], para recabar información de registro de los dispositivos de la red. Sin embargo, no se dispone de ese procedimiento en el caso del ecosistema de IoT.

2) La información del registro de errores de IoT no puede almacenarse en un único componente del ecosistema de IoT; es decir, dicha información de registro debe ser recopilada por el sistema de soporte (por ejemplo, la nube) o por el sistema de borde de IoT (por ejemplo, una IoTGW), según la configuración del ecosistema de IoT.

3) A falta de un formato normalizado de registro de errores, no es fácil correlacionar la información del registro de errores entre los diversos componentes de la IoT.

4) Si no se dispone de un método que permita tratar la información del registro de errores, el ecosistema de IoT no podrá mantener eficazmente su servicio de IoT.

En la presente Recomendación se describe una arquitectura básica del sistema de IoT para recopilar registros de errores de IoT que se utilizarán en las operaciones de gestión de incidentes. Se especifican códigos de error normalizados y un formato de registro de errores. Al convertir los códigos de error adoptados por cada fabricante de ecosistemas de IoT en códigos de error normalizados, es posible supervisar con mayor eficacia el estado de múltiples ecosistemas de IoT. Además, en el proceso de conversión de un código de error en un código de error normalizado, la situación en que se produjo el error también se registra en los registros de errores conexos. En consecuencia, pueden gestionarse globalmente los incidentes de seguridad de múltiples ecosistemas de IoT (véase un ejemplo en la cláusula I.4 del Apéndice I, Ecosistema de IoT múltiple).

7 Formato de registro de errores normalizado para el entorno de IoT

La escasez de recursos informáticos puede dificultar que los dispositivos de borde de IoT implementen nuevas funciones con el fin de gestionar los registros de errores de IoT. Sin embargo, la IoTGW normalmente dispone de mejores recursos informáticos para ello. Se genera un profuso intercambio de peticiones y respuestas entre la IoTGW y los sistemas basados en la nube, y esas comunicaciones contienen información de registro de errores de IoT. Por lo tanto, la presente Recomendación requería que una IoTGW generara información normalizada de registro de errores y la comunicara a los sistemas de computación en la nube.

7.1 Estructura básica del formato de registro de errores

Un registro de errores de IoT tiene el formato descrito en la Figura 2, basado en la notación de objetos de JavaScript (JSON) con expresiones regulares. Este formato puede transformarse para su utilización en syslog o XML (véase la nota). En el Apéndice I se presentan ejemplos de este formato.

NOTA – En la presente Recomendación no se define la longitud de cada valor de atribución. El emisor y el receptor del registro de errores deberán acordar previamente la longitud de cada valor de atributo.

```
{
   "Timestamp":
        "^([0-9]{4})-(1[0-2]|0[1-9])-(3[01]|0[1-9]|[12][0-9])T
          (2[0-3]|[01][0-9]):([0-5][0-9]):([0-5][0-9])(\.[0-9]{+})Z$",
   "Reporter": {},
   "Protocol": String,
   "Requester": {},
   "Responder": {},
```

```
  "Error Code": "/^[0-9A-F]^{+}$/",
  "Error Message": String,
  "Description": String | {},
}
```

Figura 2 – Elementos de un registro de error

En la mayoría de los casos, el notificador de este registro de errores es la IoTGW. Los atributos utilizados en este formato se definen en la cláusula 7.2.

7.2 Atributos básicos

La información del registro de errores contiene los siguientes atributos:

a) *Timestamp* (sello temporal): Se requiere un sello temporal con este atributo (véase la nota) para la emisión de un registro de errores. Por ejemplo, en el caso del 20 de septiembre de 2018 a las 13 horas, 25 minutos y 51 segundos, el sello temporal se codificará del siguiente modo: "2018-09-20T13:25:51.0Z."[b-ISO 8601-1].

NOTA – El atributo *timestamp* es obligatorio, aunque el protocolo de transmisión que comunica un registro de errores conforme a las especificaciones de la presente Recomendación también contiene un campo de sello temporal, porque la indicación temporal correspondiente al instante en que aparece el problema no suele coincidir con la hora de la transferencia.

b) *Reporter* (notificador): El *reporter* es el componente de IoT que convierte el código de error del dispositivo en un código de error normalizado y lo envía a la nube. Véase su descripción detallada en la Figura 3.

```
"Reporter":{
    "IP Address":
        "(^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
              (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)
         |(^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$)"
}
```

Figura 3 – Elementos del atributo reporter

1) Dirección del protocolo de Internet (IP): identificador único (ID) del notificador en la Ethernet.

c) *Protocol* (protocolo): Nombre de protocolo utilizado entre los dispositivos de borde de la IoTGW y la IoT.

d) *Requester* (solicitante) o *responder* (respondedor): El componente de IoT que envía una petición a un dispositivo de borde de IoT o el componente de IoT que responde a una petición. Véase su descripción detallada en la Figura 4.

```
"Requester(or Responder)": {
    "Unique ID": string,
    "Transmitted Code": "( [0-9A-F])^{+}}
```

Figura 4 – Elementos de los atributos requester y responder

1) *Unique ID* (identificador único) (opcional): Se trata de un número o un código único relacionado con cada dispositivo definido por el protocolo de la red de dispositivos de borde de IoT.

2) *Transmitted code* (código transmitido) (opcional): Contenido de los datos transmitidos. Se expresa en hexadecimales.

3) Debe expresarse como se muestra en la Figura 5 cuando se produce un error sin *requester* o *responder*, tal como ocurre en el caso de un dispositivo sensor que envía datos periódicamente sin que hayan sido solicitados.

```
"Requester(or Responder)": {}
```

Figura 5 – Formato en caso de inexistencia de requester o de responder

e) *Error code*, *error message* (código de error, mensaje de error): El código de error y el mensaje de error se especifican en el Anexo A.

f) *Description* (descripción) (opcional): Pueden incluirse frases, expresiones y subelementos de JSON cuando se requiere una notificación de la situación de los dispositivos de borde de IoT o de sus redes.

El mensaje de error puede omitirse si el ancho de banda de la comunicación es estrecho o si el tamaño del almacenamiento es limitado. La descripción puede omitirse si no es necesario incluir ningún texto adicional.

Anexo A

Códigos de error y mensajes de error

(El presente anexo forma parte integrante de esta Recomendación.)

Los códigos de error y mensajes de error se especifican en el Cuadro A.1.

Cuadro A.1 – Códigos de error y mensajes de error

Código	Mensaje	Descripción
	Inexistencia de error (0x00-0x0F)	
0x00	No Error	No se produce ningún error.
	Comunicación (0x10-0x1F)	
0x10	No Response	No hay respuesta, aunque la petición requiere una respuesta.
0x11	Communication Failed	Se detectan problemas por fallos de comunicación.
0x12	Link Down	El enlace de la interfaz de red ha dejado de funcionar.
0x1E	Extended Reasons	Código de prefijo para razones extensas.
0x1F	Other Communication Reasons	Otras razones relacionadas con la comunicación.
	Seguridad (0x20-0x2F)	
0x20	Authentication Failed	Se detectan problemas de autentificación.
0x21	Certification Failed	Se detectan problemas de certificación.
0x22	Encryption Failed	Se detectan problemas de encriptado.
0x23	Authorization Failed	Se detectan problemas de autorización.
0x2E	Extended Reasons	Código de prefijo para razones extensas.
0x2F	Other Security Reasons	Otras razones relacionadas con la autentificación, la certificación, el encriptado o la autorización.
	Instrucción (0x30-0x3F)	
0x30	Invalid Command	La instrucción es indefinida o no es válida.
0x31	Invalid Argument	El argumento excede del rango o no es válido.
0x3E	Extended Reasons	Código de prefijo para razones extensas.
0x3F	Other Command Reasons	Otras razones relacionadas con la instrucción.
	Dispositivo (0x40-0x4F)	
0x40	Device Broken	Una parte del dispositivo se ha roto de manera irrecuperable.
0x41	Device Failed	Una parte del dispositivo ha fallado pero es recuperable.
0x42	Out of Resources	Se están agotando el espacio de almacenamiento, la memoria y cualquier otro recurso informático.
0x4E	Extended Reasons	Código de prefijo para razones extensas.
0x4F	Other Device Reasons	Otras razones relacionadas con el dispositivo.
	Reservado para futuras ampliaciones (0x50-0xDF)	
	Reservado para aplicaciones privadas (0xE0-0xEF)	
	Otros (0xE0-0xEF)	
0xFF	Other Reasons	Otras razones, excepto las enumeradas anteriormente.

Apéndice I

Ejemplos de cómo utilizar los registros de error en operaciones de incidentes

(Este apéndice no forma parte integrante de la presente Recomendación.)

I.1 El atacante envía una cadena binaria aleatoria a un dispositivo de borde a través de la IoTGW

La Figura I.1 muestra a un atacante enviando una cadena binaria aleatoria a la MCU1 y la reacción correspondiente. El inicio de la cadena binaria aleatoria "01000001" identifica el dispositivo número 0001 y la función número 0100. Es decir, el atacante intenta atacar la función número 0100 del dispositivo número 0001. La MCU1 no puede entender la cadena "3A459187F43CDDE5", así que responde "000003FF(unknown command)" al dispositivo número 0000 (IoTGW).

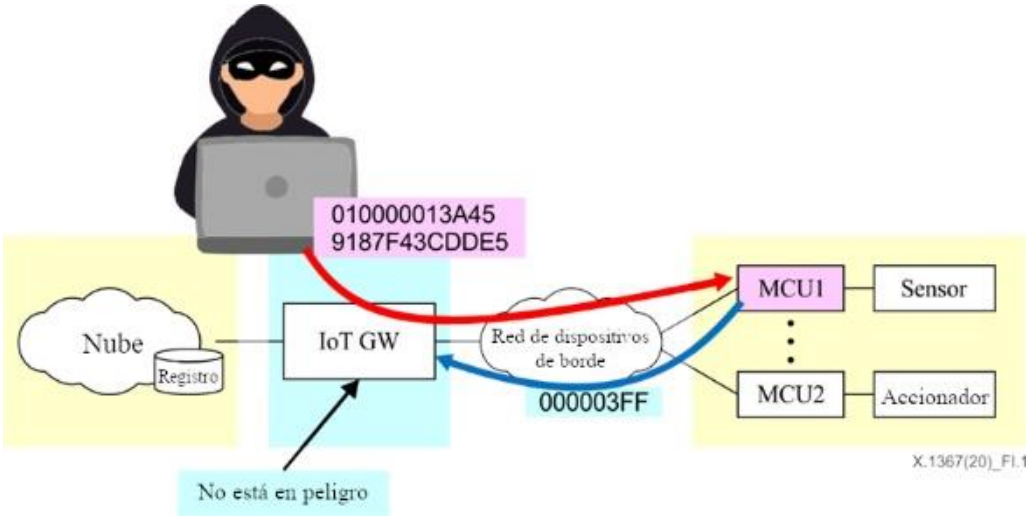


Figura I.1 – El atacante envía una cadena binaria aleatoria a la MCU1

Una vez que la IoTGW recibe "000003FF" de la MCU1, la IoTGW construye el siguiente registro y lo envía a un servidor de registro en la nube. Véase la Figura I.2.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.2.11"},
    "Protocol": "ABC company protocol",
    "Requester": {
        "Unique ID": "0000",
        "Transmitted Code": "010000013A459187F43CdDE5"
    },
    "Responder": {
        "Unique ID": "0001",
        "Transmitted Code": "000003FF"
    },
    "Error Code": "30",
    "Error Message": "Invalid Command",
}
```

Figura I.2 – Registro de errores de IoT respecto de una petición errónea (ejemplo)

I.2 El atacante envía una certificación incorrecta a un dispositivo de borde a través de una IoTGW en peligro

La Figura I.3 muestra a un atacante enviando una certificación incorrecta a la MCU2 a través de una IoTGW en peligro y la reacción correspondiente. La MCU2 identifica que la certificación no es válida, así que responde "00000010000c (certificate verification error)" al dispositivo número 0000 (una IoTGW). Sin embargo, la IoTGW está en peligro. La IoTGW nunca enviará un registro de error al servidor de registro en la nube. El sistema de detección de intrusiones (IDS) envía un registro de error de IoT en lugar de la IoTGW.

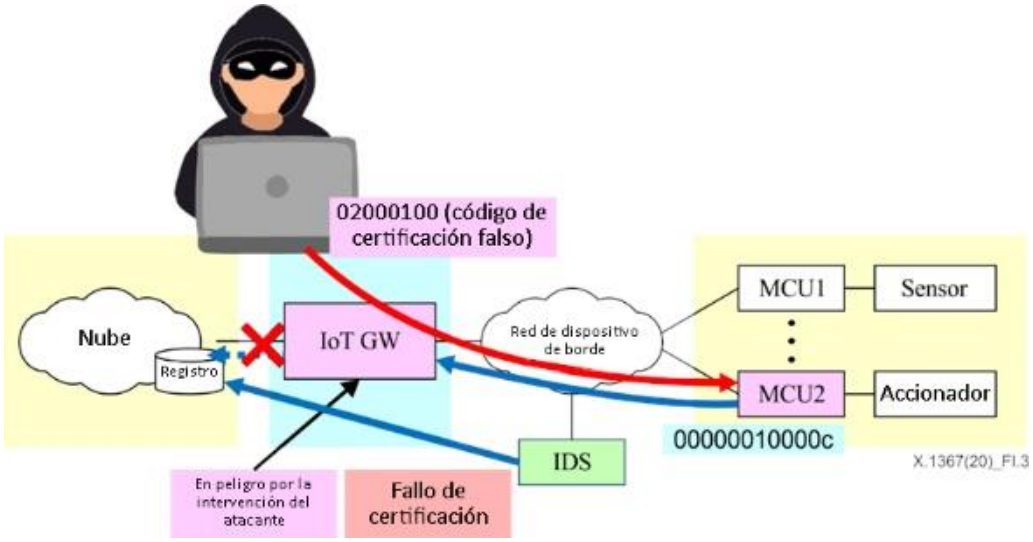


Figura I.3 – El atacante envía un código de certificación falso

El atacante envía un código de certificación falso a la MCU2, pero esta no puede reconocerlo. Entonces la MCU2 envía "00000010000c (Certificate verification error)". La IoTGW no tiene en cuenta el mensaje de respuesta de la MCU2, porque el atacante ha desactivado previamente esa defensa. Sin embargo, si el sistema tiene un IDS, este construye el registro de error de IoT como se observa en la Figura I.4 y lo envía en lugar de la IoTGW. En este caso, el IDS se convierte en el notificador.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.100.249"},
    "Protocol": "EEE Company's protocol",
    "Requester": {
        "Unique Name": "0000",
        "Transmitted Code": "02000100... (Faked certification codes)"
    },
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": "000000000010000c "
    },
    "Error Code": "21",
    "Error Message": "Certification Failed",
    "Description": {
        "Status": "This message was sent from IDS not IoTGW"
    },
}
```

Figura I.4 – Registro de error de IoT relativo a un error de verificación de certificado (ejemplo)

I.3 El atacante rompe físicamente un dispositivo sensor que envía datos regularmente sin que hayan sido solicitados

La Figura I.5 muestra a un atacante rompiendo físicamente la MCU1, que envía datos regularmente sin que hayan sido solicitados. Después de ese ataque la MCU1 no puede enviar ningún dato. En este caso, la IoTGW detecta una situación anómala relacionada con la MCU1, y envía el registro de error de IoT que se muestra en la Figura I.6.

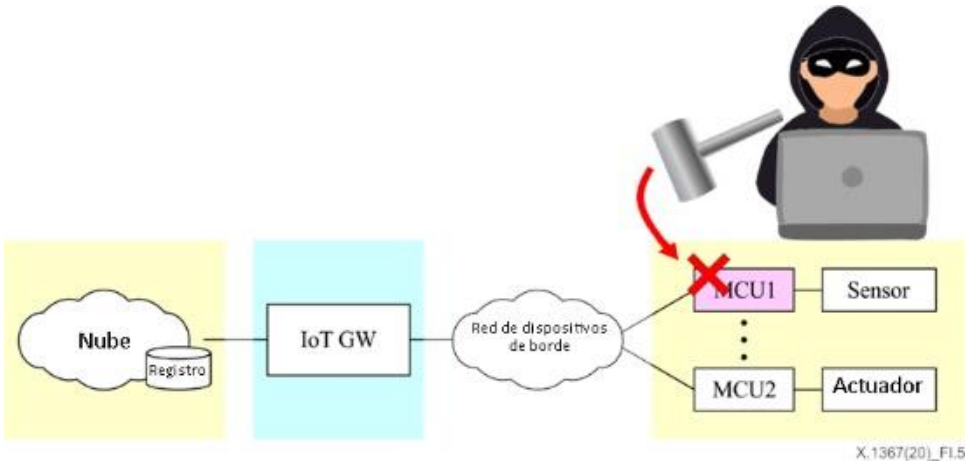


Figura I.5 – El atacante rompe físicamente la MCU1

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.10.254"},
    "Protocol": "ZZZ Company's protocol",
    "Requester": {},
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": ""
    },
    "Error Code": "11",
    "Error Message": "Communication Failed",
    "Description": {
        "Responder stopped sending data."
    },
}
```

Figura I.6 – Registro de error de IoT relativo a la pérdida de comunicación (ejemplo)

I.4 Cómo utilizar los registros de error de IoT durante la intervención en caso de incidente

Una fábrica dispone de tres ecosistemas de IoT en la misma red de área local (LAN) como se muestra en la Figura I.7.

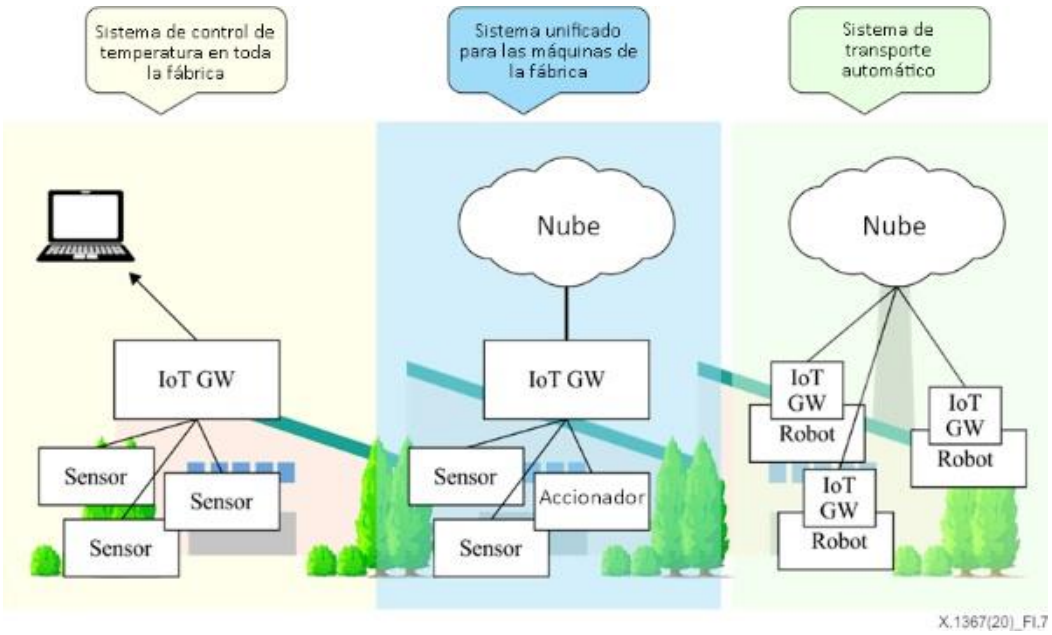


Figura I.7 – Múltiples ecosistemas de IoT en una fábrica

En este caso, un atacante puede atacar fácilmente cada dispositivo, como se muestra en la Figura I.8. Si no hay registros de error de IoT, el equipo de intervención en caso de incidentes de seguridad (SIRT) tiene dificultades para identificar las huellas del atacante, porque el SIRT no puede unificar los registros de IoT no normalizados de cada ecosistema de IoT.

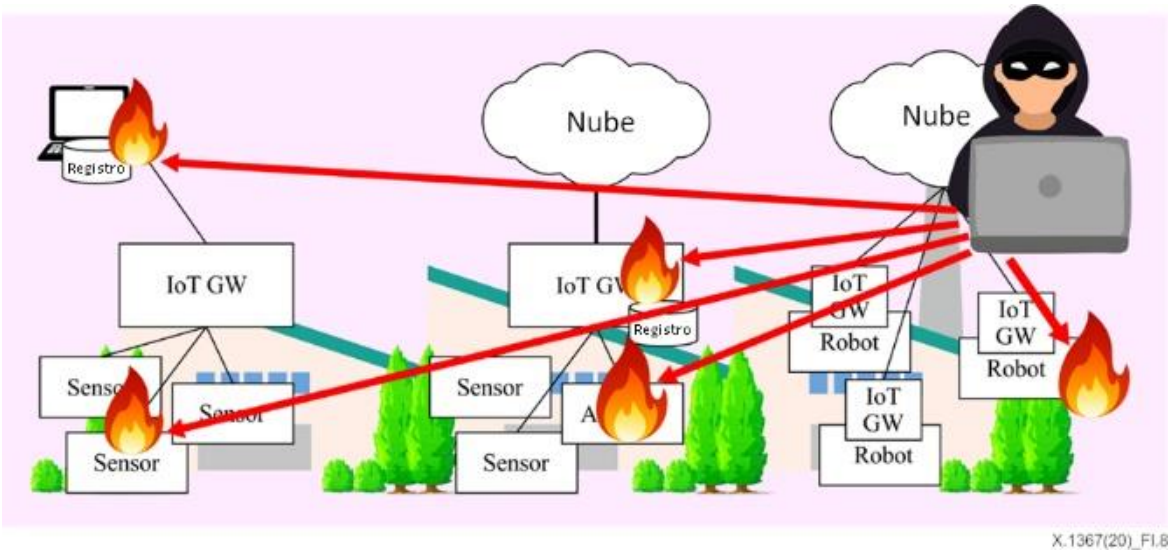


Figura I.8 – El atacante apunta a todos los ecosistemas de IoT de manera simultánea

Si los ecosistemas de IoT utilizan el formato normalizado de registro de errores de IoT, el SIRT puede unificar fácilmente todos los registros de error de IoT, como se muestra en la Figura I.9, así como unificar el syslog. De esa manera es posible identificar las huellas del atacante.

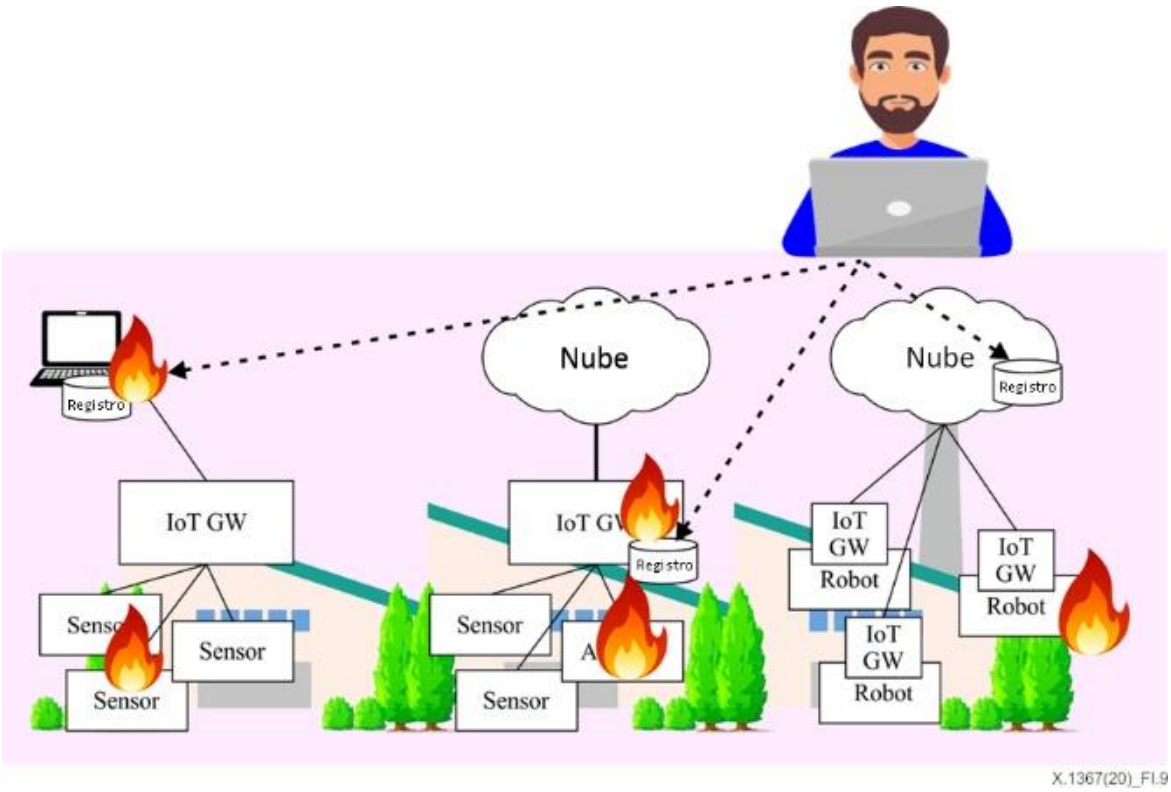


Figura I.9 – Unificar y analizar todos los registros de error de IoT

Apéndice II

Posible intervención en caso de incidente de seguridad utilizando el registro de error de Internet de las cosas

(Este apéndice no forma parte integrante de la presente Recomendación.)

El registro de error de IoT normalizado descrito en la presente Recomendación puede utilizarse durante la intervención en caso de incidentes de seguridad en un ecosistema de IoT. La Figura II.1 muestra un flujo de detección de incidentes mediante el registro de error de IoT.

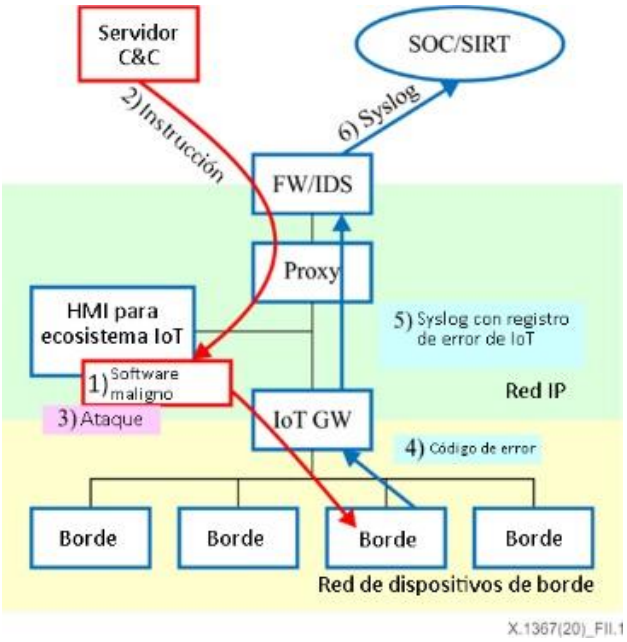


Figura II.1 – Detección de incidentes mediante el registro de error de IoT

1) El software maligno infecta de alguna manera una interfaz hombre-máquina (HMI), por ejemplo, un ordenador personal de escritorio (PC).

2) El software maligno recibe instrucciones del servidor de instrucción y control (C&C). Un cortafuegos (FW), IDS o proxy puede registrar un registro de comunicación entre el software maligno y el servidor C&C.

3) El software maligno busca una vulnerabilidad del dispositivo de borde de IoT. El dispositivo de borde de IoT envía múltiples códigos de error a la IoTGW, porque el software maligno trata de enviar frecuentes instrucciones con diversos parámetros. Sus parámetros son casi siempre incorrectos para el dispositivo de borde de IoT.

4) Por cada código de error de IoT enviado, la IoTGW envía un registro de error de IoT en el formato especificado en la presente Recomendación al FW o al IDS mediante el protocolo syslog.

5) Un proxy también envía registros de comunicación utilizando el protocolo syslog al FW o al IDS, que a su vez envía todos los registros, incluido el registro de error de IoT, con el protocolo syslog al centro de operaciones de seguridad (SOC) o al SIRT.

Los analistas de seguridad del SOC o del SIRT no pueden responder a un registro de error de IoT aislado que no guarde relación con otros registros de error de IoT. Sin embargo, pueden observar una situación anómala si el SOC o el SIRT recibe un gran número de registros de error de IoT continuamente, porque esto podría deberse a un atacante que busca una vulnerabilidad en el sistema de IoT.

La presente Recomendación permite a los analistas del SOC o del SIRT detectar ataques a los dispositivos de borde de IoT, porque el SOC o el SIRT recibe los códigos de error de IoT en el formato normalizado de registro de errores de IoT. Posteriormente comprobarán otros registros conexos, incluidas las comunicaciones entre el software maligno y el servidor C&C, y notificarán la anomalía al operador de la fábrica para que desconecte de la LAN ese PC de escritorio de HMI o para que elimine el software maligno del PC de escritorio de HMI.

Bibliografía

[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.1277] Recomendación UIT-T X.1277 (2018), *Marco de Autentificación Universal*.

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

[b-UIT-T Y.4105] Recomendación UIT-T Y.4105/Y.2221 (2010), *Requisitos para el soporte de los servicios y aplicaciones de redes de sensores ubicuos en el entorno de las redes de próxima generación*.

[b-UIT-T Y.4109] Recomendación ITU-T Y.4109/Y.2061 (2012), *Requisitos de apoyo a las aplicaciones de comunicación orientada a las máquinas en el entorno de las redes de próxima generación*.

[b-ISO 8601-1] ISO 8601-1:2019, *Date and time – Representations for information interchange – Part 1: Basic rules*.

[b-ISO 13491-1] ISO 13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*.

[b-ISO/CEI 14543-4-3] ISO/CEI 14543-4-3:2015, *Information technology – Home Electronic Systems (HES) architecture – Part 4-3: Application layer interface to lower communications layers for network enhanced control devices of HES Class 1*.

[b-ISO/CEI 17000] ISO/CEI 17000:2004, *Conformity assessment – Vocabulary and general principles*.

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

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

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*.

[b-IEEE 802.15.1] IEEE 802.15.1-2005, *IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN)*.

[b-IEEE 802.15.4] IEEE 802.15.4-2015, *IEEE Standard for low-rate wireless networks*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The syslog protocol*.

[b-oneM2M] oneM2M Partners (2017), Standards for M2M and Internet of things. Disponible en [visto el 12-02-2020]: http://www.onem2m.org/.

[b-SPI] Motorola (2001), SPI block guide, V04.01. Disponible en [visto el 12-02-2020]: https://www.nxp.com/files-static/microcontrollers/doc/ref_manual/S12SPIV4.pdf.

[b-UM10204] UM10204 (2014), *I^2C-bus specification and user manual*, Rev.6. Disponible en [visto el 12-02-2020]: https://www.nxp.com/docs/en/user-guide/UM10204.pdf.

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, 2021