NIST Informe interno
NIST IR 8425 spa

Perfil del núcleo básico de IoT para productos IoT de consumo

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffery Marron
Barbara Cuthill

Esta publicación se puede obtener gratuitamente en:
https://doi.org/10.6028/NIST.IR.8425.spa

NIST Informe interno
NIST IR 8425 spa

Perfil del núcleo básico de IoT para productos IoT de consumo

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
División de Ciberseguridad Aplicada
Laboratorio de Tecnologías de la Información

Esta publicación se puede obtener gratuitamente en:
https://doi.org/10.6028/NIST.IR.8425.spa

septiembre 2022

Departamento de Comercio de EE.UU.
Gina M. Raimondo, Secretaria

Instituto Nacional de Normas y Tecnología
Laurie E. Locascio, Directora del NIST y Subsecretaria de Comercio para Normas y Tecnología

Se pueden identificar ciertas entidades comerciales, equipos o materiales en este documento con el fin de describir adecuadamente un procedimiento o concepto experimental. Esta identificación no pretende ser una recomendación o aprobación por parte del Instituto Nacional de Normas y Tecnología (NIST), ni que las entidades, materiales o equipos sean necesariamente los mejores disponibles para el propósito.

Puede haber referencias en esta publicación a otras publicaciones actualmente en desarrollo por el NIST de acuerdo con sus responsabilidades estatutarias asignadas. La información contenida en esta publicación, que incluye a los conceptos y las metodologías, puede ser utilizada por los organismos federales incluso antes de que se completen dichas publicaciones complementarias. Así pues, hasta que se complete cada publicación, los requisitos, directrices y procedimientos actuales, cuando existan, seguirán siendo operativos. A efectos de planificación y transición, las agencias federales pueden seguir de cerca el desarrollo de estas nuevas publicaciones del NIST.

Se recomienda a las organizaciones revisar todos los borradores de publicaciones durante los períodos de comentario público y a proporcionar sus comentarios al NIST. Muchas publicaciones sobre ciberseguridad del NIST, aparte de las mencionadas anteriormente, están disponibles en https://csrc.nist.gov/publications.

Políticas de las series técnicas del NIST
Declaraciones sobre derechos de autor, uso legítimo y licencias
Sintaxis del identificador de publicación de la serie técnica del NIST

Historia de la publicación
Aprobado por la Junta de Revisión Editorial del NIST el 08 de septiembre de 2022

Cómo citar esta publicación de la serie técnica del NIST:
Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) del NIST NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

ID ORCID del autor
Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Paul Watrobski: 0000-0002-6449-3030
Jeffrey Marron: 0000-0002-7871-683X
Barbara B. Cuthill: 0000-0002-2588-6165

Información de contacto
iotsecurity@nist.gov

Instituto Nacional de Normas y Tecnología
Atención: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Esta publicación está disponible gratuitamente en inglés en el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés): https://doi.org/10.6028/NIST.IR.8425.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.IR.8425.

Informes sobre tecnología de sistemas informáticos

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

Resumen

Esta publicación documenta el perfil del consumidor del núcleo básico de Internet de las Cosas (IoT) del NIST e identifica las capacidades de ciberseguridad comúnmente necesarias para el sector de IoT del consumidor (es decir, productos IoT para uso doméstico o personal). También puede ser un punto de partida para que las empresas tengan en cuenta la compra de productos IoT. El perfil del consumidor se desarrolló como parte de la respuesta del NIST a la Orden Ejecutiva 14028 y se publicó inicialmente en *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Criterios recomendados para el etiquetado de ciberseguridad de los productos de consumo del Internet de las cosas (IoT))*. Las capacidades del perfil del consumidor se formulan como resultados de ciberseguridad que se pretenden aplicar a todo el producto IoT. Este documento también analiza los fundamentos para desarrollar el perfil del consumidor recomendado y las consideraciones relacionadas. Para elaborar el perfil del consumidor, el NIST revisó una serie de documentos de referencia y colaboró con las partes interesadas durante un año.

Palabras clave

Internet de las cosas (IoT); IoT de consumo; ciberseguridad; productos IoT; privacidad; seguridad; productos seguros.

Audiencia

El público al que va dirigido este informe está formado por fabricantes de productos de consumo, especialmente responsables de seguridad de productos, minoristas e integradores relacionados y empresas de asistencia técnica que prestan servicio a los sectores de consumo y empresarial, y organismos de ensayo y certificación interesados en establecer puntos de referencia de las capacidades de ciberseguridad de IoT.

Aviso de divulgación de patentes

AVISO: El ITL ha solicitado que los titulares de reivindicaciones de patentes cuyo uso pueda ser necesario para el cumplimiento de las orientaciones o requisitos de esta publicación divulguen dichas reivindicaciones de patentes al ITL. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de patentes de ITL, y el ITL no realizó una búsqueda de patentes para identificar qué patentes, si las hubiera, se pueden aplicar a esta publicación.

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

El ITL no garantiza ni da a entender que no se requieran licencias para evitar la infracción de patentes en el uso de esta publicación.

Índice

Lista de tablas

Lista de figuras

Agradecimientos

Los autores desean dar las gracias a todos los que contribuyeron a esta publicación, que incluye a los participantes en los talleres y otras sesiones interactivas; las personas y organizaciones de los sectores público y privado, e incluye a los fabricantes de diversos sectores, así como varias organizaciones comerciales de fabricantes, que aportaron sus comentarios durante el período de respuesta del NIST al Decreto 14028. Un agradecimiento especial a los miembros del equipo de Ciberseguridad para IoT: Rebecca Herold, Brad Hoehn y David Lemire.

1. Introducción

El 12 de mayo de 2021, el Presidente emitió la Orden Ejecutiva (EO, por sus siglas en inglés) 14028, que, entre otras directices, pedía al NIST que recomendara requisitos para un programa de etiquetado de ciberseguridad de productos IoT de consumo. Como parte de la respuesta del NIST a esta directriz[1], se creó un perfil del núcleo básico de IoT[2] para productos IoT de consumo. Este perfil formó parte de las recomendaciones que el NIST publicó en respuesta a la EO en febrero de 2022 tituladas *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [Criterios EO].

El perfil se basa en la serie NISTIR 8259 y amplía el núcleo básico de IoT para los productos IoT de consumo. NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [IR8259], proporciona orientación básica para los fabricantes de dispositivos IoT en relación con el desarrollo de dispositivos IoT que puedan ser utilizados de forma segura por los clientes. NISTIR 8259 no se dirige a ningún sector específico de IoT, sino que analiza de qué modo los fabricantes pueden abordar la ciberseguridad de los dispositivos IoT en general. NISTIR 8259A, IoT *Device Cybersecurity Capability Core Baseline* [IR8259A] y NISTIR 8295B, *IoT Non-Technical Supporting Capability Core Baseline* [IR259B] definen al núcleo básico de la capacidad de ciberseguridad de dispositivos IoT (también denominada núcleo básico). El núcleo básico es un punto de partida para que los fabricantes identifiquen las capacidades de ciberseguridad que sus clientes pueden esperar de los dispositivos IoT que crean. NISTIR 8259A analiza las capacidades de ciberseguridad de los dispositivos, que son funciones o características implementadas por el dispositivo a través de su propio hardware y software. Por ejemplo, NISTIR 8259A trata conceptos como la protección de datos, el control de acceso y la actualización de software, entre otros. NISTIR 8259B discute las capacidades de apoyo no técnicas, que son acciones tomadas por las organizaciones para apoyar la ciberseguridad del dispositivo. Por ejemplo, NISTIR 8259B trata conceptos como educación y toma de conciencia, y recepción de información y consultas (por ejemplo, por parte de fabricantes/desarrolladores).

Al igual que NISTIR 8259, estos documentos de referencia no son específicos de un sector o caso de uso, sino que presentan un punto de partida para *cualquier* dispositivo de IoT. Adaptar las capacidades básicas a un sector o caso de uso específico requiere una forma de elaboración de perfiles. El proceso de creación de perfiles mediante la serie NISTIR 8259 dirige a un creador de perfiles a recopilar información específica del sector/caso de uso e interpretar los impactos relevantes para seleccionar las capacidades de referencia más aplicables a las necesidades y el objetivo de los clientes del sector/caso de uso.

El resto de este documento describe los resultados de este proceso de elaboración de perfiles para el sector del consumo y se organiza del siguiente modo:

- La sección 2 explica la aplicabilidad prevista del perfil de consumidor a los productos IoT de consumo y define el perfil de consumidor.

[1] Para más información sobre la respuesta del NIST a la petición de recomendaciones de la EO 14028 para una etiqueta de ciberseguridad de productos IoT de consumo, visite https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

[2] Los términos *núcleo básico, núcleo básico de IoT y núcleo básico de capacidades básicas de dispositivos IoT* hacen referencia al conjunto de capacidades presentadas en los NISTIR 8259A y 8259B.

- La sección 3 describe con más detalle el proceso utilizado para elaborar el perfil del consumidor.
- En la sección 4 se analizan otras consideraciones que los lectores deben tener en cuenta al utilizar el perfil del consumidor.

2. Perfil del consumidor del núcleo básico

Esta sección se basa en el informe oficial *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [Criterios EO]. En primer lugar, se define el alcance de un "producto IoT" y, a continuación, se presenta el perfil de producto IoT de consumo del núcleo básico de IoT.

2.1. Declaración sobre el alcance de los productos IoT

Los productos IoT de consumo suelen constituir un conjunto de componentes de sistema que trabajan juntos para ofrecer una funcionalidad realizada en el punto final o componente «dispositivo» del producto. El NIST describe un dispositivo IoT como un equipo informático con al menos un transductor (es decir, sensor o actuador) y al menos una interfaz de red [IR8259]. Todos los productos IoT contienen al menos un dispositivo IoT y pueden contener únicamente este componente de producto. En muchos casos, el producto IoT se puede adquirir como una sola pieza del equipo (es decir, el dispositivo IoT), pero requiere otros componentes para funcionar, como un backend (por ejemplo, un servidor en la nube) o una aplicación de usuario complementaria en un equipo personal o teléfono inteligente.

Los productos IoT complejos pueden contener múltiples dispositivos IoT físicos, otros tipos de equipos o conectarse a múltiples backends o aplicaciones complementarias como componentes. Aunque posiblemente haya un gran número de combinaciones de componentes que puedan crear un producto IoT, es útil pensar en tres tipos específicos de componentes de productos IoT (aparte del propio dispositivo IoT, que siempre está presente en un producto IoT):

- Hardware de red/pasarela especializado (por ejemplo, un concentrador dentro del sistema en el que se utiliza el dispositivo IoT).
- Software de aplicación complementario (por ejemplo, una aplicación móvil para comunicarse con el dispositivo IoT).
- Backends (por ejemplo, un servicio en la nube, o múltiples servicios, que pueden almacenar o procesar datos del dispositivo IoT).

Algunos componentes del producto IoT, como el dispositivo o dispositivos IoT (y quizás un hardware especializado de red/pasarela[3]) estarán "en la caja" que compre el cliente.[4] Otros componentes, como el software de aplicaciones complementarias o los backends, estarán "fuera de la caja[5]", pero sin embargo forman parte del producto IoT a través del soporte que proporcionan para el funcionamiento del producto IoT. Independientemente de estas relaciones, estos componentes adicionales del producto tienen acceso al dispositivo IoT y a los datos que crea y utiliza, lo que los convierte en vectores potenciales de ataque que podrían afectar al dispositivo IoT, al cliente y a otros (por ejemplo, mediante ataques a sistemas, redes locales o Internet en general). Dado que estos componentes adicionales pueden introducir riesgos nuevos o únicos en el producto IoT, se debe poder proteger todo el producto IoT, lo que incluye a los componentes auxiliares.

Nota sobre las consideraciones relativas a la evaluación de la conformidad de los componentes IoT

Este documento analiza las capacidades a nivel de producto IoT, pero los productos IoT se definen como un conjunto de componentes de productos IoT. Al considerar el proceso de evaluación de la conformidad en este contexto, es importante tener en cuenta la complejidad de evaluar la gran variedad de combinaciones de componentes de IO que podrían crear un producto. Además, algunos de estos componentes de productos IoT pueden estar total o parcialmente *modularizados*, por lo que los clientes pueden elegir el componente o la plataforma del componente. Por ejemplo, algunos programas de aplicaciones complementarias se ejecutarán en sistemas operativos móviles o a través de un navegador web, por lo que la ciberseguridad va mucho más allá del papel que el componente pueda desempeñar en el producto IoT. En estos casos, la evaluación de la conformidad de estos componentes del producto IoT con las capacidades de ciberseguridad del perfil del consumidor debe tener en cuenta este hecho y utilizar las normas o mecanismos de conformidad existentes como parte del mecanismo de conformidad del producto IoT en la medida de lo posible. Por ejemplo, pueden existir programas de certificación de ciberseguridad del sistema operativo o de la nube que puedan demostrar un soporte parcial para las capacidades de ciberseguridad identificadas en el perfil del consumidor, pero en muchos

[3] Es posible que el cliente adquiera por separado algún hardware especial de red/pasarela, pero es necesario para que el producto IoT funcione más allá de las funciones básicas. En la mayoría de los casos en los que un producto IoT requiere la adquisición por separado de hardware especializado de red/pasarela, dicho hardware realizará tareas específicas y coherentes en la implementación de un producto IoT (por ejemplo, la traducción de protocolos). Por ejemplo, algunos productos IoT requieren conexiones de red distintas de las convencionales Wi-Fi/ethernet, como Bluetooth, Zigbee o Z-Wave, que necesitarían un *concentrador* o *pasarela* para permitir una conectividad más amplia (es decir, a través de Wi-Fi o ethernet). Es posible que este *concentrador* o *pasarela* no siempre se incluya como parte de un producto IoT, sino que, en su lugar, se asuma que forma parte de la infraestructura de red del cliente, del mismo modo que se podría asumir un enrutador Wi-Fi para los productos IoT que utilizan Wi-Fi.

[4] Los componentes "en la caja", en particular el dispositivo o dispositivos IoT que sirven como punto final del producto, se pueden considerar la *cara* del producto IoT, ya que son los que el cliente manejará, gestionará y utilizará físicamente. Aunque otros componentes pueden ser vitales para el funcionamiento del producto IoT (incluida la ciberseguridad), el dispositivo o dispositivos IoT desempeñan un papel central en el producto IoT y, en general, son el centro del funcionamiento del producto IoT.

[5] Algunos componentes "externos" pueden estar totalmente alejados del cliente, mientras que otros pueden estar físicamente presentes en el entorno del cliente (por ejemplo, dentro de su casa), pero, no obstante, vienen separados del dispositivo o dispositivos IoT.

casos el soporte que el componente IoT proporciona al producto se logrará utilizando software o hardware de aplicación adicional que puede no ser considerado o evaluado por los programas existentes. La evaluación de la ciberseguridad del producto IoT puede, por tanto, aceptar la certificación existente y evaluar la ciberseguridad del software/hardware de aplicación adicional.

En este contexto, un producto IoT se define como un dispositivo IoT o dispositivos IoT y cualquier componente adicional del producto que sea necesario para utilizar el dispositivo IoT más allá de las características operativas básicas. Por ejemplo, una bombilla inteligente no conectada puede seguir iluminando en un color, pero sus funciones inteligentes, como los cambios de color, no se pueden usar sin otros componentes del producto.

2.2. Perfil del consumidor

Esta sección define las capacidades de ciberseguridad[6] que se esperan de los productos IoT y de los desarrolladores de productos IoT como parte de un perfil de consumidor.

Se recomienda aplicar los criterios de producto al producto IoT en su conjunto, , así como a cada componente individual del producto IoT, según proceda. La mayoría de los criterios afectan directamente al producto IoT y se espera que sean satisfechos por medios de software o hardware implementados en el producto IoT. Algunos criterios se aplican al desarrollador del producto IoT más que al producto IoT directamente. Se espera que estos criterios se satisfagan mediante acciones y se apoyen en afirmaciones y pruebas del desarrollador más que del propio producto IoT.

La siguiente figura presenta las capacidades de alto nivel del producto IoT y las actividades del desarrollador del producto IoT[7] desarrolladas en base a los NISTIR 8259A y 8259B, respectivamente, que se analizan en las secciones siguientes.

[6] El término capacidad generalmente se utiliza en este documento para seguir la serie NISTIR 8259, pero estas mismas capacidades se presentaron como "resultados" en la Sección 2.2 de *Criterios recomendados para el etiquetado de ciberseguridad para productos de consumo de Internet de las cosas (IoT)*. Estos términos son sinónimos y se podrían utilizar indistintamente en el contexto de este documento y del libro blanco.

[7] En la serie NISTIR 8259, se hace referencia a los fabricantes de dispositivos IoT, que pueden ser la misma entidad que un desarrollador de productos IoT de los que se habla aquí. Sin embargo, la naturaleza multicomponente de los productos IoT aumenta la posibilidad de que la entidad que introduce un producto IoT en el mercado no haya fabricado el dispositivo o dispositivos IoT físicos, sino que haya utilizado dispositivos fabricados por otra entidad para crear un producto IoT. Por lo tanto, en este documento se utiliza el término desarrollador de productos IoT.

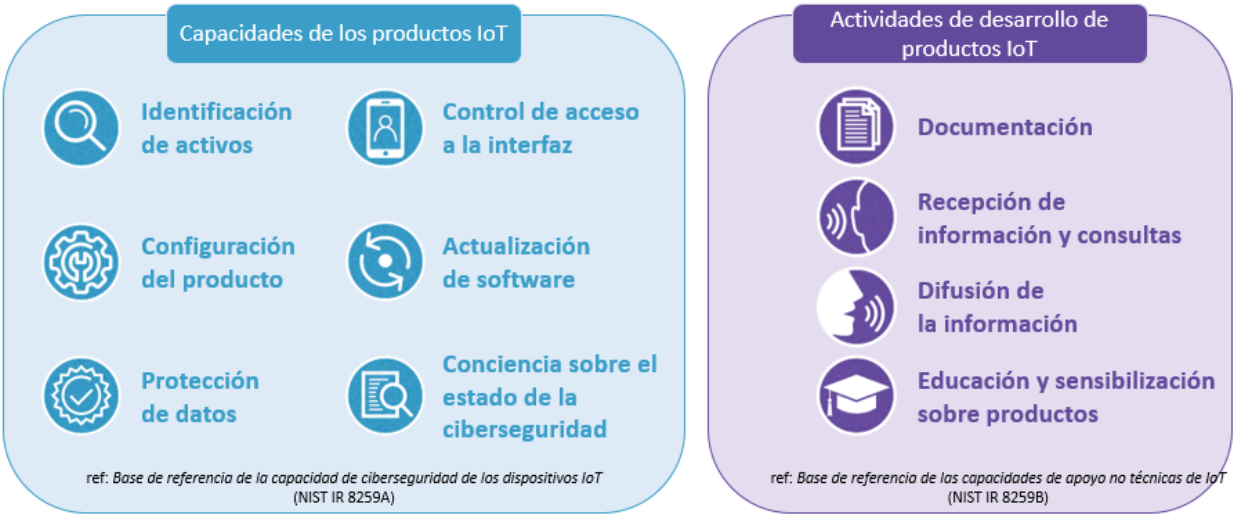

Fig. 1. Capacidades identificadas para el perfil del consumidor.

Se presentan el nombre y la definición de alto nivel de cada capacidad, seguidos de una lista alfanumérica de subcriterios para cada capacidad. Para algunos subcriterios,[8] incluye detalles adicionales sobre el resultado (es decir, texto normativo) a continuación del texto **en negrita**, mientras que la explicación adicional y los ejemplos (es decir, texto informativo) aparecen a continuación del texto *en cursiva* . Por último, cada capacidad va acompañada de una breve descripción de la utilidad prevista para la ciberseguridad.

[8] Los subcriterios pretenden ofrecer detalles adicionales sobre cómo un producto IoT puede lograr el resultado descrito en la definición de capacidades de alto nivel. Es posible que los subcriterios no abarquen todos los posibles apoyos necesarios para un resultado en todos los casos de uso, y también es posible que los subcriterios no se apliquen a todos los casos de uso.

2.2.1. Capacidades de los productos IoT

Identificación de activos

El producto IoT es identificable de forma única e inventarios de todos los IoT del producto IoT.

1. Al producto IoT se lo puede identificar de forma única por el cliente y otras entidades autorizadas (por ejemplo, el desarrollador del producto IoT).[9]
2. El producto IoT identifica de forma exclusiva cada componente del producto IoT y mantiene un inventario actualizado[10] de los componentes del producto conectados.

Utilidad de la ciberseguridad: La capacidad de identificar los productos IoT y sus componentes es necesaria para respaldar actividades como la gestión de activos para actualizaciones, la protección de datos y las capacidades forenses digitales para la respuesta a incidentes.

[9] En algunos casos, puede existir un identificador único para el propio producto IoT (independiente incluso del identificador del dispositivo IoT), pero en muchos casos, la identificación del producto IoT se puede interpretar generalmente como la identificación de uno de los componentes IoT. Para garantizar la unicidad del identificador del producto en todas las instancias del producto, normalmente se trataría del dispositivo IoT o de algún otro componente "en caja", en lugar de un componente compartido por muchas instancias, como el backend.
[10] Los inventarios pueden residir en un componente (por ejemplo, dispositivo IoT, aplicación backend) o pueden residir en múltiples componentes (por ejemplo, algunos componentes son inventariados en hardware de red/pasarela especializado) dependiendo de la arquitectura del producto IoT.

Configuración del producto

La configuración del producto IoT es modificable, existe la posibilidad de restaurar una configuración predeterminada segura, y todos y cada uno de los cambios solo pueden ser realizados por personas, servicios y otros componentes del producto IoT autorizados.

1. Las personas autorizadas (es decir, el cliente), los servicios y otros componentes del producto IoT pueden cambiar los ajustes de configuración del producto IoT a través de uno o más componentes del producto IoT.[11]
2. Las personas autorizadas (es decir, el cliente), los servicios y otros componentes del producto IoT tienen la capacidad de restaurar el producto IoT a una configuración segura por defecto (es decir, no inicializada).
3. El producto IoT aplica los ajustes de configuración a los componentes IoT aplicables.

Utilidad de ciberseguridad: La capacidad de cambiar aspectos del funcionamiento del producto IoT puede ayudar a los clientes a adaptar la funcionalidad del producto IoT a sus necesidades y objetivos. Los clientes pueden configurar sus productos IoT para evitar amenazas y riesgos específicos que conozcan en función de su apetito de riesgo.

[11] Para algunos componentes, puede haber una configuración relevante para la ciberseguridad de aspectos del componente (por ejemplo, plataforma o infraestructura de backends) que no están apropiadamente en el ámbito de gestión del producto IoT o cliente. Por ejemplo, en la mayoría de los casos, el software de aplicación que acompaña al producto IoT no debe gestionar la ciberseguridad del sistema operativo en el que se ejecuta el software.

Protección de datos

El producto IoT protege los datos almacenados en todos los componentes del producto IoT y transmitidos tanto entre los componentes del producto IoT como fuera del producto IoT frente al acceso, la divulgación y la modificación no autorizados.

1. Cada componente del producto IoT protege los datos que almacena a través de medios seguros.
2. El producto IoT tiene la capacidad de eliminar o hacer inaccesibles los datos almacenados que se recopilan del cliente, el hogar, la familia, etc., o sobre ellos.
3. Cuando se envían datos entre componentes de productos IoT o fuera del producto, se utilizan protecciones para la transmisión de datos.[12]

Utilidad de ciberseguridad: Mantener la confidencialidad, integridad y disponibilidad de los datos es fundamental para la ciberseguridad de los productos IoT. Los clientes esperarán que los datos estén protegidos y que la protección de los datos contribuya a garantizar la seguridad y funcionalidad prevista del producto IoT.

[12] Esto puede incluir la capacidad de comunicarse con componentes del producto que no pueden implementar la capacidad de Protección de Datos de la misma manera que otros componentes (por ejemplo, no pueden dar soporte a la criptografía adecuada). Cualquier comunicación de este tipo (por ejemplo, datos transmitidos con una protección inferior o limitada) debe realizarse de un modo que reduzca el riesgo subsiguiente, como el protocolo de transmisión de corto alcance o de red local (por ejemplo, Zigbee, Bluetooth) para comunicarse con algunos componentes del producto en circunstancias limitadas, pero necesarias.

Control de acceso de interfaz

El producto IoT restringe el acceso lógico a las interfaces locales y de red -y a los protocolos y servicios utilizados por dichas interfaces- únicamente a las personas, servicios y componentes del producto IoT autorizados.

1. Cada componente del producto IoT controla el acceso hacia y desde todas las interfaces (por ejemplo, interfaces locales, accesibles externamente o no, interfaces de red, protocolos y servicios) para limitar el acceso únicamente a las entidades autorizadas. **Como mínimo, el componente de producto IoT deberá:**
    a. Utilizar y tener acceso únicamente a las interfaces necesarias para el funcionamiento del producto IoT. Todos los demás canales y el acceso a los canales se eliminan o se aseguran.
    b. Para todas las interfaces necesarias para el uso del producto IoT, existen medidas de control de acceso (por ejemplo, autenticación multifactor basada en contraseña única, puertos de interfaz físicos inaccesibles desde el exterior de un componente).
    c. Para todas las interfaces, los privilegios de acceso y modificación son limitados.
2. Algunos componentes de productos IoT, aunque no necesariamente todos, disponen de medios para proteger y mantener el control de acceso a la interfaz. **Como mínimo, el producto IoT deberá:**
    a. Validar que los datos compartidos entre los componentes del producto IoT coinciden con las definiciones especificadas de formato y contenido.
    b. Evitar transmisiones no autorizadas o el acceso a otros componentes del producto.
    c. Mantenga un control de acceso adecuado durante la conexión inicial (es decir, la incorporación) y al restablecer la conectividad tras una desconexión o interrupción.

Utilidad de ciberseguridad: Enumerar y controlar el acceso a todas las interfaces internas y externas del producto IoT contribuirá a preservar la confidencialidad, integridad y disponibilidad del producto IoT, sus componentes y datos, ayudando a evitar accesos y modificaciones no autorizados.

Actualización de software

El software[13] de todos los componentes del producto IoT solo puede ser actualizado por personas, servicios y otros componentes del producto IoT autorizados con un mecanismo seguro y configurable, según proceda para cada componente del producto IoT.

1. Cada componente del producto IoT puede recibir, verificar y aplicar actualizaciones de software verificadas.
2. El producto IoT aplica medidas para mantener actualizado el software de los componentes del producto IoT (es decir, aplicación automática de actualizaciones o notificación constante al cliente de las actualizaciones disponibles a través del producto IoT).

Utilidad de ciberseguridad: El software puede tener vulnerabilidades que se descubren después de que el producto IoT se haya desplegado; las capacidades de actualización de software pueden ayudar a garantizar la entrega segura de parches de seguridad.

[13] Esto incluye el código ejecutable, así como las bibliotecas de software, los paquetes de soporte y otros datos de software no ejecutables.

Conciencia del estado de la ciberseguridad

El producto IoT admite la detección de incidentes de ciberseguridad que afecten o se vean afectados por componentes de productos IoT y los datos que almacenan y transmiten.

1. El producto IoT captura y registra de forma segura información sobre el estado de los componentes IoT[14] que se puede utilizar para detectar incidentes de ciberseguridad que afecten o se vean afectados por los componentes del producto IoT y los datos que almacenan y transmiten.

Utilidad de ciberseguridad: La protección de los datos y la garantía de una funcionalidad adecuada se pueden ver respaldadas por la capacidad de alertar al cliente cuando el dispositivo comience a funcionar de forma inesperada, lo que podría significar que se está intentando acceder sin autorización, se cargó malware, se crearon redes de bots, se produjeron errores en el software del dispositivo u otro tipo de acciones no iniciadas por el usuario del producto IoT ni previstas por el desarrollador.

[14] La información sobre el estado de los componentes de IoT que sería útil para detectar incidentes de ciberseguridad es muy contextual al producto IoT, sus componentes y su funcionamiento. En la mayoría de los casos, se debe capturar información temporal, como la marca de tiempo o los datos de ubicación (digitales o físicos). La versión de software y hardware y el estado operativo (por ejemplo, fallos conocidos o excepciones generadas) pueden ayudar a detectar vulnerabilidades de ciberseguridad (por ejemplo, un software o hardware específico puede tener vulnerabilidades conocidas). La información del estado de ciberseguridad también puede contener registros de comandos y acciones recibidos y ejecutados por el producto IoT u otros datos que sean significativos para el producto IoT y su funcionamiento y, por lo tanto, sean útiles para detectar incidentes.

2.2.2. Capacidades de apoyo no técnicas de los productos IoT

Documentación

El desarrollador de productos IoT crea, recopila y almacena[15] información relevante para la ciberseguridad del producto IoT y sus componentes antes de la compra por parte del cliente, y a lo largo del desarrollo de un producto y su posterior ciclo de vida.

1. A lo largo del ciclo de vida de desarrollo, el desarrollador del producto IoT crea o recopila y almacena información relevante para la ciberseguridad del producto IoT y sus componentes de producto, **lo que incluye**:
    a. Suposiciones realizadas durante el proceso de desarrollo y otras expectativas relacionadas con el producto IoT, **entre ellas**:
        i. Clientes previstos y casos de uso.
        ii. Uso y características físicas, incluida la seguridad de la ubicación del producto IoT y sus componentes de producto (por ejemplo, una cámara para uso dentro del hogar que tiene un interruptor de apagado en el dispositivo frente a una cámara de seguridad para uso fuera del hogar que no tiene un interruptor de apagado en el dispositivo).
        iii. Acceso a la red y requisitos (por ejemplo, requisitos de ancho de banda).
        iv. Datos creados y manejados por el producto IoT.
        v. Todas las entradas y salidas de datos previstas (lo que incluye códigos de error, frecuencia, tipo/forma, gama de valores aceptables, etc.).
        vi. Los requisitos de ciberseguridad asumidos por el desarrollador del producto IoT para el producto IoT.
        vii. Las leyes y reglamentos que cumplen el producto IoT y las actividades de apoyo relacionadas.
        viii. Vida útil prevista y costos de ciberseguridad previstos relacionados con el producto IoT (por ejemplo, precio del mantenimiento) y duración y condiciones de la asistencia.
    b. Todos los componentes de IoT, lo que incluye, entre otros, el dispositivo IoT, que forman parte del producto IoT.
    c. Cómo cumple el producto IoT los criterios básicos del producto en todos sus componentes, lo que incluye los criterios básicos que no cumplen los componentes del producto IoT y por qué (por ejemplo, la capacidad no es necesaria según la evaluación de riesgos).
    d. Consideraciones sobre el diseño del producto y el soporte relacionado con el

[15] La documentación tratada en este criterio es mantenida y controlada por el desarrollador del producto IoT. Compartir esta información puede ser apropiado y se puede limitar a técnicos autorizados y expertos en ciberseguridad que buscan más información sobre el producto IoT (por ejemplo, en la evaluación del producto IoT para el etiquetado, la investigación de una violación), pero la información documentada no está destinada, en todos los casos, a ser compartida directamente con los consumidores.

producto IoT, *por ejemplo*:

i. Todos los componentes de hardware y software, de todas las fuentes (por ejemplo, código abierto, propiedad de terceros, desarrollados internamente) utilizados para crear el producto IoT (es decir, utilizados para crear cada componente del producto).
ii. Plataforma IoT utilizada en el desarrollo y funcionamiento del producto IoT, sus componentes de producto, incluida la documentación relacionada.
iii. Fiabilidad y protección de los elementos de software y hardware implementados para crear el producto IoT y sus componentes de producto (por ejemplo, arranque seguro, raíz de confianza de hardware y enclave seguro).
iv. Consideración de los riesgos conocidos relacionados con el producto IoT y los posibles usos indebidos conocidos.
v. Desarrollo de software seguro y prácticas utilizadas en la cadena de suministro.
vi. Resultados de acreditación, certificación o evaluación de prácticas relacionadas con la ciberseguridad.
vii. La facilidad de instalación y mantenimiento del producto IoT por parte de un cliente (es decir, la facilidad de uso del producto [ISO9241]).

e. Requisitos de mantenimiento del producto IoT, *por ejemplo*:
   i. Expectativas de mantenimiento de ciberseguridad e instrucciones o procedimientos asociados (por ejemplo, plan de gestión de vulnerabilidades/parches).
   ii. Cómo identifica el desarrollador del producto IoT a las partes de soporte autorizadas que pueden realizar actividades de mantenimiento (por ejemplo, centros de reparación autorizados).
   iii. Consideraciones de ciberseguridad del proceso de mantenimiento (por ejemplo, de qué modo los datos de los clientes no relacionados con el proceso de mantenimiento siguen siendo confidenciales incluso para los mantenedores).
f. Las políticas y procesos seguros del ciclo de vida del sistema asociados con el producto IoT, **lo que incluye:**
   i. Medidas adoptadas durante el desarrollo para garantizar que el producto IoT y sus componentes estén libres de vulnerabilidades conocidas y explotables.
   ii. El proceso de trabajar con proveedores de componentes y vendedores de terceros para garantizar que la seguridad del producto IoT y sus componentes se mantiene durante todo su ciclo de vida con soporte.
   iii. Cualquier consideración posterior al fin del soporte, como el descubrimiento de una vulnerabilidad que pudiera afectar

significativamente a la seguridad, privacidad o protección de los clientes que siguen utilizando el producto IoT y sus componentes.

g. Las políticas y procesos de manejo de vulnerabilidades asociados al producto IoT, **lo que incluye**:
    i. Métodos de recepción de informes sobre vulnerabilidades (consulte más adelante Recepción de información y consultas).
    ii. Procesos para registrar las vulnerabilidades notificadas.
    iii. Política de respuesta a las vulnerabilidades notificadas, lo que incluye el proceso de coordinación de las actividades de respuesta a las vulnerabilidades entre los proveedores de componentes y terceros vendedores.
    iv. Política de divulgación de vulnerabilidades notificadas.
    v. Procesos para recibir notificaciones de los proveedores de componentes y terceros vendedores sobre cualquier cambio en el estado de sus componentes suministrados, como fin de producción, fin de soporte, estado obsoleto (por ejemplo, ya no se recomienda el uso del producto) o inseguridades conocidas.

Utilidad de ciberseguridad: Generar, capturar y almacenar información importante sobre el producto IoT y su desarrollo (por ejemplo, la evaluación del producto IoT y las prácticas de desarrollo utilizadas para crearlo y mantenerlo) puede ayudar a informar al desarrollador del producto IoT sobre la postura real de ciberseguridad del producto.

Recepción de información y consultas

El desarrollador del producto IoT tiene la capacidad de recibir información relevante para la ciberseguridad y responder a las consultas del cliente y otros sobre información relevante para la ciberseguridad.

1. El desarrollador del producto IoT puede recibir información relacionada con la ciberseguridad del producto IoT y sus componentes de producto y puede responder a consultas relacionadas con la ciberseguridad del producto IoT y sus componentes de producto de parte de clientes y otros, **lo que incluye**:
    a. La capacidad del desarrollador del producto IoT de identificar un punto de contacto para recibir información sobre mantenimiento y vulnerabilidades (por ejemplo, capacidades de notificación de errores y programas de recompensa por errores) de los clientes y otros en el ecosistema del producto IoT (por ejemplo, técnico de reparación que actúe en nombre del cliente).
    b. La capacidad del desarrollador del producto IoT para recibir consultas y responder a los clientes y otras personas del ecosistema del producto IoT sobre la ciberseguridad del producto IoT o sus componentes.

Utilidad de ciberseguridad: A medida que los productos IoT son utilizados por los clientes, estos pueden hacer consultas o informar de problemas que pueden ayudar a mejorar la ciberseguridad del producto IoT con el tiempo.

Difusión de la información

El desarrollador del producto IoT difunde (por ejemplo, al público) y distribuye (por ejemplo, al cliente o a otros en el ecosistema del producto IoT) información relevante para la ciberseguridad.

1. El desarrollador del producto IoT puede difundir a muchas o todas las entidades a través de un canal (por ejemplo, una publicación en un canal público, correos electrónicos enviados a todas las direcciones registradas de los clientes afectados) para alertar al público y a los clientes del producto IoT sobre información y eventos relevantes para la ciberseguridad a lo largo del ciclo de vida del soporte. **Como mínimo, esta información incluirá**:
    a. Condiciones de asistencia actualizadas (por ejemplo, frecuencia de las actualizaciones y mecanismo(s) de aplicación) y aviso de disponibilidad o aplicación de las actualizaciones de software.
    b. Fin del plazo de soporte o funcionalidad del producto IoT.
    c. Operaciones de mantenimiento necesarias.
    d. Nuevas vulnerabilidades de dispositivos IoT, detalles asociados y acciones de mitigación necesarias por parte del cliente.
    e. Descubrimiento de brechas relacionadas con un producto IoT y sus componentes utilizados por los clientes, detalles asociados y acciones de mitigación necesarias por parte del cliente (si las hubiera).
2. El desarrollador del producto IoT puede distribuir información relevante para la ciberseguridad del producto IoT y sus componentes de producto para alertar a las entidades apropiadas del ecosistema (por *ejemplo*, fabricantes de componentes de productos IoT o entidades de apoyo, autoridades comunes de seguimiento de vulnerabilidades, acreditadores y certificadores, organizaciones de apoyo y mantenimiento de terceros) sobre información relevante para la ciberseguridad, *por ejemplo*:
    a. Documentación aplicable recopilada durante el diseño y el desarrollo del producto IoT y sus componentes.[16]
    b. Alertas de ciberseguridad y vulnerabilidad e información sobre la resolución de cualquier vulnerabilidad.
    c. Una visión general de las prácticas y salvaguardas de seguridad de la información utilizadas por el desarrollador de productos IoT.
    d. Acreditación, certificación o resultados de la evaluación de las prácticas relacionadas con la ciberseguridad del desarrollador del producto IoT.

[16] Este subcriterio pretende indicar que la información capturada como parte de la capacidad de Documentación puede tener que ser comunicada a entidades específicas (por ejemplo, fabricantes de componentes de productos IoT o entidades de apoyo, autoridades comunes de seguimiento de vulnerabilidades, acreditadores y certificadores, organizaciones de apoyo y mantenimiento de terceros). En la mayoría de los casos, este tipo de documentación solo se compartiría con las partes interesadas que tuvieran una finalidad específica para la información (por ejemplo, la evaluación del cumplimiento) y, por lo general, no se compartiría públicamente ni siquiera con los clientes del sector de consumo.

e. Un informe o resumen de evaluación de riesgos para la postura de riesgo del entorno empresarial del desarrollador del producto IoT.

Utilidad de ciberseguridad: A medida que cambien el producto IoT, sus componentes, amenazas y mitigaciones, los clientes necesitarán estar informados sobre cómo utilizar el producto IoT de forma segura.

Educación y conciencia sobre los productos

El desarrollador del producto IoT crea conciencia y educa a los clientes y a otros en el ecosistema del producto IoT sobre la información relacionada con la ciberseguridad (por ejemplo, consideraciones, características) relacionadas con el producto IoT y sus componentes.[17]

1. El desarrollador del producto IoT crea conciencia y proporciona educación dirigida a los clientes sobre información relevante para la ciberseguridad del producto IoT y sus componentes de producto, **lo que incluye**:
    a. La presencia y el uso de capacidades de ciberseguridad de productos IoT, que **incluyan como mínimo**:
        i. Cómo cambiar los ajustes de configuración y las implicaciones de ciberseguridad de cambiar los ajustes, si las hubiera.
        ii. Cómo configurar y utilizar la funcionalidad de control de acceso (por ejemplo, establecer y cambiar contraseñas).
        iii. Cómo se aplican las actualizaciones de software y cualquier instrucción necesaria para el cliente sobre cómo utilizar la funcionalidad de actualización de software.
        iv. Cómo manejar los datos del dispositivo, incluida la creación, actualización y eliminación de datos en el producto IoT.
    b. Cómo mantener el producto IoT y sus componentes durante su vida útil, incluso después del período de soporte de seguridad (por ejemplo, entrega de actualizaciones y parches de software) por parte del desarrollador del producto IoT.
    c. De qué modo un producto IoT y sus componentes se pueden reaprovisionar o eliminar de forma segura.
    d. Opciones de manejo de vulnerabilidades (por ejemplo, manejo de configuración y parches y antimalware) disponibles para el producto IoT o sus componentes de producto que podrían utilizar los clientes.
    e. Información adicional que los clientes pueden utilizar para tomar decisiones de compra informadas sobre la seguridad del producto IoT (por ejemplo, la duración y el alcance del soporte del producto mediante actualizaciones de software y parches).

Utilidad de ciberseguridad: Habrá que informar a los clientes sobre cómo utilizar el dispositivo de forma segura para obtener los mejores resultados de ciberseguridad para los clientes y el mercado de productos IoT de consumo.

[17] La información y los conocimientos para desarrollar una educación y conciencia eficaces en relación con un producto IoT pueden residir en el desarrollador o fabricante del componente del producto IoT. Se recomienda un ecosistema de educación y conciencia que comparta información sobre la ciberseguridad de IoT, incluso antes del despliegue de un producto IoT, ya que ayudará en la implementación de esta y otras capacidades de ciberseguridad.

3. Consideraciones sobre el sector de consumo utilizadas para crear el perfil

El NIST utilizó los conceptos de elaboración de perfiles de núcleos básicos de las capacidades de ciberseguridad de los dispositivos IoT para desarrollar el perfil del consumidor. El primer paso consistió en recopilar fuentes y otra información sobre la ciberseguridad de los productos IoT de consumo. A continuación, el NIST utilizó esta información para crear el perfil del consumidor utilizando fuentes, información y conclusiones e ideas resultantes.

3.1. Recopilación de fuentes de información sobre ciberseguridad de productos IoT de consumo

El perfil del consumidor surgió de la respuesta del NIST a la EO 14028, que ordenaba al NIST desarrollar recomendaciones para un programa de etiquetas de ciberseguridad de productos IoT de consumo. Las recomendaciones eran más amplias que el desarrollo de un perfil de consumidor del núcleo básico de IoT, pero el perfil era un elemento clave de esta tarea. Por lo tanto, el NIST pudo recopilar fuentes y entablar conversaciones con partes interesadas externas sobre las necesidades y los objetivos de los clientes de productos IoT de consumo. A lo largo de un año de eventos, reuniones y otros compromisos, se recopilaron cientos de comentarios relacionados con el etiquetado de ciberseguridad para los productos IoT de consumo, muchos de los cuales informaron el perfil del núcleo básico para este sector.

El NIST también buscó en el dominio público para identificar las vulnerabilidades aplicables al sector de productos IoT de consumo. Esta información es importante para determinar una visión transversal de las vulnerabilidades de los productos IoT de consumo que pueda servir de base para determinar las amenazas y vulnerabilidades. Estas amenazas y vulnerabilidades informan el proceso de elaboración de perfiles, en particular los aspectos de seguridad mínima. La Tabla 1, reproducida de *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* Whitepaper [Camino_adelante] enumera una serie de vulnerabilidades aplicables y bien documentadas, sus categorías de ataque asociadas del MITRE ATT&CK Framework[ATT_CK] y las capacidades perfiladas que pueden ayudar a abordar la vulnerabilidad.[18]

Tabla 1. Ejemplo de vulnerabilidades IoT del consumidor y las capacidades relevantes del perfil del consumidor.

Vulnerabilidad	Capacidades relevantes del perfil del consumidor
Ataques con variantes del malware Mirai: uso de autenticación débil para permitir la carga de malware en el dispositivo y utilizarlo en ataques DDOS y de otro tipo.	

[18] Las capacidades identificadas no son exhaustivas, pero se incluyen para demostrar que las capacidades de ciberseguridad de apoyo como las detalladas en el perfil del consumidor pueden ayudar a mitigar o prevenir las vulnerabilidades identificadas. Por ejemplo, una capacidad de control de acceso a la interfaz podría haber impedido el acceso no autorizado a un dispositivo IoT.

Vulnerabilidad	Capacidades relevantes del perfil del consumidor
Acceso no autorizado al dispositivo IoT	Identificación de activos Control de acceso a la interfaz Difusión de la información Educación y sensibilización
Se puede cargar código malicioso en el dispositivo IoT	Actualización de software Conciencia sobre el estado de la ciberseguridad Educación y sensibilización
Los comandos se pueden lanzar utilizando el dispositivo	Control de acceso a la interfaz Documentación
Publicación no autorizada de datos de Fitness Tracker: los datos de localización de Fitness Tracker del personal militar se publicaron incluso cuando el producto estaba configurado para la privacidad.	
Vulnerabilidades de las aplicaciones web	Configuración del producto Conciencia sobre el estado de la ciberseguridad Documentación Difusión de la información
Vulnerabilidades de las aplicaciones móviles	Configuración del producto Conciencia sobre el estado de la ciberseguridad Documentación Difusión de la información
Posibilidad de reidentificar los datos desidentificados	Configuración del producto Protección de datos Documentación
Acceso no autorizado a datos de cámaras de seguridad domésticas: el acceso no autorizado a datos y vistas del interior y exterior de edificios se produjo con múltiples marcas de cámaras de seguridad.	
Autenticación débil	Control de acceso a la interfaz

Vulnerabilidad	Capacidades relevantes del perfil del consumidor
Intercambio de datos no autorizado	Protección de datos Documentación Difusión de la información
Falta de respuesta a las preguntas y quejas de los promotores	Recepción de información y consultas
Falta de capacidades y procedimientos de supervisión	Identificación de activos Configuración del producto Documentación
Falta de controles de registro/recopilación de datos	Identificación de activos Configuración del producto Documentación Difusión de la información Educación y sensibilización

El NIST también examinó las normas, el cumplimiento y el ecosistema de etiquetado existentes para los dispositivos y productos IoT con el fin de comprender en qué aspectos otros habían tenido en cuenta las consideraciones relativas a los productos IoT de consumo. Se revisaron aproximadamente 30 documentos fuente, incluidas leyes de ciberseguridad de la IO, catálogos de capacidades de ciberseguridad, conjuntos de capacidades de referencia y esquemas de clasificación por niveles.[19] Todos se refirieron específicamente al dispositivo IoT en sí, pero varios incluyeron la nube, la aplicación móvil, el concentrador u otros componentes externos en sus consideraciones como parte de un producto IoT. A lo largo de los períodos de comentario público y las discusiones con las partes interesadas, se apoyó la visión más amplia (es decir, de producto IoT frente a dispositivo IoT), ya que el NIST observó un gran consenso en la necesidad de incluir todos los componentes de un producto IoT en el ámbito de aplicación de un conjunto establecido de capacidades de ciberseguridad.

3.2. Evaluación de las fuentes de ciberseguridad de los productos IoT de consumo

Los documentos fuente pueden compararse más directamente con las capacidades de apoyo técnico y no técnico establecidas en los NISTIR 8259A y 8259B. De los 30 documentos fuente recopilados, una submuestra de 8 estaba más directamente relacionada con los productos de consumo de la IO. Esta submuestra se comparó con las capacidades descritas en NISTIR

[19] En la EO 14028 se pedía al NIST que estudiara la posibilidad de establecer niveles para las recomendaciones de etiquetado del IoT destinadas a los consumidores, pero la investigación del NIST y los comentarios posteriores no dieron lugar a un conjunto o marco claro y eficaz para desarrollar niveles. Las fuentes existentes que abordan los niveles no lo hacen con una visión consensuada. Además, el NIST escuchó los comentarios de que los niveles deberían reflejar niveles crecientes de riesgo relacionados con los productos IoT de consumo, pero la variedad de casos de uso de IoT de consumo hace que agrupar esos casos de uso en función del riesgo, un requisito previo para clasificarlos por niveles, sea una tarea que no podría completarse en el plazo de un año para responder a la EO 14028.

8259A/B, lo que demostró que existía una amplia coincidencia con las capacidades técnicas, aunque se utilizaron algunas capacidades técnicas comunes que no se encontraban en NISTIR 8259A para adaptar el núcleo básico al perfil del consumidor. Sin embargo, pocos documentos fuente abordaban las capacidades no técnicas desarrolladas sobre la base de NISTIR 8259B. Dado que los usuarios previstos de los dispositivos IoT de consumo no suelen ser expertos en ciberseguridad, estas capacidades de apoyo no técnicas son esenciales para garantizar un funcionamiento seguro.

Esto se confirmó a través de comentarios públicos y opiniones verbales a lo largo del trabajo sobre la respuesta de la EO, que sirvió como otra fuente de información en la que se basó el NIST para elaborar el perfil del consumidor. A través de estas fuentes, el NIST también se enteró de otras formas en las que el sector del consumo puede ser diferente al caso general o a otros sectores. Por ejemplo, la gestión de riesgos de ciberseguridad de los clientes empresariales suele estar más estructurada y formalizada en comparación con el enfoque de gestión de riesgos de ciberseguridad utilizado por los clientes del sector de consumo. Las empresas también suelen tener mayor acceso a los conocimientos de ciberseguridad que los consumidores típicos. Estas diferencias y otras percepciones tienen implicaciones sobre cómo se deben enfocar y ofrecer las capacidades de ciberseguridad. En la Tabla 2 se destacan las ideas clave utilizadas en el desarrollo del perfil de IoT del consumidor.

Tabla 2. Ideas destacadas y conclusiones clave del proceso de elaboración de perfiles de IoT de los consumidores.

Ideas destacadas	Lo más importante
Las perspectivas de ciberseguridad para el sector de consumo basadas en riesgos y vulnerabilidades son similares a las del caso básico general. (por ejemplo, los enumerados en el Tabla 1)	La mayoría de las capacidades tienen conceptos de ciberseguridad similares al núcleo básico
Las directrices de ciberseguridad a nivel de dispositivo serían insuficientes en función de las necesidades y objetivos de los clientes para este sector, incluida, entre otras cosas, su falta de distinción entre el dispositivo IoT y los componentes de apoyo.	Producto es el nivel preferido para las directrices de ciberseguridad de IoT del consumidor.
La privacidad y la seguridad son preocupaciones importantes para los productos IoT de consumo, junto con la ciberseguridad.	Las capacidades de ciberseguridad se deben diseñar para no crear riesgos en estas áreas y apoyar los enfoques generales de mitigación de riesgos para la privacidad y la seguridad.

Ideas destacadas	Lo más importante
No existe un conjunto claro y universal de necesidades y objetivos de los consumidores en materia de ciberseguridad en el sector del consumo, y el NIST identificó varios enfoques para abordar las necesidades y objetivos de los clientes entre los documentos originales, lo que incluye la revisión del panorama.	Las capacidades se deben basar en funciones de ciberseguridad universalmente aceptadas y de aplicación general.
Las necesidades y objetivos de los clientes de este sector variarán. Los clientes pueden tener conocimientos y habilidades limitados con las tecnologías IoT/IT y las funciones de ciberseguridad.	Los factores humanos relacionados con las capacidades de ciberseguridad son primordiales para mitigar los riesgos de ciberseguridad.

Estas percepciones y conclusiones conducen al NIST a las siguientes consideraciones sobre el perfil de IoT del consumidor:

1. Quedó claro que muchos dispositivos IoT de consumo se apoyan en componentes adicionales, como un back-end o una aplicación móvil, que son fundamentales para utilizar el dispositivo IoT hasta el punto de que el dispositivo no se puede utilizar de forma significativa sin estos componentes.
2. Además, los consumidores domésticos suelen tener poco control sobre estos componentes adicionales. Por lo tanto, al considerar cómo se aplicará la centricidad del dispositivo al sector de consumo, el concepto se debe ampliar más allá del dispositivo para incluir el producto completo. Este ámbito puede incluir componentes adicionales como parte de un producto IoT, lo que incluye a aquellos con los que el consumidor interactúa solo indirectamente (por ejemplo, el backend).
3. El perfil del consumidor se debe aplicar en el contexto de las percepciones y consideraciones clave del sector en materia de privacidad y seguridad. Sin embargo, las consideraciones de seguridad y privacidad son dinámicas para los productos IoT de consumo, debido a que, incluso en este sector específico, los casos de uso de los productos IoT pueden variar significativamente. Puede haber claras implicaciones de seguridad en un producto y su funcionamiento, pero no siempre es así. Lo mismo ocurre con la privacidad. Esto se ve agravado por el hecho de que diferentes casos de uso pueden compartir consideraciones generales de seguridad o privacidad, pero los detalles específicos de sus impactos o mitigaciones pueden ser muy diferentes. Todo esto significa que las capacidades de ciberseguridad del perfil del consumidor deben apoyar ampliamente una variedad de casos de uso, teniendo cuidado de no obstaculizar estas áreas.
4. Las prácticas de ciberseguridad de los clientes (es decir, los consumidores domésticos) que gestionarían los productos IoT de consumo variarán en definición y madurez. La naturaleza impredecible y ad hoc de la mitigación del riesgo del cliente para los

productos IoT de consumo pone de relieve la necesidad de que se reflejen en el perfil prácticas de ciberseguridad ampliamente útiles y generalmente recomendadas.

5. Además, una importante necesidad de ciberseguridad para este sector son las capacidades de ciberseguridad utilizables que se implementan para requerir una configuración e interacción mínima/eficiente del cliente para su uso, ya que estos clientes no tendrán conocimientos profundos o recursos que puedan aprovechar si las capacidades no son utilizables para ellos.
6. Por último, se deben utilizar normas, soluciones, implementaciones o mitigaciones específicas según convenga para la funcionalidad y el caso de uso de un producto IoT. Esto significa que no existe un único conjunto de requisitos específicos que se pueda aplicar a todos los productos IoT de consumo. Por lo tanto, el perfil del consumidor describe las directrices de ciberseguridad a nivel de producto IoT en términos de resultados que se deben alcanzar y tener soporte del producto en su conjunto, pero puede no aplicarse a todos los componentes del producto IoT de la misma manera. Es posible que algunos componentes no puedan, o no necesiten, cumplir todos los criterios.[20] Estos resultados proporcionan orientación para una variedad de tecnologías y casos de uso, pero permiten flexibilidad en la aplicación del perfil del consumidor a productos IoT específicos.[21]

El NIST aplicó estas consideraciones a las capacidades básicas de referencia NISTIR 8259A/B para adaptar el enfoque general de IoT al sector de consumo. El perfil del consumidor resultante, aunque está más directamente adaptado al sector, pretende abarcar una amplia gama de tecnologías IoT, casos de uso y consideraciones de mitigación de riesgos. Por lo tanto, la aplicación del perfil del consumidor a un producto, tipo de producto o componente de producto IoT específico puede requerir una adaptación adicional, aunque similar, mediante la recopilación y consideración de la información descrita en esta sección.

[20] Como se indica en los *Criterios recomendados para el etiquetado de ciberseguridad de los productos de consumo del Internet de las cosas (IoT)*, es posible que no todas las capacidades o subcriterios se apliquen a todos los componentes de los productos IoT o sean compatibles con ellos de la misma manera. Esto se podría deber a consideraciones de riesgo del producto, desarrollo del producto (por ejemplo, tareas de ciberseguridad delegadas a través de contratos y cadena de suministro), naturaleza de los componentes para formar el producto (por ejemplo, los backends pueden estar muy distribuidos) o limitaciones de los componentes de la IO (por ejemplo, los dispositivos pueden estar restringidos, las aplicaciones de software complementarias pueden tener acceso y funcionalidad limitados). Tener esto en cuenta a la hora de aplicar las capacidades y los subcriterios a productos del mundo real (por ejemplo, a través de un mecanismo de evaluación de la conformidad) es fundamental para un mercado y un ecosistema de ciberseguridad sólidos que puedan satisfacer necesidades y contextos dispares.

[21] El NIST recomienda a quienes dispongan de directrices, normas o programas que consideren que apoyan o se relacionan con algunos o todos los resultados reflejados en este perfil que consulten el Catálogo de referencias informativas en línea (OLIR) del NIST para obtener más información sobre cómo enviar correspondencias públicas entre su trabajo y el perfil del consumidor.

Referencias

[ATT_CK] The MITRE Corporation (2013) Adversarial Tactics, Techniques, and Common Knowledge. (The MITRE Corporation, Bedford, MA). https://attack.mitre.org/

[EO_Criteria] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.24

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8259 del NIST. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8259A del NIST. https://doi.org/10.6028/NIST.IR.8259A

[IR8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), Informe Interinstitucional o Interno (IR) 8259B del NIST. https://doi.org/10.6028/NIST.IR.8259B

[ISO9241] Organización Internacional de Normalización/Comisión Electrotécnica Internacional (2018) ISO 9241-11:2018 Ergonomía de la interacción persona-sistema - Parte 11. Ergonomía de la interacción persona-sistema: Usabilidad: Definiciones y conceptos (ISO Ginebra, Suiza). Disponible en https://www.iso.org/standard/63500.html

[Ruta_hacia_adelante] Instituto Nacional de Normas y Tecnología (2021) Etiquetado de ciberseguridad del consumidor para productos IoT: Borrador de debate sobre el camino a seguir. (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD). Disponible en: https://www.nist.gov/document/draft-paper-consumer-cybersecurity-labeling-iot-products-discussion-draft-path-forward

Apéndice A. Glosario

producto IoT de consumo
Productos IoT destinados al uso personal, familiar o doméstico.

núcleo básico
Un conjunto de capacidades de ciberseguridad de dispositivos y capacidades de apoyo no técnicas necesarias para respaldar los controles de ciberseguridad comunes que protegen los dispositivos del cliente y los datos, sistemas y ecosistemas de los dispositivos.

capacidad de ciberseguridad del producto
Características o funciones de ciberseguridad que los dispositivos informáticos proporcionan a través de sus propios medios técnicos (es decir, hardware y software del dispositivo). [IR8259]

> *Nota:* Este término es sinónimo de capacidades de ciberseguridad *del dispositivo*, tal como se definen en NISTIR 8259, pero se aplica a un producto IoT, tal como se define en este documento y no solo al dispositivo IoT.

Dispositivo IoT
Dispositivos que tienen al menos un transductor (sensor o actuador) para interactuar directamente con el mundo físico y al menos una interfaz de red (por ejemplo, Ethernet, Wi-Fi, Bluetooth) para interactuar con el mundo digital.

Producto IoT
Un dispositivo o dispositivos IoT y cualquier componente adicional del producto (por ejemplo, backend, aplicación móvil) que sea necesario para utilizar el dispositivo IoT más allá de las funciones operativas básicas.

Componente de producto IoT
Un dispositivo IoT u otro equipo o servicio digital (por ejemplo, backend, aplicación móvil) utilizado para crear productos IoT.

capacidad de apoyo no técnico
Las capacidades de apoyo no técnicas son acciones que una organización realiza en apoyo de la ciberseguridad de un dispositivo IoT.