Informe interinstitucional o interno 8259A del NIST

Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8259Aes

National Institute of
Standards and Technology
U.S. Department of Commerce

Informe interinstitucional o interno 8259A del NIST

Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT

Michael Fagan
Katerina N. Megas
División de ciberseguridad aplicada
Laboratorio de tecnología de la información

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Matthew Smith
Huntington Ingalls Industries
Annapolis Junction, Maryland

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8259Aes

Mayo de 2020

Departamento de Comercio de los EE. UU.
Wilbur L. Ross, Jr., secretario

Instituto Nacional de Normas y Tecnología
Walter Copan, director del NIST y subsecretario de Normas y Tecnología del Departamento de Comercio

Informe interinstitucional o interno 8259A del Instituto Nacional de Normas y Tecnología
24 páginas (Mayo de 2020)

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8259Aes

Los comentarios sobre esta publicación se pueden enviar al:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Correo electrónico: iotsecurity@nist.gov

Disclaimer

Informes sobre la tecnología de los sistemas informáticos

El Laboratorio de tecnología de la información (ITL, por sus siglas en inglés) del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) promueve la economía y el bienestar público de los Estados Unidos brindando liderazgo técnico a la infraestructura de medición y estándares del país. El ITL establece pruebas, métodos de prueba, datos de referencia, implementaciones de pruebas de concepto y análisis técnicos para fomentar el desarrollo y uso productivo de la tecnología de la información. Las responsabilidades del ITL incluyen la formulación de normas y directrices de gestión, administrativas, técnicas y físicas para la seguridad y la privacidad rentables de la información en los sistemas federales de información que no sea sobre seguridad nacional.

Resumen

Las capacidades de ciberseguridad de dispositivo son características o funciones de ciberseguridad que los dispositivos informáticos proporcionan por sus propios medios técnicos (es decir, el hardware y el software del dispositivo). Esta publicación define una referencia básica de las capacidades de ciberseguridad de los dispositivos de internet de las cosas (IoT), es decir, un conjunto de capacidades de los dispositivos necesarias para reforzar los controles comunes de ciberseguridad que protegen a los dispositivos, así como a los datos de los dispositivos, los sistemas y los ecosistemas de una organización. El objetivo de esta publicación es ofrecer a las organizaciones un punto de partida que puedan usar para identificar las capacidades de ciberseguridad de los dispositivos de IoT nuevos que fabricarán, integrarán o adquirirán. Esta publicación se puede usar junto con el Informe interinstitucional o interno 8259 del NIST: *Actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de IoT*.

Palabras clave

Referencia de ciberseguridad, internet de las cosas (IoT) y dispositivos informáticos protegibles.

Agradecimientos

Los autores agradecen a todos los colaboradores de esta publicación, a los participantes en los talleres y otras sesiones interactivas, a las personas y organizaciones de los sectores público y privado, incluidos los fabricantes de diversos sectores y algunas organizaciones de comercio de fabricantes, quienes contribuyeron con sus comentarios acerca del ensayo preliminar y los borradores para comentarios públicos, así como a sus colegas del NIST por la valiosa información y retroalimentación que brindaron. Reconocen de forma especial al equipo del Programa de ciberseguridad para IoT (Barbara Cuthill y Jeff Marron) y al equipo del Proyecto de aplicación de la Ley federal de administración de la seguridad de los sistemas de información (FISMA, por sus siglas en inglés) del NIST por su gran ayuda con la corrección de las copias.

Público

Esta publicación se dirige mayormente a los fabricantes de dispositivos de IoT. Asimismo, puede ser de utilidad para los clientes o integradores de dispositivos de IoT.

Índice

Aviso de divulgación de patentes

AVISO: El ITL solicitó que los titulares de reivindicaciones de patentes, cuyo uso pueda ser obligatorio para cumplir con la orientación o los requisitos de esta publicación, divulguen esas reivindicaciones al ITL. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de patentes del ITL, y el ITL no ha emprendido ninguna búsqueda de patentes para determinar aquellas que, de haberlas, se puedan aplicar a esta publicación.

A la fecha de la publicación, y después de las solicitudes para determinar las reivindicaciones de patentes cuyo uso pueda ser obligatorio para el cumplimiento con la orientación o los requisitos de esta publicación, no se ha divulgado al ITL ninguna reivindicación de patentes.

El ITL no sugiere ni formula ninguna declaración acerca de que las licencias no son obligatorias para evitar la infracción de patentes en el uso de esta publicación.

1 Introducción

Actualmente se diseñan, fabrican e implementan a un ritmo cada vez más rápido dispositivos informáticos que integran capacidades físicas o de detección y de interfaz de red. Estos dispositivos satisfacen las necesidades de los clientes en todos los sectores de la economía. Muchos de estos dispositivos informáticos se conectan a internet, y una de sus características novedosas es que combinan la conectividad y la capacidad para detectar o afectar el mundo físico. A medida que los dispositivos se vuelven más pequeños y complejos, con un número creciente de funciones, la seguridad de esos dispositivos también se hace más complicada. Esta publicación define un conjunto básico de capacidades de ciberseguridad de dispositivo que las organizaciones deben considerar cuando afrontan las exigencias de la internet de las cosas (IoT).

Las *capacidades de ciberseguridad de dispositivo* son características o funciones de ciberseguridad que los dispositivos informáticos proporcionan por sus propios medios técnicos (es decir, el hardware y el software del dispositivo). La referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT (*referencia básica*)[1] que se define en esta publicación es un conjunto de capacidades de los dispositivos necesarias para reforzar los controles comunes de ciberseguridad que protegen a los dispositivos, así como a sus datos, sistemas y ecosistemas. En cualquier contexto, es necesario considerar con atención el concepto de una referencia, y las capacidades de seguridad de los dispositivos de IoT no son la excepción.

La referencia básica se deriva de investigar los métodos comunes de gestión de riesgos a la ciberseguridad y las capacidades que se usan comúnmente para considerar los riesgos a la ciberseguridad de los dispositivos de IoT. Estos métodos y capacidades fueron refinados y validados mediante un proceso de colaboración público y privado para incorporar todos los puntos de vista. Se hicieron varias solicitudes de comentarios, y se llevaron a cabo muchos talleres y mesas redondas. El NIST tiene el compromiso de mantener un proceso abierto y transparente que facilite los comentarios de las partes interesadas y el mejoramiento iterativo.

Estas capacidades se establecieron en el contexto del Informe interinstitucional o interno 8259 del NIST, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [Actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de IoT] [2], el cual analiza consideraciones que ayudan a los fabricantes a seleccionar e implementar las capacidades de ciberseguridad que proporcionarán sus dispositivos de IoT. El informe 8259 del NIST también define la terminología y los conceptos que proporcionan un contexto crítico para entender las capacidades de ciberseguridad de dispositivo como una parte de todo el ecosistema de ciberseguridad de la IoT. Así, aunque los fabricantes son el público al que se destinan el Informe interinstitucional o interno 8259 del NIST y esta publicación, tanto fabricantes como integradores y consumidores pueden usar las consideraciones y capacidades analizadas. Para obtener más información sobre la manera en que se pueden incorporar estas capacidades en los

[1] El uso del término “referencia” en esta publicación no se debe confundir con las referencias de control de sistemas de impacto bajo, moderado y alto establecidas en la Publicación especial (SP, por sus siglas en inglés) 800-53 [1] del NIST para ayudar a los organismos federales a cumplir sus obligaciones en virtud de la Ley federal de modernización de la seguridad de la información (FISMA, por sus siglas en inglés) y otras políticas federales. En ese contexto, las referencias de control de impacto bajo, moderado y alto se aplican a un sistema de información en el que puede haber varios componentes y dispositivos. En esta publicación, “referencia” se usa en sentido genérico para denominar un conjunto de requisitos o recomendaciones fundamentales, y la *referencia básica* que se describe se aplica a los dispositivos de IoT en particular.

procesos de desarrollo de un fabricante, véase el Informe interinstitucional o interno 8259 del NIST. Otras organizaciones pueden usar la referencia básica en el contexto disponible y apropiado para estas.

Independientemente de la función de una organización, el objetivo de esta referencia es proporcionar a todas las organizaciones un punto de partida para la gestión de riesgos a la ciberseguridad de los dispositivos de IoT; sin embargo, la implementación de todas las capacidades no se considera obligatoria. Cada una de las capacidades de la referencia pueden implementarse total o parcialmente u omitirse. Queda a criterio de la organización que las implemente conocer el contexto de riesgos único en el que funciona y lo que es apropiado en sus circunstancias. Para obtener más información sobre la manera de llevar a cabo una evaluación de riesgos, véase la Publicación especial 800-30 del NIST, *Guide for Conducting Risk Assessments* [Guía para efectuar evaluaciones de riesgos] [3].

Además, esta referencia no es el único conjunto de capacidades que existe; representa una iniciativa coordinada para establecer una definición de las capacidades comunes, pero no es una lista exhaustiva. Por lo tanto, una organización que implemente la referencia puede definir capacidades que se adapten mejor a su organización. Se recomienda el uso de otras capacidades que ayuden a la gestión de riesgos a la ciberseguridad de dispositivos de IoT. Para obtener más información sobre las consideraciones para la seguridad y la privacidad de los dispositivos de IoT, véase el Informe interinstitucional o interno 8228 del NIST: *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)] [4].

2 Definición de la referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT

La Tabla 1 define la referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT, cuya función es ser una referencia predeterminada para los dispositivos mínimamente protegibles. Sin embargo, a menudo será necesario añadir capacidades de ciberseguridad de dispositivo al diseño, la integración o la adquisición de un dispositivo de IoT, o eliminarlas, para considerar mejor los riesgos comunes a la ciberseguridad de una organización. La referencia básica no especifica el modo en que se deben lograr las capacidades de ciberseguridad de dispositivo, por lo que las organizaciones que decidan adoptarla para cualquiera de los dispositivos de IoT que produzcan, integren o adquieran cuentan con gran flexibilidad para implementarla a fin de satisfacer efectivamente sus necesidades.

Cada fila de la Tabla 1 se refiere a una de las capacidades de ciberseguridad de dispositivo que figura en la referencia básica:

- La primera columna define la capacidad. Cabe señalar que la Figura 1, que se incluye en el Apéndice A, indica la manera en que la capacidad se relaciona con las áreas de mitigación de riesgos y los problemas que se definen en el Informe interinstitucional o interno 8228 del NIST, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)] [4].
- La segunda columna proporciona una lista numerada de *elementos comunes* de esa capacidad, es decir, los elementos que una organización que desee implementar la referencia básica usaría a menudo (pero no siempre) para lograr la capacidad. (Nota: la cantidad de elementos no es exhaustiva, y la numeración de estos no sigue ningún orden particular).
- La tercera columna detalla la explicación de la necesidad de incluir la capacidad y sus elementos comunes en la referencia básica.
- La última columna enumera ejemplos de referencia a la IoT que indican las fuentes existentes de orientación sobre la ciberseguridad de los dispositivos de IoT, y especifican capacidades similares o afines. La tabla solo incluye los conceptos básicos de las capacidades, por lo tanto, las referencias pueden ser muy valiosas para conocer cada capacidad con más detalle y aprender la forma de implementarla de manera razonable. Estas son las referencias que se usan en la Tabla 1:
  - **AGELIGHT**: AgeLight Digital Trust Advisory Group, *IoT Safety Architecture & Risk Toolkit (IoTSA), v. 3.1* [Arquitectura de seguridad y conjunto de herramientas para riesgos de la IoT (IoTSA), versión 3.1] [5]
  - **BITAG**: Broadband Internet Technical Advisory Group (BITAG), *Internet of Things (IoT) Security and Privacy Recommendations* [Recomendaciones para la seguridad y la privacidad de internet de las cosas (IoT)] [6]

- **CSA**: Cloud Security Alliance (CSA) IoT Working Group [Grupo de trabajo de la IoT de Cloud Security Alliance (CSA)], *Identity and Access Management for the Internet of Things* [Gestión de la identidad y el acceso a la internet de las cosas] [7]
- **CSDE**: Council to Secure the Digital Economy (CSDE) [Consejo para proteger la economía digital (CSDE)], *The C2 Consensus on IoT Device Security Baseline Capabilities* [El consenso del C2 sobre capacidades de la referencia de seguridad de los dispositivos de IoT] [8]
- **CTIA**: CTIA [Asociación de comunicación inalámbrica], *CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1* [Plan de prueba de la CTIA para certificación de la ciberseguridad de dispositivos de IoT, versión 1.0.1] [9]
- **ENISA**: Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* [Recomendaciones de referencia para la seguridad de la IoT en el contexto de las infraestructuras de información crítica] [10]
- **ETSI**: Instituto Europeo de Normas de Telecomunicación (ETSI, por sus siglas en inglés), *Cyber Security for Consumer Internet of Things* [Ciberseguridad para la internet de las cosas de los consumidores] [11]
- **GSMA**: Asociación del Sistema Global para las Comunicaciones Móviles (GSMA, por sus siglas en inglés), *GSMA IoT Security Assessment* [Evaluación de la GSMA de la seguridad de la IoT] [12]
- **IEC**: Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), *IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* [IEC 62443-4-2, edición 1.0, Seguridad para los sistemas de automatización y control industrial, Parte 4-2: Requisitos técnicos de seguridad para componentes de IACS] [13]
- **IIC**: Industrial Internet Consortium (IIC) [Consorcio de Internet Industrial], *Industrial Internet of Things, Volume G4: Security Framework* [Internet industrial de las cosas, volumen G4: Marco de seguridad] [14]
- **IoTSF**: IoT Security Foundation (IoTSF) [Fundación para la seguridad de la IoT], *IoT Security Compliance Framework, Release 2* [Marco para el cumplimiento de la seguridad de la IoT, versión 2] [15]
- **ISOC/OTA**: Internet Society/Online Trust Alliance (OTA) [Sociedad de internet/Alianza de confianza en línea], *IoT Security & Privacy Trust Framework, v2.5* [Marco de confianza en la seguridad y la privacidad de la IoT, versión 2.5] [16]
- **NEMA**: Asociación Nacional de Fabricantes Eléctricos (NEMA, por sus siglas en inglés), *Cyber Hygiene Best Practices* [Mejores prácticas de ciberhigiene] [17]

- **OCF**: Open Connectivity Foundation (OCF) [Fundación de conectividad abierta], *OCF Security Specification, Version 2.1.2* [Especificación de seguridad de la OCF, versión 2.1.2] [18]
- **PSA**: Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members [Miembros del acuerdo conjunto de partes interesadas (JSA) de la Arquitectura de seguridad de plataforma (PSA)], *PSA Certified™ Level I Questionnaire, Version 2.0 Beta* [Cuestionario *PSA Certified*™, nivel 1, versión 2.0 beta] [19]

El Apéndice B proporciona las definiciones de los términos subrayados en la Tabla 1.

Tabla 1: Referencia básica de las capacidades de ciberseguridad de dispositivo de los dispositivos de IoT protegibles

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Identificación del dispositivo: El dispositivo de IoT se puede identificar lógica y físicamente de forma exclusiva.	1. Un identificador lógico único 2. Un identificador físico único en una ubicación externa o interna del dispositivo al que pueden acceder las entidades autorizadas Nota: Los identificadores físicos y lógicos pueden representar el mismo valor, pero no es necesario que sea así.	• Esta capacidad contribuye a la gestión de activos, la cual ayuda a su vez a la gestión de vulnerabilidades, la gestión del acceso, la protección de datos y la detección de incidentes. • El identificador lógico único se puede usar para distinguir el dispositivo de todos los demás, generalmente para la gestión y la vigilancia automatizadas del dispositivo. Esto puede requerir que sea inmutable para facilitar la identificación uniforme por medio del identificador. El identificador lógico único también se puede usar para autenticar dispositivos, pero se debe tener en cuenta que hay que seleccionar un identificador apropiado para ese fin. • El identificador físico único se puede usar para distinguir el dispositivo de todos los demás cuando el identificador lógico único no esté disponible, por ejemplo, durante la implementación y la retirada del dispositivo, o después de un error de dispositivo. • La capacidad también puede hacer necesario un identificador lógico adicional que no tendrá que ser único y que se usará para fines más específicos, como la señalización de la intención del dispositivo.	• **CSA:** 1 • **CSDE**: 5.1.1 • **CTIA**: 4.13 • **ENISA**: GP-PS-10 • **GSMA**: CLP13_6.6.2, 6.8.1, 6.20.1 • **IEC**: CR 1.2 • **IIC**: 7.3, 8.5, 11.7, 11.8 • **IoTSF**: 2.4.8.1, 2.4.14.3, 2.4.14.4 • **OCF:** 7.1.1 • **PSA:** C1.4, R2.1

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Configuración del dispositivo: La configuración del software del dispositivo de IoT se puede modificar, pero solo las entidades autorizadas pueden hacer estos cambios.	1. Capacidad para modificar las opciones de configuración del software del dispositivo 2. Capacidad para permitir que solo las entidades autorizadas hagan cambios a la configuración 3. Capacidad para que las entidades autorizadas restauren el dispositivo a una configuración segura que defina una entidad autorizada	• Esta capacidad contribuye a la gestión de vulnerabilidades, la gestión del acceso, la protección de datos y la detección de incidentes. • Es posible que una entidad autorizada desee modificar la configuración de un dispositivo por diversas razones, entre otras, ciberseguridad, interoperabilidad, privacidad y facilidad de uso. Si no cuenta con una capacidad de configuración de dispositivos, la entidad autorizada no puede personalizar el dispositivo para satisfacer sus necesidades, integrarlo en su entorno, etc. • La mayoría de las capacidades de ciberseguridad dependen al menos en cierta medida de la presencia de una capacidad de configuración del dispositivo. • Es posible que las entidades no autorizadas deseen cambiar la configuración de un dispositivo por muchas razones, como lograr acceso no autorizado, hacer que el dispositivo no funcione correctamente o vigilar secretamente el entorno del dispositivo. • La capacidad para restaurar una configuración segura de un dispositivo es útil cuando la configuración actual contiene errores, se dañó o si se cree que ya no es confiable de alguna manera.	• **BITAG**: 7.1 • **CSA**: 22 • **ENISA**: GP-TM-06 • **IEC**: CR 7.4, CR 7.6 • **IIC**: 7.3, 7.6, 8.10, 11.5 • **IoTSF**: 2.4.8.17, 2.4.15 • **ISOC/OTA**: 26 • **OCF:** 5.3.3, 8.2, 12, 13.3.1 • **PSA**: C2.3, R6.1, R7.1

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Protección de datos: El dispositivo IoT puede proteger los datos que almacena y transmite contra accesos y modificaciones no autorizados.	1. Capacidad para utilizar módulos criptográficos que sean manifiestamente seguros para algoritmos criptográficos estandarizados (por ejemplo, cifrado con autenticación, hash criptográfico, validación de firmas digitales) a fin de evitar que peligre la confidencialidad y la integridad de los datos almacenados en el dispositivo y transmitidos desde este 2. Capacidad para que las entidades autorizadas impidan a todas las entidades el acceso a todos los datos del dispositivo, sin importar si este estaba o no autorizado anteriormente (por ejemplo, mediante borrado del almacenamiento interno, destrucción de claves criptográficas para datos cifrados) 3. Opciones de configuración para usarlas con la capacidad de **configuración del dispositivo**, incluida, entre otras, la capacidad de las entidades autorizadas para configurar el uso mismo de criptografía, por ejemplo, seleccionando una longitud de clave	• Esta capacidad contribuye a la gestión del acceso, la protección de datos y la detección de incidentes. • Las entidades autorizadas (por ejemplo, clientes, administradores, usuarios) desean a menudo proteger la confidencialidad de sus datos para impedir que las entidades no autorizadas accedan a ellos y los usen de manera indebida. • Las entidades autorizadas desean a menudo proteger la integridad de sus datos para evitar su modificación accidental o intencional, ya que esto podría tener una variedad de consecuencias adversas (por ejemplo, emisión del comando equivocado a un elemento del equipo, ocultación de actividad maliciosa).	• **AGELIGHT**: 5, 7, 18, 24, 25, 34 • **BITAG**: 7.2, 7.10 • **CSDE**: 5.1.3, 5.1.4, 5.1.5, 5.1.8, 5.1.10 • **CTIA**: 4.8, 5.14, 5.15 • **ENISA**: GP-OP-04, GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-39, GP-TM-40 • **ETSI**: 4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3 • **GSMA:** CLP13_6.4.1.1, 6.11, 6.12.1.1, 6.19, 7.6.1, 8.10.1.1, 8.11.1 • **IEC**: CR 3.1, CR 3.4, CR 4.1, CR 4.2, CR 4.3 • **IIC**: 7.3, 7.4, 7.6, 7.7, 8.8, 8.11, 8.13, 9.1, 10.4, 11.9 • **IoTSF**: 2.4.6.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.16.1, 2.4.16.2 • **ISOC/OTA**: 2, 17, 33 • **OCF:** 8.2, 11.2.1, 11.3, 14.2.2 • **PSA:** C1.1, C1.4, C2.4, D5.2, R2.2, R2.3, R6.1, R7.1

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Acceso lógico a interfaces: El dispositivo de IoT puede restringir el acceso lógico a sus interfaces locales y de red, así como a los protocolos y servicios que usan esas interfaces, y permitirlo solo a las entidades autorizadas.	1. Capacidad para deshabilitar lógica o físicamente cualquier interfaz local y de red que no sea necesaria para la funcionalidad principal del dispositivo 2. Capacidad para restringir lógicamente el acceso a cada interfaz de red y permitirlo solo a las entidades autorizadas (por ejemplo, autenticación de dispositivos, autenticación de usuarios) 3. Opciones de configuración para usarlas con la capacidad de **configuración del dispositivo**, incluida, entre otras, la capacidad para habilitar, deshabilitar y ajustar los umbrales de cualquier capacidad que el dispositivo pueda tener para bloquear o deshabilitar una cuenta, o para demorar más intentos de autenticación después de demasiados intentos fallidos de autenticación	• Esta capacidad contribuye a la gestión de vulnerabilidades, la gestión del acceso, la protección de datos y la detección de incidentes. • La limitación del acceso a las interfaces reduce la superficie de ataque del dispositivo y da menos oportunidades a los atacantes de ponerlo en peligro. Por ejemplo, dar a un dispositivo de IoT acceso sin restricciones a la red permite a los atacantes interactuar directamente con este, lo que aumenta considerablemente la probabilidad de que el dispositivo quede comprometido. • El acceso a las interfaces se puede limitar parcial o totalmente en función del estado del dispositivo. Por ejemplo, si un dispositivo no cuenta con las debidas credenciales de red, se limitaría todo acceso a las interfaces de red, y desde estas, con el uso de un esquema seguro de incorporación.	• **AGELIGHT**: 10, 13, 14, 15, 16, 19 • **BITAG**: 7.1, 7.2, 7.3, 7.6 • **CSA:** 2, 4, 20 • **CSDE**: 5.1.2 • **CTIA**: 3.2, 3.3, 3.4, 4.2, 4.3, 4.9, 5.2 • **ENISA**: GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-25, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM-42, GP-TM-44, GP-TM-45 • **ETSI**: 4.1-1, 4.4-1, 4.6-1, 4.6-2 • **GSMA**: CLP13_6.9.1, 6.12.1, 6.20.1, 7.6.1, 8.2.1, 8.4.1 • **IEC**: CR 1.1, CR 1.2, CR 1.5, CR 1.7, CR 1.11, CR 2.1, CR 2.2, CR 2.13, CR 7.7, EDR 2.13 • **IIC**: 7.3, 7.4, 8.3, 8.6, 11.7 • **IoTSF**: 2.4.4.5, 2.4.4.9, 2.4.5.5, 2.4.6.3, 2.4.6.4, 2.4.7, 2.4.8 • **ISOC/OTA**: 3, 12, 13, 14, 15, 16 • **NEMA**: Segmentación de redes, gestión de usuarios, dispositivos de endurecimiento • **OCF:** 5.1, 5.2, 10, 12 • **PSA:** C2.3, D2.1, D2.2, D2.3, D2.4, D3.1 D3.3, R3.1, R3.2, R3.3, R4.2, R4.5 R6.1

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Actualización de software: Solo las entidades autorizadas pueden hacer la actualización del software del dispositivo de IoT con el uso de un mecanismo seguro y configurable.	1. Capacidad para actualizar el software del dispositivo por medios remotos (por ejemplo, descarga de red) o locales (por ejemplo, medios extraíbles) 2. Capacidad para verificar y autenticar toda actualización antes de instalarla 3. Capacidad para que las entidades autorizadas reviertan el software actualizado a una versión anterior 4. Capacidad para restringir las acciones de actualización permitiéndolas solo a las entidades autorizadas 5. Capacidad para habilitar o deshabilitar la actualización 6. Opciones de configuración para usarlas con la capacidad de **configuración del dispositivo** incluidas, entre otras: a. Capacidad para configurar cualquier mecanismo de actualización remota para que inicie automática o manualmente las descargas e instalaciones de actualizaciones b. Capacidad para habilitar o deshabilitar notificaciones cuando haya actualizaciones disponibles, y para especificar quién o qué debe ser notificado	• Esta capacidad contribuye a la gestión de vulnerabilidades. • Las actualizaciones pueden eliminar vulnerabilidades de un dispositivo de IoT, lo cual disminuye la probabilidad de que un atacante lo ponga en peligro. • Las actualizaciones pueden corregir problemas operativos del dispositivo de IoT, con lo que mejora la disponibilidad, la confiabilidad, el rendimiento y otros aspectos del funcionamiento del dispositivo. • Algunas entidades autorizadas necesitarán capacidades de actualización automática para lograr sus metas y satisfacer sus necesidades de ciberseguridad, mientras que otras preferirían o necesitarían un control más directo sobre las actualizaciones y su aplicación. • Es posible que algunas organizaciones deseen la capacidad de reversión (en caso de que una actualización afecte sin querer aplicaciones críticas o la integración con otros sistemas), mientras que otras organizaciones pueden preferir eliminar el riesgo de que alguien revierta accidental o intencionalmente el software a una versión vulnerable.	• **AGELIGHT**: 1, 2, 4 • **BITAG**: 7.1 • **CSDE**: 5.1.9 • **CTIA**: 3.5, 3.6, 4.5, 4.6, 5.5, 5.6 • **ENISA**: GP-TM-05, GP-TM-06, GP-TM-18, GP-TM-19 • **ETSI**: 4.3-1, 4.3-2, 4.3-7 • **GSMA**: 7.5.1 • **IEC**: CR 3.4, EDR 3.10 • **IIC**: 7.3, 11.5.1 • **IoTSF**: 2.4.5.1, 2.4.5.2, 2.4.5.3, 2.4.5.4, 2.4.5.8, 2.4.6.1 • **ISOC/OTA**: 1, 6, 8 • **NEMA**: Actualización de dispositivos • **OCF:** 14.5 • **PSA:** C2.1, C2.2, R1.1, R1.2, R6.1

Capacidad de ciberseguridad de dispositivo	Elementos comunes	Explicación	Ejemplos de referencias de IoT
Información sobre el estado de la ciberseguridad: El dispositivo de IoT puede informar de su estado de ciberseguridad y permitir que solo las entidades autorizadas tengan acceso a esa información.	1. Capacidad para informar del estado de ciberseguridad del dispositivo 2. Capacidad para distinguir entre el momento en que un dispositivo probablemente funcionará según lo previsto y el momento en que tal vez esté en un estado degradado de ciberseguridad 3. Capacidad para restringir el acceso al indicador de estado de manera que solo las entidades autorizadas puedan verlo 4. Capacidad para evitar que toda entidad, autorizada o no autorizada, edite el estado, a excepción de las entidades responsables del mantenimiento de la información sobre el estado del dispositivo 5. Capacidad para poner la información sobre el estado a disposición de un servicio en otro dispositivo, como un servidor de registro de eventos o estados	• Esta capacidad contribuye a la gestión de vulnerabilidades y la detección de incidentes. • Conocer el estado de la ciberseguridad facilita investigar los peligros, identificar el uso indebido y solucionar ciertos problemas operativos. • La forma en que el dispositivo informa a otras entidades de un estado de ciberseguridad variará en función de las necesidades y las metas específicas del contexto, pero puede incluir la captura y el registro de información sobre eventos en un registro persistente que tal vez tenga que ser almacenado fuera del dispositivo, el envío de señales a un sistema de vigilancia para que se manejen externamente o las alertas por medio de una interfaz en el propio dispositivo de IoT.	• **CSDE**: 5.1.7 • **CTIA**: 4.7, 4.12, 5.7, 5.16 • **ENISA**: GP-TM-55, GP-TM-56 • **ETSI**: 4.7-2, 4.10-1 • **GSMA**: CLP13_6.13.1, 7.2.1, 9.1.1.2 • **IEC**: CR 2.8, CR 3.9, CR 6.1, CR 6.2 • **IIC**: 7.3, 7.5, 7.7, 8.9, 10.3, 10.4 • **IoTSF**: 2.4.7.5 • **NEMA**: Dispositivos y sistemas de vigilancia • **OCF:** 5.1, 5.7, 8.6, 12, 13.8, 13.16 • **PSA**: C1.3, D1.1, D3.2, D3.4, D3.5, D5.1, R4.1, R4.3, R4.4

Referencias

[1] *Joint Task Force Transformation Initiative* [Iniciativa de transformación del grupo de trabajo conjunto] (2013), *Security and Privacy Controls for Federal Information Systems and Organizations* [Controles de seguridad y privacidad para sistemas y organizaciones de información federales], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-53 del NIST, rev. 4. Incluye actualizaciones a partir del 22 de enero de 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[2] Fagan, M., Megas, K. N., Scarfone, K. y Smith, M. (2020), *Foundational Cybersecurity Activities for IoT Device Manufacturers* [Actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de IoT], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Informe interinstitucional o interno 8259 del NIST. https://doi.org/10.6028/NIST.IR.8259

[3] Iniciativa de transformación del grupo de trabajo conjunto (2012), *Guide for Conducting Risk Assessments* [Guía para efectuar evaluaciones de riesgos], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-30 del NIST, rev. 4. https://doi.org/10.6028/NIST.SP.800-30r1

[4] Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., Piccarreta, B., Gabel O'Rourke, D. y Scarfone, K. (2019), *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Informe interinstitucional o interno 8228 del NIST. https://doi.org/10.6028/NIST.IR.8228

[5] AgeLight Digital Trust Advisory Group (2019), *IoT Safety Architecture & Risk Toolkit (IoTSA), v. 3.1* [Arquitectura de seguridad y conjunto de herramientas para riesgos de la IoT (IoTSA), versión 3.1], (AgeLight Advisory & Research Group, Bellevue, Washington). IoT Safety Architecture & Risk Toolkit

[6] Broadband Internet Technical Advisory Group (BITAG) (2016), *Internet of Things (IoT) Security and Privacy Recommendations* [Recomendaciones para la seguridad y la privacidad de internet de las cosas (IoT)], (Broadband Internet Technical Advisory Group [BITAG], Denver, Colorado). https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[7] Cloud Security Alliance (CSA) IoT Working Group [Grupo de trabajo de la IoT de Cloud Security Alliance (CSA)] (2015), *Identity and Access Management for the Internet of Things* [Gestión de la identidad y el acceso a la internet de las cosas], (Cloud Security Alliance [CSA]). https://cloudsecurityalliance.org/download/identity-and-access-management-for-the-iot/

[8] Council to Secure the Digital Economy (CSDE) [Consejo para proteger la economía digital (CSDE)] (2019), *The C2 Consensus on IoT Device Security Baseline Capabilities* [El consenso del C2 sobre capacidades de la referencia de seguridad de los dispositivos de IoT], (Council to Secure the Digital Economy [CSDE]). https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[9] CTIA [Asociación de comunicación inalámbrica] (2018), *CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1* [Plan de prueba de la CTIA para certificación de la ciberseguridad de dispositivos de IoT, versión 1.0.1], (CTIA, Washington, DC). https://www.ctia.org/about-ctia/test-plans/

[10] Agencia Europea de Seguridad de las Redes y de la Información (ENISA) (2017), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* [Recomendaciones de referencia para la seguridad de la IoT en el contexto de las infraestructuras de informática críticas], (Agencia Europea de Seguridad de las Redes y de la Información [ENISA], Atenas, Grecia). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[11] Instituto Europeo de Normas de Telecomunicación (ETSI) (2019), *Cyber Security for Consumer Internet of Things* [Ciberseguridad para la internet de las cosas de los consumidores], Especificación técnica 103 645 V1.1.1 del ETSI[2], (Instituto Europeo de Normas de Telecomunicación [ETSI], Sophia Antipolis Cedex, Francia). https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[12] Asociación del Sistema Global para las Comunicaciones Móviles (GSMA) (2017), *GSMA IoT Security Assessment* [Evaluación de la GSMA de la seguridad de la IoT], (Asociación del Sistema Global para las Comunicaciones Móviles [GSMA], Londres, Reino Unido). https://www.gsma.com/iot/iot-security-assessment/

[13] Comisión Electrotécnica Internacional (IEC) (2019), *IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* [IEC 62443-4-2, edición 1.0, Seguridad para los sistemas de automatización y control industrial, Parte 4-2: Requisitos técnicos de seguridad para componentes de IACS], (Comisión Electrotécnica Internacional [IEC], Ginebra, Suiza). https://webstore.iec.ch/publication/34421

[14] Industrial Internet Consortium (IIC) [Consorcio de Internet Industrial] (2016), *Industrial Internet of Things Volume G4: Security Framework* [Internet industrial de las cosas, volumen G4: Marco de seguridad], (Industrial Internet Consortium [IIC], Needham, Massachusetts). https://www.iiconsortium.org/IISF.htm

[15] IoT Security Foundation (IoTSF) [Fundación para la seguridad de IoT] (2018), *IoT Security Compliance Framework, Release 2* [Marco para el cumplimiento de la seguridad de la IoT, versión 2], (IoT Security Foundation [IoTSF], Livingston, Escocia). https://www.iotsecurityfoundation.org/best-practice-guidelines/

[2] El ETSI está preparando el estándar europeo 303 645 del ETSI, que es similar, pero no idéntico, a la Especificación técnica 103 645 que se cita aquí. La versión 303 645 no se usa en esta publicación porque aún es un proyecto.

[16] Online Trust Alliance (OTA) [Alianza de confianza en línea] (2017), *IoT Security & Privacy Trust Framework v2.5* [Marco de confianza en la seguridad y la privacidad de la IoT, versión 2.5], (Online Trust Alliance [OTA], una iniciativa de la Internet Society [Sociedad de internet]). https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

[17] Asociación Nacional de Fabricantes Eléctricos (NEMA) (2018), *Cyber Hygiene Best Practices* [Mejores prácticas de ciberhigiene], (Asociación Nacional de Fabricantes Eléctricos [NEMA], Rosslyn, Virginia). https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx

[18] Open Connectivity Foundation (OCF) [Fundación de conectividad abierta] (2020), *OCF Security Specification Version 2.1.2* [Especificación de seguridad de la OCF, versión 2.1.2], (Open Connectivity Foundation [OCF], Beaverton, Oregon). https://openconnectivity.org/specs/OCF_Security_Specification_v2.1.2.pdf

[19] Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members [Miembros del acuerdo conjunto entre partes interesadas (JSA) de la Arquitectura de seguridad de plataforma (PSA)] (2020), *PSA Certified™ Level I Questionnaire, Version 2.0 Beta* [Cuestionario *PSA Certified*™, nivel 1, versión 2.0 beta], (Arm Limited, Cambridge, Reino Unido). https://www.psacertified.org/security-certification/psa-certified-level-1

[20] Johnson, A., Dempsey, K., Ross, R., Gupta, S. y Bailey, D. (2011), *Guide for Security-Focused Configuration Management of Information Systems* [Guía para la gestión de configuraciones orientada a la seguridad de los sistemas de información], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-128 del NIST. https://doi.org/10.6028/NIST.SP.800-128

[21] Barker, E., Chen, L., Roginsky, A., Vassilev, A. y Davis, R. (2019), *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [Recomendación para los esquemas de establecimiento de claves de pares que utilizan criptografía de logaritmo discreto], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-56A, rev. 3, del NIST. https://doi.org/10.6028/NIST.SP.800-56Ar3

[22] Committee on National Security Systems [Comité de Sistemas de Seguridad Nacional (CNSS, por sus siglas en inglés)] (2015), *Committee on National Security Systems (CNSS) Glossary* [Glosario del Comité de Sistemas de Seguridad Nacional], (National Security Agency [Agencia de Seguridad Nacional], Ft. Meade, Maryland), instrucción 4009 del CNSS.

[23] Souppaya, M. y Scarfone, K. (2013), *Guide to Enterprise Patch Management Technologies* [Guía para las tecnologías de gestión de parches empresariales], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-40 del NIST, rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

Apéndice A: Conocimiento de la referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT en el contexto de las necesidades y metas del cliente

Las organizaciones deben tener en cuenta que las capacidades que se presentan en la Tabla 1 son un punto de partida que ayuda a proporcionar los medios que las partes interesadas pueden necesitar para satisfacer las necesidades y lograr las metas comunes de ciberseguridad. Conocer las áreas de mitigación de riesgos que los clientes buscan es una manera de considerar las necesidades y metas de ciberseguridad que un dispositivo de IoT deberá incluir en sus capacidades de ciberseguridad de dispositivo. Por ejemplo, la Figura 1 muestra las áreas de mitigación de riesgos y los problemas descritos en el Informe interinstitucional o interno 8228 del NIST, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [4] [Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)] que solucionarían, en parte, las capacidades definidas en la Tabla 1. El Informe interinstitucional o interno 8228 del NIST cita otros problemas que las capacidades principales de ciberseguridad de dispositivo no consideran porque, por lo general, esos problemas afectan a una proporción pequeña de IoT, en comparación con la aplicabilidad de las capacidades principales.

Figura 1: Áreas de mitigación de riesgos del Informe interinstitucional o interno 8228 del NIST que incluye cada capacidad principal de ciberseguridad de dispositivo

La Figura 1 demuestra que para la referencia básica se consideró un conjunto amplio y común de áreas de mitigación de riesgos, las cuales deben conocer los fabricantes y demás lectores que usen la referencia básica como punto de partida. Aunque los dispositivos de IoT que proporcionan las capacidades básicas de ciberseguridad de dispositivo descritas en la referencia básica pueden ayudar a muchos clientes a satisfacer sus necesidades y lograr sus metas de ciberseguridad más fácilmente, en realidad, es probable que los clientes se concentren en áreas de mitigación de riesgos distintas y más específicas. Por lo tanto, las seis capacidades y elementos comunes de la Tabla 1 no se deben considerar como la definición universal y completa de las capacidades de ciberseguridad de dispositivo que necesitan todos los clientes.

Como se describe en el Informe interinstitucional o interno 8259 del NIST, los fabricantes deben tomar en cuenta los clientes probables de sus dispositivos de IoT y los casos de uso previstos para comenzar a identificar las capacidades precisas de ciberseguridad de dispositivo necesarias en cada contexto. Los fabricantes pueden definir aún más las capacidades de ciberseguridad de dispositivo empleando elementos nuevos o adicionales en función del conocimiento que tengan de sus clientes y la investigación que hagan sobre estos. Es posible que esto suponga la incorporación de capacidades de ciberseguridad de dispositivo compatibles con la mitigación de riesgos en otras áreas que no sean las que se tratan aquí (por ejemplo, penetración u otras formas de pruebas o validación de componentes, arquitecturas de red específicas para reducir riesgos) o la incorporación de elementos más exclusivos para un dispositivo de IoT compatibles con mitigaciones de riesgos y otras necesidades y metas de ciberseguridad de aplicación menos amplia, pero que, en el contexto de un cliente o de un caso de uso, sean de vital importancia. Los fabricantes también deben tener en cuenta otras consideraciones (además de las mitigaciones de riesgos que pueden afectar la ciberseguridad de los dispositivos y sus elementos) como la facilidad de uso en función del cliente y el caso de uso; las funciones y responsabilidades relacionadas con la ciberseguridad y la manera en que los clientes prevén que se asignarán; y las necesidades y metas de ciberseguridad de la sociedad (por ejemplo, protección contra la creación de redes robot) que tal vez no se reflejan directamente en las necesidades y metas del cliente.

Apéndice B: Glosario

Se definen a continuación los términos seleccionados que se usaron en este documento.

actualización	Parche, actualización u otra modificación hecha al código que corrige problemas de seguridad o funcionalidad en el software. (Definición obtenida de [23]).
configuración	"Condiciones, parámetros y especificaciones posibles con las que se puede describir u organizar un sistema de información o un componente del sistema [20]". La capacidad de configuración del dispositivo no define las opciones de configuración que deben existir, sino simplemente que existe un mecanismo para gestionar esas opciones.
entidad autorizada	Entidad a la que se concedió de forma implícita o explícita aprobación para interactuar con un dispositivo de IoT particular. Las capacidades de ciberseguridad de dispositivo de la referencia básica no especifican la manera en que se implementa la autorización para distinguir entre las entidades autorizadas y las no autorizadas, pero pueden incluir la gestión y autenticación de identidades para establecer la autorización de las entidades. La organización debe decidir la forma en que cada dispositivo implementará la autorización. Además, una entidad autorizada para interactuar de cierta manera con un dispositivo de IoT podría no estar autorizada para interactuar de otra manera con ese mismo dispositivo.
entidad	Persona, dispositivo, servicio, red, dominio, fabricante u otra parte que podría interactuar con un dispositivo de IoT.
estado degradado de ciberseguridad	Estado de ciberseguridad que indica que la ciberseguridad del dispositivo se ha visto afectada considerablemente, de manera que impide que este opere según lo previsto, o que la integridad del software del dispositivo se está infringiendo.
estado de la ciberseguridad	Condición de la ciberseguridad de un dispositivo que se expresa de manera significativa y útil para las entidades autorizadas. Por ejemplo, un dispositivo muy simple podría expresar su estado en términos de si funciona o no según lo previsto, mientras que un dispositivo complejo podría llevar registros de ciberseguridad, comprobar su integridad al arrancar y comunicar los resultados, y analizar e informar de otros aspectos del estado de su ciberseguridad.
identificador de dispositivo	Valor especial del contexto (un valor único en un contexto específico) que se asocia a un dispositivo (por ejemplo, una cadena que consiste en una dirección de red). (Definición obtenida de [21]).
identificador físico	Identificador de dispositivo que el dispositivo expresa físicamente (por ejemplo, impreso en la cubierta del dispositivo, a la vista en la pantalla del dispositivo).

identificador lógico	Identificador de dispositivo que el software del dispositivo expresa lógicamente. Un ejemplo es una dirección de control de acceso de medios (MAC, por sus siglas en inglés) asignada a una interfaz de red.
interfaz	Límite entre el dispositivo de IoT y las entidades donde tienen lugar las interacciones. (Definición obtenida de [22]). Hay dos tipos de interfaces: de red y local.
interfaz de red	Interfaz que conecta el dispositivo de IoT a una red.
interfaz local	Interfaz a la que solo se puede acceder físicamente, como un puerto (por ejemplo, bus serie universal [USB, por sus siglas en inglés], audio, video o pantalla, en serie, en paralelo, Thunderbolt) o una unidad de medios extraíble (por ejemplo, unidad de CD/DVD, ranura para tarjeta de memoria).
referencia básica	Conjunto de capacidades técnicas de los dispositivos necesarias para reforzar los controles comunes de ciberseguridad que protegen a los dispositivos, los datos de los dispositivos, los sistemas y los ecosistemas del cliente.
referencia básica de las capacidades de ciberseguridad de dispositivo	Véase *referencia básica*.
software	“Programas informáticos y datos afines que se pueden escribir o modificar de forma dinámica durante la ejecución del dispositivo” (por ejemplo, código de aplicación, bibliotecas) [1].