19 de abril de 2018

Seguridad de la IoT para formuladores de políticas

"La ciberseguridad será el desafío más apremiante de la próxima década, desafío en el que la IoT tendrá un papel fundamental".

Internet Society – Informe global de Internet 2017

Internet Society

Introducción

La naturaleza abierta de Internet crea la capacidad de conectar dispositivos, aplicaciones y servicios de backend a una escala que transforma la manera en que interactuamos con nuestro entorno y con nuestra sociedad. La Internet de las Cosas (IoT) tiene un enorme potencial para mejorar nuestro mundo. Las proyecciones sobre el impacto que tendrá la IoT sobre Internet y la economía global impresionan dado que anticipan un crecimiento explosivo del número de dispositivos conectados a la IoT y su uso en una amplia variedad de aplicaciones nuevas y fascinantes. Según una estimación, "los dispositivos conectados llegarán a 38.500 millones in 2020, un enorme aumento con respecto a los 13.400 millones de dispositivos conectados en 2015."[1]

A la vez, dados los miles de millones de dispositivos, aplicaciones y servicios de la IoT que ya están en uso y a la creciente cantidad de usuarios conectados, la seguridad de la IoT es de suma importancia. Los dispositivos y servicios de la IoT poco seguros pueden servir como puntos de entrada de ciberataques y así comprometer datos confidenciales y amenazar la seguridad de los usuarios individuales. Alimentados por redes de dispositivos para la IoT poco seguros, los ataques a la infraestructura y a otros usuarios pueden afectar la prestación de servicios esenciales como los sistemas de salud y los servicios públicos básicos, poner en peligro la seguridad y la privacidad de los demás y amenazar la capacidad de recuperación de Internet a nivel mundial.

IoT también presenta importantes desafíos en el asunto de privacidad de los datos. Se abordarán en un documento complementario sobre privacidad de datos e IoT.

¿Qué es la Internet de las Cosas (IoT)? [2]

El término 'Internet de las Cosas' se refiere a **"escenarios donde la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y elementos cotidianos que habitualmente no se consideran computadoras, y permiten que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana".[3]** La IoT incluye productos de consumo, bienes duraderos, automóviles y camiones, componentes utilizados por la industria y los servicios públicos, sensores y muchos otros. Presenta una nueva forma para que los usuarios interactúen con la red, utilizando dispositivos que no se limitan a las computadoras tradicionales, los teléfonos inteligentes y las computadoras portátiles. La IoT genera nuevas oportunidades sin precedente para aplicaciones industriales e infraestructura crítica, pero también da lugar a importantes desafíos. Muchos de los desafíos y recomendaciones abordados en este documento se centran en la IoT de consumo general, pero también son válidos para las aplicaciones industriales de la IoT y su uso en infraestructura crítica. Si bien los protocolos de comunicación local que se utilizan para la IoT, tales como Zigbee[4], LORA[5], Z-Wave[6] o Bluetooth[7], presentan sus propios desafíos, el enfoque principal de la Internet Society es cómo los sistemas de la IoT interactúan con Internet y con sus usuarios y cómo los afectan.

1 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
2 Para más recursos de Internet Society sobre IoT, vea nuestra página inicial IoT (https://www.internetsociety.org/iot/) y el documento: "The Internet of Things (IoT): An Overview"
3 https://www.internetsociety.org/doc/iot-overview
4 http://www.zigbee.org/what-is-zigbee/
5 https://www.lora-alliance.org/what-is-lora
6 http://www.z-wave.com/about
7 https://www.bluetooth.com/

Se pueden utilizar dispositivos de la IoT comprometidos, por ejemplo, cámaras web o incluso bombillas, para formar 'botnets', redes de dispositivos conectados a Internet y controlados de forma externa. Estos dispositivos —que en este contexto se suelen denominar 'bots'— se pueden infectar con software malicioso y utilizar con fines disruptivos o delictivos, por ejemplo, para atacar a otras redes, otros usuarios y la infraestructura de Internet.[8] En 2016, una botnet de dispositivos de la IoT comprometidos lanzó un ataque distribuido de denegación de servicio (DDoS) contra Dyn[9], un importante proveedor de servicios de sistema de nombres de dominio (DNS). El ataque hizo que los principales sitios web, entre ellos Twitter, Amazon y Netflix, quedaran temporalmente inaccesibles para los usuarios de Internet en algunas partes del mundo.

> A medida que se conecta una mayor cantidad de dispositivos de la IoT vulnerables, estos crean una mayor 'superficie de ataque' y aumentan la potencial escala y gravedad de los ataques DDoS basados en la IoT.

Comprender el creciente impacto que la seguridad de la IoT tiene para Internet y sus usuarios es fundamental para salvaguardar el futuro de Internet. Los fabricantes de dispositivos para la IoT, los proveedores de servicios de la IoT, los usuarios, las organizaciones de estandarización, los legisladores y los reguladores deberán tomar medidas para protegerse de las amenazas a la infraestructura de Internet, por ejemplo, los ataques DDoS basados en la IoT. También es importante comprender cómo la seguridad de la IoT afecta la confianza de los usuarios y el uso de la red.[10] La confianza es un ingrediente clave para una Internet sostenible, global y en evolución. Sin confianza, los usuarios se sienten vulnerables y marginados y son reacios a aprovechar los múltiples beneficios legítimos que ofrece Internet. La razón principal que esgrimen quienes desconfían de Internet es que creen que no es segura".[11] Dicho esto, muchos usuarios de dispositivos conectados a la IoT pueden no darse cuenta de que están interactuando con Internet. Construir un ecosistema de la IoT seguro que reduzca los riesgos y proteja contra las amenazas y que a la vez permita realizar el gran potencial que la IoT ofrece a la sociedad es fundamental, urgente y debe ser una alta prioridad para todos los interesados.

Los desafíos que presenta la IoT hacen que un enfoque de seguridad colaborativa[12] sea ahora más importante que nunca. A medida que el ecosistema de la IoT crece, también crece la cantidad de dispositivos potencialmente vulnerables conectados. Estos dispositivos no tienen por qué ser vulnerables. Junto con los actores individuales que asumen responsabilidad en sus respectivos roles, juntos debemos tomar medidas para reducir la probabilidad de que se produzcan dispositivos vulnerables, al tiempo que debemos reducir el impacto de los dispositivos vulnerables cuando llegan a la red.

Es necesario que los formuladores de políticas tomen importantes decisiones para ayudar a dar forma al futuro de la seguridad de la IoT. Este trabajo está dirigido a reguladores, legisladores y cualquier persona interesada en el desarrollo y la implementación de instrumentos de política relacionados con la seguridad de la IoT.

8 https://www.internetsociety.org/policybriefs/botnets/
9 https://www.internetsociety.org/blog/2016/10/trust-isnt-easy-drawing-an-agenda-from-fridays-ddos-attack-and-the-internet-of-things/
10 https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/
11 https://www.cigionline.org/internet-survey
12 https://www.internetsociety.org/collaborativesecurity

Consideraciones clave

Hay varios factores que se deben considerar a la hora de abordar la seguridad de la IoT. Estos incluyen:

1. **La IoT es un área en evolución que está cambiando en forma rápida y orgánica.** Prácticamente todos los días se agregan nuevas capacidades y se descubren nuevas vulnerabilidades. Todavía están surgiendo mejores prácticas y estándares para la seguridad de la IoT y el tema está siendo abordado por numerosas organizaciones alrededor del mundo.[13]

El Marco de Confianza de la Internet de las Cosas de la iniciativa OTA (Online Trust Alliance) de la Internet Society es un conjunto integral de principios estratégicos para ayudar a asegurar los dispositivos conectados a la IoT y sus datos. Gracias al proceso colaborativo este Marco ofrece recomendaciones que creemos que todos los fabricantes de la IoT deben adoptar para mejorar la seguridad y aumentar la transparencia y la comunicación de la capacidad de los dispositivos para actualizarse, así como cuestiones relacionadas con la privacidad de los datos.[14]

2. **La IoT es más que los dispositivos. Los sistemas de la IoT están interconectados y son complejos.** Incluyen software, dispositivos, sensores, plataformas y la transmisión de datos a través de Internet, así como los servicios, que incluyen el análisis y el almacenamiento de datos en la nube (potencialmente por parte de terceros). Dado que todas las partes de un sistema de la IoT deben estar protegidas para brindar seguridad a sus usuarios y a los demás usuarios de Internet, es necesario adoptar un enfoque de seguridad continuo y en capas.

3. **La seguridad interna es diferente de la seguridad externa, pero ambas son igualmente importantes.** Un sistema de la IoT puede ser atacado, afectando la privacidad y la seguridad de su usuario (por ejemplo, dejando expuesta la transmisión de video 'privada' de un monitor de bebés, controlando sistemas hogareños 'inteligentes', haciendo que los electrodomésticos se comporten de forma no deseada (y potencialmente peligrosa), monitoreando cuando los propietarios están ausentes); este es un problema de 'seguridad interna'. Pero un sistema de la IoT comprometido también se puede utilizar para lanzar ataques contra terceros u otros sistemas (por ejemplo, electrodomésticos vulnerables infectados con 'malware' (software malicioso) y luego formar parte de una botnet utilizada en un ataque DDoS sobre redes, usuarios o infraestructura); este es un problema de 'seguridad externa'. Los sistemas de la IoT se deben asegurar considerando los riesgos para otras redes y usuarios (seguridad externa), y también los riesgos para sus propios usuarios y activos (seguridad interna).

13 https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/

14 The Online Trust Alliance (OTA) es una iniciativa de Internet Society. Lea también los documentos siguientes: Securing the Internet of Things y Internet of Things, a Vision for the Future.
https://otalliance.org/iot
https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf
https://otalliance.org/system/files/files/initiative/documents/iot_visionforthefuture_0.pdf

4. **La seguridad de la IoT es una preocupación global.** Internet es una red de redes interconectadas e interdependientes donde la seguridad de una red afecta la seguridad de cualquier otra. Los sistemas vulnerables de la IoT podrían verse comprometidos desde cualquier lugar y utilizarse para atacar a cualquier persona.

5. **La seguridad por diseño es fundamental.** La seguridad de la IoT es más eficaz cuando se incluye en el proceso de diseño desde su inicio y durante todo el proceso hasta la implementación y el soporte posventa. La seguridad no puede ser eficaz si se agrega a último momento.

6. **La seguridad es un proceso continuo.** Para mantener la seguridad, los sistemas de la IoT requieren mantenimiento. Hoy en día, esto es principalmente responsabilidad de los fabricantes y proveedores de servicios para la IoT. Las actualizaciones y parches oportunos, verificables y eficaces para abordar las vulnerabilidades son un aspecto crítico de la seguridad. Los ciclos de vida de los productos y servicios son un componente fundamental de la seguridad (por ejemplo, ¿por cuánto tiempo estarán disponibles el soporte y las actualizaciones? ¿qué sucederá después que terminen?). No es raro que los dispositivos permanezcan en servicio mucho después de su vida útil con soporte oficial.

7. **Es importante investigar e informar las vulnerabilidades.** Quienes investigan en el área de la seguridad desempeñan un papel importante dado que prueban la seguridad de los dispositivos y alertan a los fabricantes y proveedores de servicios sobre las vulnerabilidades descubiertas.

8. **Las plataformas son importantes jugadores en el mercado.** Las plataformas de la IoT (por ejemplo, Homekit[15] de Apple y Weave[16] de Google), algunas de las cuales tienen una penetración de mercado considerable y creciente, permiten controlar una gran cantidad de dispositivos usando un mismo protocolo e intercambian datos para tomar decisiones informadas. Las que instalamos en nuestros hogares 'inteligentes' para controlar nuestros sistemas de aire acondicionado, iluminación, sonido y seguridad utilizan diseños cohesivos para poder interoperar fácilmente con otros dispositivos compatibles y simplificar nuestra experiencia como usuarios, ocultando la complejidad y la escala de la automatización. Las características de las plataformas pueden tener un gran impacto en el mercado de la IoT.[17] Las plataformas con fuertes requisitos de seguridad impulsan a los fabricantes y proveedores que participan a mejorar la seguridad de sus dispositivos y servicios asociados. Sin embargo, las vulnerabilidades de la plataforma pueden afectar a todos los sistemas de IoT conectados. Además, las plataformas varían en sus prácticas de privacidad, y algunas son mejores que otras.

15 https://www.apple.com/ios/home/ ; https://developer.apple.com/homekit/

16 https://nest.com/weave/

17 https://www.internetsociety.org/blog/2017/09/can-iot-platforms-apple-google-samsung-make-home-automation-systems-secure/

Desafíos

Al abordar la seguridad de la IoT es necesario reconocer múltiples desafíos. Estos incluyen:

- **La economía no favorece la seguridad.** Las presiones competitivas por lograr tiempos de comercialización más cortos y productos más baratos llevan a muchos diseñadores y fabricantes de sistemas para la IoT, incluyendo los dispositivos, aplicaciones y servicios, a dedicar menos tiempo y recursos a la seguridad. Una buena seguridad puede ser costosa de diseñar e implementar y alarga el tiempo necesario para llevar un producto al mercado. El valor comercial de los datos de usuarios significa que existe un incentivo para acumular la mayor cantidad posible durante el mayor tiempo posible, lo que va en contra de las buenas prácticas de seguridad de datos. Además, en la actualidad son pocas las formas creíbles y conocidas que tienen los proveedores para indicar a los consumidores su nivel de seguridad (por ejemplo, certificaciones y marcas de confianza[18]). Esto hace que para los consumidores sea difícil comparar la seguridad de sistemas de la IoT que compiten entre sí, lo que a su vez hace que haya menor presión por parte de los consumidores por una seguridad robusta y hace que para los proveedores sea difícil utilizar la seguridad para diferenciarse de sus competidores. Por otra parte, el costo y el impacto de una seguridad deficiente tienden a recaer sobre los consumidores y otros usuarios de Internet, no en los productores del sistema de la IoT vulnerable. Por ejemplo, si sus tuberías se congelan cuando se apaga la calefacción, o si los servicios de Internet se ven afectados por un ataque en el que participan sus dispositivos comprometidos, los productores no sienten los efectos en forma directa.

- **La seguridad requiere experiencia específica.** Implementar una seguridad sólida en los sistemas de la IoT requiere experiencia. Quienes recién ingresan al ecosistema de la IoT pueden tener poca o ninguna experiencia previa con la seguridad en Internet. Por ejemplo, un fabricante puede saber cómo hacer que un refrigerador sea seguro para el uso principal previsto (cableado eléctrico, productos químicos), pero puede no comprender la seguridad en Internet. En particular, es posible que no comprenda el potencial impacto global que podría tener el compromiso de un sistema de un refrigerador 'inteligente'.

- **Los sistemas de la IoT son complejos y todas las partes deben ser seguras.** La seguridad de un sistema es apenas tan buena como la de su eslabón más débil. En los sistemas de la IoT, puede que diferentes componentes estén bajo el control de diferentes actores en diferentes jurisdicciones (por ejemplo, un servidor puede estar ubicado en un país, mientras que el dispositivo puede ser fabricado en otro y utilizado en un tercer país), lo que dificulta la resolución cooperativa de los problemas de seguridad y hace que los desafíos que implica la aplicación transfronteriza de la ley sean particularmente problemáticos. La complejidad de las cadenas de suministro significa que evaluar la seguridad es un desafío y requiere que los sistemas estén asegurados de manera holística, coordinando entre los diferentes actores y partes del sistema. Cada vez más, los sistemas de la IoT son gestionados y/o controlados por (o al menos interactúan fuertemente con) servicios en la 'nube' gestionados de forma remota y no de forma local. La falta de transparencia y control para el usuario final también puede ser particularmente problemática.

18 Una marca de confianza es un indicador visible de conformidad con un conjunto bien diseñado de requisitos de confianza, seguridad, privacidad y/o interoperabilidad.

- **Debe mantenerse el soporte de la seguridad.** Los dispositivos, aplicaciones y servicios relacionados con la IoT habitualmente requieren parches de seguridad y actualizaciones para protegerlos contra vulnerabilidades conocidas. En general, los consumidores no poseen la capacidad técnica –y en muchos casos tampoco las interfaces de usuario– para implementar parches de manera efectiva y segura. Para complicar aún más las cosas, cuando la opción sí está disponible, los usuarios pueden optar por no parchar sus dispositivos o simplemente no saben cómo hacerlo.[19] Además, en algunos casos los usuarios tienen prohibido por contrato actualizar o reparar los sistemas ellos mismos o hacerlos reparar por especialistas independientes, por ejemplo, la maquinaria agrícola.[20] A pesar de que proveer soporte para los sistemas de la IoT a largo plazo es una tarea costosa y requiere de muchos recursos por parte de los proveedores y desarrolladores de servicios para la IoT, muchas veces no se prioriza lo suficiente.

- **Los consumidores saben poco sobre la seguridad de la IoT.** En general, el conocimiento que tienen los consumidores sobre la seguridad de la IoT es limitado, lo que afecta su capacidad para incorporar la seguridad en sus hábitos de compra o para configurar y mantener la seguridad de sus sistemas de la IoT. Los grupos de consumidores suelen tener limitaciones presupuestarias, por lo que sensibilizar y educar a los consumidores son desafíos particularmente importantes.

- **Para los usuarios puede ser difícil detectar o abordar un incidente de seguridad.** En muchos casos, los efectos de un producto o servicio del sistema IoT poco seguro no serán evidentes para el usuario (por ejemplo, puede que un monitor de bebé siga funcionando correctamente como dispositivo de monitoreo de audio y video a distancia, a pesar de haber sido comprometido y formar parte de una botnet que realiza ataques DDoS o haber sido modificado para transmitir sonido e imágenes a terceros no autorizados).También es a veces difícil de detectar cuando los datos personales pasan fuera del sistema nube de IoT. Además, muchos dispositivos conectados a la IoT carecen por completo de una interfaz de usuario o tienen una muy limitada. En estos casos (como en el anterior), puede ser difícil o imposible para un usuario interactuar directamente con el dispositivo para confirmar o realizar actualizaciones, modificar la configuración, etc.

- **Los mecanismos de responsabilidad legal existentes pueden ser poco claros.** La responsabilidad por los daños causados por la falta de una seguridad adecuada en la IoT puede ser difícil de precisar. Esto genera incertidumbre entre las víctimas a la hora de asignar responsabilidades u obtener una compensación por los daños sufridos. Una responsabilidad clara puede ser un incentivo para una mayor seguridad. En ausencia de regímenes de responsabilidad sólidos, los usuarios son en última instancia quienes pagan el precio de las fallas de seguridad.

19 Ver Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching. NTIA, Departamento de Comercio de Estados Unidos https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

20 https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

Recomendaciones y principios rectores para los gobiernos sobre la seguridad de la IoT

Los gobiernos desempeñan un papel importante en la seguridad de la IoT. Al usar su enorme poder de mercado y cuidadosamente crear e implementar políticas y regulaciones, los gobiern[21]os pueden promover mejores resultados para la seguridad de la IoT. Los gobiernos tienen una serie de ventajas que, bien utilizadas, pueden empujar a la industria hacia una autorregulación eficaz con responsabilidades claras y un mayor intercambio de información entre los fabricantes de dispositivos para la IoT, minoristas, revendedores, integradores, proveedores de servicios y consumidores individuales. Una mayor transparencia beneficia a todas las partes interesadas.

Los siguientes son principios rectores y recomendaciones que los gobiernos deben considerar al abordar la seguridad de la IoT:

Fortalecer la responsabilidad

Principio: Fortalecer la responsabilidad por la seguridad y privacidad de la IoT, estableciendo responsabilidades y consecuencias bien definidas en caso de que la protección sea inadecuada.

Recomendaciones:

- **Garantizar la seguridad jurídica:** Proveer reglas claras, predecibles y exigibles que requieran que los proveedores, desarrolladores y fabricantes de productos y sistemas para la IoT incorporen protección frente a las vulnerabilidades conocidas garantizando la existencia de mecanismos de informe, respaldando sus productos con parches y actualizaciones de seguridad, y contando con políticas de actualización y parches de seguridad claramente definidas, incluyendo una fecha final a partir de la cual ya no se ofrecerá soporte. Especialmente en el mercado de la IoT para los consumidores, las protecciones de seguridad deben ser de exclusión voluntaria, no de inclusión voluntaria (*opt-out*, no *opt-in*).

- **Fortalecer la protección del consumidor:** Los datos personales recogidos o utilizados por la IoT, especialmente los datos obtenidos por los sensores, deben estar protegidos por leyes de privacidad y protección de datos. Los gobiernos pueden facilitar una mayor seguridad y privacidad al aclarar de qué manera las leyes de privacidad, protección de datos y protección del consumidor existentes se aplican a la IoT. De manera similar a la prohibición de las representaciones engañosas sobre la seguridad de los productos, también se debe prohibir a las empresas realizar representaciones engañosas o confusas sobre la seguridad de sus productos o servicios para la IoT. Los minoristas también deben compartir la responsabilidad y no vender productos para la IoT que tengan defectos de seguridad críticos conocidos.

- **Asignar claramente la responsabilidad:** Para acabar con la incertidumbre, los gobiernos deben asignar claramente la responsabilidad a quienes pueden ejercer un mayor control sobre la seguridad de un producto o servicio. Quienes fabrican e importan productos para la IoT deben ser responsables por los defectos de seguridad de sus productos.

Promover el uso de señales de seguridad

21 Los sistemas "no solo se refieren a los sistemas que el usuario instala, sino también a los sistemas remotos (o" back-end ") involucrados en la recopilación, almacenamiento y procesamiento de datos. Es posible que estos sistemas no estén bajo el control de los usuarios o incluso dentro de su jurisdicción.

Principio: Aumentar los incentivos para invertir en seguridad mediante el fomento de un mercado para la realización de evaluaciones independientes y confiables de la seguridad de la IoT.

Recomendaciones:

- **Fomentar esquemas de certificaciones de seguridad creíbles:** Una certificación permite que una organización visibilice que un producto, servicio o sistema, ha aprobado un conjunto de pruebas de calidad o desempeño y puede ser una señal poderosa y visible de cumplimiento que permita saber si un dispositivo para la IoT utiliza las mejores prácticas o estándares. También puede ser una herramienta eficaz para asignar y demostrar la responsabilidad. (Observar que el cumplimiento puede ser autoafirmado o validado en forma externa). Mejorar la calidad de las pruebas y los esfuerzos de certificación, considerándolos como parte de un proceso y no como una instantánea correspondiente a un determinado momento, y aumentar la visibilidad de las marcas de confianza asociadas hará que el mercado presione a los fabricantes para que mejoren la seguridad y colaborará para que una mejor seguridad sea un diferenciador entre competidores.

- **Comentarios y calificaciones:** Reconocer la función que desempeñan las calificaciones y los comentarios de los consumidores a la hora de destacar la privacidad y la seguridad (o su ausencia) en la IoT.

Fomentar una cultura de seguridad entre las partes interesadas de la IoT

Principio: Fomentar la seguridad como un componente de todas las etapas del ciclo de vida del producto, incluidos el diseño, la producción y la implementación. Fortalecer la capacidad de las partes interesadas para responder y mitigar las amenazas basadas en la IoT.

Recomendaciones:

- **Apoyar los análisis de riesgos de seguridad:** Promover el uso de técnicas de evaluación de riesgos de seguridad aceptadas por la industria antes de que los productos y servicios de la IoT lleguen al mercado. Alentar a los fabricantes y proveedores de productos y servicios para la IoT para que contraten expertos de seguridad independientes para llevar a cabo las evaluaciones. Donde sea posible, los gobiernos también pueden apoyar el desarrollo de herramientas y procesos para fortalecer los análisis de riesgos de seguridad (por ejemplo, financiando investigaciones). Pueden trabajar con las agencias de financiación del gobierno y la industria para promover investigaciones que estén disponibles para el público, incluyendo mecanismos de seguridad y de política.

- **Promover mejores prácticas y principios rectores:** Promover a nivel global el uso de mejores prácticas y principios rectores de seguridad que sean revisados con frecuencia y ampliamente aceptados para guiar el diseño, la implementación y el uso de los dispositivos y servicios de la IoT.[22] Incluir estos requisitos en las políticas de adquisición.

22 Por ejemplo, el Marco de Confianza de la Internet de las Cosas de la iniciativa OTA (Online Trust Alliance) de la Internet Society y el informe de políticas de la Internet Society sobre los invariantes de Internet.
https://otalliance.org/iot/
https://www.internetsociety.org/policybriefs/internetinvariants
Ver también "Recomendaciones básicas de seguridad para la IoT en el contexto de las infraestructuras críticas" de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

- **Fomentar una cultura de seguridad:** Fomentar una cultura de seguridad entre las partes interesadas clave, incluidos los proveedores de servicios de Internet (ISP), que se extienda más allá de sus propios intereses y alcance a Internet y a sus usuarios. Por ejemplo, es útil promover el intercambio de información, incluso sobre técnicas de mitigación de amenazas. Además, ofrecer soporte a los equipos de respuesta a incidentes de seguridad informática (CSIRT) y capacitación en ciberseguridad y recursos de referencia para quienes recién se incorporan al mercado de la IoT puede ser una medida muy eficaz.

- **Fortalecer las protecciones legales para quienes investigan en seguridad:** Asegurar que los investigadores que trabajan en el área de la seguridad no corran riesgos legales por investigar las vulnerabilidades.

Ofrecer fuertes incentivos para la adopción de mejores prácticas de seguridad

Principio: Los gobiernos pueden usar sus herramientas de políticas, recursos y poder de mercado para hacer que la seguridad sea un diferenciador competitivo.

Recomendaciones:

- **Mejorar las prácticas de adquisición para la IoT:** Desarrollar prácticas más sólidas para la adquisición de dispositivos, plataformas y servicios para la IoT que enfaticen el cumplimiento de las mejores prácticas de seguridad y privacidad. Cuando los gobiernos crean un mercado para las mejores prácticas en seguridad de la IoT, las empresas responden intentando satisfacer dicha demanda, por lo que la influencia llega tanto al mercado de la IoT pública como al de la IoT privada. Donde sea posible, exigir que los proveedores de productos y servicios para la IoT obtengan certificaciones de terceros o marcas de confianza como parte de las políticas de adquisición. Los gobiernos también deben usar herramientas aceptadas por la industria para probar la IoT en sus procesos de evaluación previos a la adquisición.

- **Apoyar la educación del consumidor:** Apoyar y participar en campañas de educación y sensibilización de los consumidores para así estimular la demanda de seguridad en la IoT. Cuando los consumidores comprenden que una mejor seguridad es un elemento diferenciador en el mercado, es posible justificar un precio más alto ante los potenciales compradores.

- **Promover un papel más importante para los grupos de consumidores:** Los grupos de consumidores pueden desempeñar un papel mayor en el desarrollo, la implementación, la educación del público y la evaluación de la seguridad de la IoT. (Actualmente, los grupos de consumidores están ausentes en gran parte de las discusiones relevantes, algo que contribuye fuertemente a la magnitud del problema). Reconocer que la falta de financiamiento suele ser una barrera para que los grupos de consumidores se involucren en las discusiones sobre políticas relevantes en materia de seguridad de la IoT.

- **Asociarse con el sector de seguros:** El sector de seguros puede priorizar mejores requisitos de privacidad y seguridad como una condición para suscribir una póliza. Al tomar en cuenta la seguridad de los dispositivos de la IoT y las aplicaciones y servicios relacionados que utilizan las empresas, las agencias de seguros pueden considerar el riesgo que presentan para determinar las primas y los precios de los seguros.

Fomentar soluciones independientes de la tecnología y del proveedor

Principio: Las soluciones de seguridad no deben basarse en estándares técnicos específicos ni en productos de un proveedor determinado, sino que deben basarse en los resultados deseados, como mayor seguridad, privacidad e interoperabilidad. Es probable que estos objetivos no cambien con demasiada frecuencia, pero los medios para lograrlos sí lo harán.

Recomendaciones:

- **Las políticas y requisitos de adquisición referidos a la seguridad de la IoT deben especificar resultados, no métodos:** Dado que la IoT es un área en rápida evolución, constantemente surgen nuevas amenazas y métodos y tecnologías de seguridad. Al especificar resultados en vez de tecnologías, los desarrolladores, fabricantes y proveedores de servicios para la IoT tienen libertad para innovar. Esto ayuda a garantizar que las políticas serán más 'a prueba de futuro' y que no será necesario cambiarlas significativamente con las nuevas tecnologías. Ejemplo de ello serían los requisitos de adquisición que especifican que los dispositivos, aplicaciones y servicios deben estar actualizadas y con marcados por el parche "aplicable". Deben incluir la habilitad de validar criptográficamente y comprobar una actualización o parche, y demostrar su eficacia, sin exigir una manera particular de hacerlo.

- **Fomentar la portabilidad de los datos:** El hecho de soportar estándares abiertos interoperables permite que los usuarios tengan más control sobre sus datos dado que es más fácil transferirlos a otros servicios. A los gobiernos les conviene no vincular sus datos o los datos de sus ciudadanos con soluciones propietarias específicas, también conocido como dependencia de un proveedor (*vendor lock-in*).

Utilizar cualquier política o herramienta regulatoria de forma inteligente

Principio: Dado que la seguridad es costosa y que para los usuarios puede ser difícil reconocer o valorar la seguridad, las políticas y las leyes pueden desempeñar un papel importante en la conformación de prácticas de seguridad en la industria de la IoT. Se pueden desarrollar políticas cuyo objetivo sea influir en el ecosistema de la IoT de manera de promover mejores prácticas de seguridad, antes que exigir soluciones técnicas específicas.

Recomendaciones:

- **Las políticas o regulaciones se deben desarrollar de manera transparente y deben priorizar los intereses de los usuarios:** Para fortalecer los resultados, el desarrollo de políticas y leyes debe beneficiar a todas las partes interesadas afectadas (incluidos, entre otros, los proveedores, fabricantes, usuarios y organizaciones de consumidores). Al representar sus intereses, las organizaciones de consumidores pueden desempeñar un papel muy importante en el desarrollo de políticas. Los responsables de la formulación de políticas deben asegurarse de que las leyes que se aplican a la IoT de consumo general prioricen los intereses de los usuarios. Además, al desarrollar políticas para la IoT es necesario considerar los efectos que tienen los sistemas de la IoT poco seguros sobre otros usuarios de la red, no solo sobre los usuarios directos.

- **Regular por sector industrial puede llevar a mejores resultados:** Los principios básicos como la protección de los datos se aplican en todos los sectores. Sin embargo, los sistemas de la IoT se desarrollan y utilizan en una amplia variedad de aplicaciones y sectores industriales; por lo tanto, una regulación con un enfoque sectorial que complemente a los

principios básicos puede permitir obtener resultados de seguridad más sólidos. En algunos sectores de la industria, puede que la existencia de fuertes incentivos de mercado o las regulaciones existentes hagan que una nueva regulación sea menos necesaria que en otros. Por ejemplo, es posible que las herramientas regulatorias que son apropiadas para el sector de la salud no resulten tan útiles en el sector de los dispositivos de consumo, donde atributos como la tolerancia a las fallas pueden no ser tan fundamentales para desarrollar un producto seguro.

La Internet de las Cosas se dispone a transformar las economías y sociedades alrededor del mundo. La tecnología trae enormes oportunidades, pero también enormes riesgos. Estamos en un momento crítico en el que debemos tomar medidas para garantizar que los beneficios de la IoT superen a los riesgos de seguridad. Muchas organizaciones están trabajando arduamente en estos temas, pero es necesario que todas las partes interesadas, incluidos los formuladores de políticas, los fabricantes y los consumidores, tomen buenas decisiones sobre el futuro de la IoT y la seguridad.