Seguridad en IoT Proceso en Uruguay

Setiembre 2019

Internet Society
Capítulo Uruguay

Uruguay
Digital

PRESIDENCIA
República Oriental del Uruguay

CONTENIDO

INTRODUCCIÓN

La naturaleza abierta de Internet crea la habilidad de conectar diversos dispositivos, sistemas, aplicaciones y servicios a una escala que transforma la manera en que interactuamos con el ambiente y nuestra sociedad. Internet de las cosas (IoT) tiene un enorme potencial para mejorar el mundo. Las proyecciones del impacto de IoT en Internet y en la economía mundial son impresionantes, estimándose que en 2020 habrá 38.5 mil millones de dispositivos de este tipo que pueden ser usados para una gran variedad de actividades.

Definición de Internet de las cosas (IoT)

Según la Unión Internacional de Telecomunicaciones (UIT), desde una perspectiva amplia IoT puede considerarse una noción con repercusiones tecnológicas y sociales. Puede ser vista como una infraestructura global al servicio de la Sociedad de la Información, que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas, gracias a la interoperabilidad de Tecnologías de la Información y la Comunicación presentes y futuras. Además, gracias a la identificación, la adquisición y el procesamiento de datos, así como a las capacidades de comunicación, IoT hace uso de las cosas para ofrecer servicios a todo tipo de aplicaciones, garantizando, a su vez, el cumplimiento íntegro de los requisitos de seguridad y privacidad.

Tipos de sistemas y/o dispositivos de IoT

La variedad y la complejidad de los sistemas y/o dispositivos de IoT es muy amplia. A los efectos de diferenciar los posibles usos que ofrece, se entiende que se pueden agrupar en cuatro tipos, teniendo en cuenta las características específicas y los desafíos de seguridad.

TABLA 1: TIPOS DE SISTEMAS Y/O DISPOSITIVOS Y PRINCIPALES DESAFÍOS QUE SE IDENTIFICAN.

Tipos de sistemas y/o dispositivo	Principales desafíos de seguridad
Solo emiten datos capturados por sensores.	Debe ser posible autenticarlos y conocer la precisión de sus medidas (por ejemplo, sensor de temperatura de heladeras de medicamentos); no reciben comandos, solo reportan medidas.
Solo reciben comandos sin enviar información.	Impedir la comunicación saliente en tanto puede ser una válvula de pase de líquido (dispositivo electromecánico que se abre o cierra, llamado también "válvula solenoide") que, de hecho, no debería enviar información en condiciones normales, pudiendo ser usada maliciosamente como punto de ingreso para un ataque.

Tipos de sistemas y/o dispositivo	Principales desafíos de seguridad
Envían parámetros medidos y reciben comandos.	Incluye los dos casos y desafíos anteriores. Por ejemplo: un regulador activo de temperatura de un proceso que mide un parámetro que se está controlando o el control inteligente de temperatura de salas de cómputo de data centers.
Inteligentes autónomos.	Sistemas y/o dispositivos que, por ejemplo, miden, actúan y se comunican autónomamente con otros sistemas y/o dispositivos. Además, según las reglas de contrato de esa red autónoma, en conjunto afectan un proceso sin necesidad de una aplicación que los controle. Por ejemplo, sensores en vehículos autónomos que interactúan con otros vehículos y toman decisiones sobre el vehículo sin intervención o gestión humana.

Cada uno de los tipos de sistemas y/o dispositivos, identificados en la **Tabla 1**, representa desafíos crecientes; por ejemplo, precisión de las medidas, efecto sobre procesos y diversos riesgos para las personas.

En este sentido, para trabajar en la prevención y en el tratamiento de las vulnerabilidades, cada caso particular requiere medidas concretas en base a los potenciales riesgo que cada uno conlleva.

Actores involucrados

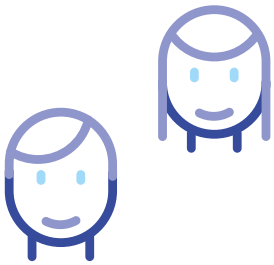
Es necesario considerar a todos los sujetos comprendidos para poder desarrollar mecanismos de seguridad en todas las etapas. A título enunciativo, se destacan los siguientes actores: fabricantes de sistemas y/o dispositivos, proveedores de sistemas y/o dispositivos, desarrolladores de sistemas y/o dispositivos, vendedores de sistemas y/o dispositivos, canales de distribución, consumidores individuales y usuarios corporativos, legisladores y hacedores de políticas, organizaciones que proporcionan plataformas de prueba, desarrolladores de estándares y de reseñas de sistemas y/o dispositivos, comunidad técnica, sociedad civil e instituciones académicas.

Consumidor de IoT

El consumidor de los sistemas y/o dispositivos de IoT puede ser cualquier persona que los utilice, incluidas las empresas de cualquier tamaño, tanto para su vida personal o consumo propio, como para su vida profesional y/o para prestar otros servicios asociados a sistemas y/o productos. Por ejemplo, los televisores inteligentes se implementan con frecuencia en salas de reuniones, así como para uso doméstico. De la misma forma, los kits de seguridad pueden ser para uso doméstico o para proteger las instalaciones de pequeñas empresas.

También son consumidores de sistemas y/o dispositivos de IoT objetos conectados a la red y sus servicios asociados. Generalmente, están disponibles para que el consumidor los compre en el comercio minorista y se usan en el hogar o como dispositivos electrónicos portátiles.

Vale destacar que el "consumidor de IoT" no siempre es consciente de su uso, lo que puede inducirlo a asumir riesgos no conocidos, como por ejemplo, aquellos vinculados a la privacidad. En este sentido, a los efectos del presente documento, se atiende especialmente a las personas que utilizan conscientemente los sistemas y/o dispositivos de IoT.



Sectores de actividad

Hay múltiples sectores de actividad en los cuales los sistemas y/o dispositivos de IoT se diseñan, crean, desarrollan y se ponen en el mercado para hacer más eficientes los procesos de automatización en general y las actividades diarias. Entre los diversos sectores se destacan: el uso privado o doméstico, el transporte, la medicina, la agricultura, la construcción, la energía, las finanzas, la banca, las redes de telecomunicaciones y el sector público.

Importancia de trabajar en la seguridad de IoT

IoT brinda un sinfín de oportunidades para las personas y las empresas. Sin embargo, con miles de millones de sistemas y/o dispositivos de IoT en uso, número que crece continuamente, trabajar en su seguridad es cada vez más crítico porque sistemas y/o dispositivos poco seguros pueden servir como puertas de entrada para ciberataques, afectar la confianza y generar daños. Entender el impacto creciente que la seguridad tiene en Internet, en los propios dispositivos y en los diversos tipos de consumidores es necesario para proteger el futuro de IoT.

En este sentido, el objetivo del presente documento es generar recomendaciones que contribuyan a que los sistemas y/o dispositivos de IoT sean seguros desde el diseño, por defecto, y que faciliten que las personas estén más informadas y seguras en el mundo digital.

Punto de partida

Para la generación del presente documento se realizó un proceso a nivel país. Participaron más de 60 personas en reuniones presenciales y trabajo colaborativo en línea, de los más diversos sectores de actividad , para lograr recoger los aportes de todos los actores interesados **(Anexo I)**.

Se partió de las siguientes premisas:

Que las personas deben ser el centro de todas las posibles soluciones.

Que la responsabilidad debe ser compartida y de todos los involucrados.

Que la protección de la privacidad y de los datos personales debe ser considerada desde el diseño y por defecto.

Que se deben adoptar prácticas de privacidad responsables con un enfoque inclusivo y colaborativo, buscando soluciones duraderas, eficientes, flexibles y con revisión periódica.

Que se deben desarrollar campañas de sensibilización destinadas a públicos específicos y atendiendo a las personas o grupos de personas más vulnerables.

Que hay una complejidad inherente y creciente al analizar los diversos escenarios en que se aplica la seguridad de los sistemas y/o dispositivos de IoT. Para cada escenario será necesario una evaluación más profunda de los riesgos y beneficios.

Que en la medida en que el funcionamiento de esta tecnología se da a escala internacional, con actores que trascienden las fronteras nacionales, se considera de buena práctica y deseable, la coordinación de acciones locales con iniciativas regionales y globales.

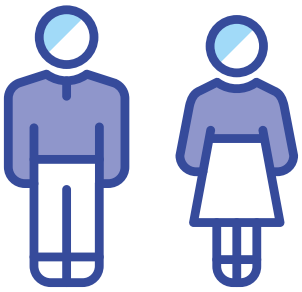
Que hay múltiples desafíos sobre los cuales se debe trabajar, siendo fundamental buscar soluciones y cooperación global para que la seguridad de la red y de los consumidores sea realmente efectiva.

Que es necesario enfocarse en todo el ciclo de vida de los sistemas y/o dispositivos.

Que los nuevos actores involucrados en el ecosistema de IoT pueden tener poca o ninguna experiencia previa en Seguridad de la Información y en Internet, lo que demanda su necesaria interacción con especialistas y una capacitación o sensibilización mínima.

Que es fundamental promover una cultura de cooperación entre los diversos actores involucrados, compartiendo información, incluyendo aquella relativa a técnicas de mitigación de riesgos e incidentes con autoridades nacionales. Todos los actores de la cadena tienen un rol muy importante en la seguridad de los sistemas y/o dispositivos de IoT, siendo esencial su participación para lograr condiciones razonables y proporcionales, coordinar esfuerzos, acordar estándares comunes y alcanzar mejores resultados.

Que es fundamental promover una cultura de cooperación entre los diversos actores involucrados, compartiendo información, incluyendo aquella relativa a técnicas de mitigación de riesgos e incidentes con autoridades nacionales. Todos los actores de la cadena tienen un rol muy importante en la seguridad de los sistemas y/o dispositivos de IoT, siendo esencial su participación para lograr condiciones razonables y proporcionales, coordinar esfuerzos, acordar estándares comunes y alcanzar mejores resultados.



CONSIDERACIONES GENERALES

IoT comprende un área que cambia rápidamente, en tanto nuevas habilidades y nuevos problemas de seguridad son descubiertos constantemente. Las mejores prácticas y estándares para la seguridad de los sistemas y/o dispositivos de IoT aún son emergentes y están siendo analizados por diversas organizaciones a nivel mundial.

IoT son sistemas y/o dispositivos interconectados, incluyendo software y hardware, como sensores y plataformas. Prestan servicios de muy diferente índole. Todas las partes deben estar protegidas, requiriéndose un enfoque de seguridad en capas.

Hay que atender la seguridad interna y externa. Los sistemas y/o dispositivos de IoT pueden ser atacados, afectando la privacidad y la seguridad del propio consumidor, pero también pueden afectar a terceros, así como a otros sistemas y/o dispositivos.

La seguridad de los sistemas y/o dispositivos de IoT es una preocupación global y la seguridad de uno impacta en la de todos.

La seguridad desde el diseño y de forma continua es esencial, siendo más efectiva cuando es incluida en el proceso desde el inicio y durante todo el ciclo de vida del sistema y/o dispositivo.

Los parches y actualizaciones oportunos, verificables y efectivos son un factor crítico para abordar las vulnerabilidades de seguridad en todo el ciclo de vida de los sistemas y/o dispositivos.

Es primordial investigar, informar y comunicar las vulnerabilidades. Los investigadores tienen un rol muy importante para testear la seguridad y alertar sobre las debilidades que se descubren.

Los sistemas y/o dispositivos varían en sus prácticas de privacidad; algunas son más recomendables que otras, siendo clave adoptar medidas de seguridad en todas las capas.

Se debe procurar identificar los diversos retos que se presentan a fin de trabajar en su mitigación.

DESAFÍOS

La economía favorece la seguridad débil. Presiones competitivas por tiempos más cortos para que salgan los sistemas y/o dispositivos al mercado, así como disminuir costos, derivan en que se dediquen menos recursos a su seguridad. Además, el valor comercial de los datos es un incentivo para su acumulación, lo que va en contra de las buenas prácticas, así como de la protección de la privacidad y de los datos personales.

En la actualidad, se dispone de pocos mecanismos para señalizar y comparar el nivel de seguridad de los sistemas y/o dispositivos (por ejemplo, a través de calificaciones), en tanto no existen estándares internacionalmente aceptados para el etiquetado de los niveles de seguridad.

Los sistemas y/o dispositivos de IoT son complejos y cada parte debe ser segura. Los diferentes componentes pueden estar bajo el control de diversos actores y en distintas jurisdicciones, haciendo difícil una solución única y coordinada.

Se debe mantener el soporte de seguridad. Los dispositivos y/o sistemas requieren actualizaciones de seguridad para estar protegidos contra vulnerabilidades.

El conocimiento que el consumidor tiene sobre la seguridad de los sistemas y/o dispositivos de IoT suele ser bajo, lo cual afecta su capacidad para tener en cuenta la seguridad en sus hábitos de compra o para configurar y mantener la seguridad de sus sistemas y/o dispositivos.

Los incidentes de seguridad pueden ser difíciles de detectar o de abordar por los consumidores. En muchos casos, los efectos no son evidentes.

Los mecanismos de responsabilidad legal existentes son poco claros o no se encuentran adaptados a las necesidades que IoT demanda. Si no se trabaja en ello, los consumidores finales serán quienes, en última instancia, terminen siendo los más perjudicados.

Todos los actores tienen un rol muy importante en la seguridad de IoT.

VÍAS DE ACCIÓN

Hay múltiples desafíos sobre los cuales se debe trabajar, siendo fundamental buscar soluciones y cooperación global para que la seguridad de los consumidores y de las redes sea realmente efectiva.

En este sentido, como vías principales de acción se propone trabajar sobre la protección del consumidor y la resiliencia en la red.

Protección al consumidor

Generar confianza y reglas claras en el ecosistema de IoT facilita el desarrollo y la innovación, produce beneficios y claridad, impulsando la universalización y la masificación de los sistemas y/o dispositivos de IoT en un contexto seguro.

Principales objetivos

Se identificó como deseable que los consumidores:

- Sepan cómo adquirir con conocimiento un sistema y/o dispositivo de IoT, por ejemplo: que atiendan las opiniones de otros consumidores, que consideren los términos y condiciones, que puedan recibir y disponer de actualizaciones que resuelvan posibles vulnerabilidades y que evalúen si es necesaria la conexión a Internet, así como conocer si se recolectan datos y el tratamiento que se les da.
- Puedan identificar fácilmente el nivel de seguridad de los sistemas y/o dispositivos, ateniendo determinados estándares.
- ctualicen los sistemas y/o dispositivos.
- Tomen medidas para atender su privacidad y proteger su información, como puede ser a través de la activación del cifrado o de la encriptación de la información, si el sistema y/o dispositivo tiene esa capacidad.
- Utilicen métodos de autenticación robustos, como puede ser: la no reutilización de contraseñas, la utilización de contraseñas seguras, y su debida administración.
- Conozcan los riesgos asociados a sus sistemas y/o dispositivos y logren implementar las medidas necesarias para mitigarlos.

En este sentido, a fin de proteger a los consumidores, conforme se desarrolla en la **Tabla 2,** se señalan determinados aspectos claves sobre los cuales sería deseable trabajar.

TABLA 2: POSIBLES ACCIONES SOBRE LAS CUALES SERÍA DESEABLE TRABAJAR PARA PROTEGER A LOS CONSUMIDORES DE LOS SISTEMAS Y/O DISPOSITIVOS DE IOT.

Aspectos a trabajar	Objetivos que se buscan en relación a los consumidores de los sistemas y/o dispositivos de IoT	Posibles vías de acción por parte del fabricante, del vendedor, del gobierno, de la sociedad civil, de la comunidad técnica o de instituciones educativas
Educación y sensibilización del consumidor.	Desarrollo de capacidades y sensibilización específica sobre la materia. Conocimiento de la importacia de atender determinados aspec-tos para poder evaluar la seguridad en sus sistemas y/o dispositivos de IoT.	Trabajar en todos los niveles educati-vos, involucrando a toda la sociedad y teniendo especialmente en cuenta a los grupos más vulnerables. Sería desea-ble diseñar y desarrollar cursos abier-tos masivos online (MOOC, por sus siglas en inglés) para los distintos grupos objetivos. Concientizar al consumidor sobre la importancia de atender la seguridad de sus sistemas y/o dispositivos de IoT durante todo el ciclo de vida. Realizar campañas informativas por diversos medios puede contribuir a generar con-ciencia, así como a impulsar a los usuarios a reportar los problemas po-tenciales de seguridad (Ver sección siguiente y Tabla 3)
Riesgos.	Capacidad de identificar y conocer los riesgos actuales y/o potenciales.	Explicar las bondades y los potenciales riesgos de los sistemas y/o dispositi-vos de IoT.
Guía de buenas prácticas.	Guía de buenas prácticas. Comprensión de las buenas prácticas de seguridad.	Facilitar información clara y sencilla sobre aspectos a atender por parte de los consumidores a fin de protegerlos adecuadamente.
Gestión de actualizaciones y parches.	Conocer las medidas que se deben adoptar para que el sistema y/o dispositivo se actualice correctamente y a tiempo.	Divulgar si el sistema y/o dispositivo es capaz de recibir actualizaciones, si las puede recibir automáticamente y qué medidas debe tomar el usuario para que se hagan efectivas. Facilitar información sobre la criticidad y sobre el tipo de problemas que solucionan.
Política de privacidad de los datos.	Comprensible y de fácil acceso.	Dar claridad sobre la política de privacidad y de seguridad, así como facilitar el acceso y la disponibilidad.
Seguridad desde el diseño y por defecto.	Capacidad de utilizar-los con confianza. Control de acceso ro-busto, uso de protoco-los de seguridad para las comunicaciones y posibilidad de bloquear puertos.	Promover la seguridad desde el diseño, estableciendo actualizaciones por de-fecto, así como reglas claras de actua-lización. Proteger el acceso a los sistemas y/o dispositivos de los usuarios. Buscar que el consumidor utilice métodos de autenticación robustos, como pueden ser la no reutilización de contraseñas, la utilización de contraseñas seguras y su debida administración. Proteger las comunicaciones. Todas las comunicaciones deberían realizarse utilizando protocolos seguros, siendo establecidos por defecto. Proteger los puertos de acceso. El dispositivo debería configurarse por defecto, de manera intuitiva y simple, utilizando puertos determinados y seguros para su funcionamiento habitual.

Aspectos a trabajar	Objetivos que se buscan en relación a los consumidores de los sistemas y/o dispositivos de IoT	Posibles vías de acción por parte del fabricante, del vendedor, del gobierno, de la sociedad civil, de la comunidad técnica o de instituciones educativas
Protección de los datos de los consumidores.	Protección de los datos en toda la cadena y en todas las capas.	Informar claramente si se almacenan datos personales, qué datos se alma-cenan, dónde se guardan, con qué fin, cómo se protegen, quién tiene acceso, cómo es el tratamiento, cómo puede el titular ejercer sus derechos, cuál es el tiempo de retención y de almacena-miento de los datos y cuándo dejarían de estar disponibles.
Minimización de datos.	Limitar la obtención de datos por parte de los sistemas y/o dispositi-vos a aquellos que sean necesarios para su funcionamiento.	Cuando los sistemas y/o dispositivos así lo permitan, se debería atender que solo utilicen los datos que sean nece-sarios para su funcionamiento. Es importante informar debidamente y obtener las autorizaciones que correspondan. En caso de requerir permisos adicionales para funciones extras, el con-sumidor debe poder consentir la nueva funcionalidad.
Asistencia al consumidor.	Acceder a sitios donde consultar y donde se atiendan los inconvenientes que puedan surgir.	Promover sitios, ya sean web (por ejemplo: chatbots, FAQ, foros, Wikis.) o físicos donde el consumidor pueda realizar reclamos, obtener información (por ejemplo: guías de buenas prácticas, políticas de privacidad, política de recolección y almacenamiento de los datos, políticas de seguridad, configuraciones, etc.), así como consultar sobre los sistemas y/o dispositivos IoT que adquirieron o vayan a adquirir.
Prevención al consumidor.	Mitigar amenazas que se detecten.	Sugerir, recomendar y prevenir al con-sumidor sobre los niveles de seguridad o de reputación de diversos sistemas y/o dispositivos de IoT.
Términos y condiciones.	Comprensibles y de fácil acceso.	Atender la claridad, la precisión, que sean fáciles de comprender y que es-tén accesibles.
Conexión de los sistemas y/o dispositivos IoT a Internet.	Comprender si es o no necesario que el sis-tema y/o dispositivo esté conectado continuamente a la red.	Informar si es o no necesario que el sistema esté conectado continuamente a la red. En caso de que no sea nece-sario, indicar claramente cómo se pue-de desconectar, en qué momentos se conecta y con qué finalidad.
Responsabilidad.	onocer la responsabilidad específica de cada uno de los actores de la cadena.	Asignar las responsabilidades específi-cas en los diversos actores de la cadena, para trabajar sobre la incertidumbre e impulsar que se atiendan más los defectos de seguridad.
Sistema de calificación.	Poder identificar fácilmente, por parte del consumidor, el grado de seguridad del sistema y/o dispositivo de IoT	Fomentar esquemas de calificación de seguridad creíbles y simples de com-prender, que faciliten identificar si un producto y/o servicio posee o no cier-tas medidas de seguridad deseables o recomendables. Asimismo, que reflejen las mejores prácticas y estándares y que posibiliten a los consumidores rea-lizar decisiones informadas a la hora de adquirir este tipo de sistemas y/o dispositivos.

Educación y sensibilización de los consumidores

Se parte de la base de que la gran mayoría de los consumidores no tiene conocimientos técnicos como para evaluar el nivel de seguridad en los sistemas y/o dispositivos de IoT.

En este sentido, para ayudarlos a comprender la importancia de atender la seguridad de los sistemas y/o dispositivos de IoT durante todo el ciclo de vida, se identifican tres momentos en el vínculo entre el consumidor y el dispositivo y/o sistema de IoT:

- "Antes" de que el consumidor seleccione el sistema y/o dispositivo de IoT.
- "Durante" el uso del dispositivo.
- La "disposición final".

Sería deseable atender diferentes aspectos en cada uno de esos momentos, conforme se señala en la **Tabla 3.**

TABLA 3: CICLO DE VIDA DE LOS SISTEMAS Y/O DISPOSITIVOS DE IOT, CONSIDERACIONES Y POSIBLES ACCIONES QUE SERÍA DESEABLE IMPULSAR.

Etapa	Consideraciones que sería deseable que el consumidor atendiera.	Posibles acciones que sería deseable impulsar por parte de los fabricantes /vendedores.
Antes de que se seleccionen los sistemas y/o dispositivos de IoT.	Considerar si disponen de facilidades para realizar consultas y recibir respuestas claras por parte de los fabricantes y/o vendedores.	Promover que sea aclarado en los términos y condiciones.
	Entender y consentir sobre la for-ma como los sistemas y/o disposi-tivos recolectan, almacenan, usan y comparten la información.	Trabajar en mejorar la accesi-bilidad y el contenido de las políticas de privacidad, y que se proporcionen respuestas claras.
	Conocer si los sistemas y/o dispositivos recogen datos innecesarios para su funcionamiento.	Indicar las funcionalidades de los servicios y/o dispositivos y cómo minimizarlas.
	Buscar si los sistemas y/o dispositivos son acreditados.	Trabajar en definir las responsabilidades.
	Revisar las reseñas de los consumidores, las etiquetas y las calificaciones; por ejemplo, si se indica que el dispositivo cumple con determinadas acreditaciones.	Utilizar acreditaciones que in-diquen que es adecuado a los estándares y mejores prácticas.
	Considerar el ciclo de vida de los sistemas y/o dispositivos de IoT y la posibilidad de mantenerlos en uso el mayor tiempo posible. Por ejemplo: verificar la disponibilidad y la duración de las actualizaciones de seguridad.	Informar sobre la duración de las actualizaciones y de los soportes.
	Chequear si los sistemas y/o dis-positivos funcionan incluso sin co-nexión a Internet, así como las funcionalidades en caso de que no haya conexión.	Atender las indicaciones técni-cas, siendo esencial que las mismas sean claras y de fácil entendimiento.
	Saber a dónde se puede recurrir para resolver los diversos proble-mas técnicos que puedan ocurrir, siendo importante mantener el comprobante de la compra.	nformar sobre las diversas formas de atención que se dispone.

Etapa	Consideraciones que sería deseable que el consumidor atendiera.	Posibles acciones que sería deseable impulsar por parte de los fabricantes /vendedores.
Durante el uso de los sistemas y/o dispositivos de IoT.	Atender y seguir las guías de buenas prácticas. Por ejemplo: guías para la configuración de la red para ayudar a mitigar el riesgo.	Promover la realización de guías de buenas prácticas, así como el desarrollo de configuraciones por defecto que sean seguras.
	Conocer dónde llevar los sistemas y/o dispositivos para reparación o resolución de problemas técnicos.	Proveer información clara y accesible de los lugares o sitios destinados a la resolución de problemas.
	Si existe la posibilidad de realizar actualizaciones durante todo el ciclo de vida.	Facilitar la gestión de las vul-nerabilidades y las correcciones por parte de los consumidores. Minimizar la posibilidad de dejar desactualizados los sistemas y/o dispositivos.
	Tener en cuenta que la seguridad de los sistemas y/o dispositivos se actualiza constantemente, por lo que hay que asegurar que se puedan recibir.	Incluir guías con recomendaciones para las configuraciones e indicar si es necesario implementar sistemas de monitoreo.
	Verificar que los sistemas y/o dispositivos en los hogares estén seguros.	Proporcionar mecanismos a los consumidores para advertirles cuando surjan problemas.
Al finalizar el uso de los sistemas y/o dispositivos de IoT.	Eliminar la información antes de desecharlos.	Recomendar guías que ayu-den a los consumidores para saber claramente la mejor forma de hacerlo o brindar asistencia para eliminar per-manentemente los datos al-macenados.
	Revertir la configuración a la predeterminada de fábrica, así como procurar la forma de disponer adecuadamente del desecho tecnológico.	Proporcionar información, re-cursos y ayudar a los consumidores a desechar sus dis-positivos de manera responsable.

Se considera que sería una buena práctica unir esfuerzos y centralizar la información a través de servicios a la ciudadanía. De esta forma, se podría facilitar un listado de sistemas y/o dispositivos de IoT y disponer de un sitio donde reportar incidentes, coordinando la colaboración de los Equipos de Respuesta ante Emergencias Informáticas (CERT , por sus siglas en inglés) o Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT , por sus siglas en inglés). De esta manera, se puede llegar rápidamente a centros especializados y tomar medidas adecuadas a tiempo. Asimismo, sería deseable generar CSIRT colaborativos, específicos para seguridad en IoT, donde participen actores de diversos sectores de actividad.

Resiliencia de la red

Los sistemas y/o dispositivos de IoT crecen constantemente a gran velocidad, lo cual los hace más atractivos para ser objeto de ciberataques o constituir un medio para su ejecución.

Estos sistemas y/o dispositivos pueden tener presencia en diversos ámbitos de actividad, requiriendo atenciones y medidas específicas, dependiendo del grado de experiencia de quienes los administran, así como de los potenciales riesgos.

En este sentido, es importante proteger la infraestructura de redes ante nuevas y potenciales amenazas, dado que los sistemas y/o dispositivos pueden afectar: (i) a los consumidores, si vulneran la privacidad, la seguridad e incluso si se interfiere en su uso; (ii) a otros dispositivos que estén conectados a la red; (iii) a la propia red, si se afecta la confianza y se desestimula el uso; y (iv) a la estabilidad, seguridad y resiliencia de las redes en general.

Los sistemas y/o dispositivos más expuestos son aquellos que están continuamente conectados a Internet; además, las personas no suelen tener los conocimientos técnicos necesarios como para saber cómo protegerlos debidamente, generando una eventual puerta de ataque que puede derivar en la vulneración de otros sistemas y/o dispositivos.

Principales objetivos

Considerando los potenciales riesgos, sería deseable:

- Identificar las amenazas y vulnerabilidades que pueden estar asociadas a los sistemas y/o dispositivos de IoT.
- Buscar formas de mitigar los diversos riesgos que se vayan identificando.
- Informar y comunicar, adaptando el mensaje al público objetivo.
- No utilizar contraseñas universales por defecto; buscar que sea obligatoria su modificación inicial y que sean seguras.
- Reportar las vulnerabilidades que se detecten, promoviendo puntos de contacto donde se pueda informar, así como la realización de auditorías y el seguimiento de los eventos de seguridad.
- Compartir el conocimiento y promover la comunicación de los hallazgos.
- Actuar a tiempo y en coordinación, en tanto contribuye a disminuir las vulnerabilidades.
- Mantener el software actualizado.
- Almacenar las credenciales de acceso y la información debidamente.
- Activar la encriptación de la información y/o de los sistemas, siempre que sea posible.
- Diseñar e implementar mecanismos de prueba de los niveles de seguridad y protección, minimizando la exposición a ataques.
- Diseñar los sistemas resilientes a fallas de la red.
- Atender la información que se recolecta y limitarla a lo estrictamente necesario.
- Facilitar la eliminación de los datos, la actualización de los sistemas y el mantenimiento de los sistemas y/o dispositivos.
- Configurar o activar reglas de detección de anomalías y que notifiquen al administrador y/o al usuario y/o al fabricante, cuando sea posible.
- Recomendar a los fabricantes que adopten determinadas medidas o controles de seguridad para acreditar la seguridad del dispositivo.
- Poder validar la correcta y segura configuración de los sistemas y/o dispositivos.
- Permitir almacenar los eventos de seguridad en repositorios externos y evitar pérdida de eventos.
- Colaboración mundial, en tanto la digitalización y la seguridad de las redes concierne y puede afectar a todos, siendo fundamental alcanzar estándares globales que faciliten la interoperabilidad técnica y la coherencia regulatoria, otorgando reglas claras, previsibilidad y transparencia.

Campañas de sensibilización

Se reconoce la importancia de realizar campañas de sensibilización dirigidas a los usuarios sobre los posibles riesgos. Se proponen tres abordajes:

- Aumentar los mecanismos de control de infraestructura que colaboren en la mitigación de posibles ataques que pongan en riesgo la disponibilidad, integridad y/o confidencialidad de los sistemas y/o dispositivos.
- Mejorar el diseño y la gestión del ciclo de vida de los sistemas y/o dispositivos de IoT, fomentando estándares, conocimiento, medidas de concientización y guías de buenas prácticas.
- Adoptar medidas relacionadas con la gestión de las redes, como por ejemplo, ayudar a proteger a los sistemas y/o dispositivos para evitar que sean atacados.

En vista de lo anterior, como se desarrolla en la **Tabla 4**, es deseable identificar potenciales riesgos a fin de buscar posibles vías de mitigación, teniendo en cuenta que la seguridad debe ser vigilada de extremo a extremo.

TABLA 4: RIESGOS POTENCIALES Y POSIBLES VÍAS DE MITIGACIÓN.

Riesgos poten-ciales de los servicios y/o dispositivos de IoT	Posibles vías de mitigación
Dispositivos inteligentes instalados para usuarios con escaso conocimiento técnico.	Teniendo en cuenta que los usuarios en general no poseen conocimientos técnicos, es importante trabajar en la seguridad desde el diseño. Por ejemplo, exigir contraseñas seguras por defecto, garantizar el uso de interfaces de programación y de configuración seguras, solicitar determinadas funcionalidades básicas y disponer de una clasificación para facilitar la identificación.
Redes en ámbitos sin una política de seguridad eficiente.	Es importante controlar y limitar el acceso. Por ejemplo, faci-litar la utilización de redes privadas, procurando que sean servicios que puedan ser brindados por proveedores que transmitan las ventajas de este tipo de redes, educando al consumidor.
La puerta de entrada puede que afecte la seguridad.	Es necesario establecer niveles de seguridad en aquellos sistemas que antes eran considerados no críticos, como pueden ser gateways residenciales, ya que pueden ser utilizados como puerta de entrada para ganar acceso a otros sistemas y/o dispositivos. Asimismo, es necesario generar medidas de seguridad más estrictas con mecanismos y sistemas capaces de repeler ataques. Los dispositivos podrían estar identificados con sellos que, por ejemplo, garanticen el cumplimiento de recomendaciones de seguridad y de estándares internacionales.
Ciberataques y el rol del proveedor de servicios.	Intentar detectar y denunciar ataques ya realzados, como puede ser el robo de identidad, así como procurar bloquear aquellos ataques que estén en progreso. Se recomienda tra-bajar en una guía de buenas prácticas de configuración de red y de cómo actuar ante ciberataques.
Condiciones de uso sin ser explicadas al usuario.	Reforzar los controles de acceso, por ejemplo utilizando es-tándares internacionales.

Considerando los riesgos, se identifican como buenas prácticas:

- Atender la seguridad desde el diseño y por defecto.
- Controlar, limitar y reforzar el acceso.
- Generar medidas de seguridad más estrictas.
- Desarrollar mecanismos capaces de detectar y bloquear ataques.
- Adoptar medidas preventivas para disminuir los riesgos de ataques.
- Realizar auditorías y seguimientos de eventos de seguridad.
- Considerar las interfaces de gestión y el comportamiento en la red.
- Realizar las actualizaciones y mantenimientos necesarios.
- Garantizar la seguridad en las comunicaciones.
- Disponer debidamente de los servicios y/o dispositivos.

Es esencial promover políticas públicas en materia de comunicación que favorezcan la concientización de la sociedad en temas de seguridad. El rol de las agencias de gobierno, de los reguladores, de la comunidad técnica y de los proveedores de IoT es fundamental para proteger las redes y los usuarios de manera cabal. Es clave promover la investigación y el desarrollo, así como su difusión.

Como se desarrolla en la **Tabla 5**, es importante considerar que también existen potenciales riesgos asociados a los proveedores de servicios y conocer las posibles soluciones.

TABLA 5: POTENCIALES RIESGOS ASOCIADOS A LOS PROVEEDORES DE SERVICIOS Y POSIBLES SOLUCIONES

Concepto.	Riesgos potenciales.	Soluciones a considerar.
Seguridad de las interfaces web.	Uso de claves por de-fecto. No bloqueo de cuenta. Vulnerabilidades de servicios web no identificadas o no tratadas.	Permitir cambio de contra-señas. Permitir bloqueo de cuenta. Conducir criterios de eva-luación (assessment) de aplicaciones web. Seguimiento de recomendaciones por parte de los proveedores de servicio.
Autenticación o autorización de acceso.	Contraseñas débiles. Mecanismos de recupe-ración de contraseñas inseguros. Falta de autenticación robusta.	Uso de contraseñas segu-ras. Verificar la seguridad de los mecanismos de recupera-ción de claves. Implementar mecanismos de autenticación robustos.
Servicios de red.	Puertos abiertos innecesariamente. Puertos expuestos a Internet. Denegación de servicio (Denial of Service o DOS).	Minimizar apertura innecesaria de puertos. Testear vulnerabilidades de servicios de red. Evitar que los dispositivos intercambien información no prevista en el diseño de la solución ofrecida o innecesaria.
Cifrado del canal de comunicación.	Envío de información sensible vía protocolos de seguridad mal configurados. Uso de protocolos de cifrados débiles.	Asegurar configuración segura y adecuada de transporte de información. Usar protocolos de cifrado robustos.

Concepto.	Riesgos potenciales.	Soluciones a considerar.
Privacidad.	Recolección de datos personales innecesarios. No proteger la información recolectada. No permitir al consumidor elegir los datos personales que son recolectados.	Minimizar la recolección de datos personales. Anonimizar los datos recogidos en caso de transferirlos a terceros o cuando no es necesaria la identificación posterior del usuario. Permitir al consumidor que decida qué datos brindar.
Interfaces de servicios de nube.	Interfaces de servicios de nube. No revisar las vulnerabilidades de las interfaces. Las contraseñas usadas son débiles. No se usa autenticación robusta.	Realizar comprobaciones en todas las interfaces. Usar siempre autenticación robusta. Usar siempre contraseñas seguras.
Interfaz móvil.	No se usa autenticación con claves seguras. No hay mecanismos de bloqueo.	Implementar bloqueos luego de cierto número de accesos no exitosos. Usar autenticación segura. Usar contraseñas seguras.
Configuración de seguridad.	Las opciones de contraseña segura no están disponibles. Las opciones de encriptación no están disponibles. No hay registros de actividad para verificar incidentes.	Disponer de registros de actividad para realizar auditorías de seguridad (accounting). Permitir seleccionar opciones de encriptado de la información. Notificar alertas de seguridad a los consumidores.
Firmware.	Los servidores de actualización no son seguros. Los updates se emiten sin encriptación. Los updates no se usan firmados.	Usar firmas digitales al proporcionar actualizaciones para verificar su autenticidad e integridad. Verificar las actualizaciones antes de instalarlas. Utilizar servidores de actualizaciones seguros.
Hardware.	Puertos USB accesibles. Acceder a sistema operativos. Imposibilidad de incluir limitaciones a los accesos para la administración.	Minimizar puertos externos accesibles innecesarios. Proteger el sistema operativo. Usar recomendaciones y buenas prácticas aceptadas internacionalmente.

IoT brinda un sinfín de oportunidades para todos. Presenta potenciales riesgos que se deben identificar para trabajar en su mitigación.

CONSIDERACIONES FINALES

El número de sistemas y/o dispositivos de IoT crece constantemente, a grandes velocidades, siendo esencial el trabajo en conjunto de forma multidisciplinaria para entender y considerar cabalmente el impacto creciente que tiene la seguridad en IoT.

Para proteger el futuro de IoT, es fundamental que los diversos actores coordinen acciones y aporten constructivamente para alcanzar en conjunto soluciones a nivel mundial que contribuyan a proteger a la red y a las personas contra potenciales amenazas. En este sentido, es recomendable seguir de cerca otros procesos nacionales, regionales y globales que puedan servir para replicar acciones colaborativas y conjuntas.

La temática está siendo estudiada y analizada a nivel mundial, de forma transversal e interdisciplinaria, a fin de alcanzar soluciones flexibles que reflejen la necesidad y la realidad, siendo importante su revisión y evaluación periódica.

La confianza es primordial para la sostenibilidad y el impulso global de Internet y de las redes en general. Construir ecosistemas seguros que reduzcan los riesgos y generen salvaguardas, así como proveer diversos mecanismos de información para que los consumidores puedan tomar decisiones informadas a la hora de adquirir equipamiento o sistemas, es clave para su adecuado desarrollo.

En vista de lo expuesto y de estándares y recomendaciones internacionales , se considera que sería deseable trabajar sobre un marco de seguridad, así como desarrollar herramientas y procesos que permitan la integración y el soporte teniendo como centro a las personas.

ANEXO I

El proceso de seguridad en IoT en Uruguay

El 22 de julio de 2019 se realizó el Primer Encuentro del Proceso Nacional sobre Seguridad en IoT en Uruguay.

Participaron más de 60 personas, entre ellas, autoridades nacionales, representantes de diversos organismos y empresas públicas y privadas, de la academia, de la sociedad civil y de la comunidad técnica.

Se compartió la motivación del proceso, haciendo énfasis en que se está en un mundo cada vez más conectado, donde hay más dispositivos y sistemas de IoT que utilizan Internet, que ofrecen muchas oportunidades, pero también tienen riesgos relativos a la seguridad y a la privacidad, sobre los cuales se debe trabajar.

Se partió de las siguientes bases: (i) la responsabilidad debe ser compartida, (ii) los usuarios deben estar en el centro de las soluciones, (iii) la protección de la privacidad y de los datos personales debe ser desde el diseño y por defecto y (iv) se deben adoptar prácticas de privacidad responsables con un enfoque inclusivo y colaborativo, buscando soluciones duraderas, eficientes, flexibles y con revisión periódica.

Se apostó por un proceso orgánico de abajo hacia arriba, con un enfoque de múltiples partes interesadas, buscando que los resultados aborden muchos de los desafíos y problemas existentes y potenciales.

Para atender lo antes mencionado, el objetivo fue desarrollar un proceso nacional para generar recomendaciones a fin de mitigar los riesgos de seguridad asociados con IoT.

Se optó por trabajar en dos áreas:

- **Protección del consumidor:** ¿Cómo se pueden generar competencias y sensibilizar a los consumidores para que puedan tomar decisiones informadas sobre los proveedores de servicios, así como comprender mejor los riesgos de la adopción y ser más activos en la protección de sus datos?
- **Resiliencia de la red:** Crece la cantidad de dispositivos conectados a Internet y existe la necesidad de desarrollar una mayor resiliencia en las redes, en los servidores y en los softwares que se utilizan, así como en los que transmiten y almacenan datos. ¿Cómo se puede mitigar el riesgo que representan los dispositivos conectados a Internet para garantizar la estabilidad de las redes?

El abordaje se realizó, al menos, desde dos visiones: institucional y tecnológica.

Se generó un repositorio público con material, el cual se nutrió con aportes de los diversos participantes, con información nacional e internacional .

El proceso se desarrolló con reuniones presenciales y trabajo colaborativo en línea.

En base a todos los aportes recibidos y al intercambio constante, a lo largo del proceso se avanzó sobre un borrador del trabajo, el cual fue ajustado en múltiples instancias hasta llegar a la versión final, la cual buscó contemplar los aportes y comentarios de todos los participantes.

Plan de trabajo

El cronograma de trabajo fue el siguiente:

Pasos	Fecha	Comentarios
Paso 1.	22 de julio.	Reunión 1.
Paso 2.	29 de julio.	Reunión 2: Grupos de trabajo.
Paso 3.	2 de agosto.	Primer borrador de trabajo.
Paso 4.	14 de agosto.	Comentarios al borrador de trabajo.
Paso 5.	20 de agosto.	Segundo borrador de trabajo.
Paso 6.	23 de agosto.	Reunión 3: Grupos de trabajo.
Paso 7.	29 de agosto.	Tercer borrador de trabajo.
Paso 8.	12 de setiembre.	Comentarios al borrador de trabajo.
Paso 9.	17 de setiembre.	Reunión 4: Grupos de Trabajo, plenaria.
Paso 10.	18 de setiembre.	Cuarto borrador de trabajo.
Paso 11.	25 de setiembre.	Comentarios finales al borrador de trabajo.
Paso 12.	30 de setiembre.	Quinto borrador de trabajo.
Paso 13.	Octubre.	Edición final del borrador.
Paso 14.	Noviembre.	Presentación de los principales resultados en la Cumbre del D9.

BIBLIOGRAFÍA

Código de prácticas de seguridad del consumidor en relación con el Internet de las cosas. DCMS, 2018, 'Secure by Design: Improving the cyber security of consumer Internet of Things: Report', https://www.gov.uk/government/publications/secure-by-design. Octubre de 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490114566519 Consultado el 12 de julio de 2019.

ENISA: "IoT Security Standards Gap Analysis". Mapping of existing standards against requirements on security and privacy in the area of IoT. V1. O. December 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490100936575 Consultado el 12 de julio de 2019.

ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures". November 2017. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498759112229 Consultado el 29 de julio de 2019.

ETSI TS 103 645 V1.1.1(2019): CYBER: Cyber Security for Consumer Internet of Things. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/499603848486 Consultado el 31 de julio de 2019.

GLOBAL CITY TEAMS CHALLENGE: "Smart and secure cities and communities challenge (SC3). A Risk Management Approach to Smart City Cybersecurity and Privacy. A Guidebook from the Cybersecurity and Privacy Advisory Committee (CPAC) Public Working Group. Julio 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495945984537. Consultado el 24 de julio de 2019.

GSMA: "IoT Security Assessment". CLP.17 V.3.0. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495964815061. Consultado el 24 de julio de 2019.

IEEE STANDARDS ASSOCIATION. IEEE Standards Activities in the Internet of Things (IoT). Noviembre de 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498755786979 Consultado el 29 de julio de 2019.

INDUSTRIAL INTERNET CONSORTIUM: "The Industrial Internet of Things: Managing and Assessing Trustworthiness for IoT in Practice". An Industrial Internet Consortium White Paper. Version 1.0. Julio 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/502051557200 Consultado el 5 de agosto de 2019.

INTERNET SOCIETY: CANADIAN MULTISTAKEHOLDER PROCESS: Enhancing IoT Security. Final Outcomes and Recommendations Report. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490100106034 Consultado el 12 de julio de 2019.

INTERNET SOCIETY: Top tips for Internet of Things security and privacy. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/491209777648 Consultado el 15 de julio de 2019.

INTERNET SOCIETY: "IoT Security for Policymakers". Abril 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/490319556578 Consultado el 12 de julio de 2019.

IOT-NOW: "New vulnerability found in internet building automation devices" https://www.iot-now.com/2019/08/13/98154-new-vulnerability-found-internet-connected-building-automation-devices/ Consultado 29 de agosto de 2019.

IOT SECURITY FOUNDATION: "IoT Cybersecurity: Regulation Ready". 2018. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495957218652. Consultado el 24 de julio de 2019.

IOT SECURITY FOUNDATION: Make it safe to connect. "Establishing principles for Internet of Things Security". URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495971368874 Consultado el 24 de julio de 2019.

IOT SECURITY FOUNDATION: White Paper: Mapping the IoT Security Foundation's Compliance Framework to ETSI TS 103 645 Standard. Febrero 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/499587357470. Consultado el 31 de julio de 2019.

ISACA: "Managing the Risk of IoT: Regulations, Frameworks, Security, Risk and Analytics". URL: https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/managing-the-risk-of-iot.aspx Consultado el 29 de agosto de 2019.

ISTR: Internet Security Threat Report. Volume 23. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/497646535147 Consultado el 26 de julio de 2019.

ITU-T: Telecommunication Standarization Sector of ITU. Y4806 (11/2017). URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498757025611 Consultado el 29 de julio de 2019.

LACNOG – M3AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1. Mayo 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/495302212082 Consultado el 23 de julio de 2019.

NRIA IoT Security Upgradability and Patching. Existing Standards, Tools and Initiatives Working Group (WG1). Catalog of Existing IoT Security Standards. Version 0.01. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/498758824895 Consultado el 29 de julio de 2019.

Organización de los Estados Americanos (OEA): "Ciberseguridad. Marco NIST". Un abordaje integral de la Ciberseguridad. Edición 5. 2019. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/517046329645 Consultado el 1 de setiembre de 2019.

ONEM2M: Facing the Challenges of M2M Security and Privacy. Phil Hawkers. 2014. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511801089415 Consultado el 22 de agosto de 2019.

OTA – Online Trust Alliance an Internet Society Initiative. IoT Confianza por Diseño. El marco de Confianza IoT de OTA. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/493760516548 Consultado el 22 de agosto de 2019.

OTA – Online Trust Alliance. Smart Home Checklist. Maximizing Security, Privacy & Personal Safety. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511799261039 Consultado el 22 de agosto de 2019.

OTA – Online Trust Alliance an Internet Society Initiative. The Enterprise IoT Security Checklist. Best Practices for Securing Consumer-Grade IoT in the Enterprise. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511800322567 Consultado el 22 de agosto de 2019.

OTA – Online Trust Alliance an Internet Society Initiative. IOT Security & Privacy Trust Framework v2.5. URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/511797067111 Consultado el 22 de agosto de 2019.

SENSORS: "The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey". URL: https://isoc.app.box.com/v/repositorio-iot-uy/file/515507947386 Consultado el 29 de agosto de 2019.

Juniper Research: "Internet of Things connected devices to almost triple to over 38 billion units by 2020". URL:

REFERENCIAS

https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020. Consultado el 31 de julio de 2019.

Recomendación UIT-T Y.4000/Y.2060 (06/2012) de la Unión Internacional de Telecomunicaciones. Descripción General de Internet de los Objetos. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I/es Consultado el 30 de julio de 2019.

"consumer: natural person who is acting for purposes which are outside his trade, business, craft or profession NOTE: Organizations, including businesses of any size, also use consumer IoT. For example, smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses". ETSI TS 103 645 V1.1.1 (2019-02). URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf Consultado el 5 de Agosto de 2019.

Traducción propia, Consumidor: es la persona física que actúa con fines ajenos al comercio, oficio, negocio o profesión. NOTA: Las organizaciones, incluidas las empresas de cualquier tamaño, también son consumidores de IoT. Por ejemplo, los televisores inteligentes se implementan con frecuencia en las salas de reuniones, y los kits de seguridad para el hogar pueden proteger las instalaciones de pequeñas empresas.

"consumer IoT: network-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail and that are typically used in the home or as electronic wearables". ETSI TS 103 645 V1.1.1 (2019-02). URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf Consultado el 5 de Agosto de 2019.

Traducción propia: Consumidor de IoT: dispositivos conectados a la red (o que se pueden conectar a la red) y sus servicios asociados que generalmente están disponibles para que el consumidor los compre en el comercio minorista y que se utilizan en el hogar o como dispositivos electrónicos portátiles.

NTIA IoT Security Upgradability and Patching: "Catalog of Existing IoT Security Standards". Versión 0.01. URL: https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf Consultado el 5 de agosto de 2019.

Participaron las siguientes organizaciones: Agencia de Gobierno Electrónico y Sociedad de la Información (Agesic), Administración Nacional de Combustibles, Alcoholes y Portland (Ancap), Administración Nacional de Telecomunicaciones (Antel), Claro, Dativa, Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (Dinatel – Miem), Fundación Ceibal, IEEE, Intendencia de Montevideo, Internet Society Uruguay, Isbel, Lacnic, Laboratorio Tecnológico del Uruguay (Latu), Liga de Defensa Comercial (Lideco), Observatic, Seciu, Sigfox, Tib, Universidad de la República - Facultad de Derecho y Facultad de Ingeniería, Universidad Católica del Uruguay, Universidad ORT, Universidad de Montevideo, Universidad Tecnológica del Uruguay (Utec), Unidad Reguladora de Servicios de Comunicaciones (Ursec), Administración Nacional de Usinas y Transmisiones Eléctricas (UTE), Youth

Uruguay.

Internet Society. URL: https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/ Consultado el 5 de agosto de 2019.

Los objetivos de aprendizaje podrían ser: (i) adquirir competencias que permitan seleccionar inteligentemente un dispositivo y/o sistema de IoT; (ii) capacidad de identificar fácilmente el nivel de seguridad de los sistemas y/o dispositivos, ateniendo determinados estándares; (iii) procedimiento para actualizar los sistemas y/o dispositivos, las aplicaciones y criterios para definir contraseñas seguras; (iv) cómo activar la encriptación si el dispositivo y/o sistema tiene la capacidad; (v) identificar la importancia de los términos de privacidad de los sistemas y/o dispositivos; (vi) conectividad de los sistemas y/o dispositivos a Internet; (vii) seguridad en la red.

Se debe hacer especial énfasis en estándares abiertos, por ejemplo, el IETF, el cual podría considerarse en conjunto con el documento de la OTA para dar un marco realizable. RFC 8576: URL: https://datatracker.ietf.org/doc/rfc8576/ Consultado el 20 de agosto de 2019.

A fin de que sea fácilmente identificable el grado de seguridad de los sistemas y/o dispositivos, el Grupo de Trabajo considera que sería positivo impulsar que institutos de estandarización acuerden criterios o recomendaciones que permitan calificar la seguridad de los sistemas y/o dispositivos de IoT, simplificando a la industria el cumplimiento y la comprensión a los consumidores. Se reconoce que se requiere un estudio profundo, que atienda normas y estándares internacionales, por lo que se recomienda la generación de un estudio específico y concreto sobre la materia.

Computer Emergency Response Team.

Computer Security Incident Response Team.

Unión Internacional de Telecomunicaciones ("ITU", por sus siglas en inglés): https://www.itu.int/rec/T-REC-Y.4806/ en Consultado el 20 de agosto de 2019.

Referencias y estándares de seguridad a modo de ejemplo y en forma no excluyente: (i) ISOC IoT Security for Policymakers 2017 Global Internet Report; (ii) ISTR. Internet Security Threat Report. Volume 23; (iii) ETSI TS 103 645 V1.1.1 (2019-02): Cyber Security for Consumer Internet of Things; (iv) ITU-T Y.4806 (11/2017) Security capabilities supporting safety of the Internet of things; (v) NIST Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop (June 28, 2018); (vi) NIST Draft NISTIR 8259 Core Cybersecurity Feature Baseline for 20 Securable IoT Devices: A Starting Point for IoT Device Manufacturers (July, 2919) https://doi.org/10.6028/NIST.IR.8259-draft; (vii) RFC 8576 Internet of Things (IoT) Security: State of the Art and Challenges (April, 2019); (viii) GSMA Descripción General de los Lineamientos de Seguridad IoT de la GSMA, Versión 2.0 (Febrero, 2018); (ix) GSMA Lineamientos de Seguridad IoT para los Operadores de Red, Versión 2.0 (26, Octubre, 2017); (x) GSMA Lineamientos de Seguridad IoT para el Ecosistema de Dispositivos Periféricos IoT , Versión 2.0 (26, Octubre, 2017); (xi) GSMA Lineamientos de Seguridad IoT para el Ecosistema de Servicios de IoT, Versión 2.0 (26 de Octubre 2017); (xii) OTA IoT Confianza por Diseño.

Link de acceso al repositorio público: https://isoc.box.com/v/repositorio-iot-uy