Informe interinstitucional o interno 8228 del NIST

Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8228es

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

Informe interinstitucional o interno 8228 del NIST

Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Ben Piccarreta
División de ciberseguridad aplicada
Laboratorio de tecnología de la información

Danna Gabel O'Rourke
Deloitte & Touche LLP
Arlington, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8228es

Junio de 2019

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 interno 8228 del Instituto Nacional de Normas y Tecnología
50 páginas (Junio de 2019)

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.IR.8228es

Los comentarios sobre esta publicación se pueden enviar al:

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

Disclaimer

Informes sobre la tecnología de los sistemas informáticos

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

Resumen

La internet de las cosas (IoT) es un conjunto de diversas tecnologías que evolucionan y se difunden con rapidez, y que interactúan con el mundo físico. Muchas organizaciones no se dan cuenta del gran número de dispositivos de IoT que ya están utilizando, ni de que los dispositivos de IoT pueden afectar a los riesgos a la ciberseguridad y la privacidad de manera distinta de los dispositivos de tecnología de la información (TI) convencionales. El objetivo de esta publicación es ayudar a los organismos federales y otras organizaciones a conocer y gestionar mejor los riesgos a la ciberseguridad y la privacidad asociados con sus dispositivos individuales de IoT durante el ciclo de vida de estos. Esta publicación es un documento introductorio que sirve de base para una serie de publicaciones planificadas sobre aspectos más específicos de este tema.

Palabras clave

Riesgo a la ciberseguridad, internet de las cosas (IoT), riesgo a la privacidad, gestión de riesgos y mitigación de riesgos.

Agradecimientos

Los autores agradecen a todos los colaboradores de esta publicación, a los participantes en los talleres y otras sesiones interactivas y a las personas y organizaciones de los sectores público y privado que contribuyeron con sus comentarios acerca de las ideas preliminares, así como a las siguientes personas del NIST: Curt Barker, Matt Barrett, Barbara Cuthill, Donna Dodson, Jim Foti, Ned Goren, Nelson Hastings, Jody Jacobs, Suzanne Lightman, Jeff Marron, Vicky Pillitteri, Tim Polk, Matt Scholl, Eric Simmon, Matt Smith, Murugiah Souppaya, Jim St. Pierre, Kevin Stine y David Wollman.

Público

Esta publicación se dirige principalmente al personal de los organismos federales cuyas responsabilidades se relacionan con la gestión de riesgos a la ciberseguridad y la privacidad de dispositivos de IoT, aunque también puede ser de utilidad para el personal de otras organizaciones. Es más probable que esta publicación sea de interés para el personal de las siguientes categorías de personal y áreas de especialización del Marco para el personal de ciberseguridad de la Iniciativa nacional para la educación en ciberseguridad (NICE, por sus siglas en inglés) [1], así como para sus colegas a cargo de la privacidad:

- Suministrar protección (SP): Gestión de riesgos (RSK), Arquitectura de sistemas (ARC), Desarrollo de sistemas (SYS)
- Operar y mantener (OM): Administración de datos (DTA), Servicios de red (NET), Administración de sistemas (ADM), Análisis de sistemas (ANA)
- Supervisar y gobernar (OV): Gestión de ciberseguridad (MGT), Dirección ejecutiva de cibernética (EXL), Gestión de programas, proyectos y adquisiciones (PMA)
- Proteger y defender (PR): Análisis de defensa de la ciberseguridad (CDA), Soporte de la infraestructura de defensa de la ciberseguridad (INF), Respuesta a incidentes (CIR), Evaluación y gestión de vulnerabilidades (VAM)
- Investigar (IN): Investigación forense digital (FOR)

Además, es posible que los fabricantes e integradores de dispositivos de IoT descubran que esta publicación es útil para entender los problemas relacionados con la gestión de riesgos a la ciberseguridad y la privacidad de esos dispositivos.

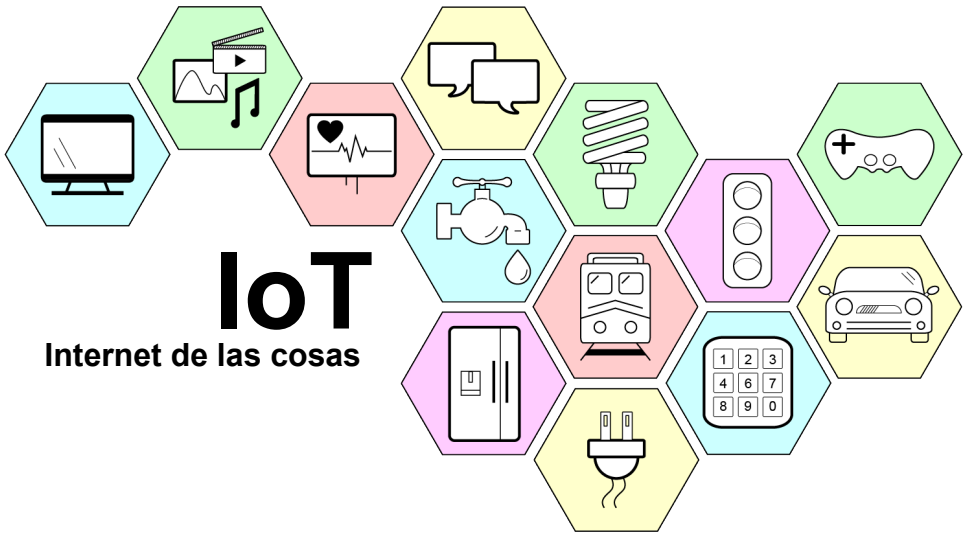
Nota para los lectores

Anteriormente, el Apéndice A incluía ejemplos de las posibles capacidades de ciberseguridad y privacidad que las organizaciones pueden desear en sus dispositivos de IoT. Ese contenido se eliminó de esta publicación y se refinará y publicará en un documento aparte.

Información sobre marcas comerciales

Resumen ejecutivo

La internet de las cosas (IoT) es un conjunto de diversas tecnologías que evolucionan y se difunden con rapidez, y que interactúan con el mundo físico. Los dispositivos de IoT son el resultado de combinar el mundo de la tecnología de la información (TI) con el mundo de la tecnología operativa (TO). Muchos dispositivos de IoT provienen de la convergencia de la informática en la nube, la informática móvil, los sistemas integrados, los macrodatos, el hardware de precio bajo y otros avances tecnológicos. Los dispositivos de IoT pueden proporcionar funcionalidad informática, almacenamiento de datos y conectividad de red a equipos que antes no los tenían, y habilitar nuevas eficiencias y capacidades tecnológicas para el equipo, como acceso remoto para vigilancia, configuración y solución de problemas. La IoT también puede incorporar capacidades para analizar datos acerca del mundo físico y utilizar los resultados para tomar decisiones mejor informadas, modificar el entorno físico y prever eventos futuros.



El alcance total de la IoT no está definido con precisión; sin embargo, es evidentemente vasto. Cada sector tiene sus propios tipos de dispositivos de IoT, como los equipos médicos especializados en el sector del cuidado de la salud y las tecnologías de carreteras inteligentes en el sector del transporte, y hay un gran número de dispositivos de IoT empresariales que todos los sectores pueden usar. Las versiones de casi todos los dispositivos electrónicos del consumidor, muchos de los cuales también están presentes en las instalaciones de organizaciones, se han convertido en dispositivos de IoT conectados: aparatos electrodomésticos, termostatos, cámaras de seguridad para el hogar, cerraduras de puertas, bombillas y televisores. [2]

Muchas organizaciones no se dan cuenta de que están utilizando un gran número de dispositivos de IoT, y es importante que entiendan el uso que hacen de la IoT porque muchos dispositivos de IoT afectan a los riesgos a la ciberseguridad y la privacidad de manera distinta de los dispositivos de TI convencionales. Una vez que las organizaciones son conscientes de su uso actual de la IoT y de su posible uso futuro, necesitan entender la manera en que las características de la IoT afectan la gestión de riesgos a la ciberseguridad y la privacidad, especialmente en lo que se refiere a la respuesta a los riesgos (aceptar, evitar, mitigar, compartir o transferir el riesgo).

Esta publicación identifica tres consideraciones de alto nivel que pueden afectar la gestión de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT en comparación con los dispositivos de TI convencionales:

1. **Muchos dispositivos de IoT interactúan con el mundo físico de maneras que los dispositivos de TI convencionales no lo hacen normalmente.** Es necesario reconocer y considerar explícitamente, desde las perspectivas de la ciberseguridad y la privacidad, el impacto potencial de algunos dispositivos de IoT que hacen cambios en los sistemas físicos y afectan con ello el mundo físico. Además, los requisitos operativos de rendimiento, confiabilidad, resiliencia y seguridad pueden contradecir las prácticas comunes de ciberseguridad y privacidad de los dispositivos de TI convencionales.
2. **El acceso, la gestión o la vigilancia de muchos dispositivos de IoT no se puede hacer de la misma manera que para los dispositivos de TI convencionales.** Para esto puede ser necesario efectuar manualmente tareas para un gran número de dispositivos de IoT, ampliar los conocimientos y las herramientas del personal para que incluya una variedad mayor de software de dispositivos de IoT, y resolver los riesgos junto con los fabricantes y otros terceros que tengan acceso a los dispositivos de IoT, o control sobre estos, de manera remota.
3. **La disponibilidad, eficiencia y efectividad de las capacidades de ciberseguridad y privacidad suelen ser diferentes para los dispositivos de IoT que para los dispositivos de TI convencionales.** Esto significa que es posible que las organizaciones tengan que seleccionar, implementar y gestionar más controles, así como determinar la manera de responder a los riesgos cuando no se dispone de controles suficientes para mitigarlos.

Los riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT se pueden considerar en términos de tres metas de mitigación de riesgos de alto nivel:

1. **Proteger la seguridad del dispositivo.** En otras palabras, evitar que un dispositivo sea usado para llevar a cabo ataques, que incluye participar en ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés) contra otras organizaciones, interceptar el tráfico de red o poner en riesgo dispositivos en el mismo segmento de red. Esta meta se aplica a todos los dispositivos de IoT.
2. **Proteger la seguridad de los datos.** Proteger la confidencialidad, integridad o disponibilidad de los datos (incluida la información de identificación personal [PII, por sus siglas en inglés]) recopilados, almacenados, procesados o transmitidos al dispositivo de IoT o desde este. Esta meta se aplica a todos los dispositivos de IoT, a excepción de los que no tengan datos que necesiten protección.
3. **Proteger la privacidad de las personas.** Proteger la privacidad de las personas afectadas por el procesamiento de PII más allá de los riesgos que gestiona la protección de la seguridad del dispositivo y de los datos. Esta meta se aplica a todos los dispositivos de IoT que procesan PII o que afectan directa o indirectamente a las personas.

Cada meta se basa en la meta anterior, sin reemplazarla ni anular la necesidad de esta. El logro de cada una de las metas de mitigación de riesgos implica tomar en cuenta un conjunto de áreas de mitigación de riesgos. Cada área de mitigación de riesgos define un aspecto de la mitigación de riesgos a la ciberseguridad o la privacidad de la IoT que se considera afectado de manera más significativa o imprevista por las consideraciones de los riesgos. Para cada área de mitigación de

riesgos las organizaciones suelen tener una o más expectativas de la manera en que los dispositivos de TI convencionales ayudan a mitigar los riesgos a la ciberseguridad y la privacidad para esa área. Por último, hay uno o más problemas que los dispositivos de IoT pueden plantear para cada expectativa. En la figura siguiente, se describe el resultado final de estos vínculos, es decir la identificación de un conjunto estructurado de problemas potenciales con la mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT cuyo origen se puede rastrear hasta las consideraciones del riesgo correspondiente.

Consideraciones de los riesgos

Por qué y de qué manera los dispositivos de IoT afectan la gestión de riesgos a la ciberseguridad y la privacidad

Metas y áreas de mitigación de riesgos

Tipos de riesgos a la ciberseguridad y la privacidad que son importantes para los dispositivos de IoT y que pueden verse más afectados por las **consideraciones de riesgos**

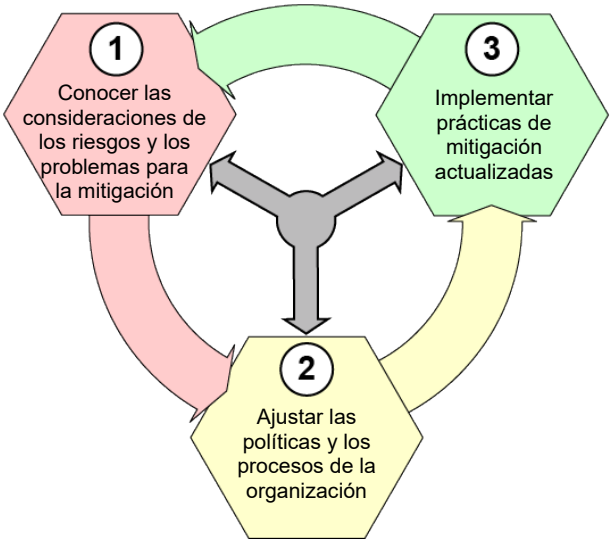
Expectativas

Cómo esperan las organizaciones que los dispositivos de TI convencionales ayuden a mitigar los riesgos a la ciberseguridad y la privacidad para las **metas y áreas de mitigación de riesgos**

Problemas

Qué problemas pueden plantear los dispositivos de IoT para las **expectativas** y cuáles son las repercusiones de esos problemas

Las organizaciones deben cerciorarse de tener en cuenta las consideraciones y los problemas de los riesgos a la ciberseguridad y la privacidad durante todo el ciclo de vida del dispositivo de IoT para las metas y áreas de mitigación de riesgos correspondientes. Esta publicación proporciona las siguientes recomendaciones para lograrlo:



1. Conocer las consideraciones de los riesgos a los dispositivos de IoT y los problemas que puedan causar a la mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT en las áreas de mitigación de riesgos correspondientes.
2. Ajustar las políticas y los procesos de la organización para solucionar los problemas de mitigación de riesgos a la ciberseguridad y la privacidad durante todo el ciclo de vida del dispositivo de IoT. En esta publicación, se citan muchos ejemplos de posibles problemas, pero cada organización necesitará personalizarlos para tener en cuenta los requisitos de la misión y otras características específicas de la organización.
3. Implementar prácticas de mitigación actualizadas para los dispositivos de IoT de la organización como se haría con cualquier otro cambio en las prácticas.

Índice

Lista de apéndices

Lista de figuras

Lista de tablas

1 Introducción

1.1 Objetivo y alcance

El objetivo de esta publicación es ayudar a las organizaciones a conocer y gestionar mejor los riesgos a la ciberseguridad y la privacidad asociados con los dispositivos individuales de internet de las cosas (IoT) durante el ciclo de vida de estos. En esta publicación, se hace hincapié en la diferencia de gestionar estos riesgos para los dispositivos de IoT en general, incluidos los dispositivos de IoT de consumidores, empresas e industrias, con respecto a los dispositivos de tecnología de la información (TI) convencionales. Se omiten todos los aspectos de la gestión de riesgos que sean mayormente los mismos para la IoT y la TI convencional, entre otros, todos los aspectos de la gestión de riesgos más allá de los dispositivos mismos de IoT, ya que estos se tratan en muchas otras publicaciones de gestión de riesgos.

Esta publicación proporciona información que sirve de base para los procesos de gestión de riesgos de las organizaciones. Después de leerla, una organización debe poder mejorar la calidad de sus evaluaciones de riesgos para los dispositivos de IoT y de su respuesta a los riesgos identificados desde el punto de vista de la ciberseguridad y la privacidad. Sin embargo, esto no significa que todos los riesgos a la ciberseguridad y la privacidad de un dispositivo de IoT se pueden plantear dentro del dispositivo mismo. Cada dispositivo de IoT funciona dentro de un entorno de IoT más amplio en el cual interactúa con otros dispositivos de IoT y que no son de IoT, así como con servicios basados en la nube, personas y otros componentes.

En el caso de algunos dispositivos de IoT, es necesario gestionar otros tipos de riesgos (como el riesgo a la seguridad, la confiabilidad o la resiliencia) al mismo tiempo que los riesgos a la ciberseguridad y la privacidad debido a los efectos que la solución de un tipo de riesgo puede tener en los demás. En esta publicación, solo se tratan los riesgos a la ciberseguridad y la privacidad. Para los lectores interesados particularmente en conocer mejor otros tipos de riesgos y su relación con la ciberseguridad y la privacidad, puede ser conveniente la lectura de la Publicación especial (SP, por sus siglas en inglés) 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)], que ofrece una perspectiva de la tecnología operativa (TO) sobre la ciberseguridad y la privacidad. [3]

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 y la privacidad.

1.2 Estructura de la publicación

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

- La Sección 2 define las capacidades que los dispositivos de IoT pueden ofrecer y que son de interés primordial debido a que afectan potencialmente a los riesgos a la ciberseguridad y la privacidad.
- La Sección 3 describen las consideraciones que podrían afectar la gestión de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT.

- La Sección 4 analiza la manera en que las consideraciones de los riesgos pueden afectar la mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT. También enumera las expectativas de la mitigación de estos riesgos en los entornos convencionales de TI, y luego explica los problemas que la IoT plantea para esas expectativas y las repercusiones potenciales de esos problemas.
- La Sección 5 ofrece recomendaciones a las organizaciones sobre la manera de resolver los problemas de la mitigación de riesgos a la ciberseguridad y la privacidad para sus dispositivos de IoT.
- Anteriormente, el Apéndice A incluía ejemplos de las posibles capacidades de ciberseguridad y privacidad que las organizaciones pueden desear en sus dispositivos de IoT. Ese contenido se eliminó de esta publicación y se refinará y publicará en un documento aparte.
- El Apéndice B contiene una lista de siglas y abreviaturas.
- El Apéndice C proporciona un glosario de los términos seleccionados que se usaron en esta publicación.
- El Apéndice D enumera las referencias hechas en la publicación.

La Figura 1 describe los temas tratados en cada sección y subsección de esta publicación.

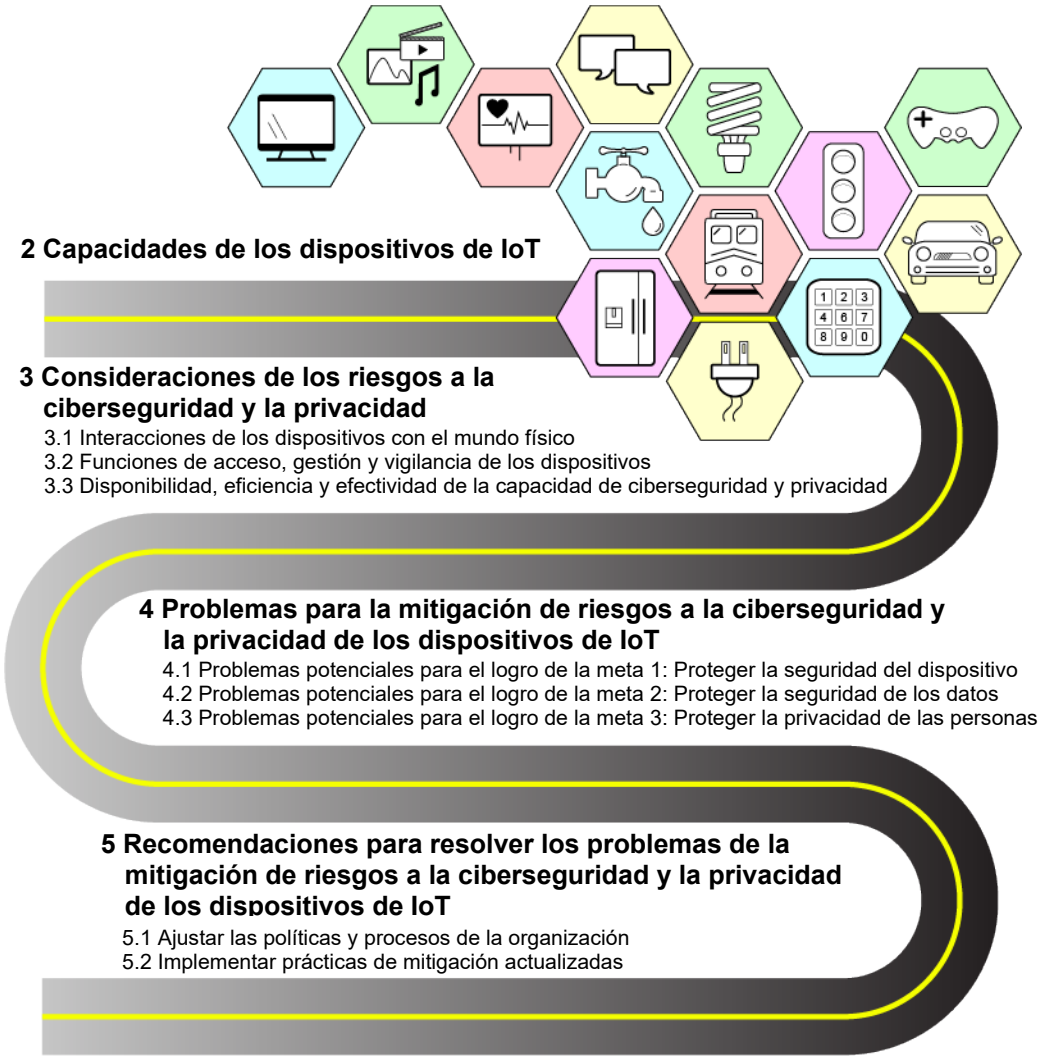


Figura 1: Temas tratados en esta publicación

2 Capacidades de los dispositivos de IoT

Cada dispositivo de IoT proporciona *capacidades* (características o funciones) que puede usar por sí solo o junto con otros dispositivos de IoT y que no sean de IoT para lograr una o más metas. Esta publicación hace referencia a los siguientes tipos de capacidades que los dispositivos de IoT ofrecen y que son de interés primordial debido a que afectan potencialmente a los riesgos a la ciberseguridad y la privacidad de manera distinta de los dispositivos de TI convencionales. Esta no es una lista exhaustiva de las capacidades posibles de los dispositivos de IoT.

- Las *capacidades de transductor* interactúan con el mundo físico y sirven como el borde entre el entorno digital y el físico. Las capacidades de transductor proporcionan la capacidad para que los dispositivos informáticos interactúen directamente con entidades físicas de interés. Cada dispositivo de IoT tiene al menos una capacidad de transductor. Los dos tipos de capacidades de transductor son:
  - *Detección*: capacidad para hacer la observación de un aspecto del mundo físico en forma de datos de medición. Los ejemplos incluyen la medición de temperatura, generación de imágenes radiográficas, detección óptica y detección de audio.
  - *Accionamiento*: capacidad para cambiar algo en el mundo físico. Los ejemplos de capacidades de accionamiento incluyen serpentines de calefacción, aplicación de cardioversión eléctrica, cerraduras electrónicas de puertas, operación de vehículos aéreos no tripulados, servomotores y brazos robóticos.
- Las *capacidades de interfaz* habilitan las interacciones de los dispositivos (por ejemplo, comunicaciones de dispositivo a dispositivo, comunicaciones de persona a dispositivo). Los tipos de capacidades de interfaz son:
  - *Interfaz de aplicación*: capacidad de otros dispositivos informáticos para comunicarse con un dispositivo de IoT por medio de una aplicación de dispositivo de IoT. Un ejemplo de capacidad de interfaz de aplicación es una interfaz de programación de aplicaciones (API, por sus siglas en inglés).
  - *Interfaz de usuario humano*: capacidad de un dispositivo de IoT y de las personas para comunicarse directamente entre sí. Los ejemplos de funciones de interfaz de usuario humano incluyen pantallas táctiles, dispositivos hápticos, micrófonos, cámaras y altavoces.
  - *Interfaz de red*: capacidad para interactuar con una red de comunicación con el fin de comunicar datos a un dispositivo de IoT, o desde este, es decir, para usar una red de comunicación. Una capacidad de interfaz de red incluye tanto hardware como software (por ejemplo, una tarjeta o un chip de interfaz de red y la implementación del software del protocolo de red que utiliza la tarjeta o el chip). Los ejemplos de capacidades de interfaz de red incluyen Ethernet, wifi, Bluetooth, evolución a largo plazo (LTE, por sus siglas en inglés) y ZigBee. Cada dispositivo de IoT tiene al menos una capacidad de interfaz de red habilitada y puede tener más de una.
- Las *capacidades de soporte* proporcionan una funcionalidad compatible con las demás capacidades de IoT. Algunos ejemplos son gestión del dispositivo y capacidades de ciberseguridad y privacidad. [2]

La Figura 2 resume estas capacidades de los dispositivos de IoT.

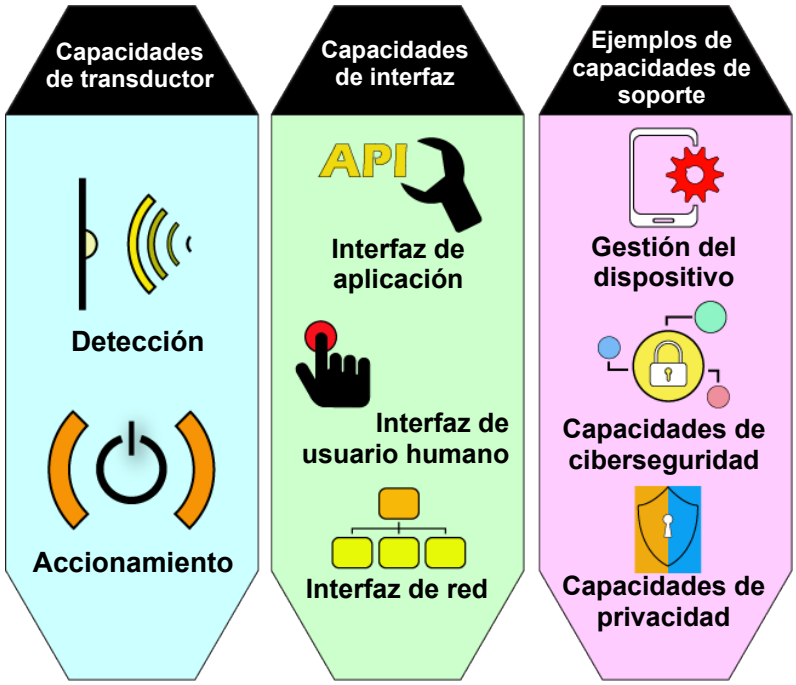


Figura 2: Capacidades de los dispositivos de IoT que afectan potencialmente a los riesgos a la ciberseguridad y la privacidad

3 Consideraciones de los riesgos a la ciberseguridad y la privacidad

Los conceptos de riesgo a la ciberseguridad y riesgo a la privacidad están relacionados, pero son distintos. El *riesgo* se define en la Publicación especial 800-37 del NIST, revisión 2, como "la medida en que una entidad es amenazada por una posible circunstancia o evento. Es normalmente una función de: (i) el efecto adverso, o la magnitud del daño, que tendría la circunstancia o el evento si llegara a ocurrir; y (ii) la probabilidad de que ocurra". [4] En cuanto a la ciberseguridad, el riesgo se trata de amenazas: la explotación de vulnerabilidades por los actores de amenazas que ponen en peligro la confidencialidad, integridad o disponibilidad de dispositivos o datos. Para la privacidad, el riesgo son *acciones problemáticas de datos*, es decir, operaciones que procesan información de identificación personal (PII) durante el ciclo de vida de la información para satisfacer las necesidades empresariales o de la misión de una organización o el procesamiento "autorizado" de PII y, como efecto secundario, causan a las personas algún tipo de problema. Como se describe en la Figura 3, los riesgos a la privacidad y a la ciberseguridad se superponen a las inquietudes por la ciberseguridad de la PII, pero también hay inquietudes por la privacidad que no tienen que ver con la ciberseguridad, e inquietudes por la ciberseguridad que no tienen que ver con la privacidad. [5]

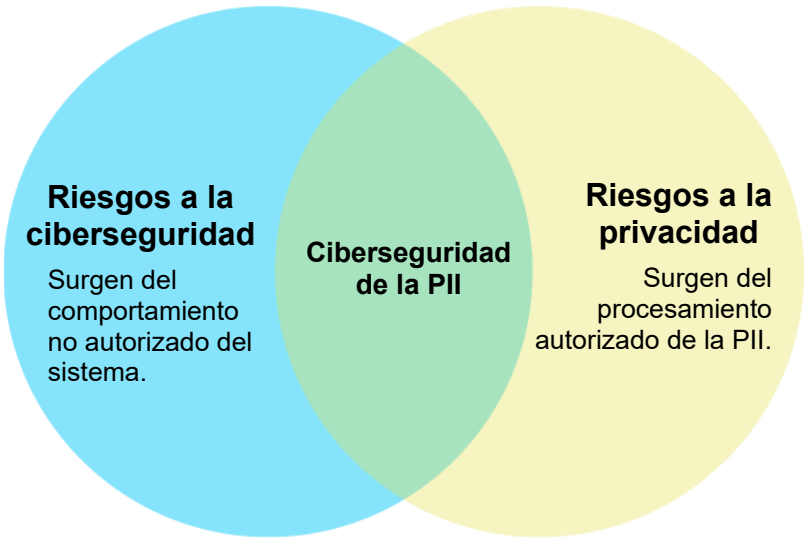


Figura 3: Relación entre los riesgos a la ciberseguridad y a la privacidad

Los dispositivos de IoT se enfrentan por lo general a los mismos tipos de riesgos a la ciberseguridad y la privacidad que los dispositivos de TI convencionales, aunque la prevalencia y la gravedad de esos riesgos suelen ser distintas. Por ejemplo, los riesgos a la seguridad de los datos son casi siempre una inquietud importante para los dispositivos de TI convencionales, pero para algunos dispositivos de IoT, es posible que no existan riesgos a la seguridad de los datos porque no tienen datos que necesiten protección.

En esta sección, se definen tres consideraciones de los riesgos a la ciberseguridad y la privacidad que pueden afectar la gestión de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT. Las organizaciones deben asegurarse de tener en cuenta estas consideraciones de los riesgos durante todo el ciclo de vida de sus dispositivos de IoT. La Sección 4 proporciona más información sobre la manera en que estas consideraciones de los riesgos pueden afectar su

mitigación, y la Sección 5 ofrece recomendaciones para las organizaciones sobre la forma de solucionar los problemas de mitigación de riesgos.

3.1 Consideración 1: Interacciones de los dispositivos con el mundo físico

Muchos dispositivos de IoT interactúan con el mundo físico de maneras que los dispositivos de TI convencionales no lo hacen normalmente.

Las interacciones con el mundo físico que facilitan los dispositivos de IoT pueden afectar a los riesgos a la ciberseguridad y la privacidad de varias maneras. Estos son algunos ejemplos:

- Siempre hay incertidumbres asociadas con los datos de sensores de IoT que representan las mediciones del mundo físico. La gestión efectiva de los datos de sensores de IoT, que incluye el conocimiento de las incertidumbres, es necesaria para evaluar la calidad y el significado de los datos, de manera que la organización pueda tomar decisiones sobre el uso de los datos y evitar la introducción de nuevos riesgos. Sin esto, tal vez se desconozcan las tasas de errores de los diferentes contextos en los que se podría usar un dispositivo de IoT[1]. La gestión efectiva de los datos de sensores de IoT es importante cuando se mitigan ataques físicos contra la tecnología de sensores, como los ataques que se llevan a cabo a través de señales inalámbricas y que podrían causar que los sensores generen resultados falsos.
- La presencia generalizada de los sensores de IoT en entornos públicos y privados puede contribuir a la agregación y el análisis de enormes cantidades de datos acerca de las personas. Estas actividades se pueden usar para influir en el comportamiento o la toma de decisiones de las personas de maneras que estas no entiendan, o dar lugar a que se revele información que las personas no deseaban revelar, incluida la reidentificación de PII que previamente fue desidentificada, lo que puede exceder el alcance previsto originalmente de la operación del dispositivo de IoT.
- Los dispositivos de IoT que tienen actuadores pueden hacer cambios en los sistemas físicos y afectar con ello el mundo físico. Es necesario reconocer y considerar explícitamente el impacto potencial de esto desde las perspectivas de la ciberseguridad y la privacidad. En el peor de los casos, una situación de riesgo podría permitir a un atacante utilizar un dispositivo de IoT para poner en peligro la seguridad de las personas, dañar o destruir equipos e instalaciones, o causar interrupciones operativas considerables. Las inquietudes por la privacidad y las libertades civiles podrían surgir de los cambios autorizados hechos a sistemas físicos y afectar la autonomía física o el comportamiento de las personas en espacios privados y públicos. Por ejemplo, los controles de acceso físico, como las cerraduras automáticas de puertas, se podrían usar para limitar el acceso a habitaciones o edificios donde haya personas dentro, o bien los controles ambientales, como la iluminación o la temperatura, se podrían usar para influir en el movimiento de las personas en los edificios.
- Las interfaces de red de IoT a menudo permiten el acceso remoto a sistemas físicos a los que antes solo se podía acceder localmente. Los fabricantes, proveedores y otros terceros

[1] Para obtener más información sobre la incertidumbre de las mediciones, véase https://www.nist.gov/itl/sed/topic-areas/measurement-uncertainty.

pueden usar el acceso remoto a los dispositivos de IoT para fines de gestión, vigilancia, mantenimiento y solución de problemas. Esto puede exponer los sistemas físicos que son accesibles a través de dispositivos de IoT a un riesgo mucho mayor. Además, estas funciones descentralizadas de tratamiento de datos pueden exacerbar algunos riesgos a la privacidad, y dificultar que las personas entiendan la manera en que funciona el sistema de IoT para que puedan tomar decisiones informadas acerca del procesamiento de su información y de sus interacciones con el sistema de IoT.

Otro aspecto importante de las interacciones de los dispositivos de IoT con el mundo físico son los requisitos operativos que los dispositivos deben cumplir en varios entornos y casos de uso. Muchos dispositivos de IoT deben cumplir con requisitos estrictos de rendimiento, confiabilidad, resiliencia, seguridad y otros objetivos. Estos requisitos pueden contradecir las prácticas comunes de ciberseguridad y privacidad de la TI convencional. Por ejemplo, las prácticas como la aplicación automática de parches se consideran generalmente esenciales para la TI convencional, aunque estas prácticas podrían tener efectos mucho más negativos en algunos de los dispositivos de IoT con actuadores, haciendo que los servicios críticos no estén disponibles y poniendo en peligro la seguridad humana. Una organización podría decidir de manera razonable que tiene que aplicar parches y seleccionar la fecha y hora para hacerlo, teniendo el personal apropiado en el lugar, listo para responder inmediatamente en caso de que ocurra algún problema. Una organización también podría decidir de manera razonable evitar la aplicación de parches en ciertos dispositivos de IoT en circunstancias normales y, en vez de ello, restringir estrictamente el acceso lógico y físico a estos para evitar la explotación de las vulnerabilidades que no tengan parches.

Otra forma de pensar en esto sería en términos de los objetivos generales de la ciberseguridad: confidencialidad, integridad y disponibilidad. En el caso de los dispositivos de TI convencionales, la confidencialidad suele recibir la atención mayor debido al valor de los datos y a las consecuencias que tendría una vulneración de la confidencialidad. Para muchos dispositivos de IoT, la disponibilidad y la integridad son más importantes que la confidencialidad debido al impacto potencial para el mundo físico. Por ejemplo, un dispositivo de IoT que sea indispensable para evitar daños a una instalación. Es posible que un atacante que pueda ver los datos almacenados en el dispositivo de IoT, o transmitidos por este, no obtenga ninguna ventaja ni valor de esos datos, pero un atacante que pueda alterar los datos podría desencadenar una serie de eventos y causar un incidente.

3.2 Consideración 2: Funciones de acceso, gestión y vigilancia de los dispositivos

El acceso, la gestión o la vigilancia de muchos dispositivos de IoT no se puede hacer de la misma manera que para los dispositivos de TI convencionales.

Los dispositivos de TI convencionales suelen proporcionar a las personas, procesos y dispositivos autorizados funciones de acceso, gestión y vigilancia de hardware y software. En otras palabras, un administrador, proceso o dispositivo autorizado puede acceder directamente al firmware, el sistema operativo y las aplicaciones de un dispositivo de TI convencional, gestionar por completo el dispositivo y su software durante todo el ciclo de vida del dispositivo según sea necesario y vigilar las características internas y el estado del dispositivo en todo momento. Los

usuarios autorizados también pueden acceder a un subconjunto restringido de las funciones de acceso, gestión y vigilancia.

En cambio, muchos dispositivos de IoT son opacos y a menudo se denominan “cajas negras”. Ofrecen poca o ninguna visibilidad de su estado y composición, incluida la identidad de los servicios o sistemas externos con los que interactúan, y poco o ningún acceso a su software y configuración, o a la gestión de estos. Es posible que la organización desconozca las capacidades que un dispositivo de IoT puede proporcionar o que está proporcionando en ese momento. En casos extremos, tal vez sea difícil determinar si un producto de caja negra es realmente un dispositivo de IoT debido a la falta de transparencia.

Las personas, procesos y dispositivos autorizados pueden encontrar uno o más de los siguientes problemas al acceder, gestionar o vigilar los dispositivos de IoT que afectan a los riesgos a la ciberseguridad y la privacidad:

- **Falta de funciones de gestión.** Es posible que los administradores no puedan gestionar completamente el firmware, el sistema operativo y las aplicaciones de un dispositivo de IoT durante todo su ciclo de vida. Las funciones que no están disponibles podrían incluir la capacidad de adquirir software, verificar su integridad, instalarlo, configurarlo, almacenarlo, recuperarlo, ejecutarlo, eliminarlo, removerlo, reemplazarlo, actualizarlo y aplicarle parches. Además, el software de un dispositivo de IoT se puede reconfigurar automáticamente cuando ocurre un evento adverso, como una falla de energía o una pérdida de conectividad de red.
- **Falta de interfaces.** Algunos dispositivos de IoT carecen de interfaces de aplicación o de usuario humano para el uso y la gestión de dispositivos. Cuando existen estas interfaces, es posible que no proporcionen la funcionalidad que suelen ofrecer los dispositivos de TI convencionales. Un ejemplo es el problema para notificar a los usuarios acerca del procesamiento de su PII que haga un dispositivo de IoT de manera que puedan dar su consentimiento formal a este procesamiento. Otro problema es la falta de estándares universalmente aceptados para las interfaces de aplicaciones de IoT que incluyan expresar y formatear datos, emitir comandos y propiciar de otro modo la interoperabilidad entre los dispositivos de IoT.
- **Dificultades con la gestión a escala.** La mayoría de los dispositivos de IoT no son compatibles con mecanismos estandarizados para la gestión centralizada, y el número total de dispositivos de IoT que deban ser gestionados puede ser abrumador.
- **Amplia variedad de software para gestionar.** El software que utilizan los dispositivos de IoT es muy diverso e incluye firmware, sistemas operativos estándar y en tiempo real, y aplicaciones. Esto complica considerablemente la gestión del software durante todo el ciclo de vida del dispositivo de IoT, y afecta áreas como la configuración y la gestión de parches.
- **Expectativas de vida útil diferentes.** Un fabricante puede planificar que un dispositivo de IoT particular se utilice solo algunos años y luego sea desechado. Una organización que compre ese dispositivo podría desear utilizarlo por más tiempo, pero es posible que el fabricante suspenda el soporte del dispositivo (por ejemplo, no distribuir parches para vulnerabilidades conocidas) sea por decisión o debido a limitaciones de la cadena de suministro (por ejemplo, el proveedor ya no ofrece parches para un componente en

particular del dispositivo de IoT). El problema de las expectativas de vida útil diferentes no es nuevo ni específico de la IoT, pero puede ser de particular importancia para algunos dispositivos de IoT debido a la seguridad, la confiabilidad y otros riesgos potenciales debidos al uso de los dispositivos más allá de su vida útil prevista.

- **Hardware que no admite mantenimiento.** Es posible que el hardware del dispositivo de IoT no admita mantenimiento, es decir, que no se pueda reparar, personalizar ni inspeccionar internamente.
- **Falta de capacidades de inventario.** Puede ser que los dispositivos de IoT que adquiera una organización no se puedan inventariar, registrar ni abastecer por medio de los procesos normales de la TI. Esto se aplica especialmente a los tipos de dispositivos que antes no tenían capacidades de red.
- **Propiedad heterogénea.** La propiedad de los dispositivos de IoT suele ser heterogénea. Por ejemplo, un dispositivo de IoT puede transferir datos para que un servicio basado en la nube que suministra el fabricante los procese y almacene. Los datos también se pueden enviar a un servicio en la nube para agregar datos de varios dispositivos de IoT en una ubicación única. Estos servicios en la nube pueden tener acceso a parte o a todos los datos de los dispositivos, o incluso acceso a los dispositivos mismos y control de estos con fines de vigilancia, mantenimiento y solución de problemas. En algunos casos, solo los fabricantes tienen autoridad para efectuar tareas de mantenimiento; una organización que intente instalar parches o hacer otras tareas de mantenimiento en un dispositivo de IoT podría anular la garantía. Además, tal vez haya poca o ninguna información disponible en la IoT acerca de la propiedad del dispositivo, especialmente de los dispositivos de IoT de caja negra. Esto podría empeorar las dificultades existentes para la corrección de problemas de privacidad, porque la falta de rendición de cuentas limitaría la capacidad de las personas para ubicar el origen y corregir o eliminar información sobre sí mismas, o para solucionar otros problemas. Otra inquietud de la propiedad heterogénea es el efecto sobre el reabastecimiento de un dispositivo; es decir, los datos que pueden seguir estando disponibles después de que se transfiere el control del dispositivo.

3.3 Consideración 3: Disponibilidad, eficiencia y efectividad de las capacidades de ciberseguridad y privacidad

La disponibilidad, eficiencia y efectividad de las capacidades de ciberseguridad y privacidad suelen ser diferentes para los dispositivos de IoT que para los dispositivos de TI convencionales.

Para los fines de esta publicación, las capacidades integradas de ciberseguridad y privacidad se denominan *capacidades anteriores al mercadeo*. El fabricante o el vendedor integran las capacidades anteriores al mercadeo en los dispositivos de IoT antes de enviarlos a las organizaciones de los clientes. Las *capacidades posteriores al mercadeo* son aquellas que las organizaciones seleccionan, adquieren e implementan ellas mismas, además de las capacidades anteriores al mercadeo. Las capacidades de ciberseguridad y privacidad anteriores y posteriores al mercado suelen ser diferentes para los dispositivos de IoT que para los de TI convencionales. Los motivos principales son:

- Muchos dispositivos de IoT no son compatibles o no pueden ser compatibles con la variedad de capacidades de ciberseguridad y privacidad que se integran normalmente en los dispositivos de TI convencionales. Por ejemplo, es posible que un dispositivo de IoT de "caja negra" no registre sus eventos de ciberseguridad y privacidad o no dé a las organizaciones acceso a sus registros. Si los dispositivos de IoT disponen de capacidades anteriores al mercadeo, estas tal vez no sean suficientes en términos de solidez o rendimiento, por ejemplo, el uso de cifrado sólido y autenticación mutua para proteger las comunicaciones podría causar demoras inaceptables[2]. Hay capacidades posteriores al mercadeo que no se pueden instalar en muchos dispositivos de IoT. Además, puede ser que las capacidades existentes anteriores y posteriores al mercadeo no se adapten para satisfacer las necesidades de IoT; por ejemplo, es posible que un dispositivo de ciberseguridad existente basado en la red para dispositivos de TI convencionales no pueda procesar también el volumen de tráfico de red y los datos que se generen de un gran número de dispositivos de IoT.
- El nivel de trabajo necesario para gestionar, vigilar y mantener las capacidades anteriores al mercadeo de cada dispositivo de IoT puede ser excesivo. En particular, cuando los dispositivos de IoT no aceptan la gestión centralizada, puede ser más eficiente implementar y usar capacidades posteriores al mercadeo centralizadas que ayuden a proteger muchos dispositivos de IoT, en lugar de intentar alcanzar el nivel equivalente de protección en cada dispositivo individual de IoT. Un ejemplo es tener una puerta única de enlace de IoT basada en red o una puerta de enlace de seguridad de IoT que proteja muchos dispositivos de IoT en lugar de tener que diseñar, gestionar y mantener un conjunto único de capacidades de protección dentro de cada dispositivo de IoT.
- Es posible que algunas capacidades posteriores al mercadeo de la TI convencional, como los sistemas de prevención de intrusiones basados en red, los servidores antimalware y los firewalls, no protejan tan efectivamente los dispositivos de IoT como protegen los de TI convencionales. Con frecuencia, los dispositivos de IoT utilizan protocolos que los controles de ciberseguridad y privacidad de TI convencional no pueden entender ni analizar. Además, los dispositivos de IoT se pueden comunicar directamente entre sí, como, por ejemplo, a través de comunicación inalámbrica punto a punto, en lugar de usar una red de infraestructura vigilada.

Es posible que un dispositivo de IoT no necesite algunas de las capacidades de ciberseguridad y privacidad de las que dependen los dispositivos de TI convencionales. Un ejemplo es un dispositivo de IoT sin capacidades de almacenamiento de datos que no necesita proteger datos en reposo. Un dispositivo de IoT también puede necesitar otras capacidades que la mayoría de los dispositivos de TI convencionales no utilizan, en especial si el dispositivo de IoT facilita interacciones nuevas con el mundo físico.

[2] Para obtener más información sobre los dispositivos informáticos de pocos recursos, consulte la solicitud de comentarios (RFC, por sus siglas en inglés) 7228 del Grupo de trabajo de ingeniería de internet (IETF, por sus siglas en inglés), *Terminology for Constrained-Node Networks* [Terminología para redes de nodos restringidos], (mayo de 2014), (https://doi.org/10.17487/RFC7228).

4 Problemas que presenta la mitigación de riesgos a la ciberseguridad y la privacidad para los dispositivos de IoT

Los riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT se pueden considerar en términos de tres metas de *mitigación de riesgos* de alto nivel, como se muestra en la Figura 4:

1. **Proteger la seguridad del dispositivo.** En otras palabras, evitar que un dispositivo sea usado para llevar a cabo ataques, que incluye participar en ataques de denegación de servicio distribuido (DDoS) contra otras organizaciones, interceptar el tráfico de red o poner en riesgo dispositivos en el mismo segmento de red. Esta meta se aplica a todos los dispositivos de IoT.
2. **Proteger la seguridad de los datos.** Proteger la confidencialidad, integridad o disponibilidad de los datos (incluida la PII) recopilados, almacenados, procesados o transmitidos por el dispositivo de IoT o desde este. Esta meta se aplica a todos los dispositivos de IoT, a excepción de los que no tengan datos que necesiten protección.
3. **Proteger la privacidad de las personas.** Proteger la privacidad de las personas afectadas por el procesamiento de PII más allá de los riesgos que gestiona la protección de la seguridad del dispositivo y de los datos. Esta meta se aplica a todos los dispositivos de IoT que procesan PII o que afectan directa o indirectamente a las personas.

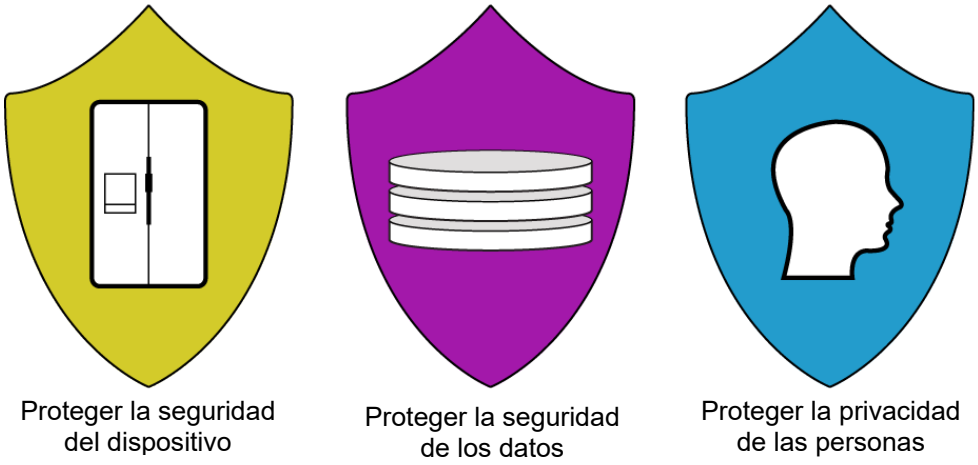


Figura 4: Metas de mitigación de riesgos

Cada meta se basa en la meta anterior, sin reemplazarla ni anular la necesidad de esta. El logro de cada una de las metas de mitigación de riesgos implica tomar en cuenta un conjunto de *áreas de mitigación de riesgos*, las cuales se definen a continuación. Cada área de mitigación de riesgos define un aspecto de la mitigación de riesgos a la ciberseguridad o la privacidad de IoT que se considera afectado de manera más significativa o imprevista por las consideraciones de riesgo definidas en la Sección 3.

Áreas de mitigación de riesgos para la meta 1: Proteger la seguridad del dispositivo.

- **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 a fin de utilizar esa información para fines de la gestión de riesgos a la ciberseguridad y la privacidad.

- **Gestión de vulnerabilidades:** Identificar y eliminar las vulnerabilidades conocidas en el software y el firmware del dispositivo de IoT para reducir la probabilidad y la facilidad de que sean explotados y queden comprometidos.
- **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.
- **Detección de incidentes de seguridad del dispositivo:** Vigilar y analizar la actividad del dispositivo de IoT en busca de señales de incidentes relacionados con la seguridad del dispositivo.

Áreas de mitigación de riesgos para la meta 2: Proteger la seguridad de los datos.

- **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.
- **Detección de incidentes de seguridad de los datos:** Vigilar y analizar la actividad del dispositivo de IoT en busca de señales de incidentes relacionados con la seguridad de los datos.

Áreas de mitigación de riesgos para la meta 3: Proteger la privacidad de las personas.

- **Gestión del flujo de información:** Mantener una asignación al corriente y precisa del ciclo de vida de la información de PII, incluido el tipo de acción de datos, los elementos de la PII que la acción de datos esté procesando, la parte que hace el procesamiento y todos los factores contextuales adicionales pertinentes al procesamiento para usarlos con fines de gestión de riesgos a la privacidad.
- **Gestión de permisos para procesar la PII:** Mantener permisos para procesar la PII a fin de evitar el procesamiento no permitido de PII.
- **Toma de decisiones informadas:** Facilitar que las personas entiendan los efectos del procesamiento de la PII y de las interacciones con el dispositivo, participen en la toma de decisiones acerca del procesamiento de la PII o las interacciones con esta y resuelvan problemas.
- **Gestión de datos desasociados:** Identificar el procesamiento autorizado de la PII y determinar la manera en que se pueda minimizar o desasociar la PII de personas y dispositivos de IoT.
- **Detección de vulneraciones de la privacidad:** Vigilar y analizar la actividad del dispositivo de IoT en busca de señales de vulneraciones relacionadas con la privacidad de las personas.

En las secciones 4.1, 4.2 y 4.3 se examina la manera en que las consideraciones de riesgo presentan problemas a los administradores de riesgos a la ciberseguridad y la privacidad para lograr cada una de las tres metas de mitigación de riesgos de los dispositivos de IoT de una organización, en otras palabras, la diferencia entre la mitigación para la IoT y para la TI convencional. La Sección 5 proporciona recomendaciones sobre la manera en que las organizaciones deben solucionar estos problemas.

4.1 Problemas potenciales para el logro de la meta 1: Proteger la seguridad del dispositivo

La Figura 5 muestra las relaciones entre los conceptos de la Sección 3 y los de la Sección 4. La Sección 3 define las tres consideraciones de riesgo, las cuales explican por qué y de qué manera los dispositivos de IoT afectan la gestión de riesgos a la ciberseguridad y la privacidad. Luego, la introducción de la Sección 4 define las metas y áreas de mitigación de riesgos que especifican los tipos de riesgos a la ciberseguridad y la privacidad importantes para los dispositivos de IoT y que pueden verse más afectados por las consideraciones de riesgo. El resto de la Sección 4 enumera las expectativas, es decir, cómo esperan las organizaciones que los dispositivos de TI convencionales ayuden a mitigar los riesgos a la ciberseguridad y la privacidad para las metas y áreas de mitigación de riesgos, los problemas que los dispositivos de IoT podrían plantear para esas expectativas y las repercusiones de esos problemas. El resultado final de estos vínculos es la identificación de un conjunto estructurado de problemas potenciales con la mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT cuyo origen se puede rastrear hasta las consideraciones del riesgo correspondiente.

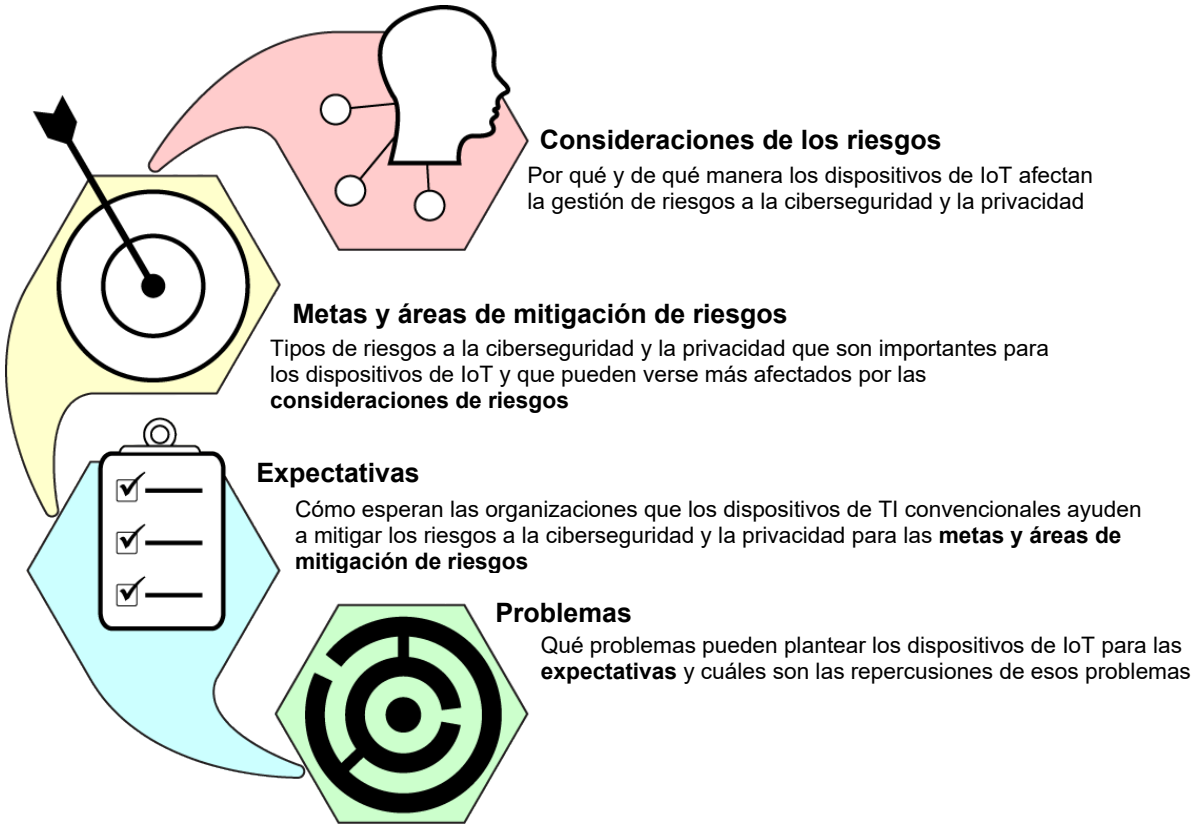


Figura 5: Relaciones entre los conceptos de la Sección 3 y los de la Sección 4

Es posible que muchos lectores no necesiten usar la información en todos los niveles de detalle descritos en la Figura 5, mientras que otros lectores necesiten solo la información en un nivel, como la lista de problemas. Este documento incluye todos los niveles a fin de explicar la base que se usa para identificar esos problemas particulares como problemas potencialmente

considerables para los dispositivos de IoT. Además, tal vez algunos lectores usen todos los niveles como base para su gestión de riesgos.

La Tabla 1 enumera las expectativas comunes acerca de las capacidades anteriores al mercadeo de los dispositivos de TI convencionales que suelen ayudar a mitigar su riesgo a la seguridad del dispositivo. Aunque estas expectativas no siempre se aplican a los dispositivos de TI convencionales, por lo general son verdaderas y han tenido gran influencia en las prácticas comunes de seguridad para esos dispositivos. Para cada expectativa, la Tabla 1 define uno o más problemas potenciales que los dispositivos individuales de IoT pueden plantear para la expectativa. Cada problema tiene su propia fila en la tabla:

- Primera columna: un resumen breve del problema, numerado para facilitar su referencia, y los números de las consideraciones de riesgo de la Sección 3 que causan el problema.
- Segunda columna: ejemplos de los controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5 [7] que podrían verse afectados negativamente en cierta medida en algunos dispositivos individuales de IoT.
- Tercera columna: las consecuencias potenciales para la organización si un número considerable de dispositivos de IoT se ve afectado por el problema.
- Cuarta columna: ejemplos de las subcategorías del Marco de ciberseguridad [6] que podrían verse afectadas negativamente en cierta medida por las consecuencias.

Las tablas en esta sección no definen los controles de la Publicación especial 800-53 del NIST ni las subcategorías del Marco de ciberseguridad en cada fila, ni suponen que estos sean equivalentes. Por ejemplo, en muchos casos, un problema afecta un aspecto de los controles de la Publicación especial 800-53 y un aspecto diferente de las subcategorías del Marco de ciberseguridad. Además, los dispositivos de IoT que no cumplen las expectativas tradicionales podrían ser un factor positivo para la mitigación de riesgos, ya que estas limitaciones podrían plantear *menos* riesgos que cuando, según las expectativas, la capacidad o la función más sólida está presente. La tabla no define estas consideraciones, sino que su objetivo es ayudar a los administradores de los riesgos a la ciberseguridad y la privacidad a entender la manera en que los dispositivos de IoT pueden o no adaptarse a sus mitigaciones existentes o repercutir en la manera en que se logran en ese momento los resultados de ciberseguridad y privacidad para su organización.

Tabla 1: Problemas potenciales para el logro de la meta 1: Proteger la seguridad del dispositivo

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Gestión de activos			
Expectativa 1: El dispositivo tiene un identificador único integrado.			
1. Es posible que el dispositivo de IoT no tenga un identificador único al que el sistema de gestión de activos de la empresa pueda acceder o que pueda entender. Consideración de riesgo 2	• CM-8, Inventario de componentes del sistema	• Puede complicar la gestión de dispositivos, incluido el acceso remoto y la gestión de vulnerabilidades.	• ID.AM-1: Se hace inventario de los dispositivos físicos y los sistemas dentro de la organización.
Expectativa 2: El dispositivo puede interactuar con los sistemas de gestión de activos de la empresa.			
2. Es posible que el dispositivo de IoT no pueda participar en un sistema centralizado de gestión de activos. Consideración de riesgo 2	• CM-8, Inventario de componentes del sistema	• Puede ser que tenga que usar varios sistemas de gestión de activos. • Puede ser que las tareas de gestión de activos se tengan que hacer manualmente.	• ID.AM-1: Se hace inventario de los dispositivos físicos y los sistemas dentro de la organización. • ID.AM-2: Se hace inventario de las plataformas y las aplicaciones de software dentro de la organización. • PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
3. Es posible que el dispositivo de IoT no esté conectado directamente a ninguna de las redes de la organización. Consideración de riesgo 2	• CM-8, Inventario de componentes del sistema	• Puede ser que tenga que usar un sistema o servicio de gestión de activos independiente, o procesos manuales de gestión de activos, para los dispositivos de IoT externos.	• ID.AM-1: Se hace inventario de los dispositivos físicos y los sistemas dentro de la organización. • ID.AM-2: Se hace inventario de las plataformas y las aplicaciones de software dentro de la organización. • PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Expectativa 3: El dispositivo puede dar a la organización suficiente visibilidad de sus características.			
4. El dispositivo de IoT puede ser una caja negra que proporcione poca o ninguna información sobre su hardware, software y firmware. Consideración de riesgo 2	• CM-8, Inventario de componentes del sistema	• Puede complicar todos los aspectos de la gestión de dispositivos y de la gestión de riesgos.	• ID.AM-1: Se hace inventario de los dispositivos físicos y los sistemas dentro de la organización. • ID.AM-2: Se hace inventario de las plataformas y las aplicaciones de software dentro de la organización. • ID.AM-4: Se catalogan los sistemas de información externos.
Expectativa 4: El dispositivo o el fabricante del dispositivo pueden informar a la organización de todo software y servicio externo que utilice el dispositivo, como software que se ejecute o descargue dinámicamente de la nube.			
5. No se pueden revelar todas las dependencias externas del dispositivo de IoT. Consideración de riesgo 2	• AC-20, Uso de sistemas externos	• No puede gestionar el riesgo del software y los servicios externos.	• DE.CM-8: Se hacen detecciones de vulnerabilidades. • PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima). • PR.PT-3: El principio de funcionalidad mínima se incorpora configurando los sistemas para proporcionar solo las capacidades esenciales.
Gestión de vulnerabilidades			
Expectativa 5: El fabricante proporcionará parches o actualizaciones para todo el software y el firmware durante la vida útil de cada dispositivo.			
6. Es posible que el fabricante no distribuya parches ni actualizaciones para el dispositivo de IoT. Consideración de riesgo 3	• SI-2, Corrección de defectos	• No se pueden eliminar las vulnerabilidades conocidas.	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
7. Puede ser que el fabricante deje de distribuir parches y actualizaciones para el dispositivo de IoT cuando aún está en uso. Consideración de riesgo 3	• SI-2, Corrección de defectos	• Es posible que no pueda eliminar las vulnerabilidades conocidas en el futuro.	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
Expectativa 6: El dispositivo tiene sus propias capacidades integradas y protegidas de gestión de configuraciones, actualizaciones y parches, o puede interactuar con los sistemas de gestión de vulnerabilidades de la empresa con esas capacidades.			
8. Es posible que el software del dispositivo de IoT no se pueda actualizar, o que no se le puedan aplicar parches. Consideraciones de riesgo 2 y 3	• SI-2, Corrección de defectos	• No se pueden eliminar las vulnerabilidades conocidas.	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
9. Puede ser demasiado arriesgado instalar parches o actualizaciones, o hacer cambios de configuración sin efectuar primero pruebas y preparativos exhaustivos, y la implementación de cambios puede requerir interrupciones operativas o causar fallas de energía accidentales. Consideración de riesgo 1	• CM-3, Control de cambios de configuración • CM-6, Opciones de configuración • SI-2, Corrección de defectos	• Puede haber demoras considerables al eliminar las vulnerabilidades conocidas.	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
10. Es posible que el dispositivo de IoT no pueda participar en un sistema centralizado de gestión de vulnerabilidades. Consideración de riesgo 2	• CM-3, Control de cambios de configuración • SI-2, Corrección de defectos	• Puede ser que se tengan que usar muchos sistemas de gestión de vulnerabilidades en lugar de uno. • Puede ser que la gestión de vulnerabilidades se tenga que hacer de forma manual y periódica (por ejemplo, instalar parches manualmente, revisar manualmente si hay errores de configuración de software).	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
11. Es posible que el dispositivo IoT no ofrezca la capacidad para cambiar la configuración del software o que no pueda proporcionar las características que las organizaciones desean. Consideración de riesgo 2	• CM-2, Configuración básica • CM-3, Control de cambios de configuración • CM-6, Opciones de configuración • CM-7, Funcionalidad mínima • SC-42, Capacidad y datos del sensor	• No se pueden eliminar las vulnerabilidades conocidas. • No se puede lograr el principio de funcionalidad mínima con la deshabilitación de funciones o servicios innecesarios. • No se puede restringir la activación y el uso del sensor.	• PR.IP-1: Se establece y mantiene una configuración de base de la tecnología de la información o los sistemas de control industrial que incorpore principios de seguridad (por ejemplo, el concepto de funcionalidad mínima). • PR.IP-3: Se establecen los procesos de control de cambios de configuración. • PR.PT-3: El principio de funcionalidad mínima se incorpora configurando los sistemas para proporcionar solo las capacidades esenciales.
Expectativa 7: El dispositivo es compatible con el uso de detectores de vulnerabilidades o proporciona capacidades integradas de identificación de vulnerabilidades y preparación de informes.			
12. Es posible que no haya un detector de vulnerabilidades que se pueda ejecutar en el dispositivo de IoT o para este. Consideración de riesgo 3	• RA-5, Detección de vulnerabilidades	• No se pueden identificar automáticamente las vulnerabilidades conocidas.	• DE.CM-8: Se hacen detecciones de vulnerabilidades.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
13. Es posible que el dispositivo de IoT no ofrezca ninguna capacidad integrada para identificar e informar de vulnerabilidades conocidas. Consideración de riesgo 3	• RA-5, Detección de vulnerabilidades	• No se pueden identificar automáticamente las vulnerabilidades conocidas.	• DE.CM-8: Se hacen detecciones de vulnerabilidades.
Gestión del acceso			
Expectativa 8: El dispositivo puede identificar de manera única a cada usuario, dispositivo y proceso que intente acceder a este de forma lógica.			
14. Es posible que el dispositivo de IoT no sea compatible con el uso de identificadores. Consideraciones de riesgo 2 y 3	• IA-2, Identificación y autenticación (usuarios de la organización) • IA-3, Identificación y autenticación de dispositivos • IA-4, Gestión de identificadores • IA-8, Identificación y autenticación (usuarios fuera de la organización) • IA-9, Identificación y autenticación de servicios	• No se pueden identificar o autenticar usuarios, dispositivos ni procesos.	• PR.AC-1: Se emiten, gestionan, verifican, revocan y auditan las identidades y credenciales para los dispositivos, usuarios y procesos autorizados. • PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).
15. Es posible que el dispositivo de IoT solo sea compatible con el uso de uno o más identificadores compartidos. Consideraciones de riesgo 2 y 3	• IA-2, Identificación y autenticación (usuarios de la organización) • IA-3, Identificación y autenticación de dispositivos • IA-4, Gestión de identificadores • IA-8, Identificación y autenticación (usuarios fuera de la organización) • IA-9, Identificación y autenticación de servicios	• No se pueden identificar usuarios, dispositivos ni procesos de manera exclusiva. Complica la gestión de credenciales debido a las credenciales compartidas.	• PR.AC-1: Se emiten, gestionan, verifican, revocan y auditan las identidades y credenciales para los dispositivos, usuarios y procesos autorizados.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
16. Es posible que el dispositivo de IoT necesite usar identificadores, pero solo en ciertos casos (por ejemplo, para acceso remoto, pero no para acceso local, o para fines de administración, pero no para uso normal). Consideraciones de riesgo 2 y 3	• IA-2, Identificación y autenticación (usuarios de la organización) • IA-3, Identificación y autenticación de dispositivos • IA-4, Gestión de identificadores • IA-8, Identificación y autenticación (usuarios fuera de la organización) • IA-9, Identificación y autenticación de servicios	• No se pueden identificar o autenticar algunos usuarios, dispositivos ni procesos.	• PR.AC-1: Se emiten, gestionan, verifican, revocan y auditan las identidades y credenciales para los dispositivos, usuarios y procesos autorizados. • PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).
Expectativa 9: El dispositivo puede evitar que se muestren los caracteres de una contraseña cuando una persona ingresa la contraseña para un dispositivo, como en un teclado o una pantalla táctil.			
17. Es posible que el dispositivo de IoT no sea compatible con la ocultación de los caracteres de contraseña que se ingresan. Consideraciones de riesgo 2 y 3	• IA-6, Comentarios del autenticador	• Aumenta la probabilidad de robo de credenciales.	• PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).
Expectativa 10: El dispositivo puede autenticar a cada usuario, dispositivo y proceso que intente acceder a este de forma lógica.			
18. Es posible que el dispositivo de IoT no sea compatible con el uso de credenciales no triviales (por ejemplo, no es compatible con el uso de identificadores, no permite cambiar las contraseñas predeterminadas). Consideraciones de riesgo 2 y 3	• IA-5, Gestión del autenticador	• No se pueden identificar o autenticar usuarios, dispositivos ni procesos, lo que aumenta la probabilidad de acceso no autorizado y manipulación indebida.	• PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
19. Es posible que el dispositivo de IoT no sea compatible con el uso de credenciales sólidas, como los tokens criptográficos o la autenticación multifactor, para las situaciones que lo ameritan. Consideración de riesgo 3	• IA-5, Gestión del autenticador	• Aumenta las probabilidades de acceso no autorizado y manipulación indebida con el uso inapropiado de credenciales.	• PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).
Expectativa 11: El dispositivo puede usar los autenticadores y los mecanismos de autenticación existentes de la empresa.			
20. Es posible que el dispositivo de IoT no sea compatible con el uso de un sistema existente de la empresa para autenticación de usuarios. Consideración de riesgo 3	• IA-2, Identificación y autenticación (usuarios de la organización) • IA-5, Gestión del autenticador • IA-8, Identificación y autenticación (usuarios fuera de la organización)	• Se necesitan una o más cuentas y credenciales adicionales para cada usuario.	• PR.AC-1: Se emiten, gestionan, verifican, revocan y auditan las identidades y credenciales para los dispositivos, usuarios y procesos autorizados. • PR.AC-7: Los usuarios, dispositivos y demás activos se autentican (por ejemplo, factor único, factor múltiple) de acuerdo con el riesgo de la transacción (por ejemplo, riesgos a la seguridad y la privacidad de las personas y otros riesgos de la organización).
Expectativa 12: El dispositivo puede hacer que cada usuario, dispositivo y proceso esté restringido a los privilegios de acceso lógico mínimos necesarios.			
21. Es posible que el dispositivo de IoT no sea compatible con el uso de privilegios de acceso lógico dentro del dispositivo que basta para una situación determinada. Consideración de riesgo 3	• AC-3, Aplicación del cumplimiento • AC-5, Separación de funciones • AC-6, Privilegio mínimo	• Permite que los usuarios, dispositivos y procesos autorizados hagan uso accidental o intencional de privilegios que no deben tener. • Permite que un atacante que logre acceso no autorizado a una cuenta tenga un acceso mayor al que debe tener la cuenta.	• PR.AC-4: Se gestionan los permisos y las autorizaciones de acceso, incorporando los principios de privilegio mínimo y separación de funciones. • PR.DS-5: Se implementan protecciones contra las pérdidas de datos. • PR.MA-1: El mantenimiento y la reparación de los recursos organizativos se hacen y registran con herramientas aprobadas y controladas.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
22. Es posible que el dispositivo de IoT no sea compatible con el uso de privilegios de acceso lógico para restringir las comunicaciones de red hacia y desde el dispositivo que basta para una situación determinada. Consideración de riesgo 3	• AC-3, Aplicación del cumplimiento • AC-4, Cumplimiento del flujo de información • AC-5, Separación de funciones • AC-6, Privilegio mínimo • AC-17, Acceso remoto • SC-7, Protección de límites	• Permite a los usuarios, dispositivos y procesos autorizados efectuar comunicaciones de red accidentales o intencionales que no deben poder efectuar. • Permite que un atacante tenga mayor acceso a la red que el previsto.	• PR.AC-3: Se gestiona el acceso remoto. • PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red). • PR.DS-5: Se implementan protecciones contra las pérdidas de datos. • PR.MA-2: Se aprueba, registra y efectúa el mantenimiento remoto de los recursos organizativos de manera que se evite el acceso no autorizado.
Expectativa 13: El dispositivo puede frustrar los intentos de obtener acceso no autorizado, y esta función se puede configurar o deshabilitar para evitar interrupciones no deseadas de la disponibilidad. (Algunos ejemplos incluyen bloquear o deshabilitar una cuenta cuando haya demasiados intentos fallidos de autenticación consecutivos, demorar otros intentos de autenticación después de los intentos fallidos y bloquear o terminar sesiones inactivas).			
23. Es posible que el uso de estas funciones de seguridad que haga el dispositivo de IoT no se pueda modificar suficientemente. Consideraciones de riesgo 1 y 3	• AC-7, Intentos no logrados de inicio de sesión • AC-11, Bloqueo del dispositivo • AC-12, Terminación de la sesión • IA-11, Reautenticación	• No se puede obtener acceso inmediato a los dispositivos de IoT cuando sea necesario usarlos o gestionarlos.	• PR.AC-3: Se gestiona el acceso remoto. • PR.AC-4: Se gestionan los permisos y las autorizaciones de acceso, incorporando los principios de privilegio mínimo y separación de funciones. • PR.MA-1: El mantenimiento y la reparación de los recursos organizativos se hacen y registran con herramientas aprobadas y controladas. • PR.MA-2: Se aprueba, registra y efectúa el mantenimiento remoto de los recursos organizativos de manera que se evite el acceso no autorizado.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Expectativa 14: El dispositivo cuenta con suficientes controles de seguridad física integrados para protegerlo de manipulación indebida (por ejemplo, embalaje a prueba de manipulaciones indebidas).			
24. El dispositivo de IoT se puede implementar en un lugar donde las personas que no estén autorizadas para acceder a este lo puedan hacer, o donde las personas autorizadas puedan acceder a este de maneras no autorizadas. Consideraciones de riesgo 1 y 2	• MP-2, Acceso a medios • MP-7, Uso de medios • PE-3, Control de acceso físico	• Permite a un atacante tener acceso físico directo a los dispositivos y manipularlos, lo que incluye agregar o eliminar medios de almacenamiento, conectar periféricos, etc.	• PR.AC-2: Se gestiona y protege el acceso físico a los activos. • PR.PT-2: Los medios extraíbles están protegidos y su uso se restringe de acuerdo con la política. • PR.MA-1: El mantenimiento y la reparación de los recursos organizativos se hacen y registran con herramientas aprobadas y controladas.
Detección de incidentes			
Expectativa 15: El dispositivo puede registrar sus eventos operativos y de seguridad.			
25. Es posible que el dispositivo de IoT no pueda registrar sus eventos operativos y de seguridad en absoluto o con suficiente detalle. Consideración de riesgo 3	• AU-2, Eventos de auditoría • AU-3, Contenido de los registros de auditoría • AU-12, Generación de auditorías • SI-4, Vigilancia del sistema	• Aumenta la probabilidad de que no se detecte la actividad malintencionada. • No se pueden confirmar ni reconstruir los incidentes a partir de las entradas de registro.	• DE.CM-7: Se vigila en busca de personal, conexiones, dispositivos y software no autorizados. • PR.PT-1: Los asientos de auditorías o registros se determinan, documentan, implementan y revisan de conformidad con la política. • RS.AN-1: Se investigan las notificaciones de los sistemas de detección.
26. Es posible que el dispositivo de IoT siga funcionando incluso cuando haya un error de registro. Consideración de riesgo 3	• AU-5, Respuesta a errores de procesamiento de auditorías	• Aumenta la probabilidad de que no se detecte la actividad malintencionada.	• DE.CM-7: Se vigila en busca de personal, conexiones, dispositivos y software no autorizados. • PR.PT-1: Los asientos de auditorías o registros se determinan, documentan, implementan y revisan de conformidad con la política.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Expectativa 16: El dispositivo puede interactuar con los sistemas existentes de gestión de registros de la empresa.			
27. Es posible que el dispositivo de IoT no pueda participar en un sistema de gestión de registros de la empresa. Consideración de riesgo 2	• AU-6, Revisión, análisis y preparación de informes de auditorías • SI-4, Vigilancia del sistema	• Puede ser que se tengan que usar muchos sistemas de gestión de registros en lugar de uno. • Puede ser que las tareas de gestión de registros se tengan que hacer manualmente. • Aumenta la probabilidad de que no se detecte la actividad malintencionada.	• DE.AE-3: Se recopilan y correlacionan los datos de eventos de varias fuentes y sensores. • DE.CM-7: Se vigila en busca de personal, conexiones, dispositivos y software no autorizados. • PR.PT-1: Los asientos de auditorías o registros se determinan, documentan, implementan y revisan de conformidad con la política.
Expectativa 17: El dispositivo puede facilitar la detección de incidentes potenciales por medio de controles internos o externos, como sistemas de prevención de intrusiones, utilidades antimalware y mecanismos de comprobación de integridad de archivos.			
28. Es posible que el dispositivo de IoT no pueda ejecutar los controles de detección internos, ni interactuar con los controles de detección externos sin afectar negativamente el funcionamiento del dispositivo. Consideraciones de riesgo 1 y 3	• SI-3, Protección contra código malintencionado • SI-7, Integridad del software, el firmware y la información	• Aumenta la probabilidad de que ocurran infecciones de código malintencionado y otras actividades no autorizadas, y de que no se detecten.	• DE.CM-1: Se vigila la red para detectar eventos potenciales de ciberseguridad. • DE.CM-4: Se detecta código malintencionado. • PR.DS-6: Se utilizan mecanismos de comprobación de integridad para verificar la integridad del software, el firmware y la información.
29. Es posible que el dispositivo de IoT no proporcione controles con la visibilidad necesaria para la detección eficiente y efectiva de incidentes. Consideraciones de riesgo 2 y 3	• IR-4, Manejo de incidentes • SI-4, Vigilancia del sistema	• Aumenta la probabilidad de que no se detecten código malintencionado y otras actividades no autorizadas.	• DE.CM-1: Se vigila la red para detectar eventos potenciales de ciberseguridad. • DE.CM-4: Se detecta código malintencionado. • PR.DS-6: Se utilizan mecanismos de comprobación de integridad para verificar la integridad del software, el firmware y la información.

Problemas para los dispositivos de IoT individuales y las consideraciones de riesgo que causan los problemas	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Expectativa 18: El dispositivo es compatible con las actividades de análisis de eventos e incidentes.			
30. Es posible que el dispositivo de IoT no proporcione a los analistas acceso suficiente a los recursos del dispositivo para hacer el análisis necesario. Consideraciones de riesgo 2 y 3	• SI-4, Vigilancia del sistema	• No se pueden usar herramientas forenses para la obtención y el análisis de información.	• RS.AN-1: Se investigan las notificaciones de los sistemas de detección. • RS.AN-3: Se hacen análisis forenses.

4.2 Problemas potenciales para el logro de la meta 2: Proteger la seguridad de los datos

La Tabla 2 sigue las mismas convenciones que la Tabla 1, pero se refiere a la protección de la seguridad de los datos. Se presupone que, si la seguridad de los datos necesita ser protegida, la seguridad de los dispositivos también lo necesitará, por lo que se tienen que considerar los problemas que figuran en ambas tablas.

Cabe señalar que la sección "Detección de incidentes" de la Tabla 1 también se aplica a la protección de la seguridad de los datos. La Tabla 1 supone que solo se deben proteger los incidentes de seguridad de dispositivos. Los mismos problemas potenciales, controles afectados, consecuencias y subcategorías del Marco de ciberseguridad se aplican también a la detección de incidentes de seguridad de los datos. Se omitieron las filas de la sección "Detección de incidentes" en la Tabla 2 para fines de brevedad.|

Tabla 2: Problemas potenciales para el logro de la meta 2: Proteger la seguridad de los datos

Problemas para los dispositivos de IoT individuales	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
Protección de datos			
Expectativa 19: El dispositivo puede impedir el acceso no autorizado a todos los datos confidenciales en sus componentes de almacenamiento.			
31. Es posible que el dispositivo de IoT no proporcione capacidades de cifrado suficientemente sólidas para los datos que almacena. Consideración de riesgo 3	• MP-4, Almacenamiento de medios • SC-28, Protección de la información en reposo	• Aumenta la probabilidad de acceso no autorizado a los datos confidenciales o de su manipulación indebida.	• PR.DS-1: Se protegen los datos en reposo. • PR.PT-2: Los medios extraíbles están protegidos y su uso se restringe de acuerdo con la política.

Problemas para los dispositivos de IoT individuales	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización	Subcategorías del Marco de ciberseguridad que se ven afectadas
32. Es posible que el dispositivo de IoT no proporcione un mecanismo para corregir los datos confidenciales antes de que se deseche o reasigne el dispositivo. Consideración de riesgo 3	• MP-6, Corrección de medios	• Aumenta la probabilidad de acceso no autorizado a los datos confidenciales.	• PR.IP-6: Los datos se destruyen de acuerdo con la política.
Expectativa 20: El dispositivo tiene un mecanismo compatible con la disponibilidad de datos por medio de copias de seguridad protegidas.			
33. Es posible que el dispositivo de IoT no proporcione un mecanismo protegido para las copias de seguridad y la restauración de sus datos. Consideración de riesgo 3	• CP-9, Copia de seguridad del sistema	• Aumenta la probabilidad de pérdida de datos.	• PR.IP-4: Se llevan a cabo, mantienen y prueban las copias de seguridad de la información.
Expectativa 21: El dispositivo puede impedir el acceso no autorizado a todos los datos confidenciales que transmita a través de las redes.			
34. Es posible que el dispositivo de IoT no proporcione capacidades de cifrado suficientemente sólidas para proteger los datos confidenciales que envía en sus comunicaciones de red. Consideración de riesgo 3	• AC-18, Acceso inalámbrico • SC-8, Confidencialidad e integridad de la transmisión	• Aumenta la probabilidad de interceptación de las comunicaciones.	• PR.DS-2: Se protegen los datos en tránsito.
35. Es posible que el dispositivo de IoT no verifique la identidad de otro dispositivo informático antes de enviar datos confidenciales en sus comunicaciones de red. Consideración de riesgo 3	• SC-8, Confidencialidad e integridad de la transmisión • SC-23, Autenticidad de la sesión	• Aumenta la probabilidad de , interceptación, manipulación, suplantación y otras formas de ataque a las comunicaciones.	• PR.DS-2: Se protegen los datos en tránsito.

4.3 Problemas potenciales para el logro de la meta 3: Proteger la privacidad de las personas

La Tabla 3 enumera los problemas potenciales para el logro de la meta 3: Proteger la privacidad de las personas con la mitigación del riesgo a la privacidad debido al procesamiento autorizado de la PII. Se siguen las mismas convenciones que en las tablas anteriores, pero se omiten las asignaciones a las subcategorías del Marco de ciberseguridad ya que el marco no considera los riesgos a la privacidad que causa el procesamiento autorizado de la PII.

Se presupone que, si la privacidad de las personas necesita ser protegida, la seguridad de los dispositivos y los datos también lo necesitará, por lo que se tienen que considerar los problemas que figuran en las tres tablas. No obstante, las organizaciones pueden usar la información de la Tabla 2 para tratar los riesgos a la privacidad que se derivan de la pérdida de confidencialidad, integridad o disponibilidad de la PII.

Tabla 3: Problemas potenciales para el logro de la meta 3: Proteger la privacidad de las personas

Problemas para los dispositivos de IoT individuales	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización
Gestión de datos desasociados		
Expectativa 22: El dispositivo funciona en un entorno federado de identidad tradicional.		
36. El dispositivo de IoT puede aportar datos que se usan con fines de identificación y autenticación, pero que están fuera de los entornos federados tradicionales. Consideración de riesgo 3	IA-8 (6), Identificación y autenticación (usuarios fuera de la organización) | Capacidad para desasociar	• Es posible que, fuera de un entorno federado tradicional, no funcionen las técnicas como el uso de tablas de asignación de identificadores y las técnicas criptográficas que mejoran la privacidad para ocultar a los proveedores de servicios de credenciales de las partes que dependen de estos, y viceversa, o para hacer los atributos de identidad menos visibles para las partes que los transmiten.
Toma de decisiones informadas		
Expectativa 23: Existen interfaces tradicionales para la interacción de la persona con el dispositivo.		
37. El dispositivo de IoT puede carecer de las interfaces que permiten a las personas interactuar con este. Consideración de riesgo 2	IP-2, Consentimiento	• Es posible que las personas no puedan dar su consentimiento para que se procese su PII ni condicionar el procesamiento adicional de atributos específicos.
38. Las funciones descentralizadas de tratamiento de datos y la propiedad heterogénea de los dispositivos de IoT dificultan los procesos tradicionales de rendición de cuentas. Consideración de riesgo 3	IP-3, Corrección	• Es posible que las personas no puedan ubicar la fuente de la PII inexacta o problemática para corregirla o para solucionar el problema.
39. El dispositivo de IoT puede carecer de interfaces que permiten a las personas leer los avisos de privacidad. Consideración de riesgo 2	IP-4, Aviso de privacidad	• Es posible que las personas no puedan leer los avisos de privacidad ni acceder a estos.

Problemas para los dispositivos de IoT individuales	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización
40. El dispositivo de IoT puede carecer de las interfaces que facilitan el acceso a la PII, o que la PII esté almacenada en lugares desconocidos. Consideración de riesgo 2	IP-6, Acceso individual	• Las personas pueden tener problemas con el acceso a su información, lo cual reduce su capacidad para gestionar su información y entender lo que está sucediendo con sus datos, y aumenta los riesgos al cumplimiento.
Gestión de permisos para procesar la PII		
Expectativa 24: Hay un control centralizado suficiente para aplicar los requisitos de políticas o reglamentarios a la PII.		
41. El dispositivo de IoT puede recolectar PII de manera indiscriminada o analizarla, intercambiarla o actuar conforme a esta en función de procesos automatizados. Consideración de riesgo 2	PA-2, Autoridad para recolectar	• La PII se puede procesar de manera que no cumpla los requisitos reglamentarios ni las políticas de una organización.
42. Los dispositivos de IoT pueden ser complejos y dinámicos, y tener una funcionalidad de detección capaz de recolectar la PII que se añade y elimina frecuentemente. Consideración de riesgo 1	PA-3, Especificación del propósito	• Puede ser que el seguimiento de la PII sea difícil de manera que las personas y los propietarios u operadores de los dispositivos no tengan suposiciones confiables acerca de la manera en que se procesa la PII, haciendo más difícil la toma de decisiones informadas.
43. Se puede acceder al dispositivo de IoT de forma remota, y dejar el uso compartido de la PII fuera del control del administrador. Consideración de riesgo 2	PA-4, Intercambio de información con partes externas	• La PII se puede intercambiar de maneras que no cumplan los requisitos reglamentarios ni las políticas de una organización.
Gestión del flujo de información		
Expectativa 25: Hay suficiente control centralizado para gestionar la PII.		
44. Los dispositivos de IoT pueden ser complejos y dinámicos, y tener una funcionalidad de detección capaz de recolectar la PII que se añade y elimina frecuentemente. Consideración de riesgo 1	PM-29, Inventario de información de identificación personal	• Puede ser difícil identificar y dar seguimiento a la PII cuando se usan métodos tradicionales de inventario.
45. Es posible que los dispositivos de IoT no sean compatibles con los mecanismos estandarizados para la gestión centralizada de datos, y el número total de dispositivos de IoT que deban ser gestionados puede ser abrumador. Consideración de riesgo 2	SC-7 (24), Protección de límites | Información de identificación personal	• Se puede interrumpir la aplicación de las normas de procesamiento de la PII destinadas a proteger la privacidad de las personas.

Problemas para los dispositivos de IoT individuales	Controles del proyecto de la Publicación especial 800-53 del NIST, revisión 5, que se ven afectados	Consecuencias para la organización
46. Es posible que el dispositivo de IoT no tenga la capacidad para admitir configuraciones como prevención de activación remota, preparación de informes de datos limitados, aviso de recolección y minimización de datos. Consideración de riesgo 3	SC-42, Capacidad y datos del sensor	• La falta de capacidades directas para mitigar los riesgos a la privacidad puede requerir controles compensadores y afectar la capacidad de una organización para optimizar la cantidad de riesgo a la privacidad que se puede reducir.
47. El dispositivo de IoT puede recopilar PII indiscriminadamente. La propiedad heterogénea de los dispositivos dificulta las técnicas tradicionales de gestión de datos. Consideración de riesgo 2	SI-12 (1), Gestión y retención de información | Límite de elementos de la información de identificación personal	• Es más probable que se retenga la PII que no sea necesaria para las operaciones.
48. Las funciones descentralizadas de tratamiento de datos y la propiedad heterogénea de los dispositivos de IoT dificultan los procesos tradicionales de gestión de datos con respecto a la comprobación de la precisión de los datos. Consideración de riesgo 2	SI-19, Operaciones de calidad de datos	• Es más probable que persista la PII imprecisa, con potencial de crear problemas a las personas.
49. Las funciones descentralizadas de tratamiento de datos y la propiedad heterogénea de los dispositivos de IoT dificultan los procesos tradicionales de desidentificación. Consideraciones de riesgo 2 y 3	SI-20, Desidentificación	• La agregación de conjuntos de datos con disparidad podría dar lugar a la reidentificación de la PII.

5 Recomendaciones para resolver los problemas de mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT

Esta sección ofrece recomendaciones para resolver los problemas de mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT. La Figura 6 resume las recomendaciones que se enumeran a continuación y, si se indica, se describen con más detalle en otra parte de esta publicación:

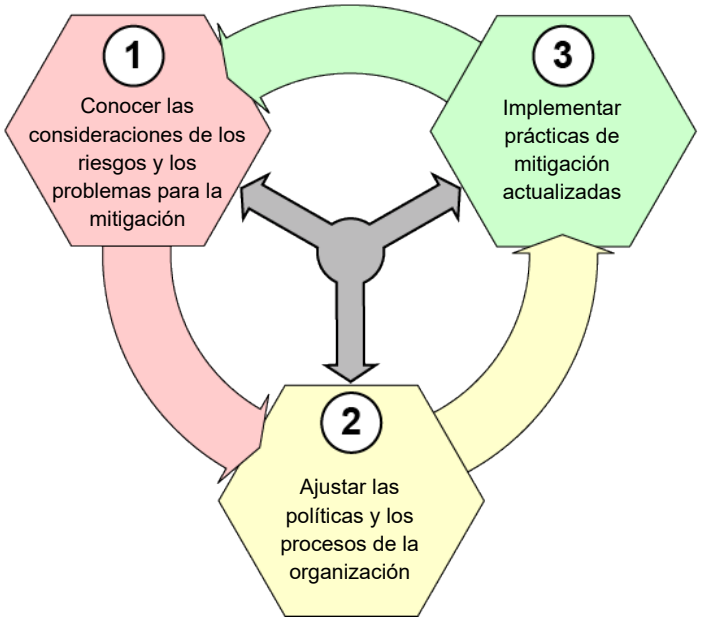


Figura 6: Resumen de las recomendaciones

1. Conocer las consideraciones de los riesgos de los dispositivos de IoT (Sección 3) y los problemas que puedan causar a la mitigación de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT en las áreas de mitigación de riesgos correspondientes (Sección 4).
2. Ajustar las políticas y los procesos de la organización para solucionar los problemas de mitigación de riesgos a la ciberseguridad y la privacidad durante todo el ciclo de vida del dispositivo de IoT. La Sección 5.1 proporciona más información al respecto. En la Sección 4 de esta publicación, se citan muchos ejemplos de posibles problemas, pero cada organización necesitará personalizarlos para tener en cuenta los requisitos de la misión y otras características específicas de la organización.
3. Implementar prácticas de mitigación actualizadas para los dispositivos de IoT de la organización como se haría con cualquier otro cambio en las prácticas (Sección 5.2).

5.1 Ajustar las políticas y los procesos de la organización

Las organizaciones deben asegurarse de tener en cuenta las consideraciones en sus políticas y procesos de ciberseguridad y privacidad durante todo el ciclo de vida del dispositivo de IoT. Las organizaciones deben describir claramente la forma en que evalúan la IoT a fin de evitar confusión y ambigüedad. Esto es de particular importancia para las organizaciones que puedan estar sujetas a leyes y reglamentos en los que la IoT se define de maneras distintas.

De igual manera, las organizaciones deben procurar que sus programas de gestión de riesgos a la ciberseguridad, la cadena de suministro y la privacidad tengan debidamente en cuenta la IoT, lo que incluye:

- Determinar cuáles dispositivos tienen capacidades de dispositivos de IoT. Establecer mecanismos para determinar si un dispositivo que se podría adquirir, o que ya se adquirió, es un dispositivo de IoT, cuando esto no sea evidente.

- Identificar los tipos de dispositivos de IoT. Saber cuáles tipos de dispositivos de IoT se usan y cuáles capacidades y fines admite cada tipo.
- Evaluar el riesgo que presenta un dispositivo de IoT. Es importante tener en cuenta el entorno particular de IoT en el que residen los dispositivos de IoT, y no solo evaluar aisladamente los riesgos de estos dispositivos. Por ejemplo, la conexión de un actuador a un sistema físico puede afectar a los riesgos de manera muy diferente que la conexión del mismo actuador a otro sistema físico.
- Determinar cómo responder a ese riesgo, sea aceptándolo, evitándolo, mitigándolo, compartiéndolo o transfiriéndolo. Como se mencionó antes, es posible que algunas estrategias de mitigación de riesgos para la TI convencional no funcionen bien para la IoT. En la Sección 4 de esta publicación, se analizan con gran detalle los problemas de la mitigación de riesgos para los dispositivos de IoT.

La gestión de riesgos a la ciberseguridad y la privacidad de algunos dispositivos de IoT puede afectar a otros tipos de riesgos e introducir nuevos riesgos a la seguridad, confiabilidad, resiliencia, rendimiento y otras áreas. Las organizaciones deben asegurarse de tomar en cuenta las compensaciones entre estos riesgos cuando toman decisiones acerca de la mitigación de riesgos a la ciberseguridad y la privacidad. Por ejemplo, supongamos que un dispositivo de IoT en particular es esencial para la seguridad. Exigir que el personal de un área protegida físicamente ingrese una contraseña para lograr acceso local al dispositivo de IoT podría demorar la intervención durante un error de funcionamiento. Otros requisitos que tengan que ver con la longitud o la complejidad de la contraseña y el bloqueo automático de cuentas después de varios intentos fallidos de autenticación consecutivos podrían causar demoras mucho más prolongadas y aumentar la probabilidad y la magnitud del daño. Las organizaciones deben aprovechar sus programas actuales para gestionar otras formas de riesgos cuando determinan la manera en que se deben gestionar los riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT.

En función de los problemas potenciales de la mitigación y las consecuencias de esos problemas, es más probable que las implementaciones de las siguientes subcategorías del Marco de ciberseguridad [6] necesiten ajustes para que las políticas y los procesos de la organización planteen adecuadamente los riesgos a la ciberseguridad durante todo el ciclo de vida del dispositivo de IoT:

- ID.AM (Identificar—Gestión de activos)
  - ID.AM-1: Se hace inventario de los dispositivos físicos y los sistemas dentro de la organización.
  - ID.AM-2: Se hace inventario de las plataformas y las aplicaciones de software dentro de la organización.
- ID.BE (Identificar—Entorno empresarial)
  - ID.BE-4: Se establecen las dependencias y funciones fundamentales para la prestación de servicios esenciales.
  - ID.BE-5: Se establecen los requisitos de resiliencia compatibles con la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo presión o ataque, durante recuperación, operaciones normales).
- ID.GV (Identificar—Gobernanza)
  - ID.GV-1: Se establece y comunica la política de ciberseguridad de la organización.

  - ID.GV-2: Se coordinan y alinean las funciones y responsabilidades de ciberseguridad con las funciones internas y los socios externos.
  - ID.GV-3: Se entienden y gestionan los requisitos legales y reglamentarios para la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles.
  - ID.GV-4: Los procesos de gobernanza y gestión de riesgos plantean los riesgos a la ciberseguridad.
- ID.RA (Identificar—Evaluación de riesgos)
  - ID.RA-1: Se identifican y documentan las vulnerabilidades de los activos.
  - ID.RA-3: Se identifican y documentan las amenazas, tanto internas como externas.
  - ID.RA-4: Se identifican los impactos potenciales y las probabilidades en el negocio.
  - ID.RA-6: Se identifican y priorizan las respuestas a los riesgos.
- ID.RM (Identificar—Estrategia de gestión de riesgos)
  - ID.RM-2: Se determina y expresa claramente la tolerancia al riesgo de la organización.
  - ID.RM-3: La determinación de la tolerancia al riesgo de la organización se basa en su función en el análisis de riesgos específicos del sector y la infraestructura crítica.
- ID.SC (Identificar—Gestión de riesgos a la cadena de suministros)
  - ID.SC-2: Se identifican, priorizan y evalúan los proveedores y terceros asociados de los sistemas, componentes y servicios de información usando un proceso de evaluación de riesgos a la cadena de suministro cibernética.
  - ID.SC-3: Se usan los contratos con proveedores y terceros asociados para implementar las medidas apropiadas diseñadas para lograr los objetivos de un programa de ciberseguridad y un plan de gestión de riesgos a la cadena de suministro cibernética de una organización.
- PR.IP (Proteger—Procesos y procedimientos para protección de la información)
  - PR.IP-3: Se establecen los procesos de control de cambios de configuración.
  - PR.IP-9: Se establecen y gestionan los planes de respuesta (respuesta a incidentes y continuidad de la empresa) y los planes de recuperación (recuperación de incidentes y recuperación de desastres).
  - PR.IP-12: Se elabora e implementa un plan de gestión de vulnerabilidades.

Asimismo, es más probable que las implementaciones de las tareas enumeradas abajo, provenientes de la Publicación especial 800-37 del NIST, revisión 2 [4], necesiten ajustarse de manera que las políticas y los procesos de la organización consideren adecuadamente el riesgo a la ciberseguridad y la privacidad durante todo el ciclo de vida del dispositivo de IoT. Cabe señalar que, aunque se puede usar el Marco de ciberseguridad para gestionar el aspecto de la privacidad relacionado con la ciberseguridad de la PII, la Publicación especial 800-37 del NIST, revisión 2, puede servir para gestionar todo el alcance de la privacidad porque integra el procesamiento autorizado de la PII en el Marco de gestión de riesgos del NIST (RMF, por sus siglas en inglés).

- Preparar, Nivel de organización, Tarea P-1: Funciones de gestión de riesgos
- Preparar, Nivel de organización, Tarea P-2: Estrategia de gestión de riesgos
- Preparar, Nivel de organización, Tarea P-3: Evaluación de riesgos; Organización
- Preparar, Nivel de sistema, Tarea P-8: Enfoque en la misión u operación
- Preparar, Nivel de sistema, Tarea P-13: Ciclo de vida de la información

- Preparar, Nivel de sistema, Tarea P-14: Evaluación de riesgos; Sistema
- Preparar, Nivel de sistema, Tarea P-15: Definición de requisitos

5.2 Implementar prácticas de mitigación de riesgos actualizadas

Es posible que las prácticas de mitigación de riesgos a la ciberseguridad y la privacidad de una organización necesiten cambios considerables debido al gran número de dispositivos de IoT y de tipos de estos dispositivos. La mayoría de las organizaciones tiene decenas de tipos de dispositivos de TI convencionales: computadoras de escritorio, computadoras portátiles, servidores, teléfonos inteligentes, enrutadores, conmutadores, firewalls, impresoras, etc. Los dispositivos de TI convencionales de un solo tipo tienden a tener capacidades similares. Por ejemplo, la mayoría de las computadoras portátiles tienen capacidades similares de almacenamiento y tratamiento de datos, capacidades de interfaz de usuario humano y de interfaz de red, y capacidades de soporte, como la gestión centralizada. Esto permite a las organizaciones determinar la manera de gestionar el riesgo para cada uno de los tipos de dispositivos de TI convencionales, con algunas personalizaciones para dispositivos y modelos de dispositivos particulares. Por lo general, las organizaciones están acostumbradas a este nivel de trabajo.

En cambio, la mayoría de las organizaciones puede tener muchos más tipos de dispositivos de IoT que de dispositivos de TI convencionales ya que, por naturaleza, la mayoría de los dispositivos de IoT tiene solo un propósito. Es posible que una organización necesite determinar cómo gestionar los riesgos para cientos o miles de tipos de dispositivos de IoT. Las capacidades varían ampliamente de un tipo de dispositivo de IoT a otro, por ejemplo, un tipo de dispositivo que carece de capacidades para almacenamiento de datos y gestión centralizada, y otro tipo que tiene muchos sensores y actuadores, usa capacidades locales y remotas de almacenamiento y tratamiento de datos y se conecta a varias redes internas y externas a la vez. La variabilidad de las capacidades causa una variabilidad similar en los riesgos a la ciberseguridad y la privacidad que repercute en cada tipo de dispositivo de IoT, así como en las opciones para mitigar esos riesgos.

Además, es posible que una organización necesite determinar la forma de gestionar los riesgos no solo en función del tipo de dispositivo, sino también del uso que se le dé a este. La manera en que se usará un dispositivo puede indicar que un objetivo de seguridad, como la integridad, es más importante que otro, como la confidencialidad, y que, a su vez, necesite mecanismos diferentes para la mitigación de riesgos. Asimismo, un dispositivo se podría usar de modo que haga que algunas de sus capacidades sean innecesarias y se puedan deshabilitar, lo que podría reducir el riesgo al dispositivo.

Apéndice A: [Eliminado]

Anteriormente, el Apéndice A incluía ejemplos de las posibles capacidades de ciberseguridad y privacidad que las organizaciones pueden desear en sus dispositivos de IoT. Ese contenido se eliminó de esta publicación y se refinará y publicará en un documento aparte que se incluirá en el sitio web de nuestro programa (https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program).

Apéndice B: Siglas y abreviaturas

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

API	Application Programming Interface [interfaz de programación de aplicaciones]
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]
IETF	Internet Engineering Task Force [Grupo de trabajo de ingeniería de internet]
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]
NICE	National Initiative for Cybersecurity Education [Iniciativa nacional para la educación en ciberseguridad]
NIST	National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología]
OMB	Office of Management and Budget [Oficina de Administración y Presupuesto]
PII	Personally Identifiable Information [información de identificación personal]
RFC	Request for Comments [solicitud de comentarios]
RMF	Risk Management Framework [Marco de gestión de riesgos]
SLA	Service Level Agreement [acuerdo de nivel de servicio]
SP	Special Publication [Publicación especial]
TI	tecnología de la información
TO	tecnología operativa

Apéndice C: Glosario

acciones de datos	"Operaciones de un sistema que procesan PII". [5]
acción problemática de datos	Operación de un sistema que procesa PII durante el ciclo de vida de la información y que, como efecto secundario, causa cierto tipo de problemas a las personas.
capacidad	Característica o función.
capacidad anterior al mercadeo	Capacidad de ciberseguridad o privacidad integrada en un dispositivo de IoT. El fabricante o el vendedor integran las capacidades anteriores al mercadeo en los dispositivos de IoT antes de enviarlos a las organizaciones de los clientes.
capacidad de accionamiento	Capacidad para cambiar algo en el mundo físico.
capacidad de detección	Capacidad para hacer la observación de un aspecto del mundo físico en forma de datos de medición.
capacidad de interfaz de aplicación	Capacidad de otros dispositivos informáticos para comunicarse con un dispositivo de IoT por medio de una aplicación de dispositivo de IoT.
capacidad de interfaz de red	Capacidad para interactuar con una red de comunicación con el fin de comunicar datos a un dispositivo de IoT o desde este. Una capacidad de interfaz de red permite que un dispositivo se conecte a una red de comunicaciones y la utilice. Cada dispositivo de IoT tiene al menos una capacidad de interfaz de red y puede tener más de una.
capacidad de interfaz de usuario humano	Capacidad de un dispositivo de IoT para comunicarse directamente con las personas.
capacidades de interfaz	Capacidades que habilitan las interacciones de los dispositivos IoT (por ejemplo, comunicaciones de dispositivo a dispositivo, comunicaciones de persona a dispositivo). Los tipos de capacidades de interfaz son: de aplicación, de usuario humano y de red.
capacidades de soporte	Capacidades que proporcionan una funcionalidad compatible con las demás capacidades de IoT. Algunos ejemplos de capacidades de soporte son la gestión del dispositivo y las capacidades de ciberseguridad y privacidad.
capacidades de transductor	Capacidades para que los dispositivos informáticos interactúen directamente con entidades físicas de interés Los dos tipos de capacidades de transductor son la detección y el accionamiento.
capacidad para desasociar	"Habilitación del tratamiento de PII o de eventos sin que se asocien a personas o dispositivos más allá de los requisitos operativos del sistema". [5]

capacidad posterior al mercadeo	Capacidad de ciberseguridad o privacidad que una organización selecciona, adquiere e implementa por sí misma; toda capacidad no incluida en la fase anterior al mercadeo.
información de identificación personal (PII)	"Información que se puede usar para distinguir o rastrear la identidad de una persona, sea como información única o combinada con otra información vinculada, o que puede ser vinculada, a una persona específica." [8]
procesamiento de PII	Operación o conjunto de operaciones relacionadas con la PII que pueden incluir, entre otras, la recolección, retención, registro, generación, transformación, uso, divulgación, transferencia y eliminación de PII.
riesgo	"Medida en la que una entidad es amenazada por una circunstancia o evento potencial, y que normalmente es una función de: (i) el efecto adverso, o la magnitud del daño, que tendría la circunstancia o el evento si llegara a ocurrir; y (ii) la probabilidad de que ocurra." [4]

Apéndice D: Referencias

[1] Newhouse, W., Keith, S., Scribner, B. y Witte, G. (2017), Marco para el personal de ciberseguridad de la Iniciativa nacional para la educación en ciberseguridad (NICE), (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-181 del NIST. https://doi.org/10.6028/NIST.SP.800-181

[2] 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).

[3] 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, revisión 2. https://doi.org/10.6028/NIST.SP.800-82r2

[4] Grupo de trabajo conjunto (2018), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [Marco de gestión de riesgos para sistemas de información y organizaciones: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Publicación especial 800-37 del NIST, revisión 2. https://doi.org/10.6028/NIST.SP.800-37r2

[5] Brooks, S., García, M., Lefkovitz N., Lightman S. y Nadeau, E. (2017), *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [Una introducción a la ingeniería de la privacidad y a la gestión de riesgos en los sistemas federales], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), Informe interinstitucional o interno 8062 del NIST. https://doi.org/10.6028/NIST.IR.8062

[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] Grupo de trabajo conjunto (2017), *Security and Privacy Controls for Information Systems and Organizations* [Controles de seguridad y privacidad para sistemas de información y organizaciones], (Instituto Nacional de Normas y Tecnología, Gaithersburg, Maryland), proyecto de la Publicación especial 800-53 del NIST, revisión 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[8] Oficina de Administración y Presupuesto (2016), *Managing Information as a Strategic Resource* [Gestión de la información como recurso estratégico], (Oficina de Administración y Presupuesto [OMB], Washington, DC), Circular A-130 de la OMB. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf