



Creación de un mundo IoT fiable y gestionado



CONTENIDOS

- 01 Desarrollo rápido de la IoT
- 06 Sistema de seguridad de extremo a extremo y de múltiples capas para la IoT
- 13 Prácticas de seguridad de la IoT
- 17 Casos típicos de seguridad de IoT
- 22 Hacia la creación de un mundo IoT fiable y gestionado
- 26 Resumen
- Abreviaturas y acrónimos
- Acerca de INCIBE, Red.es y Huawei

Resumen

La Internet de las Cosas (IoT) conecta enormes cantidades de dispositivos y ofrece diversos servicios, lo que incrementa la apertura y la complejidad de las redes. A medida que la IoT abre las puertas a un mundo nuevo donde todo es perceptible, todo está conectado y todo es inteligente, van surgiendo importantes desafíos de seguridad.

Este libro blanco analiza el desarrollo de tecnologías de seguridad de IoT, propone el uso de mecanismos de seguridad de extremo a extremo de múltiples capas para proteger la IoT y resume las prácticas de seguridad correspondientes. Las tecnologías de IoT se están desarrollando con rapidez. Sin embargo, son vulnerables a nuevos problemas y nuevas amenazas de seguridad. La seguridad de la IoT puede garantizarse solamente si la cadena industrial en su totalidad trabaja en conjunto. Por lo tanto, Huawei propone que todos los gobiernos, las organizaciones internacionales y las industrias se unan para desarrollar la seguridad de la IoT y que se esfuerzen más por orientar políticas, promulgar leyes y reglamentos, establecer normas, innovar tecnologías nuevas y desarrollar ecosistemas industriales.



1

Desarrollo rápido de la IoT

Tendencia de desarrollo de la IoT

La IoT está abriendo las puertas a una nueva era.

Esta tiene un rol importante en la transformación digital de todas las industrias. La innovación tecnológica crea enormes cantidades de conexiones, mejora sustancialmente la eficiencia y facilita la vida de las personas. El mercado de la IoT está a punto de florecer.

La IoT está impulsando la transformación digital en todas las industrias. Empresas, gobiernos, organizaciones y comunidades de todo el mundo se esfuerzan por investigar la IoT e invertir en ella, así como por recopilar, analizar y aplicar los datos que esta genera. Esto facilitará el desarrollo rápido de todas las industrias.

La IoT comenzará a formar parte de nuestras vidas, tal como ya lo ha hecho el Internet. Los hogares inteligentes, la educación inteligente, el cuidado de la salud inteligente, los wearables, el Internet de los Vehículos (IoV) y otras industrias hacen gran uso de la IoT. La conexión total brindará inmensos beneficios a las personas y a la sociedad en su totalidad.

La gran popularidad de los dispositivos móviles y el consecuente abanico de plataformas y servicios que se han desarrollado

alrededor de ellos está estimulando el crecimiento rápido del mercado de la IoT. Gartner, Inc. estima que en el mundo habrá 20.800 millones de dispositivos conectados para 2020. Esto representa una tasa de crecimiento anual compuesto (TCAC) del 34 %. La Figura 1-1 muestra una estimación del mercado de IoT según su aplicación.

Amenazas y desafíos de seguridad de la IoT

Estas tentadoras cifras se ven empañadas por desafíos significativos.

El 21 de octubre de 2016 se produjo en los Estados Unidos el mayor ataque DDoS de la historia, que forzó la desconexión de más de 100 sitios web reconocidos, entre ellos Amazon, durante varias horas. El tráfico del ataque superó 1 Tbit/s. Este ataque fue distinto a los ataques DDoS comunes generados por dispositivos de TI (tales como ordenadores y servidores). Fue generado por cámaras IP (IPC), routers domésticos, grabadoras digitales de vídeo y otros microdispositivos inteligentes que fueron infectados

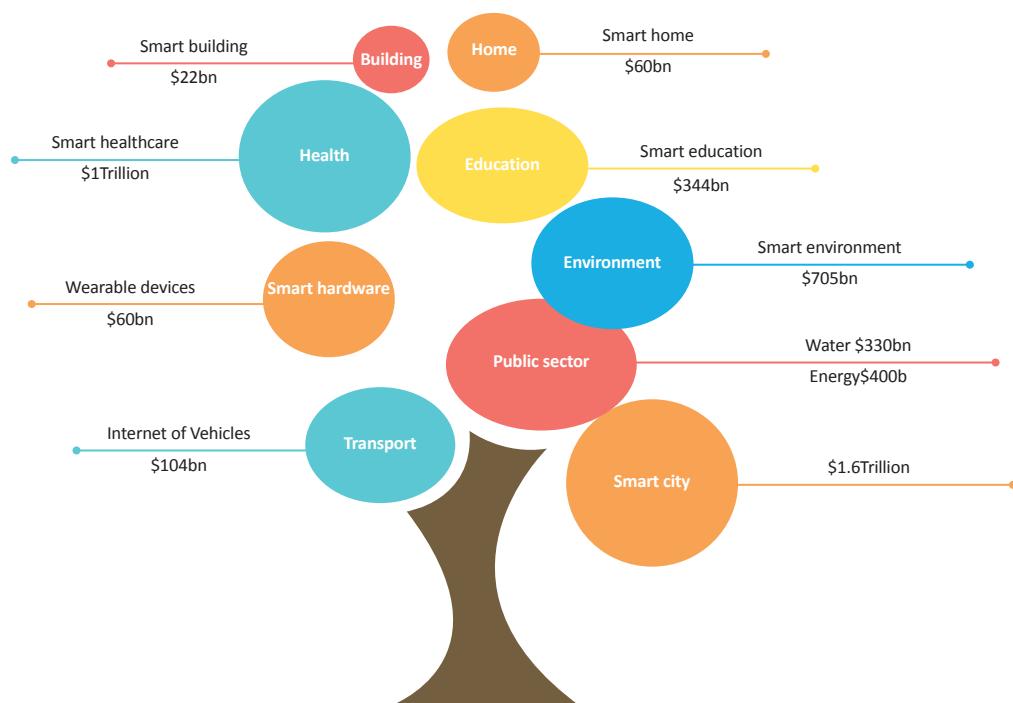


Figura 1-1 Estimación del mercado de IoT por aplicación

(Fuentes: Ovum, GSMA, Gartner)

por el malware Mirai y causaron graves problemas.

El 23 de diciembre de 2015, la distribución de energía en Ucrania fue afectada por un ataque que interrumpió el servicio de una gran cantidad de usuarios durante varias horas. Los piratas informáticos usaron el troyano BlackEnergy para acceder al sistema de gestión de la distribución de energía y fueron así capaces de emitir comandos de interrupción del servicio, borrar y sobrescribir datos del sistema y realizar operaciones de apagado.

En julio de 2015, la revista Wired reveló que piratas informáticos habían alterado remotamente la conducción de vehículos Jeep Cherokee. Fiat Chrysler Automobiles NV, empresa matriz de Jeep, tomó medidas de seguridad a nivel de red para evitar este tipo de manipulación remota. También programó una campaña de recuperación preventiva de 1,4 millones de automóviles y camiones equipados con radios vulnerables en los EE. UU.

La realidad es que las amenazas de seguridad son interminables. Las redes tradicionales siguen afrontando muchos problemas de seguridad, incluso a pesar de contar con numerosas medidas informáticas. Este desafío no se puede evitar en la era de la IoT. Una encuesta de Forrester realizada en organizaciones de todo el mundo reveló que el 47 % de las organizaciones industriales que usan o tienen planificado usar IoT ya habían experimentado problemas de seguridad en sus aplicaciones industriales . Otras investigaciones mostraron lo siguiente:

- * El 27 % de los sistemas de control fueron comprometidos o infectados.
- * El 80 % de los equipos usa una contraseña simple.
- * El 70 % de la comunicación no está cifrada.

* El 90 % de las actualizaciones de firmware no hace verificaciones de firmas. Es posible que muchos dispositivos no puedan actualizarse.

El crecimiento de la IoT mejora la productividad y facilita las vidas de las personas, pero conlleva amenazas de seguridad invasivas. Las amenazas de seguridad surgen en tres capas (como se muestra en la Figura 1-3).

Los sensores omnipresentes hacen que los puntos terminales de IoT no sean fiables.

* Los puntos terminales no se gestionan y son susceptibles a ataques físicos, manipulación indebida y falsificación.

* Es posible que los controladores de los dispositivos no sean fiables, y son fácilmente violables y controlables.

* Los parches para vulnerabilidades de software o sistemas operativos (SO) no están disponibles de manera inmediata.

* Teniendo en cuenta el coste, resultan limitados los recursos y las capacidades de cómputo de los puntos terminales. Es posible que los medios de protección tradicionales y las tecnologías de seguridad, tales como el software antivirus, no sean aplicables.

La transición de la capa de red hacia la IP y la convergencia genera amenazas.

* Los defectos en protocolos inalámbricos, por ejemplo, la falta de autenticación efectiva, pueden ocasionar vulnerabilidades en el lado del acceso.

* Las aplicaciones y los protocolos industriales privados no pueden ser identificados por los dispositivos de seguridad y son fácilmente explotables sin detección oportuna.

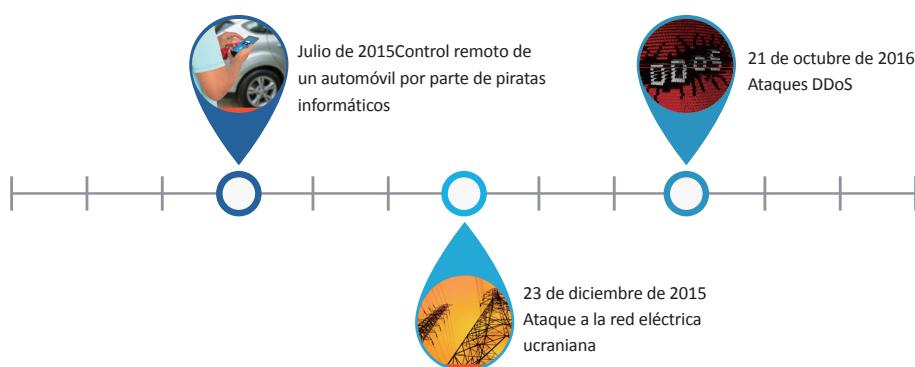


Figura 1-2 Incremento en la cantidad de incidentes de seguridad de IoT

- * El proceso de comunicación sin cifrado es propenso a ataques de intermediario (MITM), tales como secuestros, repeticiones, alteraciones e interceptación de información.

- * Las redes basadas en IP son vulnerables a los ataques y a las intrusiones que se basan en Internet.

La apertura de los servicios en las capas de plataformas y aplicaciones genera nuevas amenazas de seguridad.

- * Los dispositivos gestionados por plataformas son numerosos y muy usados, lo que dificulta sus actualizaciones y la respectiva gestión de seguridad.

- * Los nuevos protocolos de comunicación pueden ocasionar problemas de seguridad y vulnerabilidades en la capa de aplicaciones, por ejemplo, ataques de paquetes mal formados y ataques de saturación.

- * Las vulnerabilidades de las plataformas nuevas y las API abiertas facilitan la aparición de riesgos nuevos.

- * El acceso no autorizado ocasiona pérdidas de privacidad y de datos, tales como filtraciones de credenciales de autenticación.

- * La multiplicidad de los puntos de salida de diversas aplicaciones y diversos centros de datos ocasiona un alto riesgo de ataques DDoS.

- * Es posible que diversas aplicaciones de IoT no sean fiables.

Además, es posible que los dispositivos, las redes y las aplicaciones que forman parte de la IoT correspondan a una variedad de proveedores; por lo tanto, es muy difícil que un solo proveedor pueda ver toda la superficie del ataque, menos aún lograr una protección integral de la seguridad.

La privacidad es uno de los mayores desafíos legales para la IoT.

La IoT involucra una gran cantidad de dispositivos conectados que generan, envían y reciben grandes volúmenes de datos vinculados con personas, lo que deriva en la monitorización permanente de las actividades de las personas a través de muchos dispositivos distintos. Es posible que esta monitorización genere diversos requisitos acerca de la privacidad y la protección de los datos personales. Tales inquietudes no son nada nuevas; todos los cambios tecnológicos de importancia han causado preocupación acerca de la privacidad. Es correcto preocuparse por este tema ya

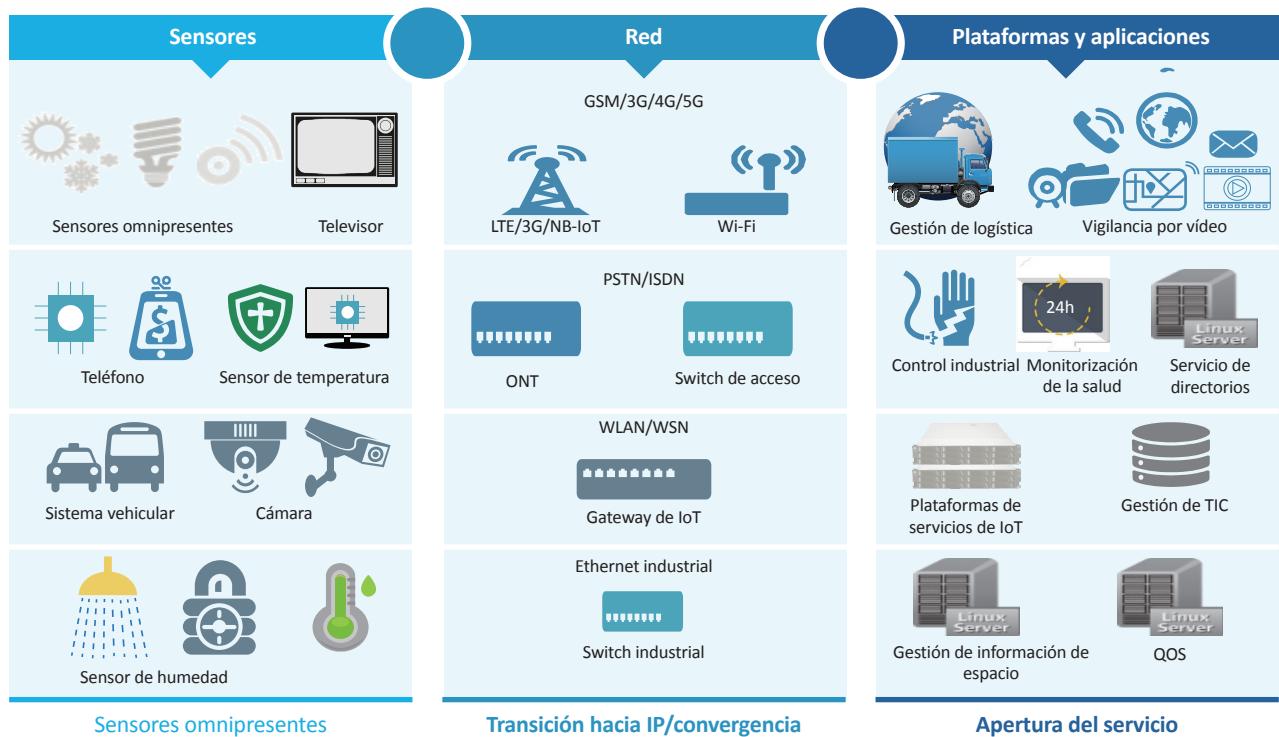


Figura 1-3 Tres capas de la IoT y sus características

que la IoT implica el uso de más dispositivos y más datos, y por ende, genera mayores desafíos.

Requisitos industriales para la seguridad de la IoT

La seguridad de la IoT es específica de cada industria (según se muestra en la Figura 1-4) y puede variar en cuanto a formas y requisitos según los atributos comerciales, los objetos de servicio, las entidades de gestión y los modos operativos de distintas industrias.

* Industria y energía: Seguridad informática de los sistemas industriales de control y redes eléctricas inteligentes, como la seguridad del servicio de cómputo inteligente (ICS) y el control de supervisión y la adquisición de datos (SCADA). Un ataque dirigido a un sistema industrial de control puede ocasionar la interrupción de todo el sistema, lo que podría detener la producción y producir un corte del suministro.

* Movilidad:

Protección de vehículos inteligentes.

Seguridad y protección de vehículos aéreos no tripulados.

Protección de sistemas de comunicación satelital.

Los ataques pueden producir graves accidentes de tránsito y

poner en peligro la vida de las personas.

* Cuidado de la salud:

Protección de dispositivos médicos conectados.

Cifrado para investigación médica y farmacéutica.

Almacenamiento seguro y omnipresente de los datos médicos.

Una situación posible donde estaría en riesgo la vida ocurriría si un pirata informático lograra controlar el desfibrilador cardioversor implantable (DCI) inalámbrico que se encuentra dentro del cuerpo de un paciente.

* Ciudad inteligente: Transmisión y almacenamiento seguros de la información recopilada por una gran cantidad de sensores. Si un sistema de control usado en el transporte ferroviario se ve comprometido, puede producirse desde una planificación inadecuada de horarios hasta un descarrilamiento.

* Finanzas: Protección de pagos móviles contra la falsificación. Las personas y las empresas inevitablemente experimentarán daños materiales en caso de fraude.

La seguridad de IoT no solo puede afectar el éxito comercial, sino también la economía nacional y el bienestar de las personas. Por lo tanto, la creación de un entorno de seguridad de IoT es una exigencia urgente.



Figure 1-4 IoT applications



2

**Sistema de seguridad de
extremo a extremo y de
múltiples capas para la IoT**

La IoT abre la puerta a amenazas de seguridad omnipresentes con impacto en una amplia gama de dispositivos, desde plataformas de sistemas hasta sensores. El mercado de IoT genera grandes expectativas pero trae consigo múltiples desafíos. Cualquier riesgo en un punto único puede poner en peligro a toda la red y a los sistemas esenciales. Por lo tanto, la seguridad debe tenerse en cuenta desde el inicio de la planificación de IoT, y debe desarrollarse un sistema de seguridad de extremo a extremo de múltiples capas (según se muestra en la Figura 2-1).

La seguridad de IoT se manifiesta en chips y dispositivos, así como en sus correspondientes sistemas operativos, redes, plataformas de gestión, aplicaciones y operaciones empresariales. Las técnicas y medidas de seguridad pueden analizarse para cada capa. Además de la protección de seguridad de cada capa, se desarrolla un sistema de defensa integral de extremo a extremo en función de la interdependencia entre los dispositivos, los canales y la nube. En este sistema, la conciencia situacional de seguridad de toda la IoT tiene una importancia especial.

Seguridad de chips y SO

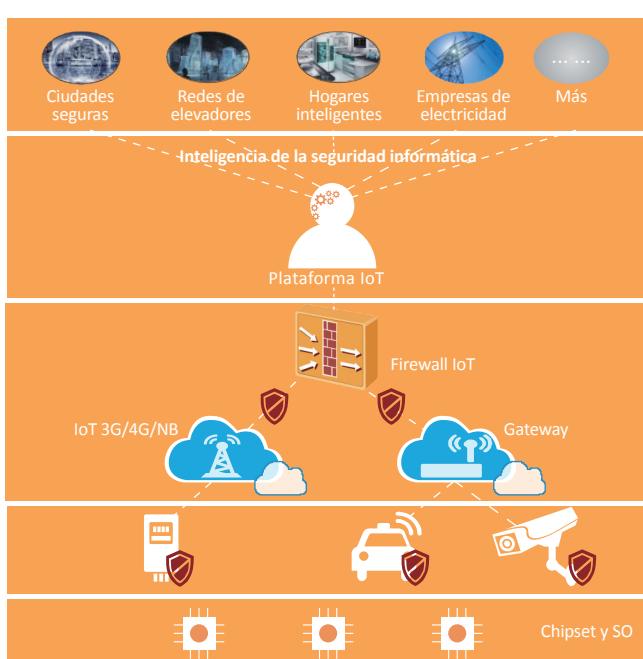
En dispositivos de IoT que tengan requisitos de seguridad muy exigentes, se prefiere el uso de chips seguros. Los proveedores de chips brindan solidez de cifrado y aislamiento a nivel de hardware mediante distintas técnicas (según se muestra en la Figura 2-2), tales como el entorno de ejecución fiable (TEE) y el módulo de plataforma

fiable (TPM) para que las claves importantes se almacenen en un chip fiable y así se eviten las filtraciones de datos. Además, se admite el arranque seguro y las firmas se verifican durante el inicio y la actualización de software y firmware para garantizar la integridad de los datos. La IoT requiere técnicas de seguridad rentables, universales y con eficiencia energética a nivel de los chips.

El SO es un elemento indispensable para una solución de seguridad completa. En mecanismos comunes de planificación de SO livianos de IoT, la memoria unificada se comparte independientemente del modo de usuario o del modo de kernel. Todas las aplicaciones y el kernel se ejecutan en modo de privilegio. Esto ocasiona muchas dudas y amenazas de seguridad respecto de los servicios del sistema.

Si se implementa el mecanismo de aislamiento de un SO seguro y liviano, el modo de usuario quedará aislado del modo de kernel, y las aplicaciones quedarán aisladas entre sí. Se admitirán mecanismos de protección de memoria y planificación aislada para el kernel con el fin de incrementar significativamente la fiabilidad y la seguridad del sistema.

Un SO seguro reorganiza y gestiona la memoria para dividir el espacio correspondiente al kernel y a las aplicaciones, usa el mecanismo syscall para separar los privilegios del modo de kernel y del modo del usuario, y usa máquinas virtuales (VM) para proteger los privilegios de distintas aplicaciones. Además, brinda interfaces configurables de protección de memoria a los usuarios en función de la unidad de



Seguridad en la nube

- * Análisis de modelos de amenazas a través de la analítica de Big Data y el aprendizaje automático.
- * Concentración sobre la seguridad de redes IoT.
- * Detección de amenazas desconocidas.
- * Alertas y bloqueo colaborativo en segundos.

Seguridad de la red

- * Identificación de firewall y filtrado de protocolos de red IoT.
- * El firewall procesa millones de eventos simultáneos.
- * Túneles de gateway y túneles inalámbricos encriptados.

Seguridad de los puntos terminales

- * Chipset (TPM/TEE).
- * Sistema operativo (aislamiento).
- * Plug-In de seguridad (liviano).

Figura 2-1 Arquitectura de seguridad de extremo a extremo de múltiples capas para IoT

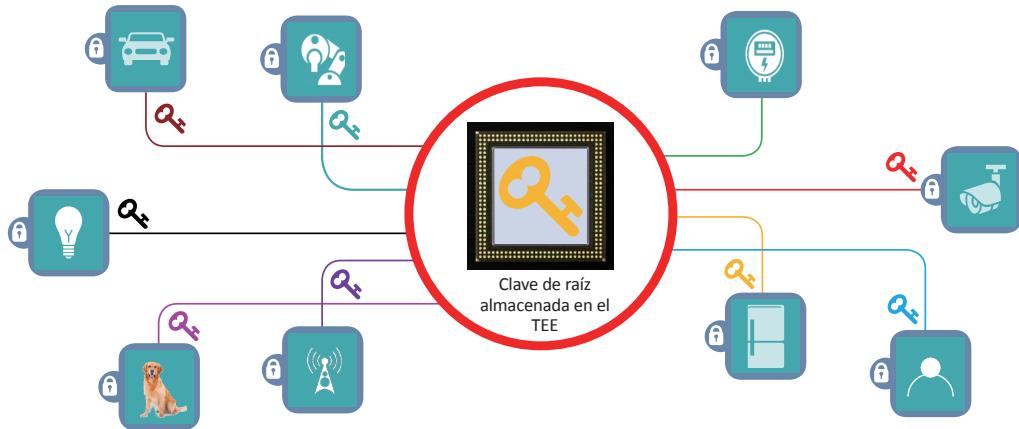


Figura 2-2 Seguridad a nivel de los chips

protección de memoria (MPU) o de la unidad de gestión de memoria (MMU). Las medidas de protección de seguridad (según se muestra en la Figura 2-3) incluyen las siguientes:

- * Diseño de distribución adecuada de la memoria.
- * Distinción entre el modo de kernel y el modo de usuario.
- * Aislamiento de procesos para aplicaciones.
- * Interfaz de protección de memoria.

El área segura creada por el mecanismo de aislamiento liviano protege al SO. Una aplicación puede crear una zona segura independiente en función del área segura usando la MPU. Las principales funciones del mecanismo de aislamiento liviano creado por el SO seguro son las siguientes:

* Control de acceso: Hay espacios aislados, se establecen canales de acceso de seguridad y se llevan a cabo tareas eficientes de gestión y control para evitar el acceso no autorizado mediante códigos maliciosos.

* Kernel de seguridad: Sienta las bases para la protección de la seguridad de la actualización de firmware (actualización inalámbrica de firmware o FOTA, según sus siglas en inglés), del almacenamiento de seguridad, de la gestión de claves, del cifrado y del descifrado, y del ID del dispositivo.

Un SO seguro puede brindar funciones tales como autenticación de identidad fiable, upgrade seguro de firmware, control de acceso al servicio de Internet, cifrado y descifrado, y gestión de claves.

Seguridad en los puntos terminales

Los puntos terminales de IoT incluyen sensores y dispositivos de

acceso que pueden recopilar datos y acceder a redes para informar tales datos. Las características de estos puntos terminales son las siguientes: menor consumo de energía, bajo coste, capacidades débiles de cómputo y almacenamiento, accesibilidad física, ciclos de vida prolongados, interfaces y protocolos complejos, etc.

La arquitectura de seguridad tradicional ya no puede satisfacer estos requisitos. Es necesaria una arquitectura de seguridad nueva para garantizar la seguridad de los puntos terminales de IoT (según se muestra en la Figura 2-4).

- * Seguridad física: Resistencia al agua, al polvo, al impacto y a las ondas electromagnéticas del entorno de IoT.
- * Seguridad del acceso: Debe evitarse que los dispositivos falsificados accedan a la red y que los puntos terminales de IoT se conviertan en zombis de ataques DDoS. Los complementos livianos de aplicaciones de seguridad que son fáciles de integrar permiten analizar las anomalías de los puntos terminales y permiten cifrar los datos de comunicación para evitar que los puntos terminales sean usados como plataforma para atacar nodos de red importantes. Además, también se requiere el uso de nuevas tecnologías, como el mecanismo liviano de autenticación obligatoria, la autenticación distribuida y la cadena de bloques.
- * Seguridad del entorno de ejecución: El mecanismo de seguridad a nivel de kernel brindado en tiempo real por el SO liviano, integrado y en tiempo real se encarga de proteger el entorno. Se admite la firma de software para el arranque seguro en el código de servicio para que solo puedan cargarse paquetes de software válidos e intactos. Se admiten las listas blancas de acceso para evitar códigos maliciosos y accesos no autorizados.

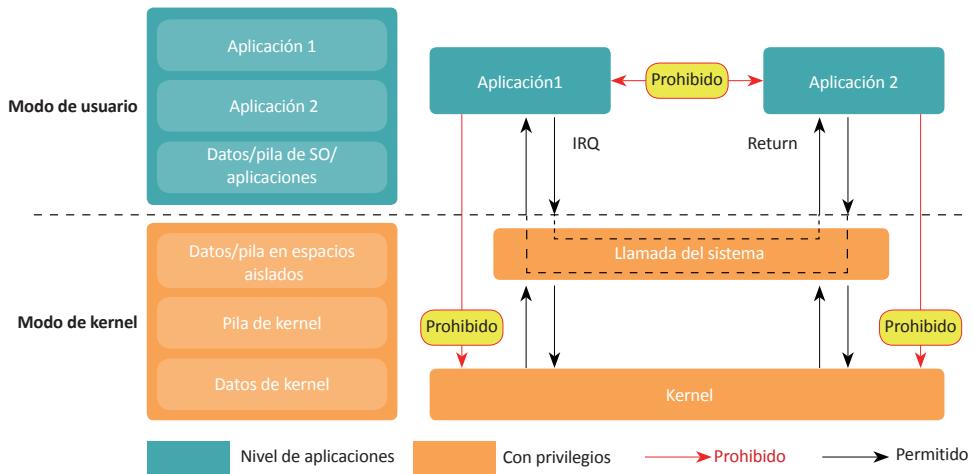


Figura 2-3 Mecanismo de seguridad del SO

* Seguridad de datos de servicio: Se adoptan medidas contra la filtración de datos y contra las copias, y también se usa el aislamiento de datos para proteger los datos locales.

* Gestión unificada: Brinda gestión de la seguridad durante todo el ciclo de vida, lo que incluye la activación del dispositivo, la autenticación de identidad, el almacenamiento seguro, el arranque seguro, la verificación de integridad, la actualización de software y la baja del dispositivo.

El hardware y el software deben considerarse en su totalidad para la seguridad de los puntos terminales de IoT, lo que incluye la seguridad a nivel del chip, la seguridad del SO y las mejoras de seguridad de los puntos terminales donde se ejecutan los SO. La disponibilidad de puntos terminales fiables y gestionados es el requisito básico para la seguridad de la IoT, debido a que esta última no puede desarrollarse ampliamente sin fiabilidad. Por lo tanto, los proveedores deben seleccionar cuidadosamente sus técnicas de seguridad para adoptar sofisticados puntos terminales de IoT en función de la confidencialidad de los datos, el nivel de inteligencia de los puntos terminales y las características de las distintas arquitecturas de red. Por ejemplo, los proveedores podrían usar técnicas de seguridad nuevas, tales como el cifrado de seguridad liviano y la autenticación distribuida, para lograr el equilibrio entre la seguridad, el consumo de recursos y los costes.

Seguridad de la capa de red

La IoT impone la necesidad de que las redes admitan diversos servicios, transmitan grandes volúmenes de tráfico y usen distintas técnicas cableadas e inalámbricas. Las técnicas cableadas incluyen

Ethernet, RS232, RS485 y PLC, y las inalámbricas incluyen GPRS, LTE, ZigBee, Z-Wave, Bluetooth y Wi-Fi. La mayoría de los mecanismos de seguridad tradicionales es aplicable al mundo de la IoT. Por ejemplo, pueden usarse los siguientes mecanismos: aislamiento de zonas de seguridad de red, autenticación en dispositivos que intentan acceder a las redes, protección automática mediante firewalls, protección contra ataques DDoS, prevención de ataques basados en aplicaciones y en la Web, y transmisión segura en los planos de control y de usuarios mediante IPsec.

La seguridad de la capa de red de la IoT se centra en los siguientes dos aspectos: la seguridad de las nuevas tecnologías de comunicación de IoT (como NB-IoT y 5G) y los mecanismos de seguridad para una gran cantidad de protocolos de propiedad exclusiva y redes industriales de control.



Figura 2-4 Medidas de seguridad de los puntos terminales

Las tecnologías NB-IoT y 5G imponen los siguientes requisitos de seguridad:

* Autenticación unificada y distribuida de los puntos terminales de IoT, que se caracteriza por el alto nivel de simultaneidad y la descentralización.

* Adaptación al software de NFV, al despliegue automático y a la programabilidad dinámica.

* Cifrado de extremo a extremo y algoritmos nuevos de cifrado liviano en un entorno abierto.

* Detección en múltiples capas de ataques lanzados mediante dispositivos de distintos proveedores y cooperación de múltiples funciones de seguridad.

La IoT debe aprovechar al máximo las características del transporte por capa física de las comunicaciones móviles inalámbricas y debe aplicar tecnologías de seguridad para autenticación, cifrado y transmisión segura con el fin de garantizar la calidad de la transmisión, evitar interceptación de información en ubicaciones desconocidas y aumentar la dificultad de lanzar ataques MITM. En cuanto a las interfaces de aire, los puntos terminales y las redes se autentican mutuamente de acuerdo con estándares inalámbricos para que solo los puntos terminales autorizados puedan acceder a redes válidas. Se establecen canales seguros entre los puntos terminales y las redes para el cifrado y la protección de integridad con el fin de evitar filtración de datos, manipulación indebida e interceptación de información.

Los puntos terminales de IoT usan una gran cantidad de interfaces dedicadas (que incluyen KNX, ModBus y CANBus) que se conectan a redes industriales de control. La mayoría de estos puntos terminales y redes han sido diseñados para ejecutarse en entornos aislados y, por lo tanto, cuentan con mecanismos de seguridad débiles. Cuando estos puntos terminales y redes pasan a formar parte del mundo de la IoT, surgen problemas de seguridad nuevos. Para solucionar estos problemas, los firewalls de IoT (según se muestra en la Figura 2-5), los gateways de seguridad y otros dispositivos deben ser capaces de hacer lo siguiente:

* Implementar análisis en profundidad y filtrado automático para protocolos industriales y aplicaciones de distintas industrias.

* Admitir cifrado para dispositivos de acceso.

* Admitir filtrado basado en listas blancas, lo que incluye el filtrado autodefinido de protocolos.

* Brindar protección automática contra ataques DDoS caracterizados por el agotamiento de los recursos de dispositivos y los ataques de tráfico de aplicaciones de múltiples industrias.

Los productos de seguridad de red también deben brindar antivirus y protección contra amenazas avanzadas y persistentes (APT) para la IoT.

Seguridad de plataformas y aplicaciones

La plataforma de gestión de IoT gestiona principalmente una gran cantidad de puntos terminales, datos, operaciones y seguridad de IoT. Como se muestra en la Figura 2-6, los datos personales son el factor de seguridad más importante para todos los tipos de gestión. Esto se debe a que es posible que una gran cantidad de datos personales de los usuarios se transmitan desde puntos terminales dispersos hacia una plataforma de IoT en la nube o hacia una plataforma de procesamiento. Por lo tanto, debe brindarse una protección adecuada a los datos personales de acuerdo con los requisitos detallados en las leyes de protección de la privacidad de los países y las regiones locales.

Además, diversas aplicaciones verticales (tales como los hogares inteligentes, la IoV y la medición inteligente) necesitan acceder a la plataforma de IoT. Deben brindarse mecanismos de aislamiento de seguridad para el almacenamiento de datos debido a que los requisitos de seguridad de estos últimos pueden variar según las aplicaciones. Además, deben garantizarse la confidencialidad y la integridad de los datos en tránsito. La información confidencial, como los datos de vídeo, debe cifrarse para el almacenamiento en la nube, y los datos deben borrararse una vez transcurrido el periodo de conservación requerido para los datos personales.

También debe considerarse la seguridad de las aplicaciones de IoT. Deben implementarse la autenticación obligatoria y el control de acceso para el acceso a la nube. Las vulnerabilidades de las aplicaciones no deben poner en peligro a los datos de aplicaciones en tránsito. Deben brindarse cifrado y aislamiento efectivos para el almacenamiento de datos en ordenadores y en puntos terminales móviles.

Conciencia situacional de seguridad

El sistema de la IoT, que incluye dispositivos, redes, plataformas y aplicaciones, no solo requiere múltiples medidas de protección de la seguridad en cada capa, sino que también requiere capacidades inteligentes de análisis de la seguridad de macrodatos para la sinergia

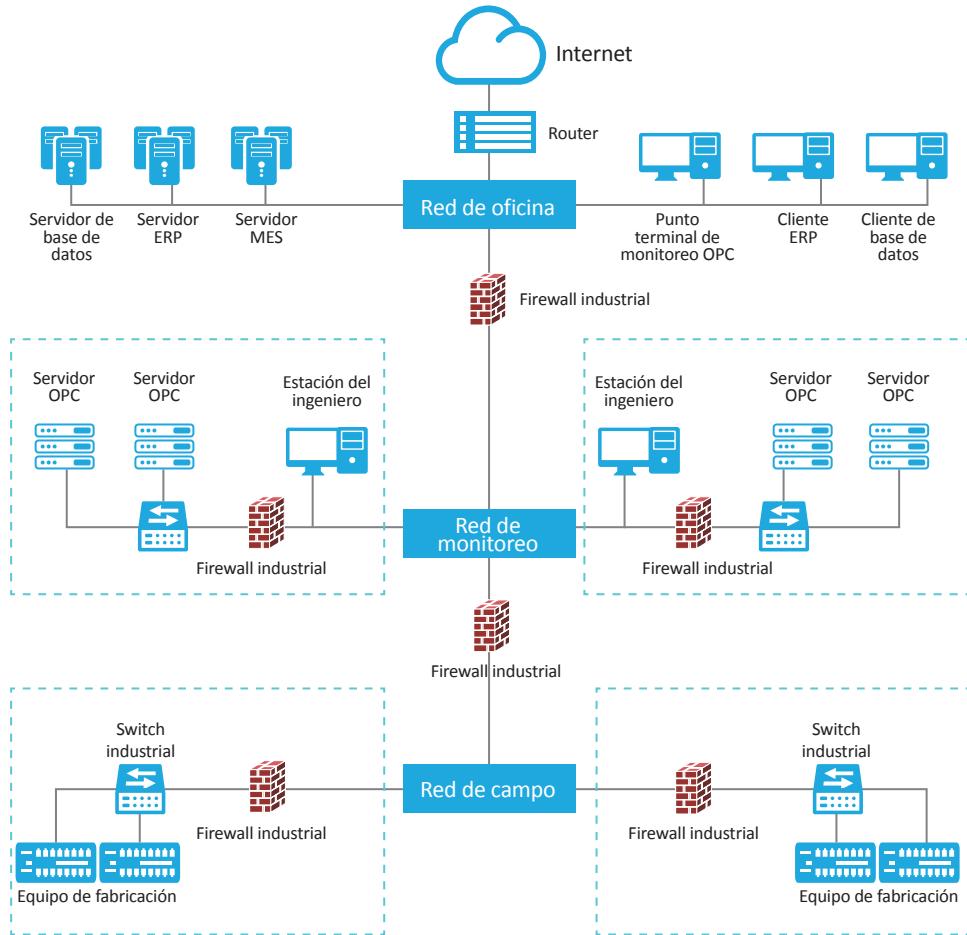


Figura 2-5 Aplicación de firewalls industriales

Gestión de seguridad de API								
Gestión del ciclo de vida de seguridad (aprovisionamiento, autenticación, upgrade de vinculación y baja)			Monitorización de seguridad y detección de anomalías (macrodatos / aprendizaje de máquinas / IDS)					
Aislamiento de datos	Gestión de claves	Cifrado de datos	Protección de integridad del software	TPM/vTPM	Protección de la privacidad			
Gestión básica del mantenimiento de seguridad (cuentas/permisos/registros)			Aislamiento de redes y protección contra ataques DoS					
Mejoras de seguridad para SO / base de datos / sistema web								
Seguridad de la plataforma de virtualización								

Figura 2-6 Seguridad de la plataforma de IoT

entre los dispositivos y la nube (como se muestra en la Figura 2-7). Esto permitirá que la IoTLogre conciencia situacional de seguridad inteligente, visualización y protección de la seguridad en toda la red, y estos serán los pilares de la seguridad de IoT en el futuro.

Debido a la gran cantidad de puntos terminales de IoT, estos son un trampolín fácil para los ataques, lo que representa una amenaza para la plataforma principal de IoT. La plataforma de análisis de la seguridad de macrodatos monitoriza y analiza el tráfico y el comportamiento de los puntos terminales y los compara con líneas de base en tiempo real para localizar rápidamente los puntos terminales infectados. Así, la plataforma puede coordinar los dispositivos de seguridad para contener la infección y aislar los puntos terminales infectados de acuerdo con las políticas de

seguridad definidas. Esta serie de acciones protegerá la plataforma principal y el sistema del servicio.

Además, la plataforma de análisis de seguridad de macrodatos puede funcionar como una plataforma unificada de monitorización y gestión de la seguridad para toda la red de IoT. Mediante la monitorización de la red y la planificación de todos los dispositivos de seguridad, la plataforma puede evitar amenazas conocidas y desconocidas, especialmente las amenazas avanzadas y persistentes (APT), tales como los ataques sufridos por la red eléctrica ucraniana. Gracias a una librería inteligente de amenazas y la conciencia situacional en toda la red, la plataforma de análisis de la seguridad de macrodatos predice la tendencia de seguridad de la IoT e implementa medidas preventivas para lograr la protección activa contra amenazas.

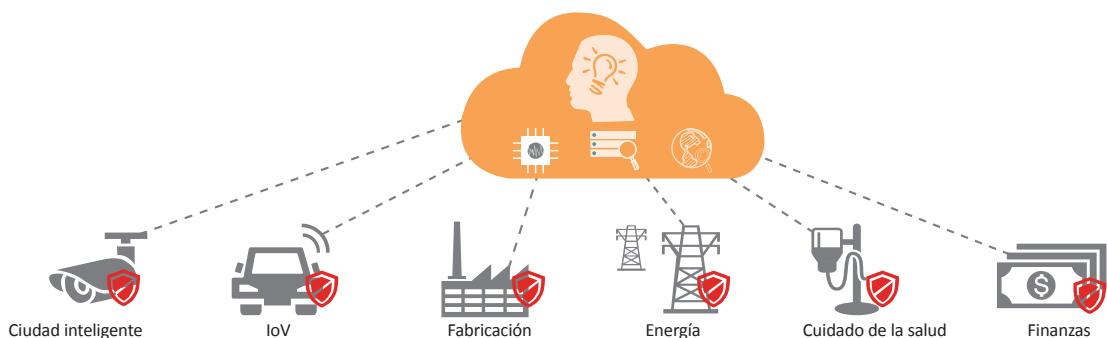


Figura 2-7 Conciencia situacional de seguridad para la sinergia entre los dispositivos y la nube

Resumen

La IoT posibilita una gran cantidad de conexiones. La seguridad no es opcional para el despliegue de la IoT; es un requisito fundamental. Los mecanismos de seguridad y protección de extremo a extremo y de múltiples capas garantizan la fiabilidad y la seguridad de las operaciones de IoT. No obstante, los problemas de seguridad de la IoT son complejos y están más relacionados con la gestión de personal, dispositivos y sistemas que con la tecnología, por lo que se requiere una solución sistemática. Están surgiendo nuevas tecnologías de IoT y con estas también surgen nuevos problemas de seguridad. Los mecanismos de seguridad y protección de extremo a extremo y de múltiples capas deben estar a la altura de las circunstancias y deben ser optimizados. En última instancia, se podrá crear un entorno operativo próspero para la IoT mediante la gestión efectiva, la protección automática y la predicción activa con la ayuda de la conciencia situacional (como se muestra en la Figura 2-8).



Figura 2-8 Seguridad y protección de la IoT



3

Prácticas de seguridad de la IoT

Los problemas de seguridad de la IoT pueden solucionarse siguiendo prácticas de seguridad conocidas de las tecnologías de la información. Esto debería llevarse a cabo durante cada etapa del proceso de despliegue, desde las etapas de investigación y diseño hasta la implementación en el mercado. También deben considerarse la evaluación de las vulnerabilidades de software y hardware, así como las mejoras de seguridad de los sistemas y las comunicaciones.

Debido al uso diversificado de los dispositivos de IoT en aplicaciones tales como entornos empresariales, vida doméstica, sistemas industriales y el sector del cuidado de la salud, deben adoptarse buenas prácticas para el uso y la configuración adecuados de los puntos terminales.

La evaluación de riesgos, el análisis de amenazas y el análisis del impacto de posibles ataques deben realizarse caso por caso para que puedan seleccionarse prácticas de seguridad adecuadas con el objetivo de lograr el mejor equilibrio entre costes, usabilidad y seguridad. Por ejemplo, un dispositivo diseñado para funcionar en el sector del cuidado de la salud debe tener en cuenta muchos más parámetros y debe aplicar prácticas de seguridad más estrictas en comparación con un reloj inteligente.

Cuando desarrollan dispositivos de IoT, los fabricantes afrontan limitaciones inherentes relacionadas con cuestiones técnicas, con el plazo de comercialización y con el coste que afectan la interoperabilidad y el diseño de los dispositivos. Algunos dispositivos están limitados por factores técnicos, como la cantidad limitada de recursos de procesamiento interno, la memoria o las exigencias de consumo de energía. Los fabricantes se ven presionados a reducir el coste unitario de los dispositivos minimizando los costes de diseño de componentes y productos. Sin embargo, también deben tener en cuenta los riesgos relacionados con los problemas de seguridad.

Prácticas de seguridad en el diseño conceptual

Como ya se ha mencionado anteriormente, es necesario prestar atención a todas las etapas posibles del ciclo de vida de despliegue de la IoT, desde el diseño y la implementación hasta el uso por parte de los clientes.

* Se debe contar con las regulaciones de mercado pertinentes y con conocimientos e investigaciones acerca de la legislación referida a la seguridad del entorno en cuestión.

* Esta etapa temprana ayudaría a determinar la viabilidad y los factores que deben considerarse en las etapas siguientes.

Prácticas de seguridad en el desarrollo tecnológico

Después de determinar las condiciones y las restricciones asociadas con el caso de uso y el entorno de operación, debe considerarse la seguridad del hardware y del software.

* Hardware

En función de las limitaciones del sector y su nivel de importancia, pueden observarse las siguientes prácticas:

Seguridad en el arranque: Adopte mecanismos para proteger el proceso de arranque y las actualizaciones fiables.

Firmware, memoria y almacenamiento: Garantice la seguridad de las actualizaciones de firmware y permita la verificación criptográfica. Verifique la posible filtración de información debido a contraseñas embebidas. Use cifrado para los medios de almacenamiento.

CPU y microcontroladores: Ante casos de uso de gran importancia, sería deseable contar con mecanismos que detecten alteraciones o ataques de ingeniería inversa para evitar la manipulación.

Acceso físico: Proteja o deshabilite interfaces tales como puertos USB y JTAG. Diseñe medidas de prevención para condiciones ambientales adversas.

Componentes de la red: Use tarjetas inalámbricas, Bluetooth o componentes RF que cumplan con las normas de seguridad vigentes.

Gestión de energía: Cuente con un mecanismo de conmutación por recuperación en caso de interrupción del suministro.

* Software

Sistema operativo: Seleccione un sistema operativo probado y aplique todas las medidas de mejoras de seguridad recomendadas para cada caso. Siga el principio del menor privilegio. Preste atención especialmente a los privilegios y permisos de los usuarios, y habilite la protección contra vulnerabilidades de seguridad para las operaciones del SO, lo que incluye la protección de ASLR, la memoria de NX y el aislamiento de procesos.



Figura 3-1 Ciclo de vida de seguridad de la IoT

Marco de trabajo de desarrollo y API: De haberlo, garantice la seguridad de su uso a través de la evaluación de vulnerabilidades y las políticas de actualización.

Actualizaciones: Cuente con una estrategia de actualizaciones para el SO y para el software, incluso en el caso de software de terceros.

Prácticas de seguridad en la funcionalidad y el despliegue

* Instalación y configuración: Cuente con un grupo de procedimientos bien diseñado para realizar la configuración y la instalación de forma segura. Obligue a los usuarios a modificar los ajustes de seguridad predeterminados, como por ejemplo la contraseña.

* Conectividad y servicios: Verifique los ajustes de red innecesarios, tales como los puertos abiertos. Establezca la obligatoriedad del cifrado en todos los tipos de comunicaciones.

* Cifrado: Seleccione una suite de cifrado probada o verifique posibles debilidades (tales como los generadores de números pseudoaleatorios) si ha de usarse cifrado de desarrollo propio.

* Cuestiones de privacidad: Garantice la protección de los datos confidenciales o privados y habilite mecanismos de destrucción de datos y almacenamiento cifrado en dispositivos y puntos terminales donde pueden guardarse tales datos.

* Autenticación y autorización: De ser necesario, adopte mecanismos seguros para interactuar y establecer conexiones con dispositivos y servicios tales como los servicios en nube.

* Copias de seguridad y recuperación ante desastres: En determinadas circunstancias, se recomienda contar con procedimientos de seguridad para garantizar las copias de seguridad y la recuperación total de los datos y del sistema operativo en caso de desastre. El almacenamiento de las copias de seguridad debe estar cifrado.

Prácticas de seguridad en las verificaciones y pruebas

Una vez creado un producto y una vez implementadas las prácticas de seguridad aplicables, el ciclo debe continuar, y se debe poner a prueba la eficacia de tales prácticas. Los puntos de control deben incluir los siguientes:

* Revisión y pruebas de hardware para detectar manipulación.

* Análisis del tráfico de la red.

* Análisis de la seguridad de las interfaces.

* Verificación de la autenticación y debilidades de los ajustes predeterminados.

* Pruebas de servicios y entradas para verificar la protección contra ataques DoS y ataques de datos aleatorios.

* Verificación de los procedimientos de copias de seguridad y recuperación en escenarios reales.

* Pruebas del mecanismo de actualización y de la verificación de integridad para el firmware y el software.

* Cumplimiento de las normas dentro de los entornos operativos.

Prácticas de seguridad para la operación y el mantenimiento de usuarios

Las medidas adoptadas en las etapas precedentes serán inútiles si quien interactúa con el dispositivo de IoT ignora las mejores prácticas de seguridad. Se deben considerar los siguientes puntos:

* Si una función o un servicio brindado en el dispositivo no se usa o no se necesita, se debe deshabilitar.

* Mantenga el dispositivo actualizado y bien configurado.

* Use contraseñas robustas y modifíquelas con regularidad.

* Si los dispositivos de IoT se deben integrar con otra infraestructura, se deben evaluar la conectividad de red y las interacciones de esta con el entorno. Posteriormente, se puede elegir una ubicación apropiada para el dispositivo. Evite las interferencias y la exposición no deseadas.

* Los dispositivos de IoT que no están en uso pueden representar un problema de seguridad por falta de control. Haga un seguimiento de dichos dispositivos y de manera alternativa borre los datos de aquellos que pasarán a desuso.

Prácticas de protección de la privacidad

¿Cómo podemos dar la bienvenida a la IoT sin sacrificar la privacidad?

La privacidad puede protegerse por medio de múltiples modos, tales como los medios tecnológicos. Sin embargo, las leyes y los reglamentos establecen un grupo mínimo y obligatorio de requisitos.

La norma principal de la Unión Europea es el Reglamento general de protección de datos (RGPD de la UE), que propone el concepto de "privacidad desde el diseño" y requiere la evaluación de impacto sobre la privacidad (EIP) para el procesamiento de datos específicos. La EIP es una herramienta útil para hacer cumplir las obligaciones relacionadas con la protección de los datos. Como se establece en el RGPD, la EIP es necesaria cuando es probable que un cierto tipo de procesamiento ocasione un alto riesgo para los derechos y las libertades de las personas físicas.

Para garantizar los derechos y las libertades individuales en la medida en

que esto sea razonablemente práctico, el Grupo de Trabajo del Artículo 29, que es la entidad consultora de la Unión Europea en cuestiones de protección de datos, brinda algunas recomendaciones, tales como las siguientes:

- * Las EIP deben realizarse con anterioridad al lanzamiento de cualquier aplicación nueva en IoT.
- * Cada parte involucrada en el mundo de la IoT debe aplicar los principios de la privacidad desde el diseño y la privacidad por defecto.
- * Muchas de las partes interesadas del mundo de la IoT solo necesitan datos agrupados, mientras que no necesitan los datos sin procesar obtenidos por los dispositivos IoT. Las partes interesadas deben borrar los datos sin procesar inmediatamente después de haber extraído los datos necesarios para el procesamiento.
- * Los fabricantes de dispositivos deben informar a los usuarios sobre los tipos de datos que los sensores obtienen y después procesan, los tipos de datos que reciben y el modo en que los datos serán procesados y combinados.
- * Los fabricantes de dispositivos deberían tener la capacidad de comunicarse con todas las partes interesadas tan pronto como el dueño de los datos revoque el consentimiento prestado o se oponga al procesamiento de dichos datos.
- * Al igual que la función "no molestar" de los smartphones, los dispositivos de IoT deberían brindar una opción de "no obtener datos" para programar o desactivar rápidamente los sensores.
- * Para evitar el rastreo de la ubicación, los fabricantes de dispositivos deberían limitar el uso de huellas digitales deshabilitando las interfaces inalámbricas cuando no estén en uso. Opcionalmente, deberían usar identificadores aleatorios (tales como direcciones MAC aleatorias para escanear redes de Wi-Fi) a fin de evitar que se use un identificador persistente para rastrear la ubicación.
- * Los usuarios tienen derecho a acceder a sus datos personales. Es necesario brindarles herramientas que les permitan exportar sus datos fácilmente en un formato estructurado común. Por lo tanto, los fabricantes de los dispositivos deberían brindar una interfaz fácil de usar para los usuarios que desean obtener datos agregados y datos sin procesar que sigan almacenados.
- * Debería existir un ajuste para diferenciar los distintos individuos que usan un mismo dispositivo, de modo que ninguno pueda obtener información sobre las actividades de los otros.
- * Los ajustes predeterminados de las aplicaciones sociales basadas en dispositivos de IoT deberían solicitar a los usuarios que revisen la información generada por sus dispositivos, que la editen y que tomen decisiones al respecto antes de la publicación en plataformas sociales.
- * Por defecto, la información publicada por dispositivos de IoT en plataformas de redes sociales no debería hacerse pública ni debería ser indexada por motores de búsqueda.
- * El permiso para usar un dispositivo conectado y para el consecuente procesamiento de datos debe ser brindado con libertad y tras haber obtenido la información correspondiente. Los usuarios no deberían ser penalizados económicamente y el acceso a las funciones de sus dispositivos no debería verse degradado si deciden no usar el dispositivo o un servicio específico.

En España, la protección de los datos es responsabilidad de la Agencia Española de Protección de Datos (AEPD), que monitoriza, a través de las partes interesadas, el cambio de las reglas del juego. Esta organización debe trabajar en cooperación con las compañías (que son quienes tienen el rol principal), pero también con los ciudadanos. Estos últimos cumplen múltiples roles: usuarios de Internet, generadores de contenidos y productores de datos; como tales, su seguridad debe ser garantizada. Para lograr este objetivo, hay lineamientos sobre la reutilización de la información en el sector público, así como para la anonimización de los datos personales. Si una empresa respeta y protege la confidencialidad de los datos, tiene más probabilidades de ganarse la confianza de sus clientes y de acrecentar su valor económico. Además, su credibilidad dentro del mercado y su valor económico en general están directamente relacionados. Teniendo esto en cuenta, es necesario afianzar la recuperación de los derechos olvidados y el llamado de atención sobre la seguridad legal de las empresas en Internet. El desarrollo de las herramientas necesarias para la normativa nueva que entrará en vigencia en 2018 también debe incentivarse. Para tal fin, el trabajo realizado por la SETSI (actualmente la SESIAD), la AEPS y las fuerzas de seguridad nacional en el próximo año tendrá una importancia crucial y fundamental.

La IoT puede aplicarse en múltiples escenarios. El presente libro blanco se limita a seleccionar y analizar algunas prácticas exitosas de su aplicación en soluciones de ciudad inteligente, hogar inteligente, red eléctrica inteligente e Internet de ascensores como referencia para las industrias verticales relacionadas con la IoT, que experimentan un rápido crecimiento. El desarrollo veloz de tecnologías nuevas de IoT siempre planteará amenazas y problemas nuevos para la seguridad. Por lo tanto, la seguridad de la IoT debe seguir evolucionando.



Casos típicos de seguridad de IoT

4

Tras años de desarrollo y exploración, el Internet de las Cosas está siendo comercializado de forma gradual. Sus usos incluyen las soluciones de ciudad inteligente y logística inteligente, y se aplicará ampliamente en áreas tales como los hogares inteligentes, los wearables, el Internet de los Vehículos y los ascensores inteligentes. El Internet de las Cosas conectará más cosas en múltiples dominios dentro de un periodo corto de tiempo y facilitará sustancialmente el desarrollo económico y la vida cotidiana. Sin embargo, no todo es de color rosa. La seguridad de las grandes redes de IoT y de los volúmenes de datos transmitidos en ellas es una preocupación importante. Cuando hay pérdidas de información o cuando los sistemas se dañan o son controlados maliciosamente, ocurren grandes pérdidas. Por lo tanto, la seguridad es un aspecto fundamental.

La infraestructura crucial del Internet industrial ya se ha convertido en un blanco para los ciberataques. Cuando la infraestructura fundamental sufre ataques y se paralizan las redes, la seguridad nacional y la estabilidad social se ven gravemente afectadas, y los daños ocasionados son invaluables. Además, hay organizaciones de piratas informáticos e incluso estados que se han unido a las filas de los atacantes con medios de agresión cada vez más profesionales, sofisticados y bien estructurados.

El lanzamiento de los vehículos Tesla y la madurez de los sistemas de vehículos inteligentes desarrollados por gigantes de Internet, tales como Apple y Google, indican que el concepto de Internet de los Vehículos se está volviendo realidad. Sin embargo, si se vulnera la seguridad de un auto inteligente, es posible que extorsionen al propietario y que se produzcan accidentes de tránsito graves, lo que pone en riesgo la vida de las personas.

Ciudad inteligente

El rápido desarrollo de las tecnologías de la información y la comunicación está cambiando la vida de las personas, así como la operación y la gestión de las ciudades. La ciudad inteligente es un concepto nuevo que se basa en dicho desarrollo. Este tipo de ciudades se está construyendo en muchos países, como China, Singapur y Tailandia. La IoT permite que las ciudades inteligentes construyan una gran red neural. La cámara IP, como elemento de red neural de la ciudad inteligente, se despliega en condiciones complejas y diversas. Consecuentemente, las cámaras IP son difíciles de gestionar pero fáciles de atacar (como se muestra en la Figura 4-2). Un ataque a las cámaras IP puede tener consecuencias graves, debido a la gran cantidad de estos dispositivos. Las amenazas a la seguridad de las cámaras IP deben analizarse para poder desarrollar medidas apropiadas de protección de la IoT (como se muestra en la Tabla 4-1) y para poder aplicar dichas medidas a la videovigilancia de manera generalizada.

Hogares inteligentes

Los hogares inteligentes adoptan tecnologías de IoT para brindar servicios hogareños, tales como el control, las comunicaciones y las compras del hogar. AT&T, Telefónica, Vodafone, Deutsche Telekom,

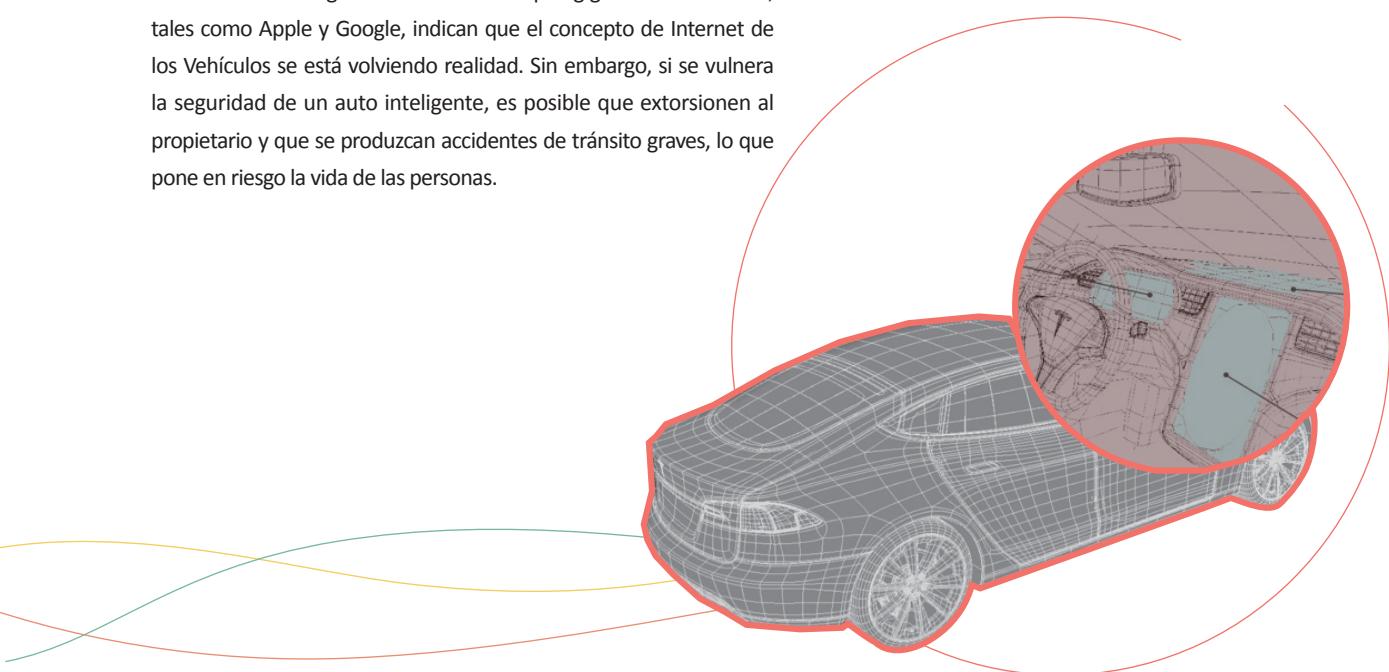


Figura 4-1 Internet de los Vehículos (IoV)

Amenaza típica de seguridad	Contramedida
Falsificación por parte de cámaras IP maliciosas	Verificación única de certificados de dispositivos. Gestión del ciclo de vida de los dispositivos.
Interceptación de información y adulteración de contenidos de vídeo, e interceptación de datos locales	Cifrado de señales y datos en túneles desseguridad. Espacios aislados para evitar la vulnerabilidad de los datos. Línea de base de amenazas basada en macrodatos.
Ataques indirectos (stepping stone)	Gestión de puertos de dispositivos. Aislamiento de la red. Línea de base de amenazas basada en macrodatos.
Contraseñas débiles, vulnerabilidades e intrusiones	Autoverificación mediante complementos de seguridad.

Table 4-1

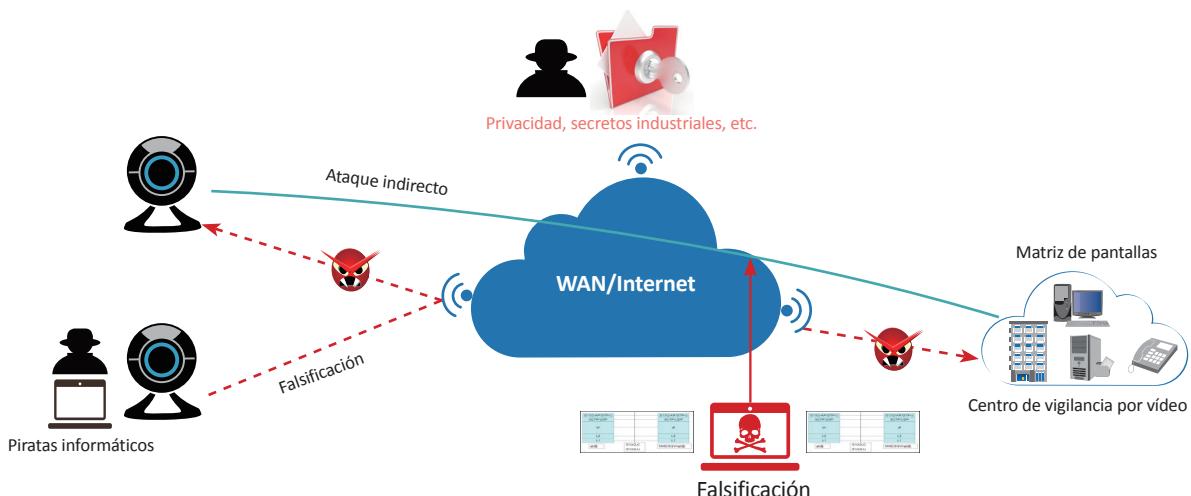


Figura 4-2 Ataque a una red de cámaras IP

China Mobile, China Telecom y China Unicom son tan solo algunos ejemplos de las empresas más grandes de la industria que están desarrollando servicios de hogar inteligente, como los de salud, entretenimiento, energía y seguridad del hogar (como se muestra en la Figura 4-3).

Las soluciones de hogar inteligente requieren mecanismos de protección de extremo a extremo y múltiples capas para garantizar la seguridad:

* Seguridad de dispositivos y sensores: Adopte canales de comunicación cifrada que usen claves compartidas por medio de protocolos de comunicación de rango corto, tales como ZigBee y Z-Wave, para garantizar conexiones seguras entre los puntos terminales y los gateways, lo que permite garantizar la seguridad de

sensores y dispositivos.

* Instale chips TPM en los gateways para implementar el arranque seguro y verificar la integridad del software y del firmware. El estado de fiabilidad de todos los dispositivos de gateway se informa a la nube y se visualiza.

* La plataforma en nube brinda capacidades de análisis de seguridad basadas en tecnologías de macrodatos y aprendizaje de máquinas, y obtiene registros, eventos e información de tráfico para analizar anomalías en los dispositivos de IoT, en el comportamiento de los usuarios de los puntos terminales y en el estado de la plataforma en nube. También puede identificar y controlar los riesgos de ataques intrusivos en los puntos terminales y la plataforma en nube.

Red eléctrica inteligente

Muchos países y muchas organizaciones desean tener una red eléctrica inteligente que sea flexible, prolífica, segura, eficiente, económica y fácil de usar. Consecuentemente, desarrollan planes de energía eléctrica y mejoran sus infraestructuras para lograr ese objetivo. En la red eléctrica inteligente se destacan cuatro módulos:



Figura 4-3 Seguridad del hogar inteligente

la infraestructura de medición avanzada (AMI), las operaciones de distribución avanzada (ADO), las operaciones de transmisión avanzada (ATO) y la gestión avanzada de activos (AAM). El sistema global de medición eléctrica está evolucionando hacia la AMI, que es la clave para una red eléctrica inteligente. En la era de la IoT, la medición precisa será crucial para el suministro eléctrico, lo que convierte al medidor inteligente en la médula de la AMI. Para el año 2020, se espera que los medidores inteligentes tengan una penetración de mercado del 59 % en todo el mundo.

Millones de medidores inteligentes permiten que las empresas de electricidad realicen mediciones inteligentes, analicen las pérdidas de línea, analicen el consumo eléctrico y cuenten con funciones de electricidad en modo prepago. Sin embargo, ataques tales como la adulteración o la falsificación de los medidores inteligentes puede tener como resultado el consumo eléctrico no registrado y los cortes de gran escala. Esto puede ocasionar pérdidas económicas,

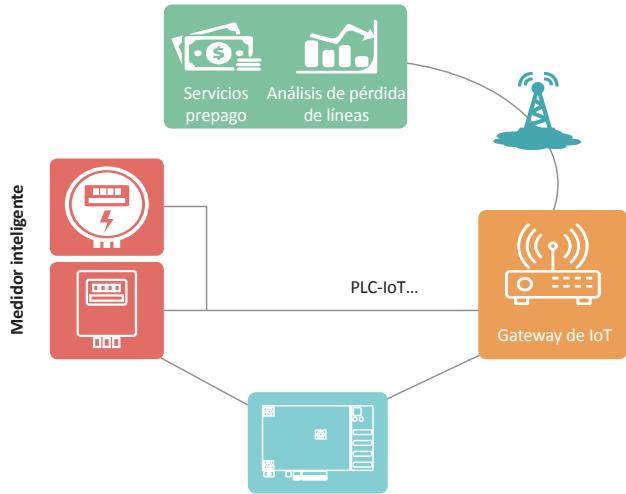


Figura 4-4 Medición inteligente

o incluso incidentes de seguridad. Los medidores inteligentes pueden convertirse en un arma muy peligrosa para atacar a la red eléctrica inteligente. Por lo tanto, es necesario prestar atención a las cuestiones de la seguridad. Los desafíos más grandes para la seguridad de la red eléctrica inteligente consisten en cómo garantizar el acceso fiable de los medidores inteligentes y cómo proteger eficazmente a las infraestructuras esenciales.

Generalmente, los medidores se instalan en exteriores y están expuestos a los riesgos de adulteración y falsificación de datos. Por lo tanto, deben tener un diseño que evite el hurto de electricidad y los accesos no autorizados mediante la autenticación eficaz de la identidad. Para la localización precisa de un hurto, las anomalías deben informarse de forma automática. Los datos de los medidores deben cifrarse para que puedan ser informados sin interceptaciones ni filtraciones. Además, la red eléctrica debe proteger a los servicios contra amenazas avanzadas persistentes, ataques DDoS, virus y otras amenazas.

Para lograr este objetivo, los proveedores de soluciones deben ser capaces de brindar soluciones de extremo a extremo y deben poder hacer entregas donde la seguridad sea un componente esencial, además de interactuar efectivamente con los usuarios para mejorar la experiencia del cliente y la calidad del suministro eléctrico, reducir las emisiones de carbono y mejorar la eficacia operativa de las empresas a un menor coste.

Internet de Ascensores

En todo el mundo, hay más de 15 millones de ascensores en uso, y dicha cantidad no cesa de aumentar. En los últimos años, se ha

asociado una cierta cantidad de accidentes con el uso de ascensores. Consecuentemente, hay una gran demanda de servicios de operación y mantenimiento (O&M) en el mercado de los ascensores.

El despliegue del Internet de Ascensores (IoE) permite controlar los ascensores por medio de la nube. Sin embargo, los problemas de seguridad pueden ocasionar la pérdida del control de los ascensores o la filtración de datos esenciales, como la ubicación de los ascensores. Para garantizar la seguridad de la IoE en su totalidad, se necesitan mecanismos de seguridad de múltiples capas que brinden seguridad para la transmisión de datos y el servicio de O&M desde varios puntos de vista (como se muestra en la Figura 4-5):

- * Chip: La información de autenticación o los paquetes de software de sensores, gateways y otros dispositivos deben ser protegidos contra la adulteración mediante la tecnología TPM.
- * Sistema operativo: Se deberían desplegar módulos de seguridad para el software subyacente a fin de garantizar la seguridad del sistema operativo y del entorno de ejecución.
- * Red: Todos los canales que conectan los ascensores a la nube deben estar cifrados para garantizar la seguridad de los datos en tránsito.
- * Plataforma en nube: Se brindan soluciones a medida para la protección de la seguridad de la plataforma en nube, lo que incluye soluciones de seguridad de aplicaciones, soluciones contra amenazas avanzadas y persistentes, soluciones de seguridad de fronteras en la nube, soluciones de seguridad de fronteras lógicas y soluciones contra DDoS.

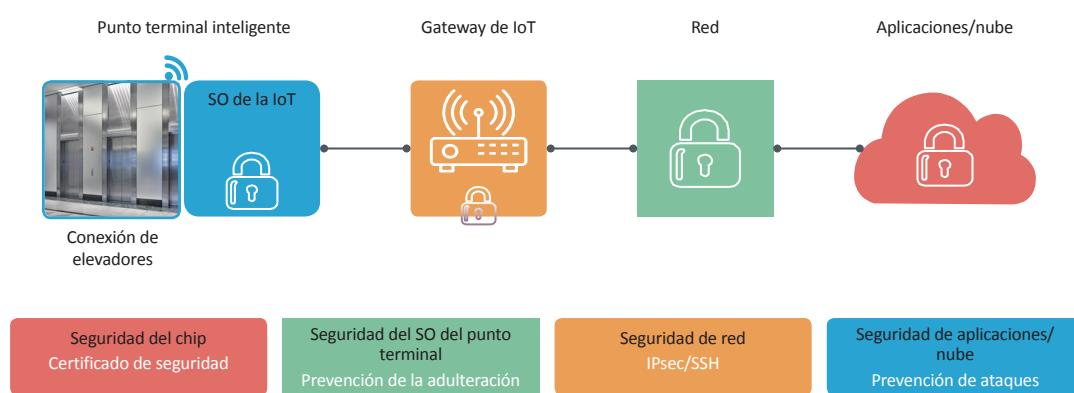
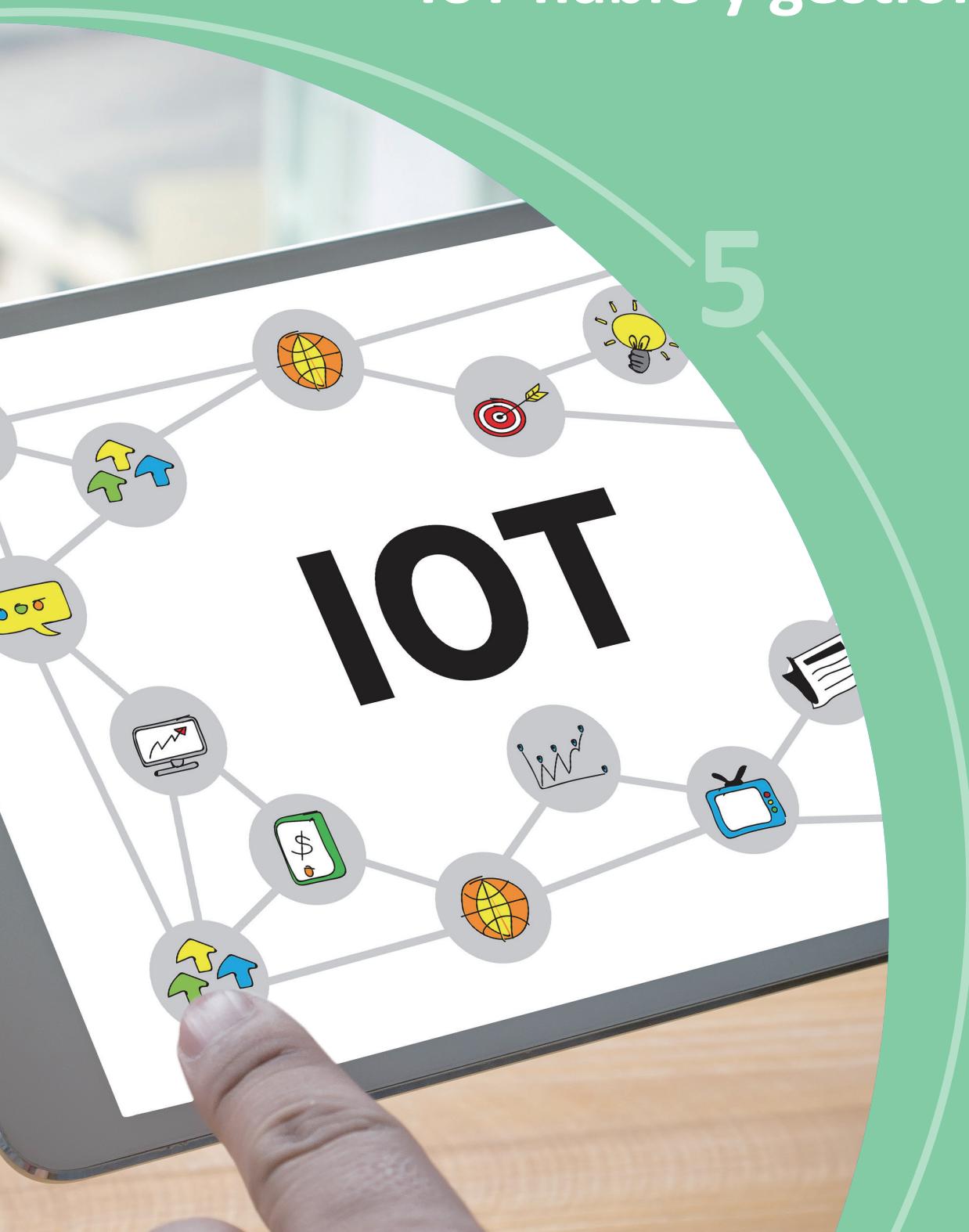


Figura 4-5 Seguridad de la Internet de Elevadores

Hacia la creación de un mundo IoT fiable y gestionado



Fomento de la industria y del gobierno

El crecimiento de la IoT ha captado el interés de una cierta cantidad de países importantes, los cuales han comenzado a desarrollar estrategias nacionales de IoT. En julio de 2016, el Instituto Nacional de Ciberseguridad de España (INCIBE) publicó las Tendencias en el mercado de la ciberseguridad para fomentar un mayor desarrollo de las capacidades de seguridad de IoT. En noviembre de 2016, el Departamento de Seguridad Nacional de los Estados Unidos publicó los Principios estratégicos para la seguridad del Internet de las Cosas, que se usan como principios orientadores para la seguridad de la IoT. El programa europeo Horizonte 2020 establece diversos temas interrelacionados, tales como la combinación de la ciberseguridad y la IoT, así como el desarrollo de sociedades seguras, lo que permite proteger la libertad y la seguridad de Europa y de sus ciudadanos. La Alianza de Internet Industrial (AII) de China establece un equipo de seguridad de IoT para mejorar los estándares y otros aspectos de la IoT.

La IoT está dando impulso a una nueva revolución industrial. Sin embargo, en muchas industrias, las necesidades de seguridad son diversas, las soluciones de seguridad no son integrales ni maduras, y los métodos de evaluación de riesgos de seguridad no son claros, como tampoco lo son las medidas tomadas contra dichos riesgos. No alcanza con que una o varias industrias orienten la seguridad de IoT, sino que se necesita un coordinador de nivel superior para orquestar a todas las industrias involucradas. Por lo tanto, los gobiernos y las organizaciones industriales deben priorizar la seguridad de la IoT como estrategia nacional y deben prestar más atención al desarrollo de políticas de seguridad, leyes, normas y estándares pertinentes para construir la IoT de manera conjunta.

Desarrollo más rápido de los estándares de seguridad de la IoT

Los estándares tienen un rol crucial en el desarrollo y la evolución de las tecnologías. Los productos y las soluciones dependen de los estándares aplicables o cumplen con ellos. De manera similar, los estándares tienen una importancia creciente para la IoT, ya que esta última combina múltiples tipos de tecnologías, desde las tecnologías de acceso subyacentes hasta las aplicaciones de capa superior en diversas industrias. Consecuentemente, la seguridad de la IoT se está convirtiendo en una inquietud importante para las organizaciones de estandarización.

En la actualidad, muchas organizaciones y alianzas de estandarización trabajan activamente para proponer y diseñar estándares de tecnologías de seguridad con el objetivo de afrontar los desafíos de la seguridad de la IoT y así lograr un ecosistema más inteligente y totalmente conectado.



Organización	Documento	Aporte a la seguridad de IoT
Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST)	Ingeniería en seguridad de sistemas	Publicó Ingeniería en seguridad de sistemas en noviembre de 2016; este documento brinda un grupo de pautas de ciberseguridad para la IoT con el objetivo de gestionar los procesos del ciclo de vida de los dispositivos conectados y proteger las necesidades de las partes interesadas.
Consortio Industrial de Internet (IIC)	Internet industrial de las cosas, volumen G4: Marco de seguridad	Publicó IoT industrial: Marco de seguridad en septiembre de 2016 con la expectativa de crear un consenso industrial generalizado sobre cómo brindar seguridad a los sistemas de IoT industrial (IIoT). Este documento apunta a garantizar que la seguridad se convierta en un elemento básico de la arquitectura de los sistemas de IIoT, y que la totalidad del sistema de IIoT sea seguro, incluso los puntos terminales y las conexiones entre componentes de sistemas.
Grupo de Tareas Especiales de Ingeniería en Internet (IETF)	RFC 7744: Casos de uso para la autenticación y la autorización en entornos restringidos; RFC 7925: Seguridad de la capa de transporte (TLS) / Perfiles de seguridad para la capa de transporte de datagramas (DTLS) para Internet de las Cosas, entre otros documentos	Realizó aportes a los protocolos de seguridad de las capas de aplicaciones, de transporte y de red, y a los protocolos de autorización y autenticación de terceros. El uso de estos protocolos es generalizado. Considerando que los dispositivos de IoT pueden verse restringidos en términos de procesamiento, memoria, tamaño de código, energía, etc., el IETF ha creado grupos de trabajo (ACE, DICE, T2TRG y CORE) para trabajar en los protocolos aplicables.
Asociación GSM (GSMA)	Pautas de seguridad de IoT	Se centra en la industria de las telecomunicaciones y ha creado un grupo de pautas de seguridad para beneficio de los operadores que pretendan desarrollar servicios de IoT. Apunta a contribuir con la creación de un consenso sobre seguridad de IoT en la industria de IoT para garantizar que se implementen las mejores prácticas a lo largo del ciclo de vida de los servicios de IoT.
oneM2M	Soluciones de seguridad oneM2M (TS-0003)	Se centra en el desarrollo de estándares de la capa de aplicaciones para la gestión de la IoT y las plataformas de habilitación de aplicaciones. Abarca requisitos, arquitecturas, especificaciones de API, soluciones de seguridad e interoperabilidad. oneM2M planea lanzar un TEE y espera que todas las partes interesadas sean capaces de gestionar y controlar sus credenciales privadas y sus políticas de seguridad de manera independiente, mediante el almacenamiento aislado y los recursos de ejecución de los nodos.
Grupo de IoT del Trusted Computing Group (TCG)	Pautas para la protección de la IoT mediante la tecnología del TCG; Guía de arquitectura: Seguridad de IoT	Para acelerar la consolidación de la seguridad de IoT, el TCG ha creado el subgrupo de IoT con el objetivo de brindar pautas sobre la aplicación de la informática fiable a la IoT. El TCG ha propuesto una serie de guías sobre políticas de seguridad y actualmente está ultimando los estándares para que se adapten mejor a las necesidades de la IoT.

Tabla 5-1 Ejemplos de aportes realizados por alianzas y organizaciones de estandarización para la seguridad de la IoT

El desarrollo de los estándares de seguridad de la IoT sigue en pañales y tiene el enfoque puesto en las pautas y los marcos de trabajo. Son pocos los estándares técnicos detallados que pueden orientar la implementación en las industrias. Por lo tanto, es urgente que las alianzas y organizaciones de estandarización aceleren el desarrollo de los estándares de seguridad pertinentes para impulsar el crecimiento veloz de la industria de la IoT.

Participación activa en el ecosistema industrial de la seguridad de IoT

La industria de la IoT, que está sumamente integrada, se está desarrollando rápidamente con necesidades diversas y amenazas crecientes. Es difícil que una sola empresa pueda satisfacer los requisitos de la IoT. Resulta necesario construir un ecosistema colaborativo y abierto de seguridad para lograr un desarrollo que beneficie a todas las partes involucradas. Las industrias, los desarrolladores, las academias y las organizaciones de estándares industriales deben trabajar estrechamente para fomentar la innovación en los negocios, la ciencia y la tecnología, y deben construir de forma conjunta un ecosistema seguro para lograr cooperación, competencia leal y desarrollos que beneficien a todas las partes involucradas.

Los ataques a la seguridad de la IoT y la protección de esta última están desequilibrados; normalmente, la protección no está a la altura de los ataques. Desde el punto de vista de la economía o el retorno de la inversión, los atacantes tienen un objetivo claro de inversión, mientras que los defensores invierten en protección de seguridad para el control de riesgos; es decir, apuntan a que los ataques no ocurran bajo ningún punto de vista. Los atacantes sofisticados pueden orientar sus ataques con enfoques específicos, mientras que los defensores deben brindar protección contra muchas incertidumbres. Por otro lado, los defensores construyen un sólido sistema de protección en un ciberespacio donde coexisten diversos productos y servicios de

seguridad. Sin embargo, los ataques a la seguridad son cada vez peores, y los ciberataques causan daños crecientes debido al uso masivo de las tecnologías de información en la era de la IoT.

Para ganar esta batalla desigual, las industrias deben seguir los preceptos de apertura, justicia y cooperación para beneficio de todas las partes involucradas. Deben construir un ecosistema de seguridad sólido para las tecnologías, los productos, las soluciones y los servicios de seguridad, a través de canales como los lineamientos de políticas, la estandarización, las comunidades de desarrolladores, las comunidades de código abierto y las alianzas industriales. Esto posibilitará la construcción de una red de protección para la IoT (como se muestra en la Tabla 5-1).

Ninguna empresa y ninguna organización pueden resolver los problemas de seguridad de IoT por sí misma. Todos los integrantes del ecosistema deben cooperar y apoyarse entre sí. Todos los proveedores de dispositivos, las empresas de consultoría, los proveedores de software de aplicaciones, los integradores de sistemas y los socios de canales deben adoptar con apertura la cooperación beneficiosa para todas las partes involucradas con el objetivo de construir de manera conjunta un ecosistema de seguridad sólido y fiable para la IoT, y deben fomentar el desarrollo sólido y rápido de la industria de la IoT.

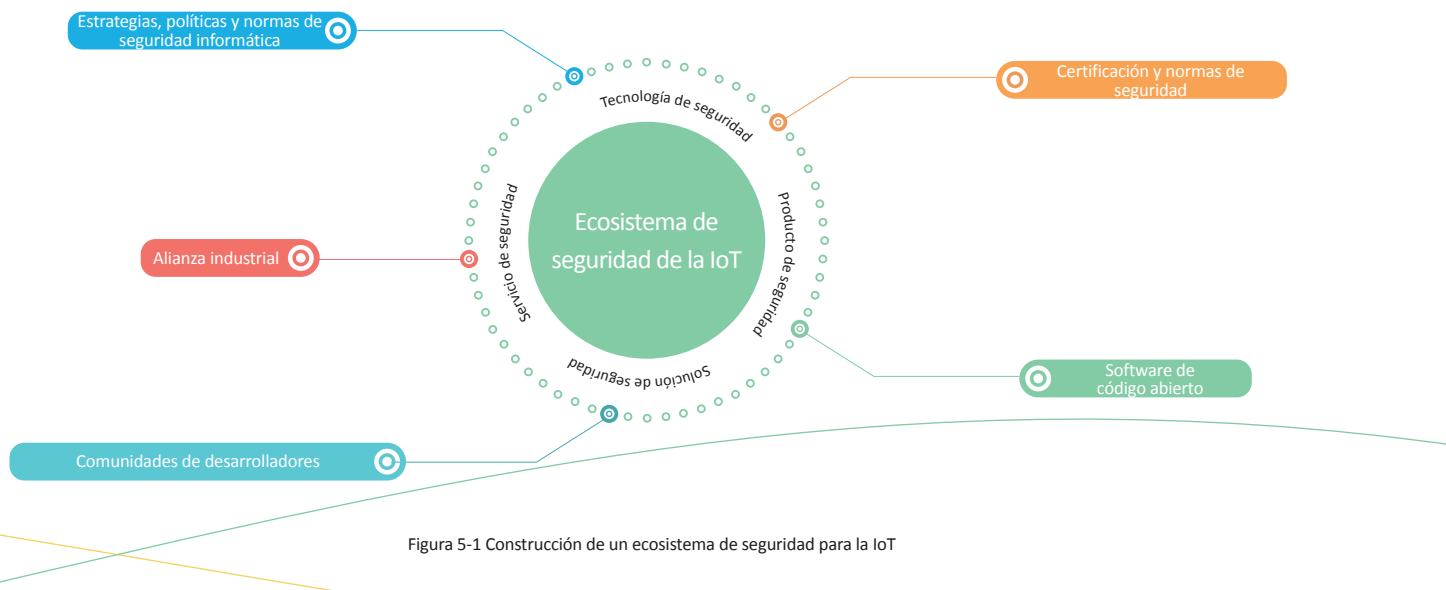


Figura 5-1 Construcción de un ecosistema de seguridad para la IoT



Resumen

6

La seguridad de la IoT involucra cada aspecto del ámbito digital, y las empresas de consultoría, las compañías y los operadores tienen altas expectativas de mercado en este sentido. Si bien la IoT ofrece muchos beneficios, también acarrea muchas amenazas. Desafortunadamente, aunque los problemas de seguridad son significativos, sigue siendo necesario concienciar al público acerca del tema. Hay una gran brecha entre la realidad y lo ideal. En el futuro, la IoT será estandarizada, simplificada y fácil de usar. Debemos abrirnos a la cooperación y la innovación desde una perspectiva global para construir de manera conjunta un mundo IoT seguro, de extremo a extremo y de múltiples capas, y debemos contribuir con el desarrollo de ideologías, teorías y arquitecturas. Sin embargo, esto llevará tiempo. Debemos aprovechar la oportunidad y trabajar juntos para acelerar el proceso.

Para lograr el ideal, la seguridad es fundamental. Para fomentar el despliegue a gran escala de la IoT, el público debe concienciarse; los gobiernos y las organizaciones internacionales deben mejorar las leyes, los reglamentos y el sistema de estándares correspondientes; además, se debe conformar un ecosistema sólido para construir un mundo fiable, bien gestionado y seguro con la IoT.

Este es el mejor momento. Un mundo IoT seguro, fiable y gestionado que sea construido y compartido por todos es el deseo de las industrias de IoT de todo el mundo, y nos beneficiará a todos.

Abreviaturas y acrónimos

API: Interfaz de plataforma de aplicaciones (Application Platform Interface)

APT: Amenaza avanzada y persistente (Advanced Persistent Threat)

CoAP: Protocolo de aplicación restringida (Constrained Application Protocol)

DDoS: Denegación de servicio distribuido (Distributed Denial of Service)

GPRS: Servicio general de radio por paquetes (General Packet Radio Service)

ICS: Sistemas de control industrial (Industrial Control Systems)

LTE: Evolución a largo plazo (Long Term Evolution)

MMU: Unidad de gestión de memoria (Memory Management Unit)

MPU: Unidad de protección de memoria (Memory Protection Unit)

MQTT: Transporte de telemetría de colas de mensajes (Message Queuing Telemetry Transport)

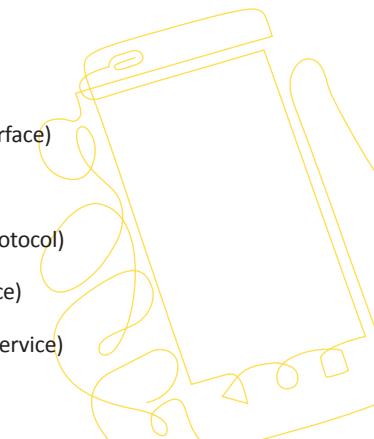
NB-IoT: Internet de las cosas de banda angosta (Narrow Band Internet of Things)

PLC: Comunicaciones por línea de alimentación eléctrica (Power Line Communication)

SCADA: Adquisición de datos y control de supervisión (Supervisory Control and Data Acquisition)

TEE: Entorno de ejecución fiable (Trusted Execution Environment)

TPM: Módulo de plataforma fiable (Trusted Platform Module)



Acerca de INCIBE, Red.es y Huawei

INCIBE

INCIBE: El Instituto Nacional de Ciberseguridad de España, S.A. es una organización que depende del Ministerio de Energía, Turismo y Agenda Digital español. Es la institución de referencia en relación con el desarrollo de la seguridad informática y la confianza digital para el público en general, para Red.es (la red española académica y de investigación) y para las empresas, especialmente los sectores de importancia estratégica.

Como centro de excelencia, INCIBE es un servicio que ofrece el gobierno español para trabajar en pos del desarrollo de la seguridad informática como instrumento de la transformación social y del desarrollo de nuevos campos de innovación. Con este fin, y con sus actividades centradas en la investigación, la prestación de servicios y la colaboración con los actores pertinentes, INCIBE dirige una serie de iniciativas de seguridad informática tanto a nivel nacional como a nivel internacional.

El CERT de Seguridad e Industria (CERTSI) es el equipo de respuesta ante emergencias de seguridad informática operado por INCIBE; se encarga de mejorar la detección y las alertas tempranas de amenazas nuevas, de dar respuesta ante incidentes de seguridad, de realizar el análisis de información respectiva y de diseñar de medidas preventivas para satisfacer las necesidades de la sociedad en general. En virtud de un acuerdo de trabajo conjunto firmado por la Secretaría de Estado de Seguridad española, INCIBE brinda servicios públicos para satisfacer las necesidades de seguridad de infraestructuras cruciales y para dar apoyo en la investigación de los delitos informáticos.

Red.es

Red.es es una entidad pública empresarial adscrita al Ministerio de Energía, Turismo y Agenda Digital (MINETAD), que desarrolla un extenso conjunto de programas para que la sociedad española se beneficie al máximo de las posibilidades que ofrecen las Tecnologías de la Información y la Comunicación (TIC). Nuestros objetivos prioritarios son generar empleo y fomentar el emprendimiento, aumentar la productividad y competitividad de las empresas españolas e incrementar el ahorro y la eficiencia en el gasto público. Al mismo tiempo, nuestro grado de conocimiento y de especialización nos permite contribuir al establecimiento de las prioridades y actuaciones de la Agenda Digital para España, que lidera la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD), en coordinación con toda la administración pública y el sector privado.

Huawei

Huawei es una compañía internacional líder en el suministro de soluciones de tecnologías de la información y la comunicación (TIC). Impulsados por las operaciones responsables, la innovación constante y la colaboración abierta, hemos creado una cartera competitiva de TIC con soluciones de extremo a extremo para redes, dispositivos y computación en nube de las telecomunicaciones y las empresas. Las soluciones, los productos y los servicios de TIC que ofrecemos se usan en más de 170 países y regiones, y dan servicios a más de un tercio de la población mundial. Contamos con más de 170.000 empleados y tenemos el compromiso de construir la sociedad informática del futuro y un mundo mejor conectado.



Copyright © 2017 Instituto Nacional de Ciberseguridad de EspaÑas, S.A. (INCIBE), Entidad Pùblica Empresarial Red.es, Huawei Technologies Co., Ltd. Todos los derechos reservados.

A los efectos del art. 32 del Real Decreto Legislativo 1/1996 de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, el Instituto Nacional de Ciberseguridad de EspaÑas, S.A. (INCIBE), Entidad Pùblica Empresarial Red.es (Red.es), Huawei Technologies Co. Ltd. (Huawei) son coautores de la presente obra en colaboraciòn. INCIBE, Red.es y Huawei se oponen expresamente a cualquier utilizaciòn fines comerciales del contenido de esta publicaciòn sin su expresa autorizaciòn, lo cual incluye expresamente cualquier reproducciòn, modifiaciòn, adaptaciòn, registro, copia, explotaciòn, distribuciòn, comunicaciòn, transmisiòn, envío, reutilizaciòn, publicaciòn, tratamiento o cualquier otra utilizaciòn total o parcial en cualquier modo, medio o formato de esta obra.

Se advierte que se trata de un documento de trabajo que puede contener errores, INCIBE, Red.es y Huawei no se hacen responsables de la adecuaciòn, exactitud de la informaciòn y/o contenidos recogidos en la misma. Esta obra podrà ser objeto de revisiòn, correcciòn o cambio sin aviso alguno. INCIBE, Red.es y Huawei no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna informaciòn contenida en esta publicaciòn, sin una consulta profesional previa. INCIBE, Red.es y Huawei se reservan los derechos de lo pactado entre los coautores de la obra en colaboraciòn, pudiendo éstos coautores explotar separadamente sus aportaciones, salvo que causen perjuicio a la explotaciòn comùn.

INCIBE  , Red.es  , HUAWEI  y  son marcas comerciales o registradas de Huawei Technologies Co., Ltd.

Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.