

**Informe interinstitucional o interno 8259 del NIST**

**Actividades fundamentales de  
ciberseguridad para los fabricantes de  
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.8259es>

**Informe interinstitucional o interno 8259 del NIST**

# **Actividades fundamentales de ciberseguridad para los fabricantes de 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.8259es>

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 8259 del Instituto Nacional de Normas y Tecnología  
42 páginas (Mayo de 2020)

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

Es posible que en este documento se identifiquen ciertas entidades, equipos o materiales comerciales para describir adecuadamente un procedimiento o concepto experimental. Tal identificación no presupone que el NIST los recomienda o los aprueba, ni tampoco que las entidades, los materiales o los equipos son necesariamente los mejores disponibles para ese fin.

Esta publicación puede hacer referencia a otras publicaciones que el NIST esté preparando actualmente de acuerdo con sus responsabilidades estatutarias asignadas. Los organismos federales pueden usar la información de esta publicación, así como los conceptos y las metodologías, incluso antes de concluir esas publicaciones complementarias. Sin embargo, hasta que se complete cada publicación, los requisitos, las directrices y los procedimientos actuales seguirán vigentes donde se hayan establecido. Con fines de planificación y transición, es conveniente que los organismos federales sigan de cerca la preparación del NIST de estas nuevas publicaciones.

Recomendamos a las organizaciones que revisen todos los borradores de las publicaciones durante los períodos en los que se someten a comentarios públicos y que aporten sugerencias al NIST. Muchas de las publicaciones del NIST sobre ciberseguridad, que no sean las antes mencionadas, están disponibles en <https://csrc.nist.gov/publications>.

**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](mailto:iotsecurity@nist.gov)

Todo comentario está sujeto a publicación en virtud de la Ley de libertad de información (FOIA, por sus siglas en inglés).

**Disclaimer**

This document was translated by the U.S. Department of State, Office of Language Services with support from the [Digital Connectivity and Cybersecurity Partnership \(DCCP\)](#).

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.8259>.

## **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**

Los dispositivos de internet de las cosas (IoT) suelen carecer de las capacidades de ciberseguridad de dispositivo que los clientes (organizaciones y personas) pueden usar para mitigar sus riesgos a la ciberseguridad. Los fabricantes pueden ayudar a los clientes al hacer más protegibles los dispositivos de IoT que fabrican equipándolos con la funcionalidad de ciberseguridad necesaria y proporcionando a los clientes la información relacionada con la ciberseguridad que necesitan. Esta publicación describe las actividades recomendadas para la ciberseguridad que los fabricantes deben considerar llevar a cabo antes de que sus dispositivos de IoT se vendan a los clientes. Con estas actividades fundamentales de ciberseguridad, los fabricantes pueden disminuir las iniciativas de ciberseguridad que necesitan los clientes. A su vez, esto puede reducir la incidencia y gravedad de los peligros para los dispositivos de IoT y de los ataques perpetrados con el uso de dispositivos comprometidos.

### **Palabras clave**

Riesgo a la ciberseguridad, internet de las cosas (IoT), fabricación, gestión de riesgos, mitigación de riesgos, dispositivos informáticos protegibles y desarrollo de software.

### **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 ayudar a los clientes de dispositivos de IoT que usan esos dispositivos y que deseen conocer mejor las capacidades de ciberseguridad de dispositivo que ofrecen y la información sobre ciberseguridad que los fabricantes pueden proporcionar.

## **Información sobre marcas comerciales**

Todas las marcas comerciales o marcas registradas pertenecen a sus respectivas organizaciones.

### **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.*

## Resumen ejecutivo

Los fabricantes están produciendo variedades y cantidades increíbles de dispositivos con servicio de internet ampliamente conocidos como internet de las cosas (IoT). Muchos de estos dispositivos de IoT no se adaptan a las definiciones estándar de los dispositivos de tecnología de la información (TI) que se han usado como base para definir las capacidades de ciberseguridad de dispositivo (por ejemplo, teléfonos inteligentes, servidores, computadoras portátiles). Los dispositivos de IoT a los que se refiere esta publicación tienen al menos un transductor (sensor o actuador) para interactuar directamente con el mundo físico, y al menos una interfaz de red (por ejemplo, Ethernet, wifi, Bluetooth, evolución a largo plazo [LTE, por sus siglas en inglés], Zigbee, banda ultraancha [UWB, por sus siglas en inglés]) que los conecta con el mundo digital. Los dispositivos de IoT mencionados en esta publicación pueden funcionar por sí solos, aunque es posible que dependan de otros dispositivos específicos (por ejemplo, un concentrador de IoT) o sistemas (por ejemplo, una nube) para algunas funcionalidades.

Muchos dispositivos de IoT cuentan con funcionalidad informática, almacenamiento de datos y conectividad de red junto con funcionalidad relacionada con los equipos que anteriormente carecían de estas funciones informáticas (por ejemplo, electrodomésticos inteligentes). A su vez, estas funciones habilitan eficiencias y capacidades tecnológicas nuevas en el equipo, como acceso remoto para vigilar, configurar y resolver problemas. La IoT también puede habilitar la recolección y el análisis de datos sobre el mundo físico y utilizar los resultados para tomar decisiones mejor informadas, modificar el entorno físico y prever eventos futuros [1].

Una gran cantidad de clientes (personas, empresas, organismos gubernamentales, instituciones educativas y otras organizaciones) adquieren y usan dispositivos de IoT. Lamentablemente, los dispositivos de IoT suelen carecer de las capacidades que los clientes puedan usar para mitigar sus riesgos a la ciberseguridad, como la funcionalidad que los clientes esperan normalmente que tengan sus computadoras de escritorio y portátiles, sus teléfonos inteligentes, sus tabletas y demás dispositivos de TI. Por consiguiente, es posible que los clientes de dispositivos de IoT deban seleccionar, implementar y administrar controles de ciberseguridad adicionales o nuevos, o modificar los controles que ya tienen. Para empeorar esta situación, tal vez los clientes no sepan que necesitan modificar los procesos existentes para dar cabida a las características únicas de la IoT. Como resultado, muchos dispositivos de IoT no están protegidos ante amenazas que están evolucionando y, por lo tanto, los atacantes pueden poner en peligro más fácilmente los dispositivos de IoT y utilizarlos para perjudicar a los clientes y llevar a cabo más actos maliciosos (por ejemplo, ataques de denegación de servicio distribuido [DDoS, por sus siglas en inglés]) contra otras organizaciones<sup>1</sup>.

---

<sup>1</sup> En 2017, se emitió la Orden ejecutiva 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [Fortalecimiento de la ciberseguridad de las redes y la infraestructura crítica federales] [2], para mejorar la postura y las capacidades cibernéticas del país ante amenazas cada vez más intensas. Esta orden ejecutiva encomendó al Departamento de Comercio y al Departamento de Seguridad Nacional la tarea de crear el *Enhancing Resilience Against Botnets Report* (Informe de mejora de la resiliencia contra las redes de robots) [3] para determinar la manera de impedir que los atacantes hagan uso de redes robot para perpetrar ataques de denegación de servicio distribuido (DDoS). Ese informe incluyó muchos elementos de acción, y esta publicación cumple dos de ellos: crear una referencia para las capacidades de ciberseguridad de los dispositivos de IoT y publicar prácticas de ciberseguridad para los fabricantes de dispositivos de IoT.

El objetivo de esta publicación es ofrecer a los fabricantes recomendaciones para mejorar los dispositivos de IoT que fabrican haciéndolos más *protegibles*. Esto se refiere a las *capacidades de ciberseguridad de dispositivo* (las características o funciones de ciberseguridad que los dispositivos proporcionan por sus propios medios técnicos, es decir, el hardware y el software del dispositivo) que ofrecen los dispositivos de IoT y que los clientes, sean organizaciones o personas, necesitan para protegerlos cuando los usan en sus sistemas y entornos. Los fabricantes de dispositivos de IoT también necesitarán a menudo ejecutar las acciones o prestar los servicios que sus clientes esperan o necesitan para planificar y mantener la ciberseguridad del dispositivo en sus sistemas y entornos. En esta publicación, los fabricantes de dispositivos de IoT aprenderán la manera de ayudar a los clientes de dispositivos de IoT considerando atentamente las capacidades de ciberseguridad de dispositivo que deberán incorporar en sus dispositivos y que los clientes deberán usar en la gestión de sus riesgos a la ciberseguridad.

Esta publicación describe seis actividades fundamentales de ciberseguridad recomendadas que los fabricantes deben considerar llevar a cabo para mejorar la protegibilidad de los nuevos dispositivos de IoT que fabriquen. Cuatro de las seis actividades afectan principalmente las decisiones y medidas que el fabricante toma antes de que poner a la venta un dispositivo (antes del mercadeo), y las dos actividades restantes tienen impacto principalmente en las decisiones y medidas que el fabricante toma después de la venta del dispositivo (después del mercadeo). Estas seis actividades permiten a los fabricantes proporcionar dispositivos de IoT más compatibles con las iniciativas de ciberseguridad que necesitan sus clientes, lo cual puede reducir a su vez la incidencia y gravedad de los peligros para los dispositivos de IoT y de los ataques perpetrados con el uso de dispositivos de IoT comprometidos. Estas actividades están diseñadas para adaptarse al proceso de desarrollo existente del fabricante y es posible que ya hayan sido efectuadas en su totalidad o en parte por ese proceso.

Cabe señalar que el objetivo de esta publicación es servir de base para la fabricación de dispositivos nuevos y no de los dispositivos que ya se hayan fabricado o se estén fabricando, aunque parte de la información contenida en esta publicación también podría ser aplicable a esos dispositivos.

### **Actividades que influyen principalmente antes del mercadeo**

- **Actividad 1: Identificar a los clientes probables, y definir los casos de uso previstos.** La identificación de los clientes y usuarios probables, así como de los casos de uso previstos de los usuarios finales de un dispositivo de IoT al comienzo de su diseño es indispensable para determinar las capacidades de ciberseguridad de dispositivo que este debe implementar y la manera de implementarlas.
- **Actividad 2: Investigar las necesidades y metas de ciberseguridad de los clientes.** Los riesgos de los clientes impulsan sus necesidades y metas de ciberseguridad. Los fabricantes no pueden entender ni prever completamente todos los riesgos de sus clientes. Sin embargo, los fabricantes pueden hacer que, por lo menos, sus dispositivos sean mínimamente protegibles por quienes esperan que serán los clientes de sus productos, y que los usarán de acuerdo con los casos de uso previstos.
- **Actividad 3: Determinar la manera de considerar las necesidades y metas del cliente.** Los fabricantes pueden determinar la manera de considerar esas necesidades y

metas haciendo que sus dispositivos de IoT cuenten con capacidades específicas de ciberseguridad de dispositivo para ayudar a los clientes a mitigar los riesgos a la ciberseguridad. Se proporciona la publicación complementaria del Informe interinstitucional o interno (IR, por sus siglas en inglés) 8259A del NIST, *IoT Device Cybersecurity Capability Core Baseline* [Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT] [4] como punto de partida para identificar las capacidades necesarias de ciberseguridad de dispositivo. Este informe es un conjunto de las capacidades de ciberseguridad de dispositivo que los clientes necesitarán probablemente para lograr sus metas y satisfacer sus necesidades.

- **Actividad 4: Planificar el soporte técnico adecuado a las necesidades y metas del cliente.** Los fabricantes pueden hacer que sus dispositivos de IoT sean más protegibles equipándolos con los debidos recursos de hardware y software compatibles con las capacidades de ciberseguridad de dispositivo que se desean. También deben considerar los recursos empresariales necesarios para mantener el desarrollo y soporte técnico continuo del dispositivo de IoT de forma que se satisfagan las necesidades y se logren las metas del cliente (por ejemplo, prácticas de codificación segura, respuesta a vulnerabilidades y corrección de defectos).

#### **Actividades que influyen principalmente después del mercadeo**

- **Actividad 5: Definir formas de comunicarse con los clientes.** Para muchos clientes será una ventaja que los fabricantes se comuniquen más claramente con ellos sobre los riesgos a la ciberseguridad relacionados con los dispositivos de IoT que los fabricantes estén vendiendo o hayan vendido. Esta comunicación se podría dirigir directamente al cliente o a otras personas que los representen, como proveedores de servicios de internet o proveedores de servicios de seguridad administrada, según el contexto y las funciones que desempeñen.
- **Actividad 6: Decidir lo que se comunicará a los clientes y la manera de hacerlo.** Hay muchas consideraciones potenciales de la información que un fabricante comunica a los clientes acerca de un producto de IoT particular y de la manera en que se comunica esa información. Algunos ejemplos de temas son:
  - las suposiciones relacionadas con el riesgo a la ciberseguridad que el fabricante haya hecho durante el diseño y la fabricación del dispositivo;
  - las expectativas de soporte técnico y vida útil del dispositivo, como el período de soporte previsto, el proceso que guiará el fin de vida útil, la posibilidad de que continúen las funciones del dispositivo después del fin de su vida útil, la manera en que los clientes puedan comunicar al fabricante las supuestas vulnerabilidades durante y después de que termina el soporte técnico del dispositivo y la manera en que los clientes puedan mantener la protegibilidad del dispositivo después de que termine el soporte técnico y al final de su vida útil;
  - la composición y las capacidades del dispositivo, como información sobre software, hardware, servicios, funciones y tipos de datos del dispositivo;

- las actualizaciones del software, por ejemplo, disponibilidad de las actualizaciones, cuándo, cómo y quién las distribuirá, y la manera en que los clientes pueden verificar el origen y el contenido de una actualización de software;
- las opciones de retirada del dispositivo, como la manera en que el cliente puede hacer la transferencia segura de la propiedad del dispositivo, si es transferible, y la posibilidad de que el cliente haga que el dispositivo quede inutilizable para su eliminación; y
- las capacidades de ciberseguridad de dispositivo que este ofrece, así como las funciones de ciberseguridad que pueda proporcionar un dispositivo equivalente o un servicio o sistema del fabricante.

## Índice

<b>Resumen ejecutivo.....</b>	<b>v</b>
<b>1 Introducción .....</b>	<b>1</b>
1.1 Objetivo y alcance.....	1
1.2 Estructura de la publicación.....	2
<b>2 Información general.....</b>	<b>3</b>
<b>3 Actividades del fabricante que tienen impacto en la fase anterior al     mercadeo del dispositivo de IoT.....</b>	<b>7</b>
3.1 Actividad 1: Identificar a los clientes probables y definir los casos de uso previstos.....	7
3.2 Actividad 2: Investigar las necesidades y metas de ciberseguridad de los clientes.....	8
3.3 Actividad 3: Determinar la manera de considerar las necesidades y metas del cliente.....	14
3.4 Actividad 4: Planificar el soporte técnico adecuado a las necesidades y metas del cliente.....	17
<b>4 Actividades del fabricante que tienen impacto en la fase posterior al     mercadeo del dispositivo de IoT.....</b>	<b>20</b>
4.1 Actividad 5: Definir formas de comunicarse con los clientes .....	21
4.2 Actividad 6: Decidir lo que se comunicará a los clientes y la manera de hacerlo .....	21
4.2.1 Suposiciones relacionadas con el riesgo a la ciberseguridad .....	22
4.2.2 Expectativas de soporte técnico y vida útil .....	22
4.2.3 Composición y capacidades del dispositivo .....	23
4.2.4 Actualizaciones de software.....	24
4.2.5 Opciones de retirada de dispositivos.....	25
4.2.6 Medios técnicos y no técnicos.....	26
<b>5 Conclusión .....</b>	<b>27</b>
<b>Referencias.....</b>	<b>28</b>

## Lista de apéndices

<b>Apéndice A: Siglas y abreviaturas.....</b>	<b>30</b>
<b>Apéndice B: Glosario.....</b>	<b>31</b>

## 1 Introducción

### 1.1 Objetivo y alcance

El objetivo de esta publicación es ofrecer a los fabricantes recomendaciones para mejorar los dispositivos de internet de las cosas (IoT) que fabrican haciéndolos más *protegibles*. Esto se refiere a las *capacidades de ciberseguridad de dispositivo* (las características o funciones de ciberseguridad que los dispositivos proporcionan por sus propios medios técnicos, es decir, el hardware y el software del dispositivo) que ofrecen los dispositivos de IoT y que los clientes, sean organizaciones o personas, necesitan para protegerlos cuando los usan en sus sistemas y entornos. Los fabricantes de dispositivos de IoT también necesitarán a menudo ejecutar las acciones o prestar los servicios que sus clientes esperan o necesitan para planificar y mantener la ciberseguridad del dispositivo en sus sistemas y entornos. En esta publicación, los fabricantes de dispositivos de IoT aprenderán la manera de ayudar a los clientes de dispositivos de IoT con la gestión de riesgos a la ciberseguridad considerando atentamente las capacidades de ciberseguridad de dispositivo que deberán incorporar en sus dispositivos y que los clientes usarán en la gestión de sus riesgos a la ciberseguridad, así como las medidas o servicios que también puedan necesitar para reforzar la protegibilidad del dispositivo de IoT y satisfacer las necesidades de los clientes.

El objetivo de esta publicación es tener en cuenta una amplia gama de dispositivos de IoT. Los dispositivos de IoT a los que se refiere esta publicación tienen al menos un transductor (sensor o actuador) para interactuar directamente con el mundo físico, y al menos una interfaz de red (por ejemplo, Ethernet, wifi, Bluetooth, evolución a largo plazo [LTE], Zigbee, banda ultraancha [UWB]) que los conecta con el mundo digital. Esta publicación no incluye los componentes de un dispositivo que no pueden funcionar en absoluto por sí solos, como procesadores o sensores que transmiten datos a una estación de base especialmente diseñada<sup>2</sup>.

Algunos dispositivos de IoT pueden depender de otros dispositivos específicos (por ejemplo, un concentrador de IoT) o sistemas (por ejemplo, una nube) para ciertas funcionalidades. Los dispositivos de IoT se utilizarán en sistemas y entornos con muchos otros dispositivos y componentes, algunos de los cuales pueden ser dispositivos de IoT, mientras que otros tal vez sean equipos convencionales de tecnología de la información (TI). Esta publicación no incluye ninguna de las partes ni las funciones del ecosistema de la IoT que no sean los propios dispositivos de IoT y las funciones del fabricante relacionadas con la ciberseguridad de esos dispositivos.

---

<sup>2</sup> En ambos casos, se prevé que estos componentes se usen junto con otros para formar un dispositivo de IoT, pero pueden contribuir a la protegibilidad de un dispositivo de IoT (véase la Sección 3.4). Dado que el tema central de esta publicación es la protegibilidad de los dispositivos de IoT para los fines del cliente, es posible que algunos o todos los conceptos que se describen no se apliquen a los componentes.

El objetivo de esta publicación es servir de base para la fabricación de dispositivos nuevos y no de los dispositivos que ya se estén fabricando, aunque parte de la información contenida en esta publicación también podría ser aplicable a esos dispositivos.

No es necesario que los lectores tengan conocimientos técnicos de la composición y las capacidades de los dispositivos de IoT, pero se supone un conocimiento básico de los principios de la ciberseguridad.

## 1.2 Estructura de la publicación

El resto de esta publicación contiene las secciones y los apéndices siguientes:

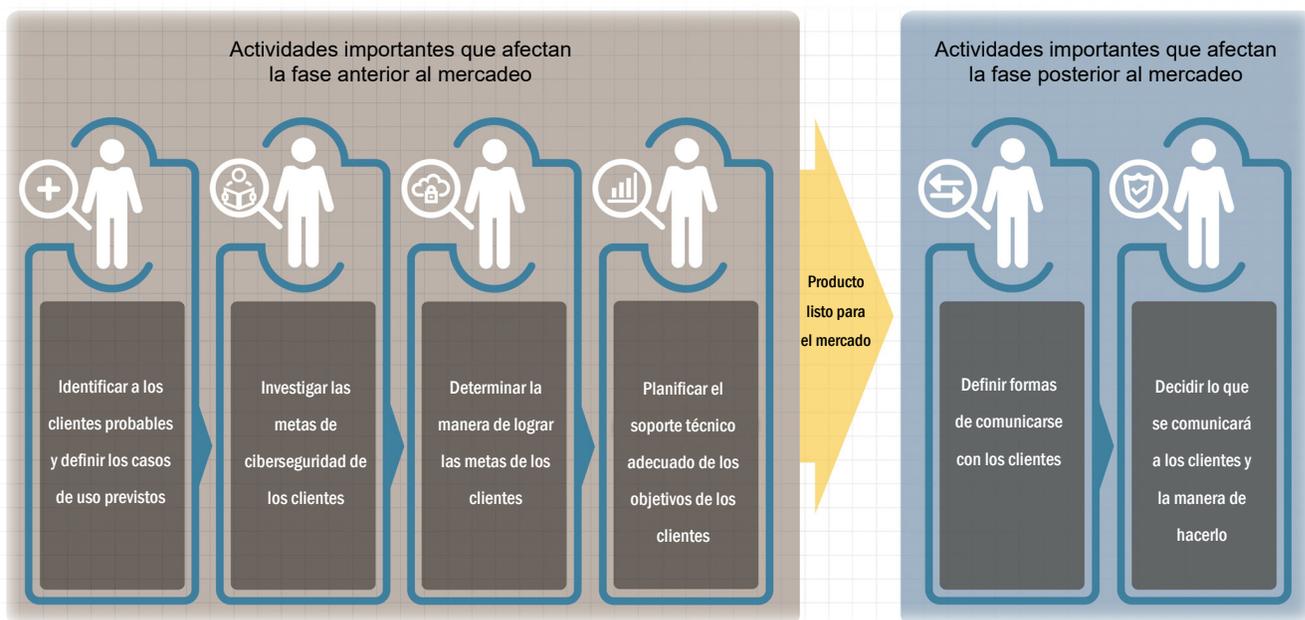
- La Sección 2 proporciona información general sobre la función clave que desempeñan los fabricantes en lo protegible que son sus dispositivos de IoT para sus clientes, por ejemplo, las áreas de mitigación de riesgos a la ciberseguridad que los clientes necesitan resolver normalmente, y un conocimiento de la ayuda que el dispositivo podría dar en esas áreas.
- Las secciones 3 y 4 describen las actividades que los fabricantes deben considerar llevar a cabo antes de que sus dispositivos de IoT se vendan a los clientes para mejorar la protegibilidad que los dispositivos de IoT ofrecen a los clientes.
  - La Sección 3 incluye las actividades que tienen impacto principalmente en las iniciativas de protegibilidad del fabricante antes de la venta del dispositivo. Las actividades de la Sección 3 son: identificar a los clientes probables y definir los casos de uso previstos; investigar las necesidades y metas de ciberseguridad de los clientes; determinar la manera de considerar las necesidades y metas del cliente; y planificar el soporte técnico adecuado a las necesidades y metas del cliente.
  - La Sección 4 incluye las actividades que tienen impacto principalmente en las iniciativas de protegibilidad del fabricante después de la venta del dispositivo. Las actividades de la Sección 4 son: definir formas de comunicarse con los clientes acerca de la ciberseguridad de los dispositivos de IoT, y decidir lo que se comunicará a los clientes y la manera de hacerlo.
- La Sección 5 es una conclusión de la publicación.
- La sección Referencias enumera las referencias hechas en la publicación.
- El Apéndice A contiene una lista de siglas y abreviaturas que figuran en este documento.
- El Apéndice B proporciona un glosario de los términos seleccionados que se usaron en esta publicación.

## 2 Información general

Esta sección proporciona una vista general de los conceptos necesarios para entender el resto de la publicación.

Desde el punto de vista del fabricante, la fase *anterior al mercadeo* de la vida de un dispositivo de IoT abarca lo que hace el fabricante *antes* de que el dispositivo se comercialice y se venda a los clientes. Toda medida que el fabricante tome para un dispositivo de IoT después de que se haya vendido, como resolver vulnerabilidades, distribuir capacidades de dispositivos nuevas o actualizadas o proporcionar información de ciberseguridad a los clientes, se considera parte de la fase *posterior al mercadeo*. Por lo general, los fabricantes son las personas que pueden identificar mejor e incorporar en sus dispositivos, al principio de la fase anterior al mercadeo, los planes para las capacidades de ciberseguridad de dispositivo que estos tendrán. Más adelante en la fase anterior al mercadeo, suele ser más complicado y costoso hacer cambios en el diseño o la implementación, y podría ser necesario demorar el lanzamiento del dispositivo. Una vez que un dispositivo está en el mercado, es posible que muchos cambios de ciberseguridad ya no sean factibles debido a las limitaciones de hardware, y los que aún se pueden hacer serán mucho más costosos y difíciles que si se hubieran hecho en la fase anterior al mercadeo.

Las secciones 3 y 4 de esta publicación describen las actividades de ciberseguridad y la planificación correspondiente que los fabricantes deben considerar llevar a cabo durante la fase anterior al mercadeo de un dispositivo de IoT. La Sección 3 explica las actividades que tienen impacto principalmente en otras actividades anteriores al mercadeo, y la Sección 4 trata las actividades que tienen impacto principalmente en las actividades posteriores al mercadeo. Las actividades de las secciones 3 y 4 se refieren a las actividades clave de ciberseguridad y representan un subconjunto de lo que los fabricantes tal vez necesiten hacer durante el proceso de desarrollo de sus productos, pero no se pretende que sean exhaustivas. Por ejemplo, a los fabricantes también les resultará más fácil diseñar y producir dispositivos de IoT protegibles si se aseguran de que su personal tenga las habilidades necesarias para desempeñar las actividades de las secciones 3 y 4.



**Figura 1: Actividades descritas en esta publicación y agrupadas por la fase afectada**

La Figura 1 muestra las actividades fundamentales de ciberseguridad que se tratan en esta publicación, organizadas por la fase en la que los resultados de las actividades se usarán para aumentar la protegibilidad del dispositivo. Como indica la figura, las actividades más importantes de cada fase se basan unas en otras dentro de esa fase, de manera que cada actividad anterior al mercadeo incorpora los resultados de las actividades previas. Si bien en las actividades importantes que tienen impacto en la fase posterior al mercadeo se pueden usar los artefactos y resultados de las actividades anteriores al mercadeo, también se puede recurrir a otras fuentes de orientación e información. El momento en el que se considera que un dispositivo ha “salido al mercado” variará según el producto, el fabricante y las circunstancias, pero se define como el momento en que un dispositivo fabricado ya no está bajo el control del fabricante (es decir, cuando ya pasó a un intermediario, como un minorista o los clientes finales). Se debe planificar que las actividades que tengan impacto principalmente en la fase posterior al mercadeo comiencen en la fase anterior al mercadeo, aunque se prevea que estas actividades contribuirán a la protegibilidad de los dispositivos de IoT durante o después de su venta (por ejemplo, informando a los clientes de la manera en que un dispositivo podría servir para satisfacer sus necesidades y lograr sus metas de ciberseguridad, lo cual puede o no incluir las metas de mitigación de riesgos).

Mejorar la protegibilidad de un dispositivo de IoT para los clientes se refiere a ayudar a los clientes a lograr sus metas de mitigación de riesgos, lo que implica identificar y resolver un conjunto de áreas de mitigación de riesgos. Incluso los clientes que no tienen metas formales de mitigación de riesgos, como los consumidores domésticos, suelen tener metas informales e indirectas de ciberseguridad (como hacer que su dispositivo de IoT cuente con la funcionalidad deseada según lo previsto, por ejemplo, automaticidad), que dependen en cierta medida de las áreas de mitigación de riesgos. En función de un análisis de las publicaciones existentes del NIST, como la Publicación especial 800-53 [5], el Marco de ciberseguridad [6] y las características de

los dispositivos de IoT, Informe interinstitucional o interno 8228 del NIST [7], se identificaron las siguientes áreas comunes de mitigación de riesgos para los dispositivos de IoT:

- **Gestión de activos:** Mantener un inventario actualizado y preciso de todos los dispositivos de IoT y sus características pertinentes durante el ciclo de vida de los dispositivos con objeto de usar esa información para fines de la gestión de riesgos a la ciberseguridad. Es necesario poder distinguir cada dispositivo de IoT de los demás para las otras áreas comunes de mitigación de riesgos: gestión de vulnerabilidades, gestión del acceso, protección de datos y detección de incidentes.
- **Gestión de vulnerabilidades:** Identificar y mitigar las vulnerabilidades conocidas en el software del dispositivo de IoT durante el ciclo de vida de los dispositivos para reducir la probabilidad y la facilidad de que sean explotados o queden comprometidos. Las vulnerabilidades se pueden eliminar instalando actualizaciones (por ejemplo, parches) y cambiando las opciones de configuración. Las actualizaciones también pueden corregir problemas operativos del dispositivo de IoT, lo cual mejora la disponibilidad, confiabilidad, rendimiento y otros aspectos de su funcionamiento. Los clientes desean a veces modificar las opciones de configuración de un dispositivo por diversas razones, entre otras, ciberseguridad, interoperabilidad, privacidad y utilidad.
- **Gestión del acceso:** Evitar el acceso físico y lógico no autorizado e indebido a los dispositivos de IoT, así como el uso y la administración de estos que hagan personas, procesos y otros dispositivos informáticos durante el ciclo de vida de los dispositivos. 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.
- **Protección de datos:** Evitar el acceso a los datos en reposo o en tránsito, y su manipulación indebida, lo cual podría exponer la información confidencial o permitir la manipulación o interrupción de las operaciones del dispositivo de IoT durante el ciclo de vida de los dispositivos.
- **Detección de incidentes:** Vigilar y analizar la actividad del dispositivo de IoT en busca de señales de incidentes relacionados con la seguridad del dispositivo y los datos durante el ciclo de vida de los dispositivos. Estas señales también son útiles para investigar peligros y solucionar ciertos problemas operativos.

Los fabricantes de dispositivos de IoT pueden solucionar estas áreas incorporando en estos las capacidades de ciberseguridad de dispositivo correspondientes. A su vez, debe ser menos difícil para los clientes proteger esos dispositivos, ya que las capacidades de los dispositivos de IoT estarán mejor alineadas con las expectativas de los clientes. Muchas de estas áreas solo se pueden resolver efectivamente (y la mayoría se resuelve con más eficiencia) al integrar en los dispositivos las capacidades de ciberseguridad de dispositivo en vez de que los clientes las proporcionen a través de sus entornos.

En las secciones 3 y 4 del Informe interinstitucional o interno 8228 del NIST [7], se analizan otras consideraciones relacionadas con la ciberseguridad que los fabricantes deben tener en cuenta al definir las capacidades de ciberseguridad de dispositivo que proporcionan los dispositivos de IoT. Además, en las tablas 1 y 2 de la Sección 4 del Informe interinstitucional o interno 8228 del NIST, se enumeran los defectos comunes en la ciberseguridad de los

dispositivos de IoT, se explica la manera en que pueden afectar negativamente a los clientes y se indican los motivos fundamentales por los que se necesita cada capacidad y elemento clave en la referencia básica que se define en la publicación complementaria Informe interinstitucional o interno 8259A del NIST: *IoT Device Cybersecurity Core Baseline* [Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT] [4].

En el caso de muchos dispositivos de IoT, es necesario gestionar otros tipos de riesgos (entre otros, a la privacidad<sup>3</sup>, la seguridad, la confiabilidad o la resiliencia) al mismo tiempo que los riesgos a la ciberseguridad debido a los efectos que la solución de un tipo de riesgo puede tener en los demás. Un ejemplo común es verificar que cuando un dispositivo falle, lo haga de manera segura. En esta publicación, solo se tratan los riesgos a la ciberseguridad. Para los lectores interesados en conocer mejor otros tipos de riesgos y su relación con la ciberseguridad, puede ser conveniente la lectura de la Publicación especial 800-82 del NIST, revisión 2, *Guide to Industrial Control Systems (ICS) Security* [Guía para la seguridad de los sistemas de control industrial (ICS, por sus siglas en inglés)] [8] y la Publicación especial 1500-201 del NIST, *Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0* [Marco de los sistemas ciberfísicos: vista general, volumen 1, versión 1.0] del Grupo de trabajo público de sistemas ciberfísicos [9].

---

<sup>3</sup> Es probable que una serie de iniciativas de privacidad actuales y recientes, incluido el Marco de privacidad del NIST, versión 1.0 (<https://www.nist.gov/privacy-framework>), sirvan de base a las capacidades necesarias de los dispositivos de IoT que sean compatibles con la privacidad. Aunque la referencia básica incluye las capacidades de ciberseguridad de dispositivo que también son compatibles con la privacidad, como la protección de la confidencialidad de los datos, no incluye las capacidades de dispositivo no relacionadas con la ciberseguridad que refuerzan la privacidad.

### 3 Actividades del fabricante que tienen impacto en la fase anterior al mercadeo del dispositivo de IoT

Los fabricantes deben considerar llevar a cabo las actividades fundamentales de ciberseguridad descritas en esta sección para hacer que el dispositivo de IoT sea más protegible para los clientes (por ejemplo, aumentar el número o la eficacia de las capacidades de ciberseguridad de dispositivo que los clientes esperan y que se ofrecen en los dispositivos de IoT). Las actividades se deben llevar a cabo en paralelo o como ampliaciones de otras actividades del fabricante anteriores al mercadeo, y tendrán impacto principalmente en esas otras actividades previas al mercadeo. Algunas de estas actividades pueden tener fines más amplios que la ciberseguridad (por ejemplo, la exploración de clientes y casos de uso previstos), los trabajos no se deben duplicar y los artefactos de todas las actividades previas al mercadeo pueden servir de base para medidas de ciberseguridad específicas. Cuanto más integradas estén estas actividades sugeridas con otras actividades anteriores al mercadeo, más probable será que se planifique mejor la ciberseguridad y se implemente en los dispositivos de IoT.

#### 3.1 Actividad 1: Identificar a los clientes probables y definir los casos de uso previstos

La identificación de los clientes probables de un dispositivo de IoT al comienzo de su diseño es indispensable para determinar las capacidades de ciberseguridad de dispositivo que este debe implementar y la manera de implementarlas. Por ejemplo, una gran empresa podría necesitar un dispositivo para integrarlo con sus servidores de gestión de registros, pero un cliente particular normal no lo necesitaría. Los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Qué tipos de personas son clientes previstos para este dispositivo?** (Por ejemplo, músicos, propietarios de pequeñas empresas, ciclistas, policías, chefs, constructores de casas, niños de edad preescolar, ingenieros eléctricos)
2. **¿Qué tipos de organizaciones son clientes previstos para este dispositivo?** (Por ejemplo, usuarios particulares, pequeños negocios minoristas, hospitales grandes, empresas energéticas con granjas solares, instituciones educativas con autobuses)

Los *clientes* son las personas u organizaciones que compran e implementan dispositivos de IoT y que suelen actuar como administradores del dispositivo con fines de ciberseguridad, haciendo uso de las capacidades de ciberseguridad de dispositivo para satisfacer sus necesidades y lograr sus metas. Además de los clientes, algunos dispositivos de IoT pueden tener otros *usuarios* que no compraron el equipo, pero que, sin embargo, interactúan con el dispositivo y también pueden tener necesidades y metas de ciberseguridad. La mayoría de los clientes actúa como usuario de los dispositivos de IoT que compra, pero no todos los dispositivos de IoT tienen otros usuarios además del cliente. El resto de esta publicación se referirá a los clientes, ya que cada dispositivo de IoT tiene un cliente, pero, como se explica a continuación, los fabricantes deben considerar *la manera* en que se puede usar un dispositivo, incluida la posibilidad de que pueda haber otros usuarios del dispositivo de IoT que no sean el cliente.

Otro paso inicial en el diseño de un dispositivo de IoT es definir los casos de uso previstos para el dispositivo en función de los clientes probables. Para definir un caso de uso, los fabricantes

pueden responder a las siguientes preguntas, según la manera en que prevén que el dispositivo se vaya a implementar y usar razonablemente:

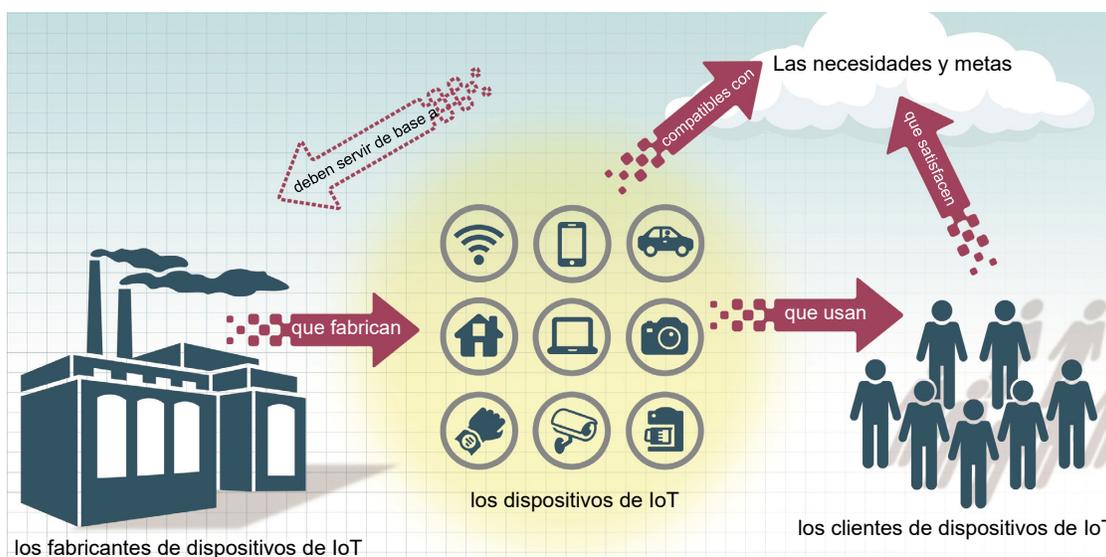
1. **¿Cómo se utilizará el dispositivo?** (Por ejemplo, con un único fin o con varios fines; integrado en otro dispositivo o sin integrar; con un usuario o cliente único o varios usuarios; para uso privado o comercial)
2. **¿En qué lugar geográfico se utilizará el dispositivo?** (Por ejemplo, países, jurisdicciones dentro de países)
3. **¿En qué entornos físicos se utilizará el dispositivo?** (Por ejemplo, en un entorno interior o exterior; fijo o móvil; público o privado; movable o no movable; en condiciones físicas y meteorológicas extremas o específicas)
4. **¿Cuánto tiempo se prevé que se usará el dispositivo?** (Por ejemplo, algunas horas; varios años; veinte años)
5. **¿Qué dependencias de otros sistemas tendrá probablemente el dispositivo?** (Por ejemplo, es necesario el uso de un concentrador de IoT particular; usa servicios de terceros en la nube para alguna funcionalidad)
6. **¿Cómo podrían los atacantes hacer uso indebido del dispositivo y ponerlo en peligro?** (Es decir, posibles uniones de amenazas y vulnerabilidades, como en un modelo de amenazas, incluida la consideración de conexiones de red que faciliten una ruta a internet que se pueda usar como vector de ataque contra otras redes o dispositivos, como un ataque de denegación de servicio distribuido)
7. **¿Qué otros aspectos del uso del dispositivo podrían ser pertinentes a los riesgos a la ciberseguridad del dispositivo?** (Por ejemplo, características operativas del dispositivo que puedan tener repercusiones en la seguridad, la privacidad u otros aspectos para los usuarios)

### 3.2 Actividad 2: Investigar las necesidades y metas de ciberseguridad de los clientes

Las necesidades y las metas de ciberseguridad se verán impulsadas principalmente, pero no del todo, por los riesgos a la ciberseguridad que afronten. Los fabricantes no pueden conocer la totalidad de los riesgos de sus clientes porque cada cliente, sistema y dispositivo de IoT se enfrenta a riesgos particulares en función de muchos factores. Sin embargo, los fabricantes pueden tener en cuenta los casos de uso previstos para sus dispositivos de IoT y hacer con ello que sus dispositivos sean al menos mínimamente protegibles por los clientes que los adquieran y usen de acuerdo con esos casos de uso. *Minimamente protegible* significa que los dispositivos cuentan con las capacidades de ciberseguridad de dispositivo que los clientes pueden necesitar para mitigar algunos riesgos comunes de ciberseguridad, ayudando con ello, al menos en parte, a lograr sus metas y satisfacer sus necesidades. Los clientes también desempeñan una función en la protección de sus dispositivos de IoT y de los sistemas que los incorporan, incluido el uso de otros medios técnicos, físicos y de procedimiento. El grado al cual un cliente puede desempeñar una función variará, pero para la mayoría de los clientes y casos de uso, las capacidades de ciberseguridad de dispositivo integradas en los dispositivos de IoT hacen normalmente que la mitigación de riesgos sea más fácil y efectiva.

Los clientes usarán *medios* para satisfacer sus necesidades y lograr sus metas. Los *medios* se definen como “un agente, herramienta, dispositivo, medida, plan o política para lograr o promover un propósito [10]”. Esta publicación hace referencia a medios técnicos o no técnicos para fines de ciberseguridad, sea que los lleve a cabo el dispositivo de IoT mismo o en otro lugar. El término que se introdujo en la Sección 1, *capacidades de ciberseguridad de dispositivo*, se refiere a los medios técnicos que usa el dispositivo de IoT mismo. Además de estos medios técnicos, puede haber otros medios técnicos y no técnicos que el fabricante use o servicios que ofrezca con los que los clientes contarán para planificar y mantener la ciberseguridad del dispositivo dentro de sus sistemas y entornos.

Como se demuestra en la Figura 2, es importante tener en cuenta las conexiones entre los fabricantes y los clientes en torno a la ciberseguridad. Los clientes que compran y utilizan dispositivos de IoT tienen pensado conectar esos dispositivos a sistemas y redes, incluida internet. A medida que los clientes adquieran estos dispositivos, procurarán protegerlos para lograr sus metas, o tal vez prevean que la protegibilidad se adapte a sus necesidades, las cuales el cliente puede o no expresar directamente. Los dispositivos de IoT compatibles con las capacidades de ciberseguridad de dispositivo que los clientes necesitan o esperan serán más fáciles de proteger, en especial con el uso de los mecanismos que los clientes ya hayan implementado. Los fabricantes pueden prever muchas metas de ciberseguridad de los clientes, especialmente las que se basan en las directrices y requisitos de ciberseguridad existentes; por ejemplo, los reglamentos podrían exigir a clientes de un sector particular que cambien todas las contraseñas predeterminadas.



**Figura 2: Conexiones entre los fabricantes y los clientes de dispositivos de IoT en torno a la ciberseguridad**

Los riesgos a la ciberseguridad para los dispositivos de IoT se pueden considerar en términos de dos mitigaciones de riesgo de alto nivel. La primera es salvaguardar la ciberseguridad del dispositivo mismo, con el fin de evitar que se use de forma indebida para afectar negativamente al cliente o atacar a otras organizaciones, o que no proporcione la funcionalidad que el cliente espera. La segunda es salvaguardar la confidencialidad, integridad o disponibilidad de los datos

(incluida la información personal) recopilados, almacenados, procesados o transmitidos por el dispositivo de IoT o desde este.

Para obtener información sobre las necesidades y metas de los clientes relacionadas con la salvaguardia de la ciberseguridad del dispositivo y la confidencialidad, integridad y disponibilidad de los datos, los fabricantes pueden responder a las siguientes preguntas para cada uno de los casos de uso previstos:

1. **¿Cómo interactuará el dispositivo de IoT con el mundo físico?** El impacto de algunos dispositivos de IoT en el mundo físico, sea directamente a través del accionamiento o indirectamente a través de la medición, podría causar la incompatibilidad de los requisitos operativos de rendimiento, confiabilidad, disponibilidad, resiliencia y seguridad con las prácticas comunes de ciberseguridad para los dispositivos de TI convencionales. Por ejemplo, muchos dispositivos críticos para la seguridad deben seguir proporcionando algunas o todas las funcionalidades en caso de que ocurra un incidente de ciberseguridad, un problema de red u otras condiciones adversas.
2. **¿Cómo tendrán que acceder las personas, procesos y otros dispositivos autorizados al dispositivo de IoT, gestionarlo y vigilarlo?** Estos son algunos ejemplos:
  - Es importante considerar los métodos que los clientes del dispositivo usarán probablemente para gestionar el dispositivo. Un dispositivo de IoT podría admitir la integración con sistemas empresariales comunes (por ejemplo, gestión de activos, gestión de vulnerabilidades, gestión de registros) para dar a los clientes que tengan estos sistemas mayor control y visibilidad del dispositivo. Para un dispositivo de IoT que se tiene intención de usar solo en entornos residenciales, esta capacidad no sería importante; los clientes esperan una forma fácil de gestionar sus dispositivos, o incluso desean que el fabricante haga toda la gestión del dispositivo en su nombre (por ejemplo, la instalación automática de parches). Un dispositivo de IoT utilizado por una pequeña empresa también podría ser gestionado por un tercero en representación de la empresa.
  - Por lo general, hacer un dispositivo muy configurable es más deseable en los entornos de organizaciones y menos en los de clientes particulares. Es menos probable que un cliente particular entienda la importancia de las opciones detalladas de configuración de la ciberseguridad y, por lo tanto, configure incorrectamente un dispositivo, debilitando su seguridad y aumentando la probabilidad de que peligre. También es poco probable que algunos clientes particulares deseen cambiar las opciones de configuración después de la implementación inicial del dispositivo. Sin embargo, es posible que muchos clientes, entre otros, clientes industriales, empresariales y particulares, deseen ciertas opciones de configuración, como la habilitación o deshabilitación de los servicios de sincronización del reloj para el dispositivo y la opción de usar un servidor de tiempo para la sincronización del reloj. La configuración del dispositivo podría omitirse por completo en los casos en los que no sea necesario aprovisionar o personalizar el dispositivo de ninguna manera durante o después de su implementación (por ejemplo, cuando no sea necesario conectarlo a una red inalámbrica ni asociarlo a un usuario en particular).

- Considerar lo accesible que es el dispositivo, sea lógica o físicamente. Si se considera como ejemplo una máquina de IoT expendedora de alimentos ubicada en un lugar público y conectada a internet para que los proveedores puedan hacer el seguimiento del inventario y el estado de la máquina, los usuarios de la máquina expendedora no tendrían que confirmar su identidad para insertar dinero y comprar un bocadillo. Sin embargo, la máquina expendedora estaría también muy expuesta a un ataque físico.
  - Considerar si el dispositivo de IoT debería tener una interfaz de programación de aplicaciones (API, por sus siglas en inglés) que admita la integración, el soporte o el desarrollo de terceros. El acceso a una API se debe considerar y gestionar cuidadosamente como una interfaz lógica, ya que puede ofrecer acceso y funcionalidad considerables a las entidades autorizadas.
  - Considerar dejar que los clientes deshabiliten las capacidades de ciberseguridad de dispositivo que puedan afectar negativamente las operaciones. Un ejemplo es una capacidad destinada a disuadir ataques de fuerza bruta contra contraseñas, como cuando se bloquea una cuenta después de demasiados intentos fallidos de autenticación. Esa capacidad puede causar accidentalmente una denegación de servicio para la persona o el dispositivo que se está tratando de autenticar. En entornos críticos para la seguridad, es posible que tales interrupciones al acceso no sean aceptables debido al peligro que causarían. Con frecuencia, los clientes necesitan flexibilidad para configurar esas funciones o para deshabilitarlas por completo.
  - Considerar las expectativas de vida útil del dispositivo y la manera en que esto podría afectar las capacidades de ciberseguridad de dispositivo que sean viables después de la vida útil prevista. Algunas funciones de ciberseguridad del dispositivo, como las actualizaciones de software, necesitarán desarrollo y trabajo continuos para proporcionar las ventajas de ciberseguridad previstas. Además, es posible que algunos dispositivos de IoT tengan características no basadas en TI que pueden exceder, y se espera que lo hagan, la vida útil prevista de la ciberseguridad o la funcionalidad de los componentes de TI del dispositivo.
3. **¿Cuáles son los requisitos de ciberseguridad conocidos del dispositivo de IoT?**  
Los fabricantes pueden identificar los requisitos conocidos en sus casos de uso, como reglamentos de ciberseguridad específicos del sector, leyes específicas del país, obligaciones contractuales o expectativas y costumbres de los clientes para tener presentes esos requisitos durante la identificación de capacidades del dispositivo.
4. **¿Cómo pueden interferir las características operativas o del entorno del dispositivo en el uso de las capacidades de ciberseguridad de dispositivo del dispositivo de IoT?**  
Por ejemplo, los dispositivos que se prevé usar en redes de ancho de banda bajo o poco confiables probablemente no podrían utilizar ciertas capacidades del dispositivo, como un mecanismo de actualización seguro. Dependiendo de esa red para descargar actualizaciones grandes saturaría la conexión de red, interrumpiendo otros usos, y tardaría demasiado en obtener las actualizaciones para el dispositivo. Los fabricantes podrían considerar estrategias de actualización alternativas, como cambiar sus procesos para reducir el tamaño de las actualizaciones, o distribuir actualizaciones a los administradores en conexiones de red de alta velocidad y hacer que los administradores transfieran manualmente las actualizaciones al dispositivo de IoT (lo cual introduce otros riesgos de

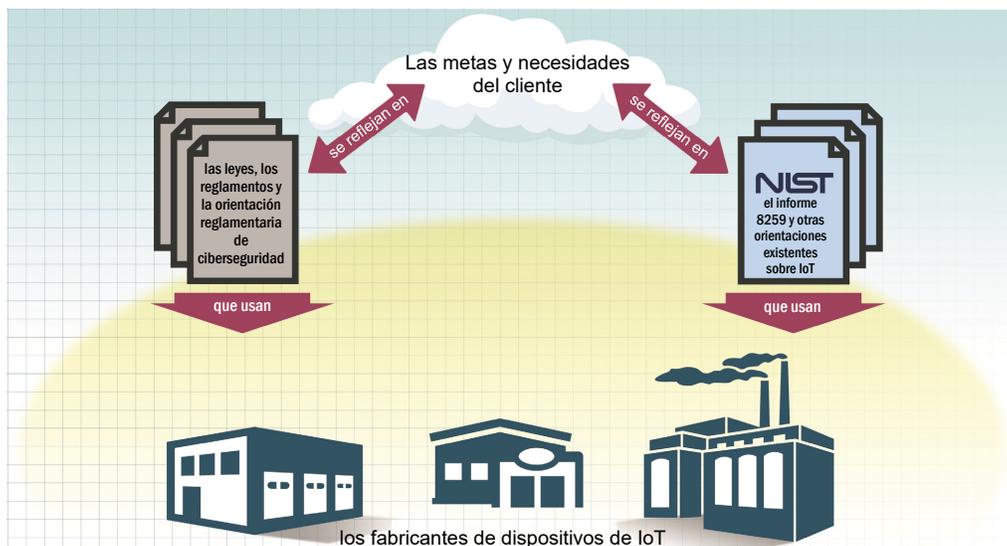
ciberseguridad, debidos al malware que se transmite por medios extraíbles, que necesitarían ser mitigados).

En otro ejemplo, es posible que algunos dispositivos de IoT, como los equipos médicos conectados, proporcionen a los clientes funcionalidades críticas no basadas en TI, de manera que los clientes puedan necesitar estas funciones de dispositivo para seguir operando incluso durante un estado de ciberseguridad degradado o cuando las funcionalidades relacionadas con TI (por ejemplo, una conexión a internet) no estén disponibles. La consideración cuidadosa del comportamiento del dispositivo en un caso de ciberseguridad degradada o de acceso reducido a la red o a los datos es importante para que los fabricantes determinen mejor la manera en que un dispositivo debe manejar las condiciones adversas.

5. **¿Cuál será la naturaleza de los datos del dispositivo de IoT?** Existe una gran variabilidad en los datos almacenados por los dispositivos de IoT. Algunos dispositivos no almacenan ningún dato, mientras que otros almacenan datos que podrían causar daños considerables si hay entidades no autorizadas que logran acceder a estos o modificarlos. Conocer la naturaleza de los datos previstos en un dispositivo en el contexto de los clientes y de los casos de uso ayuda a los fabricantes a identificar las capacidades de ciberseguridad de dispositivo que puedan ser necesarias para proteger los datos del dispositivo, como cifrado de datos, autenticación de dispositivos y usuarios, validación de datos, control del acceso y copias de seguridad y restauración.
6. **¿Cuál es el grado de confianza en el dispositivo de IoT que los clientes podrían necesitar?** Es posible que los clientes esperen ciertas capacidades e implementaciones de ciberseguridad de dispositivo que admitan garantías específicas para la ciberseguridad del dispositivo o los datos. Por ejemplo, en algunos contextos, se podría lograr una confianza mayor en que los datos están protegidos incorporando la protección de los datos en uso en el dispositivo. Esto iría más allá de las metas habituales de protección de datos (por ejemplo, la protección de datos en reposo y en tránsito).
7. **¿Qué complejidades presentará el dispositivo de IoT que interactúa con otros dispositivos, sistemas y entornos?** Por ejemplo, la complejidad se puede deber a los usos nuevos de la IoT y de los dispositivos de IoT, a las combinaciones nuevas de estos dispositivos entre sí y con los dispositivos de TI convencionales, y al aumento de las interconexiones entre dispositivos y sistemas. Estas complejidades podrían significar una nueva funcionalidad (con posibles repercusiones en la seguridad o la privacidad de las personas) que se conectará por medio de tecnologías de red a sistemas que no mitigan debidamente estos riesgos. Un dispositivo de IoT que transmita imágenes desde el interior de una residencia, como un monitor inteligente para bebés, o que modifique el entorno hasta el punto de ocasionar un peligro, como un horno inteligente, podría necesitar salvaguardias que no se consideran normalmente para los dispositivos de TI convencionales. La IoT también puede presentar complejidades relacionadas con la escala, lo que podría dificultar la gestión y el soporte continuos de los dispositivos.

Como se muestra de modo conceptual en la Figura 3, los fabricantes de dispositivos de IoT pueden usar fuentes diversas para obtener la información que necesitan a fin de responder a estas preguntas y otras. En algunos casos, los clientes y los casos de uso previstos indicarán las leyes, reglamentos u orientación voluntaria existentes para la ciberseguridad y otros aspectos del

funcionamiento del dispositivo. Por ejemplo, los dispositivos de IoT destinados a ser usados por el gobierno federal estarían protegidos mediante controles derivados de la orientación sobre ciberseguridad del sistema para los organismos federales (por ejemplo, la Publicación especial 800-53 del NIST [5]: Marco de ciberseguridad [6]), lo cual en algunos casos identifica o sugiere las capacidades específicas de ciberseguridad de dispositivo que un organismo necesitaría para reforzar los controles en su sistema. Para algunos casos de uso, la orientación puede ir más allá de los riesgos de ciberseguridad, pero seguirá teniendo repercusiones directas o indirectas en la ciberseguridad, como los dispositivos en el sector médico que necesitan cumplir con los reglamentos de la Administración de Alimentos y Medicamentos de los Estados Unidos (FDA, por sus siglas en inglés) y la Ley de portabilidad y responsabilidad de seguros de salud (HIPAA, por sus siglas en inglés). Es posible que, para cumplir las recomendaciones de la FDA y los requisitos de la HIPAA, un dispositivo de IoT necesite protecciones estrictas de confidencialidad, integridad o disponibilidad de los datos mucho mayores que las que se incluyen en un dispositivo de IoT promedio. Cuando los fabricantes conocen estos reglamentos en el contexto de su dispositivo y de su caso de uso previsto, pueden determinar si es posible satisfacer las necesidades y lograr las metas de sus clientes en el sector médico, y la mejor manera de hacerlo. Muchos sectores industriales también tendrán un consenso o una orientación voluntaria que se espera que las partes interesadas sigan de diversas formas, entre otras, marcos, referencias y mejores prácticas.



**Figura 3: Necesidades y metas de ciberseguridad del cliente que se reflejan y se basan en muchos reglamentos y documentos de orientación aplicables**

Para algunos clientes o sectores, es posible que esa orientación explícita por escrito no esté disponible ni se pueda usar (por ejemplo, debido a la gran variabilidad de las necesidades y metas de los clientes dentro de un sector). Para los dispositivos destinados a ser usados por estos clientes, la determinación de sus necesidades y metas tal vez requiera el uso de otras formas de información, como obtenerla directamente de los clientes o llevar a cabo investigaciones secundarias para entender mejor sus necesidades y metas.

### **3.3 Actividad 3: Determinar la manera de considerar las necesidades y metas del cliente**

Después de investigar las necesidades y metas de ciberseguridad de los clientes y los casos de uso previstos del dispositivo de IoT, los fabricantes pueden determinar la manera de considerar esas necesidades y metas para ayudar a los clientes a mitigar los riesgos de ciberseguridad. Para cada necesidad o meta de ciberseguridad, el fabricante puede responder a esta pregunta: **¿Cuáles de los siguientes es un medio adecuado (o una combinación de medios adecuada) para satisfacer la necesidad o lograr la meta?**

- El dispositivo de IoT puede proporcionar los medios técnicos a través de sus capacidades de ciberseguridad de dispositivo (por ejemplo, mediante el uso de las capacidades de ciberseguridad integradas en el sistema operativo del dispositivo, o haciendo que el software de la aplicación del dispositivo proporcione esas capacidades de ciberseguridad).
- Otro dispositivo relacionado con el dispositivo de IoT (por ejemplo, una puerta de enlace o un concentrador de IoT también del fabricante, una puerta de enlace o un concentrador de IoT de terceros) puede facilitar los medios técnicos en lugar del dispositivo de IoT (por ejemplo, al actuar como intermediario entre el dispositivo de IoT y otras redes proporcionando funcionalidad de comando y control para el dispositivo de IoT).
- Otros sistemas y servicios que actúen o no en representación del fabricante pueden proporcionar los medios técnicos (por ejemplo, un servicio basado en la nube que almacena de forma segura los datos de cada dispositivo de IoT, proveedores de servicios de internet y otros proveedores de infraestructura).
- Además de medios técnicos y su soporte, los fabricantes u otras organizaciones y servicios que representan al fabricante también pueden facilitar medios no técnicos (por ejemplo, comunicación de las expectativas de vida útil y soporte, divulgación de planes de corrección de defectos).
- El cliente puede seleccionar e implementar otros medios técnicos y no técnicos para mitigar los riesgos a la ciberseguridad. (El cliente también puede optar por responder a los riesgos a la ciberseguridad de otras maneras, entre otras, aceptarlos o transferirlos). Por ejemplo, un dispositivo de IoT que esté diseñado para usarse en las instalaciones de un cliente y que cuenta con estrictos controles de seguridad física.

Cabe señalar que no hay necesariamente una correspondencia uno a uno entre las necesidades o metas y los medios; por ejemplo, tal vez sean necesarios muchos medios técnicos para lograr una meta, mientras que un solo medio técnico podría lograr muchas metas. Además, no es posible ni necesario solucionar todas las necesidades y metas por medios técnicos, y algunos medios técnicos pueden necesitar otros medios no técnicos para lograr la protegibilidad inicial y continua (por ejemplo, conocimiento de las capacidades de ciberseguridad de dispositivo que están disponibles en un dispositivo de IoT, capacidad para obtener e instalar actualizaciones de software).

Además de identificar los medios adecuados para considerar cada necesidad y meta de ciberseguridad, los fabricantes también pueden responder a esta pregunta relacionada con los medios técnicos que proporcionan a través de su dispositivo de IoT: **¿Con qué solidez se debe implementar cada medio técnico para satisfacer la necesidad o lograr la meta de ciberseguridad?** La solidez de los medios técnicos se refiere a la efectividad total de las implementaciones de los medios y guarda relación con la confianza que un cliente espera tener en su dispositivo de IoT. Si se desea que los clientes confíen más en un dispositivo, especialmente en que permanecerá en un estado protegido y fuera del control o acceso de entidades no autorizadas, es probable entonces que los medios técnicos implementados en ese dispositivo, o con este, tengan que ser más sólidos. Estos son algunos ejemplos de consideraciones potenciales de la solidez:

- si es necesario implementarla en el hardware o el software (por ejemplo, un componente criptográfico de hardware emparejado con el software para usar la funcionalidad del hardware);
- los datos que se deben proteger, los tipos de protección que necesita cada instancia de datos (es decir, confidencialidad, integridad, disponibilidad) y la solidez necesaria de la protección;
- la solidez de la autenticación de la identidad de una entidad que se necesita antes de conceder acceso si la entidad es una persona (por ejemplo, PIN, contraseña, frase de contraseña, autenticación de dos factores) o un sistema o dispositivo (por ejemplo, claves de API, certificados);
- si es necesario validar los datos recibidos o introducidos en el dispositivo (por ejemplo, para confirmar la legitimidad de una actualización, para restringir la capacidad de datos con formato incorrecto a fin de omitir los controles de acceso); y
- la facilidad con la que se pueden revertir las actualizaciones de software si ocurre un problema (por ejemplo, capacidad de reversión, capacidad contra la reversión).

En última instancia, los fabricantes pueden agregar los medios técnicos identificados para todas las necesidades y metas a fin de responder a la siguiente pregunta: **¿Qué medios técnicos proporcionarán el propio dispositivo de IoT, otros dispositivos relacionados con el dispositivo de IoT y otros sistemas y servicios que representen al fabricante y al cliente, y la solidez necesaria que debe tener cada uno de esos medios?** El resto de esta sección se dedica a la primera parte de la pregunta: ¿Qué medios técnicos proporcionará el propio dispositivo de IoT (es decir, las capacidades de ciberseguridad de dispositivo)?

La identificación de esas capacidades de ciberseguridad que el dispositivo necesita proporcionar se debe hacer lo antes posible en los procesos de su diseño, de modo que las capacidades se puedan tener en cuenta al seleccionar o diseñar el hardware y el software del dispositivo de IoT. Para dar a los fabricantes de dispositivos de IoT un punto de partida que puedan usar para identificar las capacidades necesarias de ciberseguridad de dispositivo, la publicación complementaria Informe interinstitucional o interno 8259A del NIST, *IoT Device Cybersecurity Capability Core Baseline* [Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT], define una referencia esencial para las capacidades de ciberseguridad de

dispositivo (*referencia básica*)<sup>4</sup>, es decir, un 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. La referencia básica se deriva de los métodos comunes de gestión de riesgos a la ciberseguridad que se enumeran en el Informe interinstitucional o interno 8259A del NIST.

La referencia básica es solo un conjunto de las capacidades de ciberseguridad de dispositivo que pueden ser necesarias en un dispositivo de IoT, y los fabricantes deben consultar otras fuentes para obtener o identificar las debidas capacidades e implementaciones de ciberseguridad de los dispositivos para los clientes y casos de uso previstos, como se explica en la Sección 3.2. Los fabricantes pueden seguir un proceso para vincular la mitigación, necesidades y metas de ciberseguridad con las capacidades específicas de ciberseguridad de dispositivo. Este proceso se usó para crear la referencia básica que se define en el Informe interinstitucional o interno 8259A del NIST, en la que se usaron mitigaciones, necesidades y metas de ciberseguridad de alto nivel comunes a muchos clientes a fin de determinar las capacidades de ciberseguridad de dispositivo típicas que necesitaban muchos de esos clientes. Los fabricantes pueden así implementar estas capacidades dentro de sus dispositivos de IoT para que el mayor número de clientes logre el mayor número de metas que sea factible. Asimismo, puede haber otras referencias del NIST o de otras entidades para las capacidades de ciberseguridad de dispositivos de IoT, algunas de las cuales pueden haber sido diseñadas para satisfacer las necesidades de grupos de clientes particulares, sectores industriales, casos de uso, etc. Estos recursos, al igual que la referencia básica, ayudan a los fabricantes a identificar más rápidamente las capacidades de ciberseguridad de dispositivo necesarias para el contexto en el que se usará su dispositivo de IoT. El NIST también podría distribuir otras publicaciones de la serie del Informe interinstitucional o interno 8259 del NIST que definan más referencias para las capacidades.

Dado que el cliente y el contexto del caso de uso decidirán y moldearán las capacidades de ciberseguridad de dispositivo, los distintos dispositivos de IoT necesitarán conjuntos diferentes de capacidades de ciberseguridad. El nivel alto y amplio de la referencia básica se refiere a que será necesario generar un perfil de esta para dispositivos de IoT específicos en función de las necesidades y metas específicas relacionadas con los dispositivos en los contextos dentro de los cuales se prevé que se usarán. El sector de los dispositivos de IoT (por ejemplo, el sector médico, usuarios particulares infraestructuras críticas), el caso de uso (por ejemplo, actuadores críticos de vida, sensores críticos de seguridad) u otros factores contextuales (por ejemplo, las necesidades específicas del cliente) pueden guiar las necesidades y las metas. Se puede generar un perfil de las capacidades de ciberseguridad de dispositivo a partir de la referencia básica y ampliarse de diversas maneras. Es posible que las capacidades nuevas o más complejas que no se identificaron en la referencia básica se incluyan en un dispositivo. Las capacidades de ciberseguridad de dispositivo de la referencia básica también se pueden ampliar y adaptar con

---

<sup>4</sup> 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 del NIST, *Security and Privacy Controls for Federal Information Systems and Organizations* [Controles de seguridad y privacidad para sistemas y organizaciones de información federales] [5], 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 que se aplicarían a dispositivos de IoT particulares diseñados para uso como componentes dentro de sistemas.

elementos nuevos o más específicos para las capacidades que se adapten mejor a lo que ciertos clientes necesitan o prefieren.

### **3.4 Actividad 4: Planificar el soporte técnico adecuado a las necesidades y metas del cliente**

Es importante que los fabricantes consideren la manera de tener en cuenta las necesidades y metas identificadas de sus clientes más allá de la selección de capacidades específicas de ciberseguridad de dispositivo y sus implementaciones de alto nivel. Esto incluye tener en cuenta la forma de proporcionar recursos informáticos compatibles con las capacidades de ciberseguridad de dispositivo y las medidas externas al dispositivo que puedan ser necesarias para seguir considerando las necesidades y metas de ciberseguridad.

Los fabricantes pueden hacer que sus dispositivos de IoT sean más protegibles equipándolos con los debidos recursos de hardware (por ejemplo, procesamiento, memoria, almacenamiento, tecnología de redes, energía) y de software compatibles con las capacidades de ciberseguridad de dispositivo que se desean. Por ejemplo, el cifrado basado en software requiere mucho procesamiento, y un dispositivo con procesamiento limitado y sin ningún cifrado basado en hardware no podría proporcionar lo que los clientes necesitan. Otro ejemplo es que algunos dispositivos no son compatibles con el uso de redes de sistema operativo o de protocolo de internet (IP, por sus siglas en inglés), y uno o ambos podrían ser necesarios para admitir muchas capacidades de ciberseguridad de dispositivo.

Al diseñar o seleccionar recursos de hardware y software para dispositivos, los fabricantes pueden responder a las siguientes preguntas para los clientes y casos de uso previstos a fin de identificar las necesidades de aprovisionamiento y problemas potenciales:

1. **Tomando en consideración los períodos de soporte técnico y la vida útil previstos, ¿cuál posible uso futuro se deberá tener en cuenta?** Por ejemplo, si un dispositivo tiene una vida útil de diez años, tal vez sea necesario actualizar el algoritmo de cifrado o la longitud de la clave que el dispositivo usará durante ese tiempo, y el nuevo algoritmo o la longitud de la clave pueden requerir más recursos de procesamiento que el algoritmo o la longitud de clave actuales. Para la vida útil del dispositivo, se considera la manera en que este puede tener en cuenta las necesidades y metas de ciberseguridad, incluida la “protección contra la obsolescencia” de las capacidades de ciberseguridad de dispositivo y sus implementaciones.
2. **¿Se debe usar una plataforma de IoT establecida en lugar de adquirir e integrar componentes particulares de hardware y software?** Una *plataforma de IoT* es un componente del hardware del dispositivo de IoT que cuenta con software compatible ya instalado y configurado para que lo use un fabricante como base para un nuevo dispositivo de IoT. Una plataforma de IoT también puede ofrecer servicios o aplicaciones de terceros, o un kit de desarrollo de software (SDK, por sus siglas en inglés) para agilizar el desarrollo de aplicaciones de IoT. Los fabricantes pueden elegir una plataforma de IoT con suficientes recursos y protección en lugar de diseñar hardware, instalar y configurar un sistema operativo, crear nuevos servicios basados en la nube, escribir aplicaciones para dispositivos de IoT y aplicaciones móviles desde cero, y efectuar otras tareas que son propensas a errores y que, por lo general, tienen mayor

probabilidad de introducir vulnerabilidades nuevas en el dispositivo de IoT en comparación con la adopción de una plataforma establecida.

3. **¿Alguna de las capacidades de ciberseguridad de dispositivo se debe basar en hardware?** Un ejemplo es tener una raíz de confianza de hardware que proporcione almacenamiento confiable para claves criptográficas y permita hacer un arranque seguro y confirmar la autenticidad del dispositivo. Además, los fabricantes deben considerar si esas capacidades que se basan en hardware serán actualizables. Por ejemplo, en algunos casos, los clientes necesitarán una raíz de confianza de hardware que sea inmutable y no desee nunca actualizaciones ni cambios para esa funcionalidad; sin embargo, estas limitaciones podrían ser perjudiciales para la protegibilidad continua de otros clientes.
4. **¿Tiene el hardware o el software (incluido el sistema operativo) capacidades de dispositivos innecesarias que repercutan en la ciberseguridad? De ser así, ¿se pueden deshabilitar para evitar su explotación y uso indebido?** Por ejemplo, un dispositivo puede tener interfaces locales en su cubierta externa que sean útiles o esenciales para algunos casos de uso, o para casos de uso previstos en el futuro, pero el dispositivo puede ser implementado en lugares públicos por algunos clientes probables donde esas interfaces estarían expuestas a un posible ataque. Las soluciones posibles para este problema serían, entre otras, ofrecer una cubierta a prueba de manipulación indebida para evitar el acceso físico a las interfaces, e incluir una opción de configuración que las deshabilite lógicamente.

Los fabricantes deben considerar las prácticas de desarrollo seguras<sup>5</sup> que sean las más apropiadas para ellos y sus clientes al planificar la manera de tener en cuenta adecuadamente las necesidades y metas de los clientes. Asimismo, pueden responder a preguntas como las siguientes en función de los clientes y casos de uso previstos para identificar otras prácticas seguras de desarrollo que se deban adoptar a fin de mejorar la ciberseguridad de los dispositivos de IoT:

1. **¿Cómo está protegido el código del dispositivo de IoT contra el acceso no autorizado y la manipulación indebida?** (Por ejemplo, un repositorio de código bien protegido, funciones de control de versiones, firma de código)
2. **¿Cómo pueden los clientes verificar la integridad del hardware o el software del dispositivo de IoT?** (Por ejemplo, raíz de confianza del hardware, validación de firma de código, comparación del hash criptográfico)
3. **¿Qué verificación se hace para confirmar que la seguridad del software de terceros que se usa en el dispositivo de IoT satisface las necesidades de los clientes?** (Por

---

<sup>5</sup> Los fabricantes de dispositivos de IoT que deseen obtener más información sobre las prácticas seguras de desarrollo de software pueden consultar el informe técnico del NIST, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SDDF)* [Mitigación del riesgo de vulnerabilidades de software mediante la adopción de un marco para el desarrollo seguro de software (SSDF, por sus siglas en inglés)] [11], en el que se destacan las prácticas seleccionadas para el desarrollo seguro de software. Cada una de estas prácticas se recomienda ampliamente en las publicaciones existentes sobre desarrollo seguro de software, y el informe técnico contiene referencias de casi 20 de esas publicaciones.

ejemplo, comprobar si existen vulnerabilidades conocidas que aún no se hayan corregido, revisar o analizar el código legible, probar el código ejecutable)

4. **¿Qué medidas se adoptan para minimizar las vulnerabilidades en el software para dispositivos de IoT que sale al mercado?** (Por ejemplo, seguir prácticas de codificación seguras, hacer una validación de entrada sólida, revisar y analizar el código legible, probar el código ejecutable, configurar el software para que tenga opciones de configuración seguras y predeterminadas, revisar el código con respecto a las bases de datos de vulnerabilidades conocidas)
5. **¿Qué medidas se adoptan para aceptar informes sobre posibles vulnerabilidades en el software del dispositivo de IoT y responder a ellas?** (Por ejemplo, programas de respuesta a vulnerabilidades, vigilancia de bases de datos de vulnerabilidades, uso de un servicio de inteligencia sobre amenazas, desarrollo y distribución de actualizaciones de software)
6. **¿Qué procesos se han establecido para evaluar y priorizar la corrección de todas las vulnerabilidades en el software del dispositivo de IoT?** (Por ejemplo, estimar el trabajo de corrección, estimar el impacto potencial de la explotación, estimar los recursos del atacante necesarios para convertir la vulnerabilidad en un arma)

## 4 Actividades del fabricante que tienen impacto en la fase posterior al mercadeo del dispositivo de IoT

En algún momento, los fabricantes de dispositivos de IoT comercializarán y venderán sus productos para ponerlos en manos de los clientes e iniciar la fase posterior al mercadeo del proceso de fabricación. Incluso en esta fase, mientras los clientes están evaluando posibles adquisiciones de productos, y después de que los dispositivos de IoT se venden a los clientes, los fabricantes siguen desempeñando la función de considerar las necesidades y metas de ciberseguridad de los clientes y dispositivos de IoT. Por ejemplo, es posible que los fabricantes tengan que responder a informes de vulnerabilidades y generar actualizaciones críticas. Estas actividades de ciberseguridad fundamentales pueden beneficiar a los clientes y su capacidad para proteger los dispositivos durante su vida útil, especialmente al momento de evaluar y adquirir los dispositivos de IoT disponibles en el mercado. Un aspecto que a menudo se pasa por alto tanto en las fases de mercadeo y posterior al mercadeo es la comunicación relacionada con la ciberseguridad. Para muchos clientes, sería una ventaja que los fabricantes se comunicaran más claramente con ellos, o con quienes los representan, sobre los riesgos a la ciberseguridad y la consideración de sus necesidades y metas relacionadas con los dispositivos de IoT que los fabricantes producen. En esta sección, se analizan las medidas que toma el fabricante con objeto de lograr la protegibilidad facilitando que los clientes conozcan e identifiquen cómo se diseñan los dispositivos de IoT para satisfacer sus necesidades y lograr sus metas de ciberseguridad cuando los fabricantes implementan las dos actividades amplias que se tratan en esta sección.

En las secciones anteriores, se explicó la forma en que los fabricantes pueden identificar los medios técnicos o no técnicos que los clientes y usuarios de sus dispositivos de IoT pueden necesitar para fines de ciberseguridad, incluidas las *capacidades de ciberseguridad de dispositivo*. Esta sección se destina a ayudar a los fabricantes a determinar lo que deben comunicar a los clientes y usuarios acerca de los riesgos a la ciberseguridad y la manera de hacerlo, y las necesidades y metas de los clientes que se toman en cuenta en relación con sus dispositivos de IoT. Algunas consideraciones describen otras capacidades de ciberseguridad de dispositivo o medidas o servicios apropiados para los clientes que el fabricante puede implementar y que deban comunicarles a estos.

La planificación de estas actividades (por ejemplo, responder a las preguntas presentadas para cada actividad), que probablemente no termina por completo hasta que un dispositivo de IoT se encuentra en la fase posterior al mercadeo, se efectúa mejor cuando se dispone de la información necesaria por medio de diversas actividades anteriores al mercadeo, como las que se tratan en la Sección 3. Aunque las actividades 1 a 4 pueden servir de base para la planificación y ejecución de las actividades presentadas en esta sección, no se consideran como un requisito previo. Esto permite que algunos o todos los aspectos de la planificación de las actividades 5 y 6 se lleven a cabo junto con otras actividades anteriores al mercadeo. Es posible que las consideraciones mencionadas en estas actividades no se apliquen a todos los clientes o fabricantes, pero, para otras personas, esas mismas consideraciones pueden ser indispensables.

#### 4.1 Actividad 5: Definir formas de comunicarse con los clientes

Comunicar claramente la información de ciberseguridad puede hacer necesario formas diversas de comunicación para tipos distintos de clientes en función de sus expectativas y recursos. Los fabricantes pueden responder a preguntas como las siguientes para definir las formas de comunicación:

1. **¿Qué terminología entenderá el cliente?** Por ejemplo, es probable que un usuario particular tenga menos conocimientos técnicos que los puntos de contacto de una gran empresa (por ejemplo, los administradores de sistemas). Además, es posible que los profesionales de TI y ciberseguridad ya se hayan familiarizado con las convenciones, como referirse a una vulnerabilidad usando su número en la lista de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés).
2. **¿Cuánta información necesitará el cliente?** Dar a algunos clientes demasiada información podría abrumarlos y hacer más difícil que encuentren la información que necesitan. Por lo general, tampoco conviene ofrecer información insuficiente, salvo en los casos en que revelar la información podría tener repercusiones negativas más amplias, por ejemplo, publicar detalles técnicos de una vulnerabilidad recién descubierta antes de tener una actualización para corregirla.
3. **¿Cómo y dónde se proporcionará la información?** La información se puede proporcionar en uno o más lugares lógicos o físicos. Algunos ejemplos incluyen manuales de usuario, condiciones de servicio y otra documentación del producto, sitios web, correos electrónicos y el dispositivo de IoT y sus aplicaciones correspondientes (por ejemplo, aplicaciones móviles). Para los clientes, es una ventaja encontrar fácilmente la información cuando la necesitan.
4. **¿Cómo se puede verificar la integridad de la información?** Para algunas formas de comunicar información, como los correos electrónicos, es posible que los clientes deseen una manera de determinar si la información es legítima (por ejemplo, que no sea una tentativa de ingeniería social).
5. **¿Tendrán que comunicarse los clientes con el fabricante?** Por ejemplo, es posible que los clientes soliciten actualizaciones u otros datos necesarios para el mantenimiento de sus dispositivos. También pueden descubrir vulnerabilidades u otros problemas que desean comunicar. El fabricante debe probar la funcionalidad, utilidad y eficacia de los canales de comunicación entre el cliente y el fabricante para verificar que los clientes y otras personas (por ejemplo, investigadores de seguridad) puedan usar esos canales.

#### 4.2 Actividad 6: Decidir lo que se comunicará a los clientes y la manera de hacerlo

Hay muchas consideraciones potenciales de la información que un fabricante comunica a los clientes acerca de un producto de IoT particular y de la manera en que se comunica esa información. El resto de esta sección contiene ejemplos de temas que sería conveniente que los fabricantes incluyeran en sus comunicaciones y, para algunos ejemplos, ideas sobre la manera en que se podría comunicar esa información.

#### 4.2.1 Suposiciones relacionadas con el riesgo a la ciberseguridad

Para entender la manera en que los riesgos de los clientes pueden diferir de las expectativas del fabricante, sería útil para algunos clientes conocer las suposiciones relacionadas con la ciberseguridad que el fabricante hizo al diseñar y desarrollar el dispositivo, como las que figuran a continuación:

1. **¿Quiénes eran los clientes previstos?** Por ejemplo, algunos dispositivos de IoT se diseñan teniendo en cuenta un sector o tipo de cliente específico, lo que podría afectar no solo las capacidades de ciberseguridad de dispositivo que se implementan, sino también la manera en que funcionan esas capacidades.
2. **¿Cuál era el uso previsto del dispositivo?** Por ejemplo, algunos dispositivos de IoT tienen fines previstos específicos en los sistemas, los cuales pueden indicar las consideraciones de ciberseguridad de los clientes. Además, se supone y se espera que algunos dispositivos de IoT se usen en sistemas particulares, lo que posiblemente cree dependencias para la ciberseguridad que los clientes necesitarían conocer (por ejemplo, un dispositivo necesita un sistema de vigilancia al cual se pueda conectar para fines de ciberseguridad).
3. **¿En qué tipos de entornos se usaría el dispositivo?** Es posible que los clientes necesiten saber, por ejemplo, cuando un dispositivo de IoT no sea protegible si se encuentra en un lugar público o si se usa sin otro dispositivo que proporcione algunas o todas las capacidades de ciberseguridad de dispositivo en lugar del dispositivo de IoT. El ancho de banda y la latencia de la red, así como otros factores del entorno, también pueden afectar las suposiciones hechas acerca de las capacidades que se incorporarán y la manera de implementarlas.
4. **¿Cómo se distribuirían las responsabilidades entre el fabricante, el cliente y otros?** Por ejemplo, puede ser útil que algunos clientes sepan si el uso completo y la implementación de las capacidades de ciberseguridad de dispositivo y las tareas correspondientes (como actualizaciones de software, configuración de dispositivos, protección y destrucción de datos y administración de dispositivos) son responsabilidad de una o varias partes.

#### 4.2.2 Expectativas de soporte técnico y vida útil

La comunicación de las expectativas de soporte técnico y vida útil del dispositivo ayuda a los clientes a planificar la mitigación de riesgos a la ciberseguridad durante el ciclo de vida de soporte del dispositivo, el cual podría ser más breve que el tiempo que el cliente desea usar el dispositivo. Para determinar la información que se comunicará a los clientes, los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Durante cuánto tiempo se prevé dar soporte técnico al dispositivo?** Informar a los clientes por cuánto tiempo dispondrán de actualizaciones y soporte técnico puede ayudarles a planificar el uso y mantenimiento seguros de los dispositivos durante un período apropiado.
2. **¿Para cuándo se prevé el final de la vida útil del dispositivo? ¿Cuál será el proceso de fin de vida útil?** Es conveniente que los clientes planifiquen la retirada de un

dispositivo cuando el fabricante considere que este se encuentra al final de su vida útil. Sería útil que estos clientes recibieran un aviso con cierta anterioridad (por ejemplo, seis meses antes) al fin de la vida útil de manera que estén preparados para ello.

3. **¿Cuál funcionalidad, si la hay, tendrá el dispositivo después de que concluya el soporte técnico y al final de su vida útil?** Es conveniente que los clientes sepan si podrán seguir usando un dispositivo después del fin de su vida útil, aun cuando los servicios basados en la nube u otras funciones ya no estén disponibles.
4. **¿Cómo pueden los clientes informar al fabricante de posibles problemas que repercutan en la ciberseguridad, como vulnerabilidades del software? ¿Se aceptarán esos informes una vez que termine el soporte técnico? ¿Se aceptarán esos informes después del fin de la vida útil?** Algunos ejemplos de métodos para informar incluyen números de teléfono, direcciones de correo electrónico y formularios web.
5. **¿Cómo pueden los clientes mantener la protegibilidad incluso después de que haya concluido el soporte técnico oficial del dispositivo (por ejemplo, cuando un fabricante o una organización de terceros que desempeña una función de ciberseguridad suspende por completo o termina el soporte del dispositivo)? ¿Estarán disponibles los archivos o datos esenciales en un foro público para que otros, incluso los clientes mismos, sigan ofreciendo soporte técnico para el dispositivo de IoT?** Por ejemplo, un fabricante que cierre su negocio puede ofrecer la base de código de su producto en un foro de código abierto para dejar que la comunidad ofrezca desarrollo y soporte técnico continuos.

#### 4.2.3 Composición y capacidades del dispositivo

La comunicación de información acerca del software, hardware, servicios, funciones y tipos de datos de los dispositivos facilita que los clientes entiendan y gestionen mejor la ciberseguridad de sus dispositivos, especialmente si se prevé que los clientes desempeñen una función importante en la gestión de la ciberseguridad de estos. Para determinar la información que es importante comunicar a los clientes, los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Qué información necesitan los clientes sobre los aspectos generales relacionados con la ciberseguridad del dispositivo, entre otros, su instalación, configuración (incluido el endurecimiento), uso, gestión, mantenimiento y eliminación?** Algunos ejemplos son la manera en que el dispositivo se puede conectar de forma segura a un sistema o red, las opciones de configuración que afectan la ciberseguridad y la forma en que lo hacen y las maneras reconocidas como no seguras de usar el dispositivo.
2. **¿Cuál es el efecto potencial en el dispositivo si la configuración de ciberseguridad se ajusta para que sea más restrictiva que la configuración predeterminada?** Por ejemplo, algunos dispositivos pueden perder cierta funcionalidad a medida que sus configuraciones de ciberseguridad se hagan más estrictas.
3. **¿Cuál información sobre el inventario necesitan los clientes acerca del software interno del dispositivo, como versiones, estado de los parches y vulnerabilidades conocidas? ¿Necesitan los clientes tener acceso al inventario actual a pedido?** Por ejemplo, es posible que algunos clientes deseen conocer las vulnerabilidades reconocidas para poder solucionarlas por otros medios, mientras que otros clientes tal vez quieran saber el estado actual de los parches de software.

4. **¿Qué información necesitan los clientes sobre las fuentes de software, hardware y servicios del dispositivo?** Algunos ejemplos de las fuentes son el desarrollador del software de IoT del dispositivo, el fabricante del procesador del dispositivo y el proveedor de un servicio basado en la nube que utilice el dispositivo<sup>6</sup>.
5. **¿Qué información necesitan los clientes sobre las características operativas del dispositivo para poder protegerlo adecuadamente? ¿Cómo se debe facilitar esta información?** Por ejemplo, se puede atender mejor a algunos clientes cuando la información se presenta en un sitio web, mientras que otros hacen mejor uso de la información por medio de un protocolo estandarizado de máquina a máquina. En algunos casos, como en la señalización de la intención del dispositivo, esta información se podría proporcionar mejor a través del dispositivo mismo.
6. **¿Qué funciones puede ejecutar el dispositivo?** Esto incluye no solo las capacidades de ciberseguridad de dispositivo, sino también cualquier otra función que repercute en la ciberseguridad, por ejemplo, la transmisión de datos a un sistema remoto o el uso de un micrófono y una cámara para capturar audio y video.
7. **¿Qué tipos de datos puede recopilar el dispositivo? ¿Cuáles son las identidades de todas las partes (incluido el fabricante) que pueden acceder a esos datos?** Por ejemplo, es posible que algunos clientes necesiten saber si la información sobre ubicaciones o los comandos de voz recolectados por el dispositivo se pueden almacenar en una nube y si, posiblemente otras partes, pueden acceder a estos para otros fines (por ejemplo, para agregación o análisis).
8. **¿Cuáles son las identidades de todas las partes (incluido el fabricante) que tienen acceso al dispositivo o cualquier grado de control sobre este?** Por ejemplo, un tercero que proporcione soporte técnico en representación del fabricante podría actualizar de forma remota el software y la configuración del dispositivo.

#### 4.2.4 Actualizaciones de software

Los fabricantes que comunican información sobre actualizaciones de software ayudan a los clientes a planificar mitigaciones de riesgos a la ciberseguridad y a mantener la ciberseguridad de sus dispositivos, especialmente en respuesta a amenazas emergentes. Para determinar la información acerca de actualizaciones que es importante comunicar a los clientes, los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Estarán disponibles las actualizaciones? De ser así, ¿cuándo estarán disponibles?** Por ejemplo, saber si las actualizaciones se proporcionarán de acuerdo con un programa establecido o esporádicamente ayudará a los clientes a planificar su aplicación.
2. **¿En qué circunstancias se emitirán las actualizaciones?** Los ejemplos incluyen el control de la ejecución de software defectuoso y la corrección de una vulnerabilidad previamente desconocida en un protocolo estándar.

---

<sup>6</sup> Las técnicas, como la lista de materiales de software (SBOM, por sus siglas en inglés), se pueden considerar una manera de comunicar esta información e información similar a los clientes con uniformidad y efectividad. La Dirección Nacional de Telecomunicaciones e Información tiene más información disponible sobre la SBOM (<https://www.ntia.gov/SBOM>).

3. **¿Cómo se pondrán a la disposición o se distribuirán las actualizaciones? ¿Se notificará cuando haya actualizaciones disponibles o cuando se instalen?** Por ejemplo, los clientes pueden planificar mejor la instalación de actualizaciones si saben que deben descargarlas por medio de un portal específico y aplicarlas al dispositivo. También puede ser útil a los clientes recibir avisos de que debe instalarse una actualización, o de que ya se instaló, incluso en los casos en que la distribución e instalación de la actualización de software sean automáticas y no requieran ninguna respuesta del cliente ni de los usuarios.
4. **¿Qué entidad (por ejemplo, el cliente, el fabricante, un tercero) es responsable de hacer las actualizaciones? ¿O puede el cliente designar a la entidad que tendrá la responsabilidad (por ejemplo, el fabricante la instala automáticamente)?** Por ejemplo, para algunos clientes es útil saber que un tercero pondrá a disposición ciertas actualizaciones y que el fabricante proporcionará otras. También puede ser conveniente para algunos clientes conocer sus funciones, responsabilidades y opciones en lo que se refiere a las actualizaciones.
5. **¿Cómo pueden los clientes verificar y autenticar las actualizaciones?** Algunos ejemplos son la comparación de hash criptográfico, la validación de firmas de código y la dependencia del software que proporciona el fabricante para hacer automáticamente la verificación y autenticación de las actualizaciones.
6. **¿Qué información se debe proporcionar con cada actualización individual?** Algunos ejemplos son la naturaleza de la actualización (por ejemplo, correcciones de errores, capacidades modificadas o nuevas) y cualquier efecto que la instalación de la actualización podría tener en las opciones de configuración existentes de un cliente.

#### 4.2.5 Opciones de retirada de dispositivos

Los fabricantes que comunican información sobre las opciones de retirada de dispositivos (por ejemplo, la capacidad de “dar de baja” el dispositivo, posiblemente mediante un restablecimiento de datos o haciendo que el dispositivo quede inutilizable) ayudan a los clientes a planificar para hacerlo de manera segura. Para determinar la información acerca de actualizaciones que es importante comunicar a los clientes, los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Desearán los clientes transferir la propiedad de sus dispositivos a otra persona? De ser así, ¿qué necesitarán hacer los clientes para que quienes asuman la propiedad no puedan acceder a los datos de usuario y de configuración en el dispositivo y los sistemas asociados con este (por ejemplo, los servicios basados en la nube que usa el dispositivo)?** Por ejemplo, es posible que un cliente desee vender un edificio que contiene dispositivos inteligentes de automatización de edificios, pero quiera asegurarse de que todos los datos se hayan eliminado de los dispositivos antes de que el comprador del edificio tenga acceso a ellos.
2. **¿Desearán los clientes hacer que sus dispositivos queden inutilizables? De ser así, ¿cómo pueden los clientes lograrlo?** Por ejemplo, se puede hacer que algunos dispositivos de IoT queden inutilizables por medios lógicos (por ejemplo, como los que se ejecutan a través de una aplicación móvil), y que para otros se utilicen medios físicos (por ejemplo, un botón en el dispositivo).

#### 4.2.6 Medios técnicos y no técnicos

La comunicación de información sobre las capacidades de ciberseguridad del dispositivo (los medios técnicos dentro de este), los medios técnicos que puede proporcionar un dispositivo equivalente o un servicio o sistema del fabricante, los medios no técnicos que proporciona el fabricante o terceros, y los medios no técnicos que los clientes tengan que aplicar ellos mismos, facilita a los clientes entender mejor la manera de gestionar el riesgo al dispositivo. Para determinar la información sobre las capacidades de ciberseguridad de dispositivo que es importante comunicar a los clientes, los fabricantes pueden responder a preguntas como las siguientes:

1. **¿Cuáles medios técnicos puede proporcionar:**
  - a. **el dispositivo mismo (capacidades de ciberseguridad de dispositivo)?** Los ejemplos incluyen cifrado que el dispositivo emplea para proteger los datos, presencia de un identificador físico en el dispositivo y mecanismos de autenticación y autorización que el dispositivo usa para limitar el acceso a sus interfaces de red.
  - b. **un dispositivo relacionado?** Por ejemplo, un concentrador de IoT o un dispositivo móvil al que esté asociado el dispositivo de IoT puede aplicar o admitir algunos medios técnicos.
  - c. **un servicio o sistema del fabricante?** Un ejemplo serían los medios técnicos que proporciona un servidor de internet o un servicio alojado en la nube.
2. **¿Qué medios no técnicos pueden proporcionar el fabricante u otras organizaciones y servicios que actúen en representación del fabricante?** Los ejemplos incluyen muchos de los conceptos descritos en esta sección, como la expectativa de vida útil, los planes de actualización de software y las opciones de retirada. Además de los que se tratan en esta sección, puede haber otros medios no técnicos (por ejemplo, la manera de informar de un defecto o vulnerabilidad) que sería conveniente que los clientes conocieran y entendieran.
3. **¿Cuáles medios técnicos o no técnicos debe proporcionar el cliente, o debería considerar suministrar?** Algunos ejemplos son usar controles de seguridad basados en redes (por ejemplo, un firewall) para evitar el acceso directo al dispositivo desde internet y hacer auditorías de la implementación y configuración de los dispositivos para facilitar que se cumplan los requisitos de cumplimiento.
4. **¿Cómo se prevé que cada uno de los medios técnicos y no técnicos afecte a los riesgos a la ciberseguridad?** Por ejemplo, la debida implementación de la protección de datos ayuda a mitigar los riesgos a la confidencialidad, pero también puede reducir la disponibilidad (por ejemplo, si los datos no se pueden descifrar o se descifran lentamente), lo cual podría aumentar los riesgos a la disponibilidad.

## 5 Conclusión

En esta publicación, se analizan seis actividades relacionadas con la ciberseguridad para los fabricantes de dispositivos de IoT y se dan ejemplos de las preguntas que los fabricantes pueden responder para cada actividad. Los fabricantes que decidan llevar a cabo una o más de estas actividades fundamentales de ciberseguridad deben determinar la aplicabilidad de las preguntas de ejemplo y formular otras que ayuden a conocer las necesidades y metas de ciberseguridad de los clientes, incluidas las capacidades de ciberseguridad de dispositivo que los clientes esperan. Las preguntas resaltadas para cada actividad son un punto de partida y no definen por completo cada actividad. Además, el proceso descrito en esta publicación no presupone que la función de los fabricantes se limita a proporcionar las capacidades que exigen una acción de los clientes, sino que debe hacer que los fabricantes entiendan mejor las necesidades y metas de sus clientes en el contexto de los dispositivos de IoT, lo que podría requerir capacidades automatizadas u otras medidas de soporte no técnicas. Para algunos clientes y casos de uso, dar al cliente responsabilidad limitada de la ciberseguridad (cuando sea posible y apropiado) puede hacer que se logren mejores resultados de ciberseguridad en los ecosistemas que cuando se deja a los clientes toda la carga.

## Referencias

- [1] Simmon, E. (publicación próxima) *A Model for the Internet of Things (IoT)* [Un modelo para la internet de las cosas (IoT)], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland).
- [2] Orden ejecutiva 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [Fortalecimiento de la ciberseguridad de las redes y la infraestructura crítica federales], DCPD-201700327 (11 de mayo de 2017). <https://www.govinfo.gov/app/details/DCPD-201700327>
- [3] Departamento de Comercio (2018), *A Road Map Toward Resilience Against Botnets* [Una hoja de ruta para la resiliencia contra las redes robot], (Departamento de Comercio, Washington, DC). [https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%2012918%20for%20posting\\_0.pdf](https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%2012918%20for%20posting_0.pdf)
- [4] Fagan, M., Megas, K. N., Scarfone, K. y Smith, M. (2020), *IoT Device Cybersecurity Capability Core Baseline* [Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Informe interinstitucional o interno 8259A del NIST. <https://doi.org/10.6028/NIST.IR.8259A>
- [5] *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>
- [6] Instituto Nacional de Normas y Tecnología (2018), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [Marco para la mejora de la ciberseguridad en infraestructuras críticas, versión 1.1], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland). <https://doi.org/10.6028/NIST.CSWP.04162018>
- [7] 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>
- [8] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. y Hahn, A. (2015), *Guide to Industrial Control Systems (ICS) Security* [Guía para la seguridad de los sistemas de control industrial (ICS)], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-82 del NIST, rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>

- [9] *Cyber-Physical Systems Public Working Group* [Grupo de trabajo público de sistemas ciberfísicos] (2017), *Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0* [Marco de los sistemas ciberfísicos: vista general, volumen 1, versión 1.0], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 1500-201 del NIST. <https://doi.org/10.6028/NIST.SP.1500-201>
- [10] Merriam-Webster (2017), *Webster's Third New International Dictionary Unabridged* [Tercer diccionario internacional nuevo de Webster, íntegro], (Merriam-Webster, Springfield, Massachusetts).
- [11] Dodson, D., Souppaya, M. y Scarfone, K. (2019), *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* [Mitigación del riesgo de vulnerabilidades de software mediante la adopción de un marco para el desarrollo seguro de software (SSDF)], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Informe técnico del NIST sobre ciberseguridad. <https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final>

## Apéndice A: Siglas y abreviaturas

Se definen a continuación las siglas y abreviaturas seleccionadas que se usaron en este documento.

API	Application Programming Interface [interfaz de programación de aplicaciones]
CVE	Common Vulnerabilities and Exposures [vulnerabilidades y exposiciones comunes]
DDoS	Distributed Denial of Service [ataque de denegación de servicio distribuido]
FISMA	Federal Information Security Modernization Act [Ley federal de modernización de la seguridad de la información]
FOIA	Freedom of Information Act [Ley de libertad de información]
ICS	Industrial Control System [sistema de control industrial]
IoT	Internet of Things [internet de las cosas (IoT)]
IP	Internet Protocol [protocolo de internet]
IR	Internal Report [Informe interinstitucional o interno]
ITL	Information Technology Laboratory [Laboratorio de tecnología de la información]
LTE	Long-Term Evolution [evolución a largo plazo]
MAC	Media Access Control [control de acceso de medios]
NIST	National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología]
PII	Personally Identifiable Information [información de identificación personal]
ROM	Read-Only Memory [memoria de solo lectura]
SBOM	Software Bill of Materials [lista de materiales de software]
SDK	Software Development Kit [kit de desarrollo de software]
SP	Special Publication [Publicación especial]
SSDF	Secure Software Development Framework [marco para el desarrollo seguro de software]
TI	tecnología de la información
USB	Universal Serial Bus [bus serie universal]
UWB	Ultra-Wideband [banda ultraancha]
wifi	Wireless Fidelity [fidelidad inalámbrica]

## Apéndice B: Glosario

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

actuador	Parte de un dispositivo de IoT con capacidad para cambiar algo en el mundo físico [7].
capacidad de ciberseguridad de dispositivo	Característica o función de ciberseguridad que proporciona un dispositivo de IoT por sus propios medios técnicos (es decir, hardware y software del dispositivo).
dispositivo de IoT mínimamente protegible	Dispositivo de IoT que tiene las capacidades de ciberseguridad de dispositivo (es decir, hardware y software) que los clientes pueden necesitar para implementar los controles de ciberseguridad utilizados para mitigar algunos riesgos comunes a la ciberseguridad.
interfaz de red	Interfaz que conecta un dispositivo de IoT a una red (por ejemplo, Ethernet, wifi, Bluetooth, evolución a largo plazo [LTE], Zigbee, banda ultraancha [UWB]).
medios	“Agente, herramienta, dispositivo, medida, plan o política para lograr o promover un resultado [10]”.
plataforma de IoT	Componente del hardware del dispositivo de IoT que cuenta con software compatible ya instalado y configurado para que lo use un fabricante como base para un nuevo dispositivo de IoT. Una plataforma de IoT también puede ofrecer servicios o aplicaciones de terceros, o un kit de desarrollo de software para agilizar el desarrollo de aplicaciones de IoT.
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 <i>referencia básica</i> .
sensor	Parte de un dispositivo de IoT con capacidad para proporcionar una observación de un aspecto del mundo físico en forma de datos de medición [7].
transductor	Parte de un dispositivo de IoT con capacidad para interactuar directamente con una entidad física de interés. Los dos tipos de transductores son sensores y actuadores [7].