



NIST IR 8259B spa

Base de referencia de las capacidades de apoyo no técnicas del IoT

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold

Esta publicación puede obtenerse gratuitamente en:
<https://doi.org/10.6028/NIST.IR.8259B.spa>

NIST IR 8259B spa

Base de referencia de las capacidades de apoyo no técnicas del Internet de las cosas

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas

*División de seguridad cibernética Aplicada
Laboratorio de Tecnologías de la Información*

Rebecca Herold
*La Profesora de Privacidad
Des Moines, IA*

Esta publicación puede obtenerse gratuitamente en:
<https://doi.org/10.6028/NIST.IR.8259B.spa>

Agosto 2021



U.S. Department of Commerce
Gina M. Raimondo, Secretaria

Instituto Nacional de Normas y Tecnología
*James K. Olthoff, Desempeñando las funciones y obligaciones no exclusivas del Subsecretario de Comercio
para Normas y Tecnología y Director del Instituto Nacional de Normas y Tecnología*

Instituto Nacional de Normas y Tecnología Informe Interinstitucional o Interno 8259B
30 páginas (July 2021)

Esta publicación puede obtenerse gratuitamente en:
<https://doi.org/10.6028/NIST.IR.8259B.spa>

Ciertas entidades comerciales, equipos o materiales se podrán identificar en este documento con el fin de describir adecuadamente un procedimiento o concepto experimental. Dicha identificación no tiene como objetivo implicar una recomendación o aprobación por parte del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), ni que las entidades, materiales o equipos sean necesariamente los mejores disponibles para el propósito.

Puede haber referencias en esta publicación a otras publicaciones que actualmente están siendo elaboradas por el NIST de acuerdo con sus responsabilidades estatutarias asignadas. La información contenida en esta publicación, incluidos los conceptos y metodologías, puede ser utilizada por los organismos federales incluso antes de que se completen dichas publicaciones complementarias. Por lo tanto, hasta que cada publicación esté terminada, los requisitos, directrices y procedimientos actuales, cuando existan, seguirán siendo operativos. Por motivos de planificación y transición, los organismos federales pueden hacer un seguimiento detenido de la elaboración de estas nuevas publicaciones por parte del NIST.

Se alienta a las organizaciones a que revisen todos los bocetos de publicaciones durante los períodos de comentarios públicos y proporcionen sus comentarios al NIST. Muchas publicaciones sobre la seguridad cibernética del NIST, aparte de las mencionadas anteriormente, están disponibles en <https://csrc.nist.gov/publications>.

Los comentarios acerca de esta publicación pueden enviarse a:

National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología)
Attn: División de seguridad cibernética Aplicada, Laboratorio de Tecnología de la Información
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Correo electrónico: iotsecurity@nist.gov

Todos los comentarios están sujetos a divulgación en virtud de la Ley de Libertad de Información (FOIA, por sus siglas en inglés).

Traducción realizada por TaikaTranslations LLC bajo contrato con NIST [1333ND23PNB770271]. Traducción oficial del Gobierno de EE.UU.

Translated by TaikaTranslations LLC under contract with NIST [1333ND23PNB770271]. Official U.S. Government translation.

Esta publicación está disponible gratuitamente en inglés en el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés): <https://doi.org/10.6028/NIST.IR.8259B>.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): <https://doi.org/10.6028/NIST.IR.8259B>.

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología de la Información (ITL, por sus siglas en inglés) del Instituto Nacional de Normas y Tecnología (NIST) promueve la economía y el bienestar público de Estados Unidos proporcionando liderazgo técnico para la infraestructura de medición y normalización del país. El ITL diseña pruebas, métodos de prueba, datos de referencia, implementaciones de prueba de concepto y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. Las responsabilidades del ITL incluyen la elaboración de normas y directrices de gestión, administrativas, técnicas y físicas para la seguridad rentable y la privacidad de la información no relacionada con la seguridad nacional en los sistemas de información federales.

Resumen

Las capacidades de apoyo no técnicas son acciones que realiza un fabricante o una organización de terceros en apoyo de la seguridad cibernética de un dispositivo de Internet de las cosas (IoT, por sus siglas en inglés). Esta publicación define una *línea base de capacidades de apoyo no técnicas* de los fabricantes de dispositivos de Internet de las Cosas (IoT), que es un conjunto de capacidades de apoyo no técnicas generalmente necesarias de los fabricantes u otros terceros para apoyar los controles comunes de seguridad cibernética que protegen los dispositivos de una organización, así como los datos, sistemas y ecosistemas de los dispositivos. El propósito de esta publicación es proporcionar a las organizaciones un punto de partida para identificar las capacidades de apoyo no técnicas necesarias en relación con los dispositivos del IoT que fabricarán, integrarán o adquirirán. Esta publicación debe utilizarse junto con el Informe interno del Instituto Nacional de Normas y Tecnología 8259 (NISTIR, por sus siglas en inglés), *Actividades básicas de seguridad cibernética para fabricantes de dispositivos de IoT* y NISTIR 8259A, Base de referencia de capacidades de seguridad cibernética para dispositivos de IoT.

Palabras clave

línea base de seguridad cibernética; Internet de las cosas (IoT); dispositivos informáticos seguros.

Agradecimientos

Los autores desean agradecer a todos los que han contribuido a esta publicación, incluidos 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, así como a varias organizaciones comerciales de fabricantes, que proporcionaron comentarios sobre el contenido público preliminar, y a los colegas del NIST que ofrecieron valiosas contribuciones y comentarios. Queremos agradecer especialmente a Brad Hoehn y David Lemire, miembros del equipo de Seguridad Cibernética para IoT, y al equipo del Proyecto de Implementación de la Ley Federal de Modernización de la Seguridad de la Información (NIST FISMA, por sus siglas en inglés), por su amplia ayuda.

Público

El público principal de esta publicación son los fabricantes de dispositivos de IoT, especialmente con el papel emergente de los responsables de seguridad de los productos. Esta publicación

también puede ayudar a los clientes o integradores de dispositivos de IoT.

Aviso de divulgación de patentes

AVISO: ITL ha solicitado que los titulares de reivindicaciones de patentes cuyo uso pueda ser necesario para el cumplimiento de la orientación o los requisitos de esta publicación divulguen dichas reivindicaciones de patentes a ITL. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de patentes de ITL, e ITL no ha realizado una búsqueda de patentes para identificar qué patentes, si las hubiera, pueden aplicarse a esta publicación.

En la fecha de publicación y tras la(s) solicitud(es) de identificación de reivindicaciones de patentes cuyo uso pueda ser necesario para el cumplimiento de las orientaciones o requisitos de esta publicación, ITL no ha identificado ninguna reivindicación de patente de este tipo.

El ITL no declara ni implica que no se requieran licencias para evitar la infracción de patentes en el uso de esta publicación.

Índice

1	Introducción.....	1
2	Base de referencia de las capacidades de apoyo no técnicas de IoT	4
	Referencias	11

Lista de apéndices

	Appendix A— Acrónimos	13
	Appendix B— Glosario	14

1 Introducción

Los dispositivos de Internet de las Cosas (IoT) frecuentemente no cuentan con capacidades de seguridad cibernética integradas en el dispositivo, así como con asistencia no técnica pertinente a la seguridad cibernética. Los clientes pueden utilizar este tipo de información para ayudar a mitigar los riesgos de seguridad cibernética relacionados con los dispositivos de IoT y su uso. La amplia gama de conectividad posible para los dispositivos de IoT, y la capacidad de estos dispositivos para interactuar con el mundo físico, significa que la seguridad de estos dispositivos con frecuencia se convierte en una prioridad; pero es un reto para los clientes cuando no cuentan con el apoyo adecuado.

Esta publicación debe ser utilizada y entendida dentro del contexto de NISTIR 8259, *Actividades básicas de seguridad cibernética para los fabricantes de dispositivos de IoT* [1] y NISTIR 8259A, *Línea base de la capacidad de seguridad cibernética de dispositivos de IoT* [2]. NISTIR 8259 analiza las consideraciones para los fabricantes con el fin de ayudarlos a elegir e implementar las capacidades de seguridad cibernética del dispositivo que proporcionarán sus dispositivos de IoT. El 8259A analiza las capacidades técnicas de seguridad cibernética de los dispositivos, que son características o funciones de seguridad cibernética que los dispositivos proporcionan a través de sus propios medios técnicos (es decir, hardware y software del dispositivo), y establece una base de referencia de las capacidades de seguridad cibernética de los dispositivos que los clientes de dispositivos de IoT suelen necesitar.

Para complementar la línea de base central de NISTIR 8259A, la línea de base central de capacidades de apoyo no técnicas de IoT es un conjunto de acciones realizadas por fabricantes y/o terceros de apoyo designados (denominados partes de apoyo). Estas acciones ayudarán a otros (por ejemplo, clientes, usuarios finales) a utilizar las capacidades de seguridad cibernética de los dispositivos IoT, y apoyarán la seguridad cibernética continua del dispositivo de IoT y el sistema y las redes a las que se conecta el dispositivo (el ecosistema digital). Proporcionar este apoyo no técnico a la seguridad cibernética a través de materiales educativos u otros tipos de herramientas y acciones no técnicas puede beneficiar a todo el ecosistema de dispositivos de IoT y permitir a los fabricantes apoyar mejor la seguridad cibernética de los dispositivos a lo largo de todo su ciclo de vida. Tanto las capacidades de seguridad cibernética de los dispositivos como las capacidades de apoyo no técnicas son vitales para que los clientes puedan alcanzar sus necesidades y objetivos. De manera similar a la base de referencia de capacidades de seguridad cibernética de dispositivos de IoT en NISTIR 8259A, esta base de referencia de capacidades de apoyo no técnicas de IoT tiene como objetivo proporcionar a las organizaciones un punto de partida para el establecimiento de acciones no técnicas que respalden la gestión de riesgos de seguridad cibernética de dispositivos de IoT.

Específicamente, esta publicación describe cuatro capacidades de apoyo no técnicas recomendadas relacionadas con el ciclo de vida completo de la gestión de la seguridad cibernética que los fabricantes deben implementar para respaldar los dispositivos de IoT que fabrican durante toda su vida útil: 1) Documentación; 2) Recepción de información y consultas; 3) Difusión de información; y 4) Educación y concienciación.

La elección por parte de un fabricante de capacidades de apoyo no técnicas tiene en cuenta la finalidad del dispositivo de IoT y los usos previstos. Estas acciones permiten que los clientes

comprendan e identifiquen más fácilmente cómo se construyen los dispositivos de IoT para atender sus necesidades de seguridad cibernética, así como las expectativas de los fabricantes sobre cómo debe utilizarse el dispositivo de IoT de forma segura. La figura 1 muestra las cuatro capacidades de apoyo no técnicas incluidas en esta línea de base.

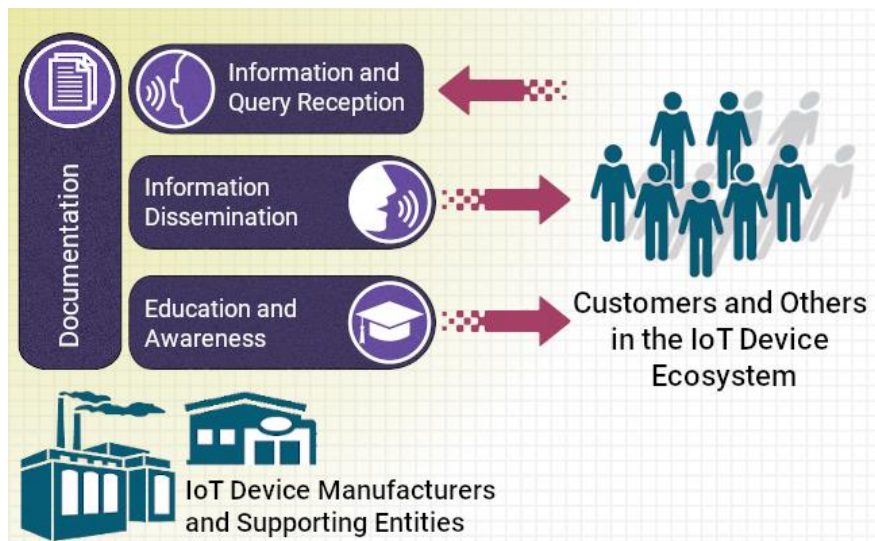


Imagen 1: Cómo utilizarán los clientes y otras personas del ecosistema de dispositivos de IoT las capacidades de la línea de base si las proporcionan los fabricantes de dispositivos de IoT y las entidades de apoyo.

La *documentación* recopila información que los clientes potenciales y otras personas del ecosistema pueden necesitar saber sobre los dispositivos de IoT y las formas en que pueden protegerse, así como los datos y sistemas asociados. Dicha documentación también suele ser necesaria antes de la compra y a lo largo del ciclo de vida del dispositivo IoT para el cliente y otras personas del ecosistema (por ejemplo, auditores y evaluadores). Esta documentación respalda el tratamiento adecuado del riesgo, el cumplimiento y la garantía desde perspectivas internas y externas cuando el dispositivo de IoT y los sistemas asociados se implementan en el entorno del cliente. Tal y como se muestra en la Figura 1, la documentación actúa como pilar de apoyo para otras capacidades no técnicas. Esto se debe a que otras capacidades no técnicas, incluidas las de la línea de base de apoyo no técnico de IoT, utilizarán la información capturada a través de la documentación para personalizar su entrega.

La *recepción de información y consultas* se produce después de la compra y permite que los clientes y otras personas del ecosistema (p. ej., investigadores, organizaciones de calificación de productos) envíen preguntas y otra información relacionada con la seguridad del dispositivo de IoT y los sistemas asociados. El fabricante y las partes de apoyo pueden entonces responder. La recepción de información y consultas puede ayudar a los clientes y a otras personas de diversas maneras a lo largo del ciclo de vida de un dispositivo de IoT, por ejemplo, permitiendo a los fabricantes y a las entidades de apoyo de terceros a que adapten y actualicen sus servicios de apoyo (p. ej., proporcionados a través de otras capacidades de apoyo no técnicas) a las necesidades y objetivos de seguridad cibernética de los clientes.

La *divulgación de la información* permite que la información siga llegando a los clientes y a otras personas del ecosistema sobre la seguridad cibernética de sus dispositivos de IoT y sistemas

asociados. Los clientes y otros se beneficiarán de 1) la divulgación de vulnerabilidades de seguridad cibernética recién descubiertas para el dispositivo, los sistemas y el software asociados, etc. y 2) notificaciones sobre actualizaciones de dispositivos de IoT, como actualizaciones de software, cambios de algoritmos, nuevos protocolos o cambios en los proveedores que utiliza el fabricante para actualizar la seguridad cibernética, que pueden afectar a los riesgos de seguridad cibernética.¹

La *sección Educación y concienciación* proporciona el contenido educativo necesario para ayudar a los clientes y a otras personas en el uso seguro y la protección de los dispositivos de IoT y los sistemas, software y hardware asociados. Al hacer que los clientes y otras personas del ecosistema conozcan mejor cómo proteger los dispositivos de IoT y cómo utilizar de la manera más eficaz las capacidades de seguridad cibernética del dispositivo, los fabricantes pueden ayudar a reducir el número de ocurrencias y la gravedad relacionada con los compromisos de los dispositivos de IoT, frustrar los ataques contra los dispositivos y reducir el número de vulnerabilidades que se explotan y conducen a dispositivos comprometidos.

Los clientes son los destinatarios típicos de las capacidades de apoyo no técnicas, pero es posible que algunos clientes no puedan utilizar estas capacidades de apoyo no técnicas directamente. En este último caso, la capacidad podría ser empleada por otras entidades del ecosistema de dispositivos de IoT (p. ej., proveedores, organizaciones comerciales o profesionales, grupos de defensa y medios de comunicación tecnológicos) para ayudar a los clientes a atender sus necesidades y objetivos.

Esta línea de base se ha desarrollado tras revisar diversos documentos de orientación de diversas fuentes y recibir contribuciones de las partes interesadas. Representa un esfuerzo coordinado para elaborar una definición de capacidades comunes, no una lista exhaustiva. La base de referencia tiene como objetivo ser un punto de partida flexible. Los fabricantes y las partes interesadas pueden utilizar la base de referencia de capacidades de apoyo no técnicas de IoT en el contexto de las actividades de NISTIR 8259 que les resulten apropiadas. Es importante señalar que los fabricantes y terceros de apoyo deben implementar las capacidades de apoyo no técnicas que respalden las necesidades de gestión de riesgos de los clientes del dispositivo de IoT dentro de su ecosistema digital previsto. De esta manera, cada una de las capacidades de apoyo no técnicas de la línea de base se implementará de forma consistente con las necesidades y expectativas de dichos clientes. Si son necesarias capacidades de apoyo adicionales para permitir el uso seguro de los dispositivos, se alienta a las organizaciones a considerar la definición de capacidades de apoyo adicionales que se adapten mejor a su(s) caso(s) de uso.

¹ Un recurso que apoya tanto la Recepción de Información como la Difusión de Información a otros en el ecosistema sobre vulnerabilidades se encuentra en el *Borrador NIST SP 800-216: Directrices Federales sobre la Divulgación de Vulnerabilidades [17]*. Este documento recomienda directrices para establecer un marco federal de divulgación de vulnerabilidades y destaca la importancia de gestionar adecuadamente los informes de vulnerabilidades y comunicar la minimización o eliminación de vulnerabilidades.

2 Base de referencia de las capacidades de apoyo no técnicas de IoT

La tabla 1 define la línea base de las capacidades de apoyo no técnicas de los dispositivos de IoT que, en combinación con la línea base de las capacidades (técnicas) de seguridad cibernética de los dispositivos de NISTIR 8259A, pueden hacer posible la seguridad de un dispositivo de IoT. La siguiente tabla se ha elaborado a partir de los conceptos de la Sección 4 de NISTIR 8259, que destaca la importancia de la comunicación con los clientes y otras personas del ecosistema de dispositivos de IoT acerca de la seguridad cibernética, y de la Sección 3, que proporciona muchos ejemplos de información que los clientes y otras personas pueden necesitar saber acerca de los dispositivos de IoT o del diseño del dispositivo.

La Tabla 1 es un punto de partida de alto nivel para que los fabricantes de dispositivos de IoT comprendan cómo pueden tener que planificar y apoyar las necesidades y objetivos de seguridad cibernética del cliente de forma no técnica. Las dificultades de la fabricación de dispositivos de IoT pueden hacer que organizaciones distintas del fabricante del dispositivo proporcionen apoyo crítico de seguridad cibernética, como algunas o todas las capacidades de apoyo no técnicas descritas en esta publicación. Por lo tanto, el objetivo de esta guía incluye a las partes de apoyo (p. ej., proveedor de servicios en la nube y proveedor de servicios contratado) que pueden desempeñar un papel en una o más de las acciones de la Tabla 1, además del fabricante.

Las capacidades de apoyo no técnicas de la Tabla 1 describen al destinatario del valor de la capacidad como el *cliente* (es decir, aquellos con los que se realizan las *comunicaciones*). Esto se deriva de la hipótesis de que el cliente de un dispositivo de IoT tendrá necesidades, objetivos y responsabilidades de seguridad cibernética relacionados con el dispositivo de IoT. Para un cliente o caso de uso específico, puede haber otras personas o entidades del ecosistema de dispositivos de IoT que pueden formar parte de esa comunicación. Por ejemplo, un cliente empresarial puede contar con varios contratistas o entidades de apoyo, así como con empleados a los que puede ser necesario comunicar la información descrita en la tabla. Alternativamente, el propietario de un edificio que incorpore dispositivos de IoT necesitará transmitir información a los inquilinos del edificio que utilicen dichos dispositivos de IoT. En este caso, también hay que señalar cómo los futuros propietarios/usuarios de los dispositivos de IoT (es decir, los futuros inquilinos) pueden no ser considerados *clientes* en el sentido tradicional. Por último, para algunos sectores, además del cliente, puede haber entidades sólidas del ecosistema de terceros (p. ej., revisores y evaluadores de productos, minoristas y proveedores) que pueden utilizar capacidades de apoyo no técnicas para ayudar a mejorar la seguridad cibernética para el sector en general.

Las acciones específicas enumeradas en la tabla pretenden reflejar las acciones típicas que muchos clientes y otros en el ecosistema de dispositivos de IoT esperan que los fabricantes y las partes de apoyo tomen para apoyar las necesidades y objetivos de seguridad cibernética. Los fabricantes pueden elegir y personalizar las capacidades no técnicas en función de los casos de uso previstos y de los clientes del dispositivo de IoT, con ejemplos y justificaciones proporcionados para proporcionar información adicional sobre las expectativas de los clientes o por qué estas acciones son importantes. Al igual que con NISTIR 8259A, se necesitaría más contexto para articular capacidades de apoyo no técnicas específicas. Pueden ser necesarios otros tipos de capacidades de apoyo no técnicas para abordar mejor el contexto del sistema en el que se utiliza el dispositivo de IoT y también en consideración de los riesgos de seguridad

cibernética del sistema² de cada organización usuaria de dispositivos de IoT. Las organizaciones que decidan adoptar las capacidades no técnicas básicas de referencia para cualquiera de los dispositivos de IoT que produzcan, integren o adquieran tienen una flexibilidad considerable a la hora de identificar las acciones para implementar aquellas capacidades que puedan abordar con mayor eficacia el uso de dispositivos de IoT dentro del propio sistema de los clientes y sus objetivos y finalidad para el uso de dispositivos de IoT.

Cada fila de la Tabla 1 abarca una de las capacidades de apoyo no técnicas del dispositivo en la línea base de capacidades de apoyo no técnicas de IoT:

- La primera columna describe la capacidad de apoyo no técnica.
- La segunda columna presenta una lista numerada de acciones comunes dentro de esa capacidad de apoyo. Se refieren a acciones que una organización que implanta la capacidad de apoyo no técnica utilizaría con frecuencia (pero no siempre) para lograr la capacidad. Es importante comprender que las acciones no pretenden ser exhaustivas ni se presentan en un orden determinado.³
- La tercera columna explica los motivos por los que se necesita la capacidad de apoyo no técnico.
- La última columna enumera ejemplos de referencia de IoT que indican fuentes existentes de orientación sobre seguridad cibernética de dispositivos IoT que especifican una capacidad similar o relacionada. Dado que la tabla sólo cubre los aspectos básicos de las capacidades, las referencias pueden ser muy valiosas para entender cada capacidad con más detalle y aprender a implementar cada capacidad de una manera razonable. A continuación se indican las referencias utilizadas en la Tabla 1:
 - **AGELIGHT:** Grupo Asesor sobre confianza digital AgeLight, "Kit de herramientas de riesgos y arquitectura de seguridad de IoT v4.0" [7].
 - **CTA:** Asociación de Tecnología de Consumo, «Instituto Nacional Estadounidense de Normalización (ANSI)/Norma CTA - Norma de seguridad cibernética de referencia para dispositivos y sistemas de dispositivos: ANSI/CTA-2088" [8]
 - **CSDE:** Consejo para la Seguridad de la Economía Digital (CSDE), "El Consenso C2 sobre las Capacidades de Línea Base de Seguridad de Dispositivos de IoT" [9]
 - **ETSI:** Instituto Europeo de Normas de Telecomunicaciones, "Seguridad cibernética para el Internet de las cosas de los consumidores: Requisitos básicos v2.1.0" [10].
 - **IoTSF:** Fundación de Seguridad de IoT (IoTSF), "Marco de Cumplimiento de Seguridad de IoT v2.1" [11]

² Tenga en cuenta que las "organizaciones de usuarios" podrían ser diferentes de la "organización de clientes". Por ejemplo, un sistema de calefacción, ventilación y aire acondicionado conectado puede ser adquirido por el propietario del edificio (organización del cliente), pero utilizado por los inquilinos del edificio (usuarios).

³ Estas acciones comunes mencionan con frecuencia los datos típicos implicados; sin embargo, los elementos de datos específicos implicados en muchas de estas acciones pueden variar considerablemente debido a la variedad de dispositivos de IoT disponibles.

Tabla 1: Capacidades de apoyo no técnicas

Capacidad de apoyo no técnica	Acciones comunes	Justificación	Ejemplos de Referencia de IoT
<p>Documentación Capacidad del fabricante y/o de la entidad de apoyo del fabricante, para crear, recopilar y almacenar información pertinente a la seguridad cibernética del dispositivo de IoT antes de la compra por parte del cliente, y a lo largo del desarrollo de un dispositivo y su posterior ciclo de vida.</p>	<ol style="list-style-type: none"> 1. Documentar las suposiciones hechas durante el proceso de desarrollo y otras expectativas relacionadas con el dispositivo de IoT, tales como: <ol style="list-style-type: none"> a. Clientes y casos de uso previstos b. Uso y características físicas c. Acceso a la red y requisitos (p. ej., requisitos de ancho de banda) d. Datos creados y manejados por el dispositivo e. Entradas y salidas de datos previstas (incluidos los códigos de error, frecuencia, tipo/forma, gama de valores aceptables, etc.) f. Requisitos de seguridad cibernética asumidos para el dispositivo de IoT g. Leyes y reglamentos que cumplen el dispositivo de IoT y las actividades de apoyo relacionadas h. Vida útil prevista, costos de seguridad cibernética anticipados relacionados con el dispositivo de IoT (p. ej., precio del mantenimiento) y plazo de apoyo 2. Documentar las capacidades de seguridad cibernética del dispositivo, como las detalladas en NISTIR 8259A, que se implementan en el dispositivo de IoT y cómo configurarlas y utilizarlas. 3. Documentar el diseño del dispositivo y las consideraciones de apoyo relacionadas con el dispositivo de IoT, tales como:⁴ <ol style="list-style-type: none"> a. Plataforma de IoT⁵ utilizada en el desarrollo y funcionamiento del dispositivo de IoT y documentación relacionada b. Protección de los componentes de software y hardware del dispositivo de IoT (por ejemplo, arranque seguro, raíz de confianza de hardware y enclave seguro). c. Consideración de los riesgos conocidos relacionados con el dispositivo de IoT y los posibles usos indebidos conocidos d. Desarrollo de software seguro y prácticas utilizadas en la cadena de suministro e. Acreditación, certificación y/o resultados de la evaluación de prácticas relacionadas con la seguridad cibernética. 	<ul style="list-style-type: none"> • Esta capacidad apoya la difusión de información y la educación y concienciación. • Los fabricantes y/o las entidades de apoyo deben considerar la documentación a lo largo de su ciclo de vida de desarrollo con el fin de capturar la información pertinente para la seguridad cibernética cuando esté disponible con el fin de garantizar el acceso a esta información cuando sea necesario. La documentación comenzará como recursos internos para un fabricante y/o entidad de apoyo que pueden utilizarse de diversas maneras. • La documentación de la información de seguridad cibernética es fundamental para la evaluación de riesgos que un fabricante debe realizar (como se discute en NISTIR 8259). • La documentación de la información sobre seguridad cibernética puede proporcionarse con el fin de ayudar a los clientes potenciales de dispositivos de IoT a tomar decisiones de compra. Las organizaciones de clientes pueden exigir dicha documentación a fin de garantizar que el dispositivo de IoT cumplirá todos los requisitos de seguridad cibernética de la organización del cliente. • La documentación proporciona una importante fuente de información sobre seguridad cibernética que ayuda a permitir el uso seguro del dispositivo de IoT por parte de los clientes. • La documentación también puede ser importante para auditorías, homologaciones u otras certificaciones. • La documentación acerca de los requisitos de mantenimiento, especialmente en relación con las partes de apoyo contratadas por el fabricante y el proveedor para realizar el mantenimiento, los cambios de dispositivos, etc., apoya la necesidad del fabricante, la entidad de apoyo y/o los clientes de planificar adecuadamente las actividades de mantenimiento. 	<ul style="list-style-type: none"> • AGELIGHT: 11, 12 • ETSI: Disposición 4.1 • IoTTSF: 2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.3.7, 2.4.12.5 • CSDE: 5.2.3

Esta publicación puede obtenerse gratuitamente en: <https://doi.org/10.6028/NIST.IR.8259B>

Capacidad de apoyo no técnica	Acciones comunes	Justificación	Ejemplos de Referencia de IoT
Documentación (continuación)	4. Documentar los requisitos de mantenimiento para el dispositivo de IoT, tales como: <ul style="list-style-type: none"> a. Expectativas de mantenimiento de seguridad cibernética e instrucciones o procedimientos asociados para el cliente (p. ej., gestión de cuentas, actividades de mantenimiento locales y/o remotas, y plan de gestión de vulnerabilidades/parches). b. Cuándo se llevará a cabo el mantenimiento por las partes de apoyo que necesitarán acceso (remoto o in situ) a los dispositivos de IoT del cliente y sus requisitos contractuales de seguridad de la información c. Consideraciones de seguridad cibernética del proceso de mantenimiento (p. ej., cómo se mantienen confidenciales los datos del cliente no relacionados con el proceso de mantenimiento, incluso para los encargados del mantenimiento) 	<ul style="list-style-type: none"> • La documentación de la información sobre seguridad cibernética permite comprender mejor los riesgos potenciales relacionados con el dispositivo de IoT, lo que puede informar a los clientes y a otros en el ecosistema de dispositivos de IoT y orientar el apoyo continuo de mitigación de riesgos. • La documentación ayuda al personal con la responsabilidad de proteger los dispositivos de IoT dentro del sistema a comprender la implementación y el funcionamiento de los controles y a evitar el uso indebido y el compromiso por parte de entidades no autorizadas. • La documentación puede utilizarse para proporcionar información sobre la gestión del riesgo de la cadena de suministro, la respuesta ante incidentes y otras funciones críticas de seguridad cibernética, y para respaldarlas. 	(consulte más arriba)

Esta publicación puede obtenerse gratuitamente en: <https://doi.org/10.6028/NIST.IR.8259B>

⁴ Aunque esta información sería proporcionada por una lista de materiales de software (SBOM, por sus siglas en inglés), lo que se está discutiendo aquí es significativamente menos de lo que generalmente se entiende por una SBOM. Encontrará más información sobre la SBOM en <https://www.ntia.gov/SBOM>.

⁵ Una plataforma de IoT suele ser una herramienta basada en SaaS proporcionada/alojada por un proveedor externo que se utiliza para apoyar la gestión de dispositivos y puntos finales de IoT, la conectividad y la gestión de redes, la gestión, el procesamiento y el análisis de datos, el desarrollo de aplicaciones, la seguridad cibernética, el control de acceso, el monitoreo, el procesamiento de eventos y la interfaz/integración. La documentación sobre dicho tercero puede proporcionar información importante sobre las prácticas y vulnerabilidades de seguridad cibernética de la cadena de suministro para que el usuario de IoT pueda determinar con mayor precisión los riesgos relacionados con el uso de una plataforma de IoT.

Capacidad de apoyo no técnica	Acciones comunes	Justificación	Ejemplos de Referencia de IoT
<p>Recepción de información y consultas: La capacidad del fabricante y/o entidad de apoyo para recibir información y consultas del cliente y otros relacionados con la seguridad cibernética del dispositivo de IoT.</p>	<ol style="list-style-type: none"> 1. La capacidad del fabricante y/o entidad de apoyo para recibir información sobre mantenimiento y vulnerabilidades (p. ej., capacidades de notificación de errores y programas de recompensas por errores) de sus clientes y otros en el ecosistema de dispositivos de IoT. 2. La capacidad del fabricante y/o entidad de apoyo para responder a las consultas de clientes y terceros sobre seguridad cibernética del dispositivo de IoT (p. ej., atención al cliente). 	<ul style="list-style-type: none"> • Esta capacidad proporciona información de los clientes y otros en el ecosistema de dispositivos de IoT para que el fabricante la utilice en las capacidades de apoyo no técnicas de Difusión de Información y Educación y Concienciación. • Es posible que los clientes y otras personas del ecosistema de dispositivos de IoT deseen, o estén obligados, a informar sobre las vulnerabilidades que identifiquen en un dispositivo de IoT. • Los fabricantes pueden utilizar los informes de consultas y vulnerabilidades comunes para identificar maneras de mejorar la seguridad cibernética del dispositivo de IoT. • Algunos clientes pueden necesitar apoyo adicional para suministrar y utilizar de forma segura un dispositivo de IoT. • Apoya las responsabilidades de los clientes, relacionadas con la seguridad cibernética, como permitirles obtener información especializada sobre seguridad cibernética que puede utilizarse de forma proactiva para la seguridad cibernética (p. ej., inteligencia y mitigación de amenazas, investigaciones forenses digitales y reaprovisionamiento y eliminación seguros). 	<ul style="list-style-type: none"> • CTA: VUL-002, VUL-003 • AGELIGHT: 9 • ETSI: Disposición 5.2-1 • IoTTSF: 2.4.3.11, 2.4.3.12 • CSDE: 5.2.1, 5.2.2

Esta publicación puede obtenerse gratuitamente en: <https://doi.org/10.6028/NIST.IR.8259B>

Capacidad de apoyo no técnica	Acciones comunes	Justificación	Ejemplos de Referencia de IoT
<p>Divulgación de información: La capacidad del fabricante y/o entidad de apoyo para difundir y distribuir (p. ej., al cliente u otros en el ecosistema del dispositivo de IoT) información relacionada con la seguridad cibernética del dispositivo de IoT.</p>	<ol style="list-style-type: none"> 1. Los procedimientos de apoyo a la capacidad del fabricante y/o entidad de apoyo para alertar a los clientes del dispositivo de IoT y a otros sobre la información pertinente en materia de seguridad cibernética, tales como: <ol style="list-style-type: none"> a. Documentación aplicable capturada durante el diseño y desarrollo del dispositivo de IoT b. Condiciones de soporte de las actualizaciones de software (p. ej., frecuencia de las actualizaciones y mecanismo(s) de aplicación) y aviso de disponibilidad y/o aplicación de las actualizaciones de software c. Fin del plazo de soporte o funcionalidad del dispositivo de IoT d. Operaciones de mantenimiento necesarias e. Alertas de seguridad cibernética y vulnerabilidad e información sobre la resolución de cualquier vulnerabilidad f. Una descripción general de las prácticas y salvaguardias de seguridad de la información utilizadas por el fabricante y/o la entidad de apoyo g. Resultados de la acreditación, certificación y/o evaluación de las prácticas relacionadas con la seguridad cibernética del fabricante y/o la entidad de apoyo h. Un informe o resumen de evaluación de riesgos para la postura de riesgo del entorno empresarial del fabricante. 2. Los procedimientos de apoyo a la capacidad del fabricante y/o entidad de soporte para notificar a los clientes de eventos relacionados con la seguridad cibernética e información relacionada con un dispositivo de IoT a lo largo del ciclo de vida de soporte, tales como: <ol style="list-style-type: none"> a. Nuevas vulnerabilidades de dispositivos de IoT, detalles asociados y acciones de mitigación b. Descubrimiento de brechas relacionadas con un dispositivo de IoT utilizado por los clientes y explicaciones sobre cómo realizar las correcciones o acciones asociadas para evitar brechas similares en otros dispositivos. 	<ul style="list-style-type: none"> • Esta capacidad respalda la seguridad cibernética continua del dispositivo al mantener a los clientes informados de los desarrollos y las nuevas capacidades de información y configuración después de que se haya desarrollado y proporcionado la documentación inicial. La divulgación de la información permite el soporte, la administración y el mantenimiento necesarios para garantizar un rendimiento y una seguridad cibernética eficaces y eficientes de los dispositivos y sistemas de IoT. • Las organizaciones de clientes pueden necesitar estar informadas acerca de las actividades relacionadas con la seguridad cibernética en el dispositivo de IoT, como actualizaciones de software, cambios de algoritmos, nuevos protocolos o cambios en los proveedores utilizados por el fabricante para actualizar la seguridad cibernética, especialmente si el dispositivo de IoT es crítico para sus operaciones. • Las organizaciones de clientes querrán mantenerse informadas sobre la seguridad cibernética de los dispositivos de IoT para permitirles ajustar sus mitigaciones y mantener un nivel adecuado de garantía de riesgo. • Las organizaciones de clientes pueden necesitar conocer las prácticas de seguridad cibernética del fabricante y/o de las entidades de apoyo que han hecho o tendrán acceso ocasional o continuo a los dispositivos de IoT para permitirles asegurarse de que las otras partes no aumenten inaceptablemente el riesgo de seguridad cibernética del cliente. • Las organizaciones de clientes pueden utilizar esta información para conocer el compromiso del fabricante con la seguridad de la información y determinar el nivel de riesgo considerado por el fabricante en relación con el dispositivo. • Las organizaciones de clientes pueden ver certificaciones, acreditaciones y evaluaciones de seguridad cibernética para lo que suele ser una garantía de terceros de información aceptable que describe prácticas de seguridad cibernética, de redes, de aplicaciones y relacionadas. 	<ul style="list-style-type: none"> • CTA: REP-005 EoL/EoS-001, EoL/EoS-002, DIN-001, DIN-002 • AGELIGHT: 1, 4, 20, 21, 22, 23, 32, 36 • ETSI: Disposiciones 5.3-11, 5.3-12, 5.3-13, 5.3-14, 5.3-16 • IoTSF: 2.4.3.9, 2.4.3.14, 2.4.5.35, 2.4.5.36 • CSDE: 5.2.3

Capacidad de apoyo no técnica	Acciones comunes	Justificación	Ejemplos de Referencia de IoT
<p>Educación y concienciación: La capacidad del fabricante y/o entidad de apoyo para crear conciencia y educar a los clientes y otros en el ecosistema de dispositivos de IoT sobre información relacionada con la seguridad cibernética, consideraciones, características, etc. del dispositivo de IoT.</p>	<ol style="list-style-type: none"> 1. Educar a los clientes del dispositivo de IoT y a otros en el ecosistema sobre la presencia y el uso de las capacidades de seguridad cibernética del dispositivo. Por ejemplo, puede ser importante educar a los clientes y a otros sobre: <ol style="list-style-type: none"> a. Cómo utilizar los identificadores del dispositivo b. Cómo cambiar los ajustes de configuración c. Cómo configurar y utilizar la funcionalidad de control de acceso d. Cómo utilizar la funcionalidad de actualización de software, incluidos aspectos como la validación de actualizaciones y/o la reversión que pueden formar parte de la capacidad de seguridad cibernética del dispositivo. 2. Educar a los clientes y a otras personas sobre cómo se puede volver a suministrar o desechar un dispositivo de IoT de forma segura. 3. Hacer que los clientes y otras personas sean conscientes de sus responsabilidades en materia de seguridad cibernética relacionadas con el dispositivo de IoT y cómo las responsabilidades pueden ser compartidas entre ellos y otros, como el fabricante del dispositivo de IoT. (p. ej., en relación con el mantenimiento del dispositivo de IoT) 4. Haga que los clientes y otros conozcan las hipótesis y expectativas clave relacionadas con la seguridad cibernética del dispositivo de IoT que se documentaron, a lo largo de todo el ciclo de vida de uso de los dispositivos de IoT, teniendo en cuenta la finalidad del dispositivo de IoT y los usos previstos. Dichos supuestos deben incluir las dependencias clave del dispositivo de IoT que afectan a la seguridad cibernética (p. ej., los requisitos de conectividad y el uso de servicios de terceros cuando está en funcionamiento). 5. Educar a los clientes y a otras personas sobre cómo realizar copias de seguridad de los datos recopilados o extraídos del dispositivo de IoT y sobre cómo acceder a los datos almacenados en la nube o en otros repositorios. 6. Educar a los clientes y a otras personas sobre las opciones de gestión de vulnerabilidades (p. ej., gestión de configuración y parches y antimalware) disponibles para el dispositivo de IoT o el sistema asociado que podrían utilizar los clientes. 	<ul style="list-style-type: none"> • Esta capacidad respalda el aprovisionamiento seguro y la asistencia continua en materia de seguridad cibernética. • En el caso de los dispositivos de IoT con una amplia gama de casos de uso, algunos clientes pueden necesitar más capacitación que otros para aprovisionar y utilizar de forma segura un dispositivo de IoT. • La complejidad de los sistemas, dispositivos y casos de uso de IoT significa que es importante que los fabricantes tengan conciencia y eduquen a los clientes y a otras personas sobre la seguridad cibernética de sus dispositivos de IoT. • Las regulaciones y leyes existentes exigen que los fabricantes y/o entidades de apoyo proporcionen a los clientes acceso a los datos que los fabricantes y/o entidades de apoyo tienen sobre ellos y también que hagan que dichos datos sean portátiles para que los clientes puedan tomar esos datos y utilizarlos en otros lugares. • Capacitación reforzada mediante comunicaciones de concienciación ocasionales y continuas. Algunos ejemplos de capacitación son: <ul style="list-style-type: none"> • concienciación sobre seguridad cibernética, • instrucción en el uso de las capacidades de seguridad cibernética, y • comprensión de los soportes de responsabilidades relevantes para la seguridad cibernética. <p>La capacitación puede resultar en un uso más seguro del dispositivo de IoT y los sistemas asociados y prevenir errores que podrían resultar en incidentes de seguridad cibernética. Una capacitación eficaz también puede reducir el número de vulnerabilidades que se aprovechan y conducen a dispositivos comprometidos.</p>	<ul style="list-style-type: none"> • AGELIGHT: 20, 21, 22, 23, 32, 34, 36 • ETSI: Disposiciones 5.2-1, 5.11-3, 5.12-2, 5.12-3, 6-1, 6-5 • IoTTSF: 2.4.12.9, 2.4.12.10, 2.4.12.11, 2.4.12.12 • CSDE: 5.2.3

Referencias

- [1] Fagan M, Megas KN, Scarfone K, Smith M (2020) Actividades básicas de seguridad cibernética para fabricantes de dispositivos de IoT (Foundational Cybersecurity Activities for IoT Device Manufacturers). (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8259 del NIST. ((National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259.) <https://doi.org/10.6028/NIST.IR.8259>
- [2] Fagan M, Megas KN, Scarfone K, Smith M (2020) Línea de base del núcleo de la capacidad de seguridad cibernética de los dispositivos de IoT (IoT Device Cybersecurity Capability Core Baseline) (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD) (National Institute of Standards and Technology, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8259A del NIST. <https://doi.org/10.6028/NIST.IR.8259A>
- [3] Boeckl K, Fagan M, Fisher W, Lefkowitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (2018) Consideraciones para gestionar los riesgos de seguridad cibernética y privacidad de Internet de las Cosas (IoT) (Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks). (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8228 del NIST ((National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228). <https://doi.org/10.6028/NIST.IR.8228>
- [4] Fagan M, Megas, KN, Marron, J, Brady KG, Jr, Cuthill BB, Herold R (2020) Creación de un perfil utilizando la línea de base básica de IoT y la línea de base no técnica (Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline). (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Borrador del Informe Interinstitucional o Interno (IR) 8259C del NIST ((National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C). <https://doi.org/10.6028/NIST.IR.8259C-draft>
- [5] Instituto Nacional de Normas y Tecnología (2020) Catálogos de requisitos de seguridad cibernética para dispositivos de IoT (National Institute of Standards and Technology (2020) IoT Device Cybersecurity Requirement Catalogs). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD). Disponible en <https://github.com/usnistgov/IoT-Device-Cybersecurity-Requirement-Catalogs>.
- [6] Iniciativa de transformación de la fuerza laboral (2012) Guía para realizar Evaluaciones de riesgo (Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments). (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Publicación Especial del NIST (SP) 800-30, Rev. 1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.) <https://doi.org/10.6028/NIST.SP.800-30r1>
- [7] Grupo Asesor sobre confianza digital AgeLight (2020) Kit de herramientas de riesgos y arquitectura de seguridad de IoT v4.0. Actualizado el 24 de febrero de 2020. Disponible en <https://www.agelight.com/iot>
- [8] Asociación de Tecnología de Consumo (2020) ANSI/CTA-2088 - *Estándar básico de seguridad cibernética para dispositivos y sistemas de dispositivos* (Asociación de Tecnología de Consumo, Arlington, VA). (Consumer Technology Association (2020) ANSI/CTA-2088 - Baseline Cybersecurity Standard for Devices and Device Systems (Consumer Technology Association, Arlington, VA). Disponible en <https://csde.org/projects/c2-consensus/>
- [9] Consejo para la Seguridad de la Economía Digital (2019) El Consenso C2 sobre las Capacidades de Línea Base de Seguridad de Dispositivos de IoT. Disponible en https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

- [10] Instituto Europeo de Normas de Telecomunicación (2020) ETSI EN 303 645 v2.1.0 - *Seguridad cibernética para la Internet de las cosas de los consumidores: (European Telecommunications Standards Institute (2020) ETSI EN 303 645 v2.1.0 - Cyber Security for Consumer Internet of Things:)* Requisitos de línea de base (Instituto Europeo de Estándares de Telecomunicaciones, Valbonne, Francia). (*Baseline Requirements* (European Telecommunications Standards Institute, Valbonne, France). Disponible en https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- [11] Fundación de Seguridad de IoT (2020) *Marco de Cumplimiento de Seguridad de IoT v2.1. (IoT Security Foundation (2020) IoT Security Compliance Framework v2.1.)* (Fundación para la Seguridad de Internet de las Cosas, Livingston, Reino Unido). (Internet of Things Security Foundation, Livingston, Reino Unido). Disponible en <https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/>
- [12] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guía para la gestión de la configuración de sistemas de información centrada en la seguridad (Guide for Security-Focused Configuration Management of Information Systems). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD), Publicación especial (SP) 800-128 del NIST. <https://doi.org/10.6028/NIST.SP.800-128>
- [13] Joint Task Force (2020) Controles de seguridad y privacidad para sistemas de información y organizaciones (Security and Privacy Controls for Information Systems and Organizations). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD), Publicación especial (SP) 800-53, Rev. 5 del NIST. Incluye actualizaciones a partir del 10 de diciembre de 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [14] Souppaya M, Scarfone K (2013) Guía de tecnologías de gestión de parches para empresas (Guide to Enterprise Patch Management Technologies). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD), Publicación especial (SP) 800-40, Rev. 3 del NIST. <https://doi.org/10.6028/NIST.SP.800-40r3>
- [15] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recomendación para esquemas de establecimiento de claves por pares utilizando criptografía de logaritmo discreto (Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD), Publicación especial (SP) 800-56A, Rev. 3 del NIST. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- [16] Comité de Sistemas de Seguridad Nacional (2015) Glosario del Comité de Sistemas de Seguridad Nacional (CNSS, por sus siglas en inglés) (Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary). (Agencia de Seguridad Nacional, Ft. Meade, MD), Instrucción del CNSS (CNSSI N.º 4009 (National Security Agency, Ft. Meade, MD, CNSS Instruction (CNSSI) No. 4009.)). Disponible en <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- [17] Schaffer K, Mell P, Trinh H. (2021) Recomendaciones para las directrices federales sobre divulgación de vulnerabilidades (Recommendations for Federal Vulnerability Disclosure Guidelines). (National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología), Gaithersburg, MD), Resumen de la publicación especial (SP) 800-216 del NIST. <https://doi.org/10.6028/NIST.SP.800-216-draft>

Appendix A Acrónimos

A continuación, se definen algunos acrónimos y abreviaturas utilizados en este documento.

ACD	División de Seguridad Cibernética Aplicada (Applied Cybersecurity Division)
CNSS	Committee on National Security Systems (Comité de Sistemas Nacionales de Seguridad)
FISMA	Federal Information Security Modernization Act (Ley Federal de Modernización de la Seguridad de la Información)
IoT	Internet of Things (Internet de las cosas)
ITL	Information Technology Laboratory (Laboratorio de Tecnología de la Información)
IR	Internal Report (Informe interno)
MAC	Media Access Control (control de acceso a los medios)
NIST	National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología)
SBOM	Software Bill of Materials (lista de materiales de software)
SP	Special Publication (Publicación especial)

Appendix B Glosario

A continuación se definen algunos términos utilizados en este documento.

Comunicaciones	Las acciones y actividades asociadas que se utilizan para intercambiar información, proporcionar instrucciones, dar detalles, etc. En el contexto de este documento, las comunicaciones se refieren a toda la gama de actividades relacionadas con el suministro de información para apoyar el uso seguro de los dispositivos de IoT. Las comunicaciones incluyen el uso de herramientas como llamadas telefónicas, correos electrónicos, guías de usuario, clases presenciales, manuales de instrucciones, seminarios web, instrucciones escritas, vídeos, cuestionarios, documentos de preguntas frecuentes (FAQ) y cualquier otro tipo de herramienta para dichos intercambios de información.
Configuración [7, adaptado]	Las posibles condiciones, parámetros y especificaciones con las que se puede describir u organizar un sistema de información o un componente del sistema. La capacidad de Configuración de Dispositivos no define qué ajustes de configuración deben existir, simplemente que existe un mecanismo para gestionar los ajustes de configuración.
Base de referencia básica	Un conjunto de capacidades técnicas del dispositivo necesarias para apoyar los controles comunes de seguridad cibernética que protegen los dispositivos del cliente y los datos, sistemas y ecosistemas del dispositivo.
Cliente [12]	La organización o persona que recibe un producto o servicio.
Capacidad de seguridad cibernética del dispositivo	Características o funciones de seguridad cibernética que los dispositivos informáticos proporcionan a través de sus propios medios técnicos (es decir, hardware y software del dispositivo).
Identificador de dispositivo [10, adaptado]	Valor único en un contexto -un valor único dentro de un contexto específico- que se asocia a un dispositivo (por ejemplo, una cadena consistente en una dirección de red).
Entidad	Persona, dispositivo, servicio, red, dominio, fabricante u otra parte que pueda interactuar con un dispositivo de IoT.

Plataforma de IoT	Una plataforma de IoT suele ser una herramienta basada en SaaS ⁶ proporcionada/alojada por un proveedor externo que se utiliza para apoyar la gestión de dispositivos y puntos finales de IoT, la conectividad y la gestión de redes, la gestión, el procesamiento y el análisis de datos, el desarrollo de aplicaciones, la seguridad cibernética, el control de acceso, el monitoreo, el procesamiento de eventos y la interfaz/integración. La documentación sobre dicho tercero puede proporcionar información importante sobre las prácticas y vulnerabilidades de seguridad cibernética de la cadena de suministro para que el usuario de IoT pueda determinar con mayor precisión los riesgos relacionados con el uso de una plataforma de IoT.
Mantenimiento [11]	Cualquier acto que impida el fallo o mal funcionamiento del dispositivo de IoT y el equipo de apoyo o que restaure su capacidad operativa.
Capacidad de apoyo no técnica	Las capacidades de apoyo no técnicas son acciones que realiza una organización de terceros en apoyo de la seguridad cibernética de un dispositivo de IoT.
Base de referencia de las capacidades de apoyo no técnicas	La línea de base de capacidades de apoyo no técnicas es un conjunto de capacidades de apoyo no técnicas generalmente necesarias de los fabricantes u otros terceros para apoyar los controles comunes de seguridad cibernética que protegen los dispositivos de una organización, así como los datos, sistemas y ecosistemas de los dispositivos.
Software	Programas informáticos y datos asociados que pueden escribirse o modificarse de forma dinámica durante la ejecución del dispositivo (p. ej., código de aplicación, bibliotecas).
Partes de apoyo	Proveedores de servicios de sistemas externos al fabricante a través de una variedad de relaciones entre el consumidor y el productor que incluyen, pero no se limitan a: empresas conjuntas; asociaciones empresariales; acuerdos de subcontratación (es decir, a través de contratos, acuerdos interinstitucionales, acuerdos de líneas de negocio); acuerdos de licencia; y/o intercambios en la cadena de suministro. Los servicios de apoyo incluyen, por ejemplo, telecomunicaciones, servicios de ingeniería, energía, agua, software, soporte técnico y seguridad.
Plazo de soporte	El período de tiempo durante el cual el fabricante o las partes de soporte prestarán asistencia al dispositivo para acciones y materiales tales como sustituciones de piezas, actualizaciones de software, avisos de vulnerabilidad, preguntas de soporte técnico, etc.

⁶ Software como servicio

Capacitación	Enseñar a las personas los conocimientos y las habilidades y competencias pertinentes y necesarias en materia de seguridad cibernética que les permitirán comprender cómo utilizar y configurar los dispositivos de IoT para que puedan utilizarlos de la manera más segura posible.
Actualización [9]	Un parche, una actualización u otra modificación del código que corrige problemas de seguridad y/o funcionalidad del software.