Seguridad en IoT Proceso en Uruguay

Setiembre 2019

Internet Society
Capítulo Uruguay

Uruguay
Digital

PRESIDENCIA
República Oriental del Uruguay

CONTENIDOS

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 [i] 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. [ii]

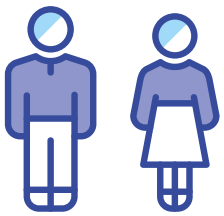
Importancia de trabajar en la seguridad de IoT

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 [iii] , para lograr recoger los aportes de todos los actores interesados.



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 desarrollar campañas de sensibilización destinadas a públicos específicos y atendiendo a las personas o grupos de personas más vulnerables.
- Que hay múltiples desafíos sobre los cuales se debe trabajar, siendo fundamental la 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 ciberseguridad.
- Que es fundamental promover una cultura de cooperación entre los diversos actores involucrados.

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. [iv]

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.

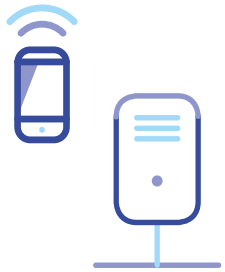
Hay que atender la seguridad interna y externa. Los sistemas y/o dispositivos de IoT pueden ser atacados, afectando la privacidad y la seguridad del propio consumidor, pero también pueden afectar a terceros, así como a otros sistemas y/o dispositivos.

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.

DESAFÍOS

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

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.

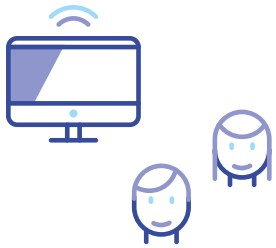
En la actualidad, se dispone de pocos mecanismos para señalizar y comparar el nivel de seguridad de los sistemas y/o dispositivos (por ejemplo, a través de calificaciones), en tanto no existen estándares internacionalmente aceptados para el etiquetado de los niveles de seguridad.

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.

VÍAS DE ACCIÓN

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

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 líneas de acción identificadas

A continuación, se plantean posibles acciones sobre las cuales sería deseable trabajar para proteger a los consumidores de los sistemas y/o dispositivos de IoT.

Educación y sensibilización del consumidor. Desarrollo de capacidades y sensibilización específica sobre la materia. Conocimiento de la importancia de atender determinados aspectos para poder evaluar la seguridad en sus sistemas y/o dispositivos de IoT.

Riesgos. Capacidad de identificar y conocer los riesgos actuales y/o potenciales.

Guía de buenas prácticas. Comprensión de las buenas prácticas de seguridad.

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.

Política de privacidad de los datos. Comprensible y de fácil acceso.

Seguridad desde el diseño y por defecto. Capacidad de utilizarlos con confianza. Control de acceso robusto, uso de protocolos de seguridad para las comunicaciones y posibilidad de bloquear puertos.

Protección de los datos de los consumidores. Protección de los datos en toda la cadena y en todas las capas.

Minimización de datos. Limitar la obtención de datos por parte de los sistemas y/o dispositivos a aquellos que sean necesarios para su funcionamiento.

Asistencia al consumidor. Acceder a sitios donde consultar y donde se atiendan los inconvenientes que puedan surgir.

Prevención al consumidor. Mitigar amenazas que se detecten.

Términos y condiciones. Comprensibles y de fácil acceso.

Conexión de los sistemas y/o dispositivos IoT a Internet. Comprender si es o no necesario que el sistema y/o dispositivo esté conectado continuamente a la red.

Responsabilidad. Conocer la responsabilidad específica de cada uno de los actores de la cadena.

Sistema de calificación[v]. Poder identificar fácilmente, por parte del consumidor, el grado de seguridad del sistema y/o dispositivo de IoT.

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 líneas de acción identificadas

A continuación, se plantean posibles acciones sobre las cuales sería deseable trabajar para proteger la resiliencia de la red.

Riesgos. 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.

Comunicación con el usuario. Informar y comunicar, adaptando el mensaje al público objetivo.

Contraseñas. No utilizar contraseñas universales por defecto; buscar que sea obligatoria su modificación inicial y que sean seguras.

Gestionar las vulnerabilidades. 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.

Actualización. Mantener el software actualizado.

Protección de los datos. Almacenar las credenciales de acceso y la información debidamente. Activar la encriptación de la información y/o de los sistemas, siempre que sea posible.

Seguridad por diseño. 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.

Almacenamiento de datos. 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.

Reporte de fallas. Configurar o activar reglas de detección de anomalías y que notifiquen al administrador y/o al usuario y/o al fabricante, cuando sea posible.

Configuración por defecto. 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.

Respaldo. Permitir almacenar los eventos de seguridad en repositorios externos y evitar pérdida de eventos.

Cooperación global. 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.

CONSIDERACIONES FINALES

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

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 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.

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.

REFERENCIAS

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

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.

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.

iReferencias y estándares de seguridad a modo de ejemplo y en forma no excluyente:

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.