Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1369

(01/2022)

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 las plataformas del servicio IoT

Recomendación UIT-T X.1369

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 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.1350–X.1369**
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DTL)	X.1400–X.1429
Seguridad de aplicaciones (2)	X.1450–X.1459
Seguridad de 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	
Protección de 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.1369

Requisitos de seguridad para las plataformas del servicio IoT

Resumen

En la Recomendación UIT-T X.1369 se especifican los requisitos de seguridad para las plataformas del servicio de la IoT. Se analizan las amenazas y los riesgos de seguridad para las plataformas de servicio comerciales de IoT y se describen medidas de seguridad que pueden mitigar las amenazas y los retos en materia de seguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1369	07-01-2022	17	11.1002/1000/14799

Palabras clave

IoT, plataforma de servicio, requisitos de seguridad, riesgos 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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores 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/.

© UIT 2022

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.1369

Requisitos de seguridad para las plataformas del servicio IoT

1 Alcance

En esta Recomendación se especifican los requisitos de seguridad para las plataformas del servicio IoT. Se analizan las amenazas y los riesgos de seguridad para las plataformas de servicio de la IoT y se describen medidas de seguridad que pueden mitigar las amenazas y los riesgos de seguridad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. A la fecha de esta publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación a que estudien la posibilidad de utilizar 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 actualmente vigentes. En el marco de la presente Recomendación, la referencia a un documento, en tanto que documento autónomo, no le confiere carácter de Recomendación.

[ISO/CEI 30141] ISO/CEI 30141:2018, *Arquitectura de referencia de la Internet de las cosas*.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza el siguiente término definido en otros documentos:

3.1.1 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.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 plataforma del servicio IoT: plataforma del sistema en el que se conectan dispositivos IoT y se ejecutan aplicaciones IoT.

Desde una perspectiva funcional, las plataformas del servicio IoT proporcionan, en particular, funciones de gestión de los dispositivos, gestión de las conexiones, facilitación de aplicaciones y análisis del negocio. Desde el punto de vista de la gestión de los datos, la plataforma del servicio IoT recopila, almacena y procesa datos (incluidos datos personales e información confidencial de los usuarios) para las aplicaciones IoT y los análisis avanzados.

4 Abreviaturas y acrónimos

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

API Interfaz de programación de aplicación (*application programming interface*)

CSRF Falsificación de petición en sitios cruzados (*cross site request forgery*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DoS Denegación de servicio (*denial of service*)

IMEI	Identidad internacional del equipo móvil (*International Mobile Equipment Identity*)
PVLAN	VLAN Privada (*private VLAN*)
SIM	Módulo de identificación del abonado (*subscriber identity module*)
SQL	Lenguaje de consulta estructurado (*structured query language*)
SSRF	Falsificación de petición en el servidor (*server-side request forgery*)
VLAN	Red de área local virtual (*virtual local area network*)
VM	Máquina virtual (*virtual machine*)
VMM	Controlador de máquina virtual (*virtual machine monitor*)
XSS	Secuencia de comandos en sitios cruzados (*cross site script*)

5 Convenios

En la presente Recomendación: la expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

6 Visión general

La [ISO/CEI 30141] define el modelo de referencia IoT basado en entidades que se muestra en la Figura 1. La plataforma de servicio IoT es un componente clave del *subsistema de aplicaciones y servicios* que se muestra en esta figura, que proporciona capacidades como gestión de dispositivos, gestión de conexiones, facilitación de aplicaciones y análisis de los servicios. La plataforma de servicio IoT también realiza la recopilación, el almacenamiento y el análisis de datos para las aplicaciones IoT.

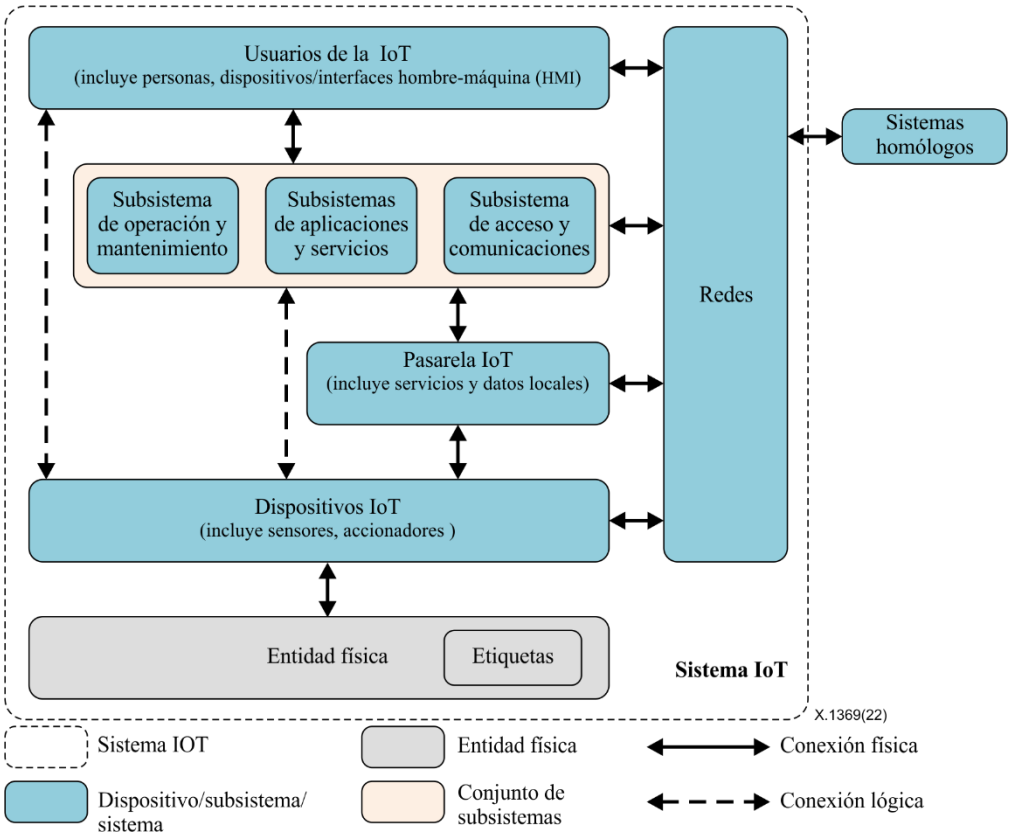

Figura 1 – Modelo de referencia IoT basado en entidades [ISO/CEI 30141]

En general, las plataformas del servicio IoT pueden dividirse en cuatro partes, a saber, el sistema de gestión de dispositivos, el sistema de gestión de la conectividad, el sistema de habilitación de aplicaciones y el sistema de análisis del negocio.

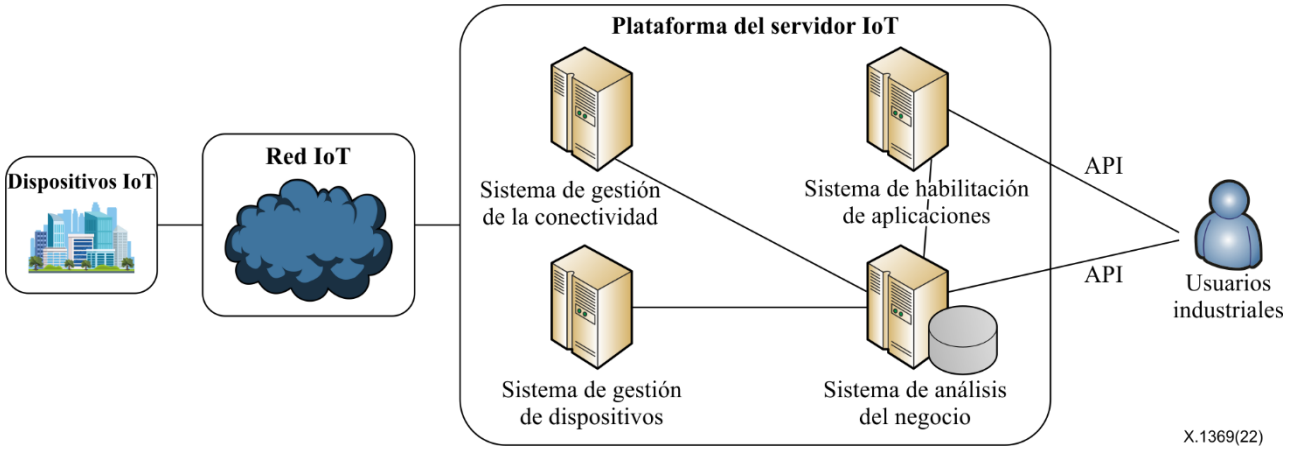

Figura 2 – Visión general de una plataforma del servicio IoT

- Sistema de gestión de dispositivos

Es el sistema de gestión de los dispositivos IoT. Proporciona la supervisión remota, la reconfiguración, la actualización de *software*, la actualización del sistema, análisis de fallos, la gestión del ciclo de vida y otras funciones.

- Sistema de gestión de la conectividad

Es el sistema de gestión centralizada de la tarjeta del módulo de identificación del abonado (SIM). Está dedicado a las aplicaciones de redes celulares y permite el autoservicio de los usuarios, como la solicitud de información sobre la utilización de datos y el estado de la conexión, la recarga de una SIM y la gestión del tráfico.

- Sistema de habilitación de aplicaciones

Es una plataforma para un servicio de "plataforma como servicio" que ofrece diferentes funciones de interfaces de programación de aplicación (API) para dar soporte a la implementación de diferentes sistemas de servicios. Con el sistema, los operadores de telecomunicaciones abren sus capacidades básicas de telecomunicaciones (datos, SMS, teléfono, autentificación, facturación, etc.) a diferentes sistemas de servicios, como el transporte inteligente, las ciudades inteligentes, el hogar inteligente, etc.

- Sistema de análisis del negocio

El sistema recopila diferentes datos del sistema de gestión de dispositivos, el sistema de gestión de la conectividad y el sistema de habilitación de aplicaciones para analizar y generar resultados visuales de los análisis para los operadores y los consumidores.

La seguridad de una plataforma del servicio IoT tiene una función importante en todo el entorno de la IoT. Cualquier debilidad de la plataforma, o ataque a la misma, afectará la seguridad de los dispositivos, las redes y los datos relacionados con la misma. Una plataforma del servicio IoT es vulnerable a amenazas como denegación de servicio (DoS), elevación de privilegios, accesos no autorizados, fuerza bruta, ejecución arbitraria de código, etc., que pueden provocar intrusiones malintencionadas, fugas de información sensible, órdenes maliciosas a los dispositivos u otros efectos perjudiciales.

En esta Recomendación, se analizan los riesgos de seguridad de las plataformas del servicio IoT. Se propone una metodología para un marco de seguridad y diversas medidas de seguridad.

La seguridad del servicio IoT abarca la seguridad de la infraestructura, la seguridad del sistema, la seguridad de los datos y la seguridad de las aplicaciones, desde el nivel más bajo hasta el más alto. La seguridad de las API y la seguridad operativa involucran los cuatro ámbitos anteriores. En los apartados 7 a 9, se describen en detalle los riesgos de seguridad, el marco de seguridad y los requisitos de seguridad, respectivamente, en base a estos seis aspectos.

7 Amenazas de seguridad para una plataforma del servicio IoT

7.1 Amenazas de seguridad para las aplicaciones

Las amenazas de seguridad para las aplicaciones incluyen los ataques desde la web, los accesos no autorizados, la elevación de privilegios y las vulnerabilidades del servicio, entre otros.

7.1.1 Ataques desde la web

Las plataformas del servicio IoT utilizan tecnologías web habituales, así como tecnologías de comunicación, macrodatos, computación en la nube, entre otros. En consecuencia, heredan los principales riesgos de seguridad de todas estas tecnologías, como los ataques por denegación de servicio distribuida (DDoS), los ataques por fuerza bruta, la inyección de lenguaje de consulta estructurado (SQL), las vulnerabilidades de las secuencias de comandos en sitios cruzados (XSS), las vulnerabilidades por falsificación de peticiones en sitios cruzados (CSRF), las vulnerabilidades por falsificación de peticiones en el servidor (SSRF), etc.

7.1.2 Acceso no autorizado y elevación de privilegios

Muchas aplicaciones IoT se instalan en la plataforma centralizada. Ello hace difícil un aislamiento de seguridad eficaz y el control de acceso entre las diferentes aplicaciones, pudiendo conducir a accesos, operaciones y elevaciones de privilegios no autorizados. Por otro lado, la situación es más propensa a la elevación de privilegios y los accesos no autorizados entre diferentes usuarios y dispositivos.

7.1.3 Vulnerabilidades del servicio

Las aplicaciones IoT tienen unas lógicas de servicio complejas y numerosos protocolos de aplicación que pueden provocar fallos en los procesos de diseño y de realización, y en consecuencia, dar lugar a vulnerabilidades y malas utilizaciones de los servicios. En algunos escenarios de las aplicaciones IoT, se pueden controlar los terminales a través de la plataforma. Una plataforma afectada puede poner en peligro un gran número de terminales y afectar a su vez a la fabricación industrial y la vida social de los usuarios.

7.1.4 Exposición de capacidades

Como plataforma de habilitación de aplicaciones, una plataforma IoT puede proporcionar diferentes funciones de API para dar soporte a la implementación de diferentes sistemas de servicios. Aporta funcionalidad para diferentes servicios, pero esta apertura de capacidades también puede suponer riesgos para la plataforma. Desarrolladores no autorizados pueden acceder a las capacidades y diferentes servicios pueden hacer un mal uso de las mismas. Además, la apertura de las capacidades básicas de telecomunicaciones (datos, SMS, teléfonos, autentificación, facturación, etc.) puede facilitar los ataques al núcleo de la red de telecomunicaciones si este no está bien protegido.

7.2 Riesgos de seguridad para los datos

La confidencialidad, la integridad y la disponibilidad constituyen la base de la seguridad de los datos. Sin embargo, durante los procesos de recopilación, transmisión, migración, almacenamiento, procesamiento y destrucción de los datos existen muchos riesgos.

7.2.1 Fugas de datos

Los terminales IoT suelen recopilar los datos de las aplicaciones IoT y transmitirlos a la plataforma, y los datos de esas aplicaciones están generalmente almacenados en la plataforma. En consecuencia, un atacante puede acceder a los datos si éstos no están adecuadamente protegidos, mediante ataques por inyección de SQL, ataques por desbordamiento de memoria, aumento de privilegios, entre otros.

7.2.2 Alteración de datos

Los datos se pueden corromper, reproducir o modificar durante la transmisión. Durante los procesos de transmisión y almacenamiento de los datos de las aplicaciones, un atacante puede corromper los datos si éstos no están protegidos adecuadamente. Por ejemplo, el atacante puede reproducir información utilizada o falsificar información y enviarla a la plataforma IoT si no se analiza la integridad de los datos durante la transmisión.

7.3 Riesgos de seguridad para el sistema

7.3.1 Vulneración de cuentas

Si las cuentas de los administradores para el sistema operativo de la plataforma del servicio IoT no son suficientemente complicadas, o está abierto un puerto innecesario del sistema, las cuentas pueden ser vulneradas mediante fuerza bruta o monitorización, entre otros. Un control de acceso inadecuado también pone en peligro la seguridad del sistema.

7.3.2 Abuso de privilegios

Los servicios IoT prestados por la plataforma funcionan con el sistema operativo y el *software* intermedio. Si el sistema operativo o el *software* intermedio no se actualizan a su debido tiempo, existen riesgos de que un sistema o un *software* intermedio en una versión antigua presenten vulnerabilidades que pueden utilizar los piratas informáticos para una elevación de los privilegios.

7.4 Riesgos de seguridad para la infraestructura

La infraestructura es vulnerable en cuanto a seguridad física, seguridad de red y seguridad de virtualización, así como frente a riesgos de seguridad de los equipos.

7.4.1 Riesgos físicos

El entorno físico de la plataforma IoT también afecta a la seguridad. Por ejemplo, es vulnerable frente a amenazas naturales como terremotos, inundaciones, tormentas y tornados. Por otro lado, instalaciones como los sistemas de alimentación y refrigeración, o incluso los propios sistemas de seguridad, pueden suponer un riesgo para dicha plataforma. Además, también deben considerarse factores humanos, susceptibles de provocar destrucciones deliberadas, robos, explosiones, etc.

7.4.2 Riesgos de red

Los atacantes pueden analizar Internet para encontrar puntos de acceso de las plataformas del servicio IoT. La falta de aislamiento de la red respecto de las plataformas de servicios puede facilitar el acceso a los datos de diferentes servicios.

7.4.3 Riesgos de la virtualización

La tecnología de virtualización de servidores ha mejorado mucho la eficiencia de la construcción, la flexibilidad operativa y los beneficios económicos de las plataformas IoT, si bien conlleva asimismo nuevos riesgos. Por ejemplo, los fallos de diseño del controlador de máquina virtual (VMM) hacen posible que los atacantes se introduzcan en los servidores virtuales ompt y la compartición de una tarjeta de red con la máquina virtual del mismo servidor facilita la expansión de los problemas de seguridad. Existen también otro tipo de riesgos como el salto entre máquinas virtuales (VM), los ataques de DoS y las vulnerabilidades de la gestión remota de la plataforma.

7.5 Riesgos de seguridad para las interfaces

Las interfaces de una plataforma del servicio IoT incluyen las interfaces web, las API de terceros y las API del servidor de soporte del vendedor, que pueden suponer riesgos por fugas de información, secuencias de comandos en sitios cruzados, una autentificación o un control de acceso débiles.

7.6 Riesgos de seguridad operativos

Durante la operación y el mantenimiento, se puede interrumpir el servicio debido a actuaciones operacionales incorrectas del personal de operación y mantenimiento. Por ejemplo, el personal puede utilizar una memoria flash USB infectada por *malware* o borrar datos accidentalmente. También deben tenerse en cuenta las conexiones inusuales, las contraseñas por defecto, los ataques malintencionados y los mecanismos de auditoría.

8 Arquitectura de seguridad de una plataforma del servicio IoT

La arquitectura de seguridad de una plataforma del servicio IoT se centra en seis aspectos de los requisitos de protección de la seguridad: la seguridad de las aplicaciones, la seguridad de las interfaces, la seguridad de los datos, la seguridad del sistema, la seguridad de la infraestructura y la seguridad operativa.

La arquitectura general de la seguridad se muestra en la Figura 3:

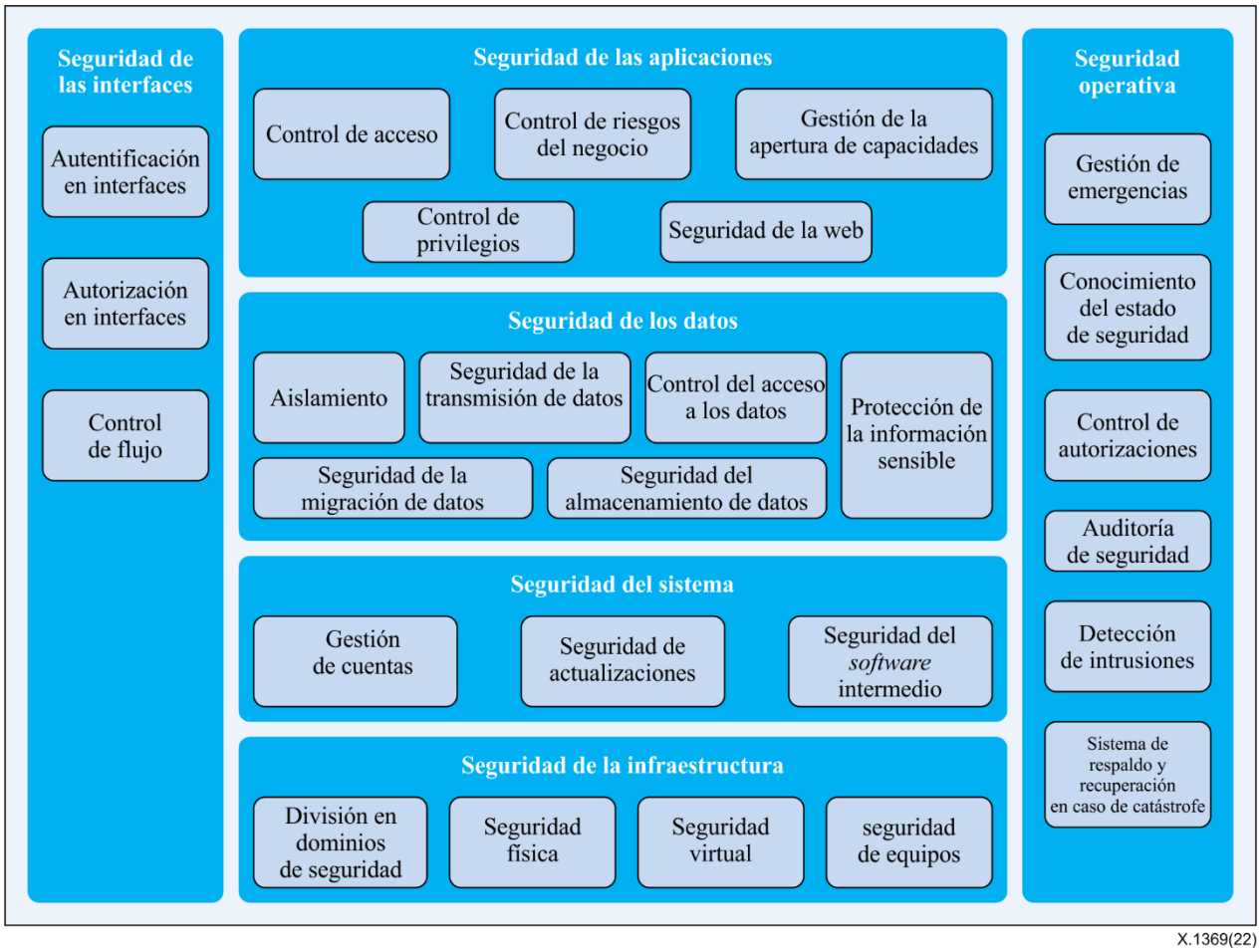

Figura 3 – Arquitectura de seguridad de una plataforma del servicio IoT

8.1 Seguridad de las aplicaciones

La seguridad de las aplicaciones incluye el control de acceso, el control de privilegios, el control de riesgos del negocio, la seguridad de la web y la gestión de la apertura de capacidades, que deberían permitir resolver los problemas de elevación de privilegios, los accesos no autorizados, etc.

8.2 Seguridad de los datos

La seguridad de los datos incluye el aislamiento, la seguridad de la transmisión de datos, el control de acceso a los mismos y la seguridad del almacenamiento de datos, que deberían permitir resolver los problemas de las fugas de datos personales y otros problemas de la seguridad de los datos.

8.3 Seguridad del sistema

La seguridad del sistema incluye la gestión de cuentas, la seguridad de las actualizaciones del *software* y la seguridad del *software* intermedio, que deberían permitir resolver los problemas de la utilización malintencionada de las vulnerabilidades conocidas.

8.4 Seguridad de la infraestructura

La seguridad de la infraestructura incluye la división en dominios de seguridad, la seguridad física, la seguridad virtual y la seguridad de los equipos, que deberían permitir resolver los problemas de la utilización malintencionada de las vulnerabilidades conocidas.

8.5 Seguridad de las interfaces

La seguridad de las interfaces incluye la autentificación de las interfaces, la autorización de las interfaces y el control de flujo, que deberían permitir resolver los problemas de acceso no autorizado a información de identificación personal, la inyección de SQL, entre otros.

8.6 Seguridad operativa

La seguridad operativa incluye la gestión de las emergencias, el conocimiento del estado de seguridad, el control de autorizaciones, las auditorías de seguridad, la detección de intrusiones, un sistema de respaldo y recuperación en caso de catástrofe, que deberían permitir resolver los problemas relacionados con la seguridad operativa.

9 Requisitos de seguridad para una plataforma del servicio IoT

9.1 Seguridad de las aplicaciones

La plataforma de servicio debe ser capaz de prevenir los ataques de Internet en la zona de demarcación, especialmente los ataques a los macrodatos, la computación en la nube, las aplicaciones web y otras tecnologías. Debe proporcionarse la capacidad de prevenir la DDoS, la alteración de los datos, las intrusiones y los virus para garantizar el funcionamiento seguro y estable de la plataforma de servicio.

9.1.1 Control de acceso

9.1.1.1 Control de acceso de usuarios

1) El sistema de identificación de usuarios debe diseñarse para asignar una etiqueta de identidad única para cada usuario; dicha etiqueta debe seguir siendo la misma, aunque el usuario cambie el número de teléfono móvil, el buzón de correo u otros datos.
2) Se debe implementar una detección periódica de las contraseñas débiles. Además, la contraseña debe encriptarse durante el proceso de transmisión. Para los servicios de alta seguridad, debe considerarse un mecanismo de sustitución periódico y obligatorio de la contraseña.

3) La utilización de mensajes cortos dinámicos debe gestionarse de manera estricta. Deben adoptarse medidas de seguridad como la verificación en segundo plano, la invalidación inmediata tras el uso, la limitación del número de inicios de sesión erróneos, el rechazo a la devolución en respuesta, etc.

4) Se debe utilizar un mecanismo de códigos gráficos de autentificación en caso de inicio de sesión. Deben utilizarse medidas de aleatorización del fondo como el ruido de fondo, la no binarización, la antisegmentación, líneas cruzadas, la distorsión y rotación de las fuentes, entre otras, para evitar un reconocimiento rápido por parte de las máquinas.

5) La plataforma debe tener la capacidad de controlar los riesgos y medidas anticolisión. Debe tener la capacidad de identificar los accesos legítimos. Por ejemplo, debe evitarse el cracking violento mediante la limitación numérica de los inicios de sesión erróneos, la dirección IP, el ID del dispositivo, el tiempo de bloqueo, el modo de desbloqueo y las conexiones simultáneas.

6) Durante los procesos de restablecimiento y recuperación de la contraseña, debe verificarse de manera rigurosa la identidad para evitar que se sortee la autentificación y que se falsifique la identidad.

9.1.1.2 Control de acceso de aplicaciones

1) Construir un sistema de identificación de aplicaciones y asignar un identificador único a cada aplicación.

2) Debe autentificarse la validez de la aplicación que accede a la plataforma. Solo debe autorizarse el acceso de aplicaciones autentificadas a la plataforma de servicio para llevar a cabo las invocaciones posteriores del servicio.

3) Se prohíbe transferir las claves como texto sin formato o aplicar una transformación con algoritmos débiles (como MD5) durante el proceso de autentificación de la aplicación.

4) Se deben asignar claves diferentes a las diferentes aplicaciones, y deben soportarse funciones de gestión de las claves para la generación, distribución, almacenamiento y actualización de las mismas.

5) Debe autentificarse la invocación de interfaces para limitar el alcance de los recursos y la autoridad operativa que pueden utilizarse.

9.1.1.3 Control de acceso de dispositivos

1) Debe desarrollarse un sistema de identificación de dispositivos. Asignar un identificador único a cada dispositivo IoT y enlazar el identificador con la información del dispositivo correspondiente, como el fabricante del dispositivo, el tipo de dispositivo, el molde, entre otros.

2) Asignar una clave de dispositivo única a cada dispositivo mediante un esquema de distribución previa de claves, un esquema de intercambio de claves, etc. La clave del dispositivo y el identificador del dispositivo deben estar ligados conjuntamente. Deben soportarse funciones de gestión de las claves para la generación, distribución, almacenamiento y actualización de las mismas.

3) Ejecutar una autentificación de la identidad cuando el dispositivo accede a la plataforma. Solo debe autorizarse el acceso de dispositivos autentificados a la plataforma de servicio para llevar a cabo las invocaciones posteriores del servicio.

4) Se prohíbe transferir las claves como texto sin formato o aplicar una transformación con algoritmos débiles (como MD5) durante el proceso de autentificación de la aplicación.

9.1.2 Control de privilegios

1) Debe soportarse la gestión de la clasificación y agrupamiento de usuarios. Deben concederse privilegios diferentes en función de la clasificación y agrupamiento de los diferentes usuarios. Solo debe autorizarse a los usuarios autorizados el acceso a los datos especificados y a realizar las operaciones correspondientes.
2) Deben concederse privilegios diferentes en función de la clasificación de las diferentes aplicaciones. Solo debe autorizarse a las aplicaciones autorizadas a invocar las capacidades de servicio especificadas y a realizar las operaciones correspondientes.
3) Deben concederse privilegios diferentes en función de la clasificación de los diferentes dispositivos. Solo debe autorizarse a los dispositivos autorizados el acceso a la información y los datos especificados y a realizar las operaciones correspondientes.

9.1.3 Control de riesgos del negocio

9.1.3.1 Gestión y control de la seguridad de las tarjetas IoT

Las funciones de comunicación de las tarjetas IoT deben limitarse de manera estricta para los diferentes tipos de servicios en base al principio de "las mínimas, necesarias y controlables". Por ejemplo, las funciones de voz, los mensajes cortos deben ser unidireccionales en algunos de los casos, y la función de datos debe restringirse cuando el flujo de datos no es normal.

9.1.3.2 Gestión y control de la seguridad del servicio

Debe existir la capacidad de limitar la cantidad total y la frecuencia del flujo de datos, los mensajes cortos, la voz, etc. y de cortar el servicio cuando la cantidad supera el umbral definido.

9.1.3.3 Control del comportamiento de los usuarios

Debe limitarse la cantidad total de flujo, la frecuencia y el tiempo de acceso de los usuarios a la plataforma. Cuando los usuarios tienen un comportamiento inusual, debe cortarse el acceso inmediatamente.

9.1.3.4 Supervisión de las anomalías de los dispositivos

Debe supervisarse el comportamiento de los dispositivos. Cuando se detectan comportamientos inusuales de los dispositivos (como, por ejemplo, horas no habituales, visitas inusuales, zonas de localización anormales) deben generarse alarmas y proporcionarse mecanismos de procesamiento.

9.1.3.5 Supervisión de los riesgos del servicio

Deben analizarse los datos de los terminales IoT en múltiples dimensiones como la cantidad total y el flujo máximo, para poder detectar las anomalías del servicio rápidamente. Durante el funcionamiento del servicio, también debe supervisarse el uso abusivo del servicio. Por ejemplo, debe detectarse la separación de los dispositivos y las tarjetas controlando los números de identidad internacional del equipo móvil (IMEI) de los dispositivos. Al mismo tiempo, utilizando los macrodatos recopilados sobre el funcionamiento del terminal puede mejorarse la capacidad de detectar, analizar y hacer frente a los riesgos de seguridad desde un punto de vista global.

9.1.4 Seguridad de la web

1) Debe proporcionarse una fuerte capacidad contra los ataques de DDoS, y deben personalizarse las estrategias contra la DDoS (por ejemplo, tracción del tráfico, limpieza del tráfico de red, etc.) para el nivel de aplicación y el nivel de red.
2) La plataforma debe disponer de la capacidad de analizar vulnerabilidades de la web y poder detectar y prevenir los problemas de seguridad como la carga de ficheros, la inyección de SQL, las vulnerabilidades XSS, las vulnerabilidades CSRF y las vulnerabilidades SSRF.

3) La plataforma debe disponer de la capacidad de analizar las vulnerabilidades del servidor y de detectar vulnerabilidades del sistema de información, incluidas vulnerabilidades de seguridad, problemas de la configuración de seguridad, vulnerabilidades de seguridad del sistema de aplicaciones y las contraseñas débiles.

4) La plataforma debe disponer de la capacidad de limitar el tiempo de conexión a la base de datos y de acceso a la red de las aplicaciones web para evitar un consumo innecesario de recursos.

5) La plataforma debe disponer de la capacidad de detección de intrusiones, almacenamiento de las IP del origen, el tipo de ataque, la finalidad del ataque y el tiempo del ataque de la intrusión y generar alarmas cuando se produce una intrusión grave.

9.1.5 Gestión de la apertura de capacidades

9.1.5.1 Autentificación de la identidad

El sistema de habilitación de aplicaciones debe soportar la autentificación de la identidad. Cuando los desarrolladores solicitan y aplican algunas funciones de las API, es necesario autentificar la legitimidad de los desarrolladores y las aplicaciones, y no debe poder falsificarse la identidad de los desarrolladores y las aplicaciones legítimos.

9.1.5.2 Refuerzo y protección de las aplicaciones

El sistema de habilitación de aplicaciones debe tener la función de soportar el refuerzo y protección de las aplicaciones que invocan las funciones de las API, para proteger a la aplicación de ser alterada o descompilada.

9.1.5.3 Protección de la seguridad de los datos

El sistema de habilitación de aplicaciones debe asegurar la confidencialidad e integridad de la información sensible relacionada con las cuentas, las credenciales de los usuarios y las aplicaciones, evitar el robo o la alteración de la información durante el almacenamiento, la transmisión y la utilización. Por ejemplo, la información sensible transmitida entre las aplicaciones IoT y la plataforma debe estar encriptada, y debe analizarse la protección de su integridad, garantizando que la información sensible no se expone a entidades y procesos no autorizados, o que estos no la modifican, alteran o reproducen.

9.1.5.4 Autentificación de la capacidad de invocación

El sistema de habilitación de aplicaciones debe soportar la autentificación y la autorización de la capacidad de invocación. Cuando la aplicación invoca una capacidad, debe autentificarse la frecuencia, la cantidad total y el tipo de capacidad que el desarrollador y la aplicación pueden invocar. La capacidad solo debe invocarse después de la autorización.

9.1.5.5 Supervisión de la capacidad de invocación

El sistema de habilitación de aplicaciones debe soportar la supervisión de la frecuencia, el tiempo y la cantidad total de invocación de la capacidad. Cuando se supera el límite o el comportamiento es inusual, la función debe pararse inmediatamente y generar una alarma al mismo tiempo.

9.2 Seguridad de los datos

La plataforma debe proteger los datos durante todo el ciclo de vida, incluidos el almacenamiento, la transmisión y la utilización, entre otros. Se debe realizar periódicamente una copia de respaldo de los datos críticos del servicio para recuperación en caso de destrucción y deben protegerse los procesos, así como debe garantizarse su confidencialidad, integridad y disponibilidad.

9.2.1 Aislamiento de los datos

Datos diferentes deben utilizarse y almacenarse en entornos aislados. La plataforma debe poder aislar la información sensible de manera lógica y controlar la interacción entre los diferentes ámbitos de manera estricta.

9.2.2 Seguridad de la transmisión de datos

1) La información sensible transmitida entre la plataforma de servicio y los dispositivos IoT u otras plataformas de servicio (incluidas las contraseñas de administrador en segundo plano, las contraseñas de acceso al sistema operativo, las contraseñas de acceso a los dispositivos de red y las respuestas de protección de las contraseñas asociadas con dichas contraseñas) debe protegerse de manera confidencial.
2) Debe protegerse la integridad de la información sensible entre plataformas de servicio, dispositivos IoT y otras plataformas de servicio.

9.2.3 Control de acceso

La plataforma debe soportar la función de control de acceso, por ejemplo, deben establecerse diferentes políticas de acceso para las bases de datos de diferentes sistemas de virtualización, para garantizar que los usuarios solo pueden actuar dentro de la autorización de la base de datos del sistema de servicios correspondiente y no pueden acceder a los datos de otros sistemas de servicios no autorizados.

9.2.4 Seguridad del almacenamiento de datos

1) Los datos deben clasificarse de acuerdo con su importancia, y deben adoptarse diferentes mecanismos en función del nivel de clasificación de los datos. Por ejemplo, los datos menos importantes pueden almacenarse en texto sin formato, mientras que debe garantizarse la confidencialidad de los datos importantes.
2) La plataforma debe proporcionar mecanismos seguros de almacenamiento de las claves. Por ejemplo, almacenar las claves dentro de la máquina de encriptación o un intermediario (proxy) específico para garantizar que no se producen fugas de las claves.
3) Debe protegerse la integridad de los datos y es necesario proporcionar mecanismos de detección de la integridad de los datos sensibles, para que se puedan detectar a tiempo los daños o la pérdida de dichos datos. Los datos muy sensibles incluyen los nombres de usuario, los números de cuentas, etc.
4) La plataforma debe proporcionar mecanismos completos de copia de respaldo y de recuperación de los datos. Si se destruyen o pierden datos, debe utilizarse el mecanismo de copia de respaldo para restablecer los datos garantizando que no se pierden los datos después de que se produzca el accidente.
5) La plataforma debe tener la capacidad de almacenar todo tipo de datos y archivos, y la función de eliminar los datos y los archivos temporales de manera automática y periódica.
6) El espacio de almacenamiento de archivos, directorios y bases de datos del sistema debe liberarse o redistribuirse, y debe poder quedar totalmente limpio e irrecuperable.

9.3 Seguridad del sistema

El sistema utilizado por la plataforma debe tener en cuenta la gestión de cuentas, la seguridad de las actualizaciones del *software* y la seguridad del *software* intermedio, lo que debe permitir la resolución de los problemas de utilización malintencionada de las vulnerabilidades conocidas.

9.3.1 Gestión de cuentas

1) El sistema de la plataforma debe generar de manera automática registros de actividad del sistema, como la información de inicio de sesión de los usuarios, la información operativa, etc.
2) Para los sistemas cuyo mantenimiento se realiza a distancia por protocolo HTTP, el sistema debe soportar los protocolos de encriptación como HTTPS.
3) Para los sistemas con interfaces de caracteres, debe soportarse el cierre automático de sesión de las cuentas en función del tiempo.
4) El sistema debe tener en cuenta el control de acceso de los recursos del servidor, por ejemplo, estableciendo un modelo de categorías y definiendo la política de seguridad adecuada para controlar los accesos de los usuarios de las diferentes categorías a los recursos del servidor.

9.3.2 Seguridad de las actualizaciones del *software*

1) Las versiones/parches de seguridad del sistema operativo deben actualizarse a tiempo.
2) Solo debe permitirse la instalación de los componentes y aplicaciones necesarios.
3) El sistema debe abrir solo los puertos necesarios y cerrar los innecesarios.

9.3.3 Seguridad del *software* intermedio

1) Las versiones/parches de seguridad del *software* intermedio deben actualizarse a tiempo.
2) Deben deshabilitarse las interfaces innecesarias del *software* intermedio para evitar la pérdida de información del sistema.
3) Las características del *software* intermedio (nombre del *software*/información del número de versión) debe estar protegido para evitar la pérdida de informaciones del sistema.

9.4 Seguridad de la infraestructura

La seguridad de la infraestructura debe considerar la división en dominios de seguridad, la seguridad física, la seguridad virtual y la seguridad de los equipos, que debe permitir resolver los problemas de utilización malintencionada de las vulnerabilidades conocidas.

9.4.1 División en dominios de seguridad de red

1) Los dominios de seguridad deben estar separados entre las plataformas de servicio y la Internet, entre plataformas de servicio y sistemas de soporte internos, y entre diferentes sistemas de servicios alojados en la plataforma. Las fronteras de los dominios de seguridad deben establecerse entre el dominio de acceso y los otros dominios, entre el dominio de acceso y el dominio del núcleo, y entre dominios del núcleo.
2) Diferentes sistemas de servicios de la plataforma de servicio deben estar separados en diferentes redes de área local virtuales (VLAN) y diferentes dominios de seguridad deben utilizar diferentes segmentos de VLAN. Los sistemas de servicios diferentes de cada dominio de seguridad deben utilizar VLAN diferentes, y todas las VLAN están aisladas por defecto. En una misma VLAN, debe soportarse el aislamiento de VM en diferentes niveles de seguridad del mismo sistema de servicios, como la separación de las sub-VLAN con la tecnología de VLAN privadas (PVLAN).
3) Debe establecerse una política de acceso compartido. Por ejemplo, establecer la configuración estratégica del acceso compartido de diferentes dominios de seguridad dentro de un sistema de servicios, y el acceso compartido entre diferentes sistemas de servicios.
4) Debe soportarse la función de aislamiento de los dominios de seguridad. Por ejemplo, la red de la plataforma puede estar separada en dominio de gestión, dominio de servicio, dominio de interfaces, etc. Los dispositivos de diferentes funciones deben distribuirse en diferentes

dominios de seguridad. La detección de intrusiones y el control de acceso deben implantarse en los bordes de los dominios de seguridad.

9.4.2 Seguridad física

1) El entorno físico debe cumplir los requisitos de protección y seguridad de la instalación, el suministro eléctrico, contra incendios, contra el agua, contra la electricidad estática, la temperatura y el control de humedad.

9.4.3 Seguridad virtual

1) La plataforma debe soportar la protección del hipervisor, el aislamiento de VM, el refuerzo del sistema anfitrión en la nube, la supervisión de la seguridad de VM, la protección frente al *malware*, el control de las aplicaciones y otras funciones para la protección frente los problemas comunes de seguridad en la virtualización.

9.4.4 Seguridad de equipos

1) Las instalaciones físicas deben cumplir los requisitos de configuración básicos para la protección y la seguridad, y los requisitos de pruebas. Deben instalarse tecnologías de computación fiables para mejorar la seguridad de las instalaciones.

9.5 Seguridad de las interfaces

La seguridad de las interfaces incluye la autentificación de las interfaces, la autorización de las interfaces y el control de flujo, que deberían permitir resolver los problemas de acceso no autorizado a información identificable personalmente, la inyección de SQL, entre otros.

9.5.1 Autentificación de las interfaces

1) La plataforma debe tener la capacidad de verificar la legitimidad entre sistemas de servicios, a fin de evitar el acceso a la plataforma y la utilización no autorizada de la misma.

2) La plataforma de servicios debe tener la función de almacenar el registro completo de operaciones de los recursos invocados.

9.5.2 Autorización de las interfaces

1) La plataforma de servicios debe disponer de la función de autorización de acuerdo con la gama de direcciones IP del origen. Además de proporcionar una contraseña estática, la plataforma de servicios invocada también necesita autorizar la gama de direcciones IP.

2) Para las interfaces que requieren derechos de acceso de los usuarios, debe existir un mecanismo de acceso de una lista de autorizados/rechazados para impedir el acceso ilegal de los usuarios.

9.5.3 Control de flujo

1) La plataforma debe disponer de la capacidad de controlar la velocidad del flujo definiendo la política de control del flujo, puede modificarse el valor de configuración de la política de acuerdo con el ajuste del funcionamiento en el servidor de soporte de la API. Cuando el número de solicitudes simultáneas supera el límite, se rechazan las solicitudes en exceso y se responde con un mensaje de error.

9.6 Seguridad operativa

La seguridad operativa incluye la gestión de emergencias, el conocimiento del estado de seguridad, el control de autorizaciones, las auditorías de seguridad, la detección de intrusiones y un sistema de respaldo y recuperación en caso de catástrofe, que deberían permitir resolver los problemas relacionados con la seguridad operativa.

9.6.1 Gestión de emergencias

1) La plataforma debe establecer el mecanismo para responder a los incidentes de emergencia, como los incidentes de ciberseguridad, los incidentes de seguridad en el lugar de trabajo, etc.

2) Organizar regularmente simulacros de emergencias y establecer un sistema periódico de simulacros de los planes de emergencia.

9.6.2 Conocimiento del estado de seguridad

1) Se recomienda crear un sistema de conocimiento del estado de seguridad para realizar la supervisión, la evaluación, la alerta temprana, la visualización y la respuesta centralizada de los problemas de seguridad, de manera a mejorar la supervisión de la amenaza de seguridad de la red, el conocimiento de la situación, la respuesta de emergencia, el seguimiento y otras capacidades, y mejorar las operaciones de seguridad y la eficiencia del mantenimiento.

9.6.3 Control de autorizaciones

1) La plataforma debe realizar las autentificaciones y las autorizaciones necesarias para diferentes operaciones de la plataforma. Para los privilegios de nivel alto, solo el personal de confianza del sistema puede realizar las operaciones de los privilegios de nivel alto.

2) La plataforma debe establecer un modelo de categorías, y controlar el acceso de los usuarios a los recursos del servidor de acuerdo con las políticas de seguridad.

9.6.4 Auditoría de seguridad

1) Deben registrarse y almacenarse en un registro todas las operaciones de los administradores.

2) Cuando casi se agote el espacio de almacenamiento, debe garantizarse que no se pierde el registro de auditoría.

3) Debe realizarse una copia de respaldo de los registros de auditoría.

4) Los registros de auditoría deben protegerse frente a los accesos, la modificación y la destrucción no autorizados.

5) Los registros de auditoría deben exportarse y eliminarse.

6) El acceso a los registros debe realizarse de manera segura para garantizar la confidencialidad y la integridad del proceso de transmisión.

7) La plataforma debe disponer de las funciones de supervisión en tiempo real y de auditoría periódica de los comportamientos inusuales, como las conexiones inusuales, los accesos inusuales y las aplicaciones anormales, en base al análisis del tráfico, la auditoría de los registros, bancos de prueba, entre otros, y deben proporcionarse alertas oportunas y capacidad de eliminación de acuerdo con el comportamiento inusual detectado.

9.6.5 Detección de intrusiones

1) La plataforma debe desplegar equipos de detección de las intrusiones a fin de detectar todo tipo de intrusiones de forma oportuna.

9.6.6 Sistema de respaldo y recuperación en caso de catástrofe

1) En caso de incendio, terremoto u otras catástrofes, la plataforma debe poder conmutarse sobre el sistema de respaldo redundante situado en otra ubicación, en un tiempo que permita la continuidad del servicio.

2) La plataforma debe soportar la recuperación en caso de catástrofe de los datos sensibles (como los datos de servicio, los datos de facturación, los datos de configuración del sistema, los registros de mantenimiento y operación de los administradores, la información de usuario, etc.) para garantizar que cuando se eliminan los datos críticos de manera malintencionada, el sistema puede recuperarse a tiempo.

Bibliografía

[b-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*.

[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 X.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube*.

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

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, 2022