Revista Ingenio
UFPS Ocaña
"Journal of Engineering Sciences"

Original Article DOI: https://doi.org/10.22463/2011642X.2667

El reto del desarrollo seguro de aplicaciones IoT en un mercado acelerado

The challenge of secure development of IoT applications in an accelerated market

M.Sc. Johan Smith Rueda-Rueda[1]

[1]*Grupo de Investigación, Desarrollo e Innovación para la Transformación Digital, Think Link, Colombia, http://orcid.org/0000-0001-6715-8353, Email: johan.rueda@thinklink.com.co*

Como citar: J. S. Rueda, "El reto del desarrollo seguro de aplicaciones IoT en un mercado acelerado", *Revista Ingenio*, vol. 18, n°1, pp 54-6, 2021, doi: https://doi.org/10.22463/2011642x.2667.

Fecha de recibido:23 de julio de 2020
Fecha aprobación:15 de diciembre de 2020

RESUMEN

Palabras claves:

Aplicación IoT, ciberseguridad, ciclo de vida de desarrollo seguro, desarrollo ágil, ingeniería de seguridad.

Un sistema de Internet de las cosas (IoT) comprende dispositivos, aplicaciones y servicios que se integran para soportar procesos organizacionales. Los desarrolladores IoT se enfrentan a diversos retos tecnológicos y de seguridad; sumado a esto, un mercado cambiante y altamente competitivo. El panorama de la seguridad en IoT refleja un reto para la ciberseguridad, porque se deben gestionar y controlar una variedad de amenazas cibernéticas y vectores de ataque que pueden ser usadas por los cibercriminales para comprometer infraestructuras tecnológicas. La seguridad es un requisito de calidad de los sistemas IoT, y como tal, debe ser atendida desde las fases de diseño y desarrollo. Este artículo aborda el reto del desarrollo seguro de dispositivos y aplicaciones IoT en un mercado que exige desarrollo y actualizaciones de forma ágiles, y presenta dos alternativas propuestas en la literatura para gestionar el desarrollo seguro con la filosofía del desarrollo ágil. De igual forma, invita a orientar esfuerzos de investigación, desarrollo tecnológico y formativo en temas relacionados con la implementación de la ciberseguridad en el desarrollo seguro de aplicaciones IoT.

ABSTRACT

Key words:

Agile development, cybersecurity, IoT application, security development lifecycle – SDL, security engineering.

An IoT system comprises devices, applications, and services that are integrated to support organizational processes. IoT developers face various technological and security challenges; added to this, a highly competitive and changing market. The IoT security landscape reflects a challenge for cybersecurity because a variety of cyber threats and attack vectors must be managed and controlled that can be used by cybercriminals to compromise technological infrastructures. Security is a quality requirement for IoT systems, and as such, it must be addressed from the design and development phases. This article addresses the challenge of secure development of IoT devices and applications in a market that demands products and updates in an agile way and presents two alternatives proposed in the literature to manage secure development with the philosophy of agile development. Likewise, it invites you to guide research, technological development, and training efforts on issues related to the implementation of cybersecurity in the secure development of IoT applications.

1. Introducción

El Internet de las cosas – IoT, del inglés *Internet of Things,* puede definirse como una red de objetos físicos y virtuales con identificación propia, que interactúan entre sí y con su entorno a través de internet [1]. El ecosistema IoT comprende objetos, comunicaciones, aplicaciones y análisis de datos [2]; y tiene diversos dominios de aplicación, como la industria, agricultura, logística, salud, edificaciones inteligentes, seguridad ciudadana, monitoreo ambiental, ciudades inteligentes y educación [3-4].

En el desarrollo de aplicaciones IoT se enfrentan diversos retos tecnológicos y de seguridad. Los retos tecnológicos se puede hacer referencia a factores como la comunicación inalámbrica, consumo de energía, escalabilidad, identificación de los nodos sensores, entre otros. Asimismo, se debe enfocar en la seguridad y la privacidad de los datos [5-6], la confianza de los recursos en las aplicaciones IoT [7-8], y la gestión de identidad, por nombrar algunos.

Garantizar la seguridad es necesario en todos los dominios de aplicación del IoT. Por ejemplo, las aplicaciones IoT en el dominio de la salud manejan datos sensibles de los pacientes a los que se le deben garantizar la privacidad [9-10-11]; las aplicaciones para ciudades inteligentes toman datos sobre el comportamiento de personas y sus círculos sociales, o controlan la infraestructura de la ciudad, como sistemas de seguridad o sistemas de tráfico o transporte, por nombrar

Autor para correspondencia
Correo electrónico: johan.rueda@thinklink.com.co (M.Sc. Johan Smith Rueda-Rueda)

algunos, afectando el funcionamiento normal de la misma [11-12]; o las aplicaciones IoT para industria, en el que un incidente puede generar daños físicos e incluso amenazar vidas humanas [13]. Esto también se ve reflejado en otras aplicaciones del IoT como las redes eléctricas inteligentes o *Smart Grids* [14], las casas inteligentes [15] y con los dispositivos vestibles [16], por nombrar algunos ejemplos.

El mercado es cada vez más competitivo y sus condiciones exigen que los desarrollos y actualizaciones de las aplicaciones IoT se realicen en periodos cortos de tiempo. Por esta razón, los métodos de desarrollo ágil son una buena opción para desarrollar sistemas de forma iterativa e incremental. En este punto, la dificultad para los desarrolladores ya no radica en cómo desarrollar software y sistemas de forma ágil, sino que se centra en abordar un ciclo de vida de desarrollo seguro y ágil, que se alineen con los plazos cortos de desarrollo relacionados con los proyectos ágiles.

Este artículo presenta la necesidad del implementar el desarrollo seguro de aplicaciones IoT, que incluye dispositivos y su firmware, software de aplicación y comunicaciones. La creación de soluciones IoT en el mercado actual, que exige un desarrollo y actualizaciones de forma ágiles, requiere la integración de buenas prácticas de la ingeniería del software y la ingeniería de seguridad. A lo anterior se suma las medidas de ciberseguridad necesarias para asegurar la aplicación IoT [17].

El resto del artículo está dividido en 5 secciones. En la sección 2 se presenta un panorama de la inseguridad en IoT desde tres perspectivas: las amenazas cibernéticas, los dispositivos IoT vulnerables y las medidas de seguridad deficientes en el diseño y desarrollo de aplicaciones y sistemas IoT. La sección 3 se centra en la seguridad como requisito de calidad de los sistemas IoT, y cómo pueden atenderse desde la ingeniería del software usando métodos de desarrollo tradicionales y ágiles. Finalmente se presentan las conclusiones de este trabajo.

2. Panorama de la inseguridad en IoT

En esta sección se presenta un panorama de los retos de seguridad que afrontan los desarrolladores o implementadores de aplicaciones IoT desde tres perspectivas: (i) amenazas cibernéticas; (ii) dispositivos IoT vulnerables; y (iii) medidas de seguridad deficientes en el diseño y desarrollo de aplicaciones y sistemas IoT.

2.1 Amenazas cibernéticas en IoT

Los ciberdelincuentes han enfocado su atención en el creciente auge que ha tenido el IoT como tendencia tecnológica en años recientes. El ecosistema IoT, que incluyen una gran variedad de dispositivos, comunicaciones, plataformas y servicios, ha ampliado los vectores de ataque hacia las infraestructuras tecnológicas.

Una de las amenazas de seguridad que enfrenta las aplicaciones IoT es el software malicioso o malware. Se han desarrollado diferentes tipos de programas maliciosos para IoT, como son troyanos, gusanos y *ransomware*.

Un troyano es un programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad del sistema que invoca el programa [18]. Algunos ejemplos de troyanos para IoT son: IRCTelnet, un troyano que apunta a dispositivos IoT basados en Linux, con el propósito de agregar esos dispositivos a una red de equipos infectados conocidas como *botnet*, y de esta forma llevar a cabo ataques de denegación de servicios distribuidos, DDoS – *Distributed Denial-of-Service* [19]; y *NyaDrop*, que atacan los puertos del protocolo de red Telnet y abrir una puerta trasera en el dispositivo infectado y si el dispositivo IoT utiliza una arquitectura MIPS (*Microprocessor without Interlocked Pipeline Stages*) de 32 bits descarga el troyano Nya [20].

Además, se han desarrollado troyanos enfocados al hardware a nivel de dispositivo y de red [21]: a nivel de dispositivos, existen troyanos enfocados a explotar los circuitos integrados criptográficos inalámbricos, permitiendo robar información confidencial y ocultar los datos filtrados como estructura "agregada" del perfil de transmisión, aprovechando las variaciones del proceso; y a nivel de la red, este tipo de troyanos pueden enfocarse en el hardware de redes inalámbricas, permitiendo robar información sensible en 802.11a/g y explotando el espacio no utilizado entre estándares inalámbricos, punto de funcionamiento del dispositivo y especificaciones.

Un *malware* de tipo gusano se define como un programa autónomo que es autorreplicable y autopropagable, que utiliza mecanismos de redes para difundirse [22]. Para IoT se encuentran ejemplos como: ArduWorm, un gusano para Arduino Yun [23]; Darlloz, un gusano utilizado para la minería de monedas criptográficas, que apunta a arquitecturas Intel x86, ARM, MIPS y arquitecturas PowerPC [24]; Hajime, un gusano para dispositivos IoT que se propaga en dispositivos que ejecutan servidores Telnet con credenciales predeterminadas inseguras [25]; y un gusano llamado *radiation*, el cual está dirigido a dispositivos de televisión de circuito cerrado [26].

El *ransomware*, en términos generales, es un tipo de

malware que impide o limita el acceso de los usuarios a un sistema, ya sea bloqueando la pantalla del sistema o cifrando los archivos de los usuarios a menos que se pague un rescate para obtener la clave de descifrado [27].

Ya enfocándose en el IoT, se empezó a utilizar el concepto de *ransomware of Things* – RoT [28], y es una forma especializada de *ransomware* que busca tomar el control de un dispositivo cuyo propósito principal no es el procesamiento de datos o las comunicaciones digitales, que son los blancos de ataque tradicionalmente; sino que se enfocan en otra clase de dispositivos, como por ejemplo, un coche, o cualquier otro dispositivos conectado a Internet [29]. La primera víctima de este tipo de *malware* fue el sistema de llave electrónica de un hotel austriaco de cuatro estrellas en 2017 [30]. Este tipo de *malware* pone en riesgo los datos críticos, e incluso la vida, como los ataques ya conocidos por los hospitales y la infraestructura crítica [31].

En la Tabla 1, se presenta una taxonomía de amenazas en los sistemas IoT y los activos que son afectados por ellas.

2.2 Dispositivos IoT Vulnerables

El IoT integra una gran cantidad de dispositivos que interactúan a través de Internet. Un dispositivo con una seguridad deficiente ya sea en el proceso de fabricación o implementación, aumenta el riesgo la seguridad y la privacidad de los usuarios y empresas, y la integridad de los usuarios y las personas.

Los dispositivos vulnerables conectados pueden ser utilizados para el montaje de ataques contra cualquier tipo de destino y servicio de Internet y ataques contra las redes internas que alojan estos dispositivos conectados [32].

Todo dispositivo conectado a Internet puede ser vulnerables, lo que representa un riesgo para las organizaciones y las personas que lo usan en la cotidianidad de sus hogares, y los pueden usar como punto de acceso inicial para el robo de credenciales y datos [33]. Estos dispositivos son un gran atractivo para los cibercriminales, ya que, en el caso de las organizaciones, muchos de ellos no están bajo el control y monitorización del departamento de TI.

Tabla 1. Taxonomía de amenazas en sistemas IoT y activos afectados por ellas

Categoría	Amenaza	Activos afectados
Ataques/ abusos	Malware	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend
	Secuencias de exploits	Dispositivos IoT; otros dispositivos del ecosistema IoT; infraestructura
	Ataques dirigidos	Plataforma y backend; infraestructura; información
	Denegación de servicio distribuido (DDoS)	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; infraestructura
	Falsificación de dispositivos malicioso	Dispositivos IoT; otros dispositivos del ecosistema IoT; infraestructura
	Ataques a la privacidad	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; información
	Modificación de información	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; información
Escuchas/ Interceptación/ Secuestro	Ataque Man-in-the-middle	Información; comunicaciones; dispositivos IoT
	Secuestro de protocolo de comunicación IoT	Información; comunicaciones; dispositivos IoT; toma de decisiones
	Intercepción de información	Información; comunicaciones; dispositivos IoT
	Reconocimiento de red	Información; comunicaciones; dispositivos IoT; infraestructura
	Secuestro de sesión	Información; comunicaciones; dispositivos IoT
	Obtención de información	Información; comunicaciones; dispositivos IoT
	Reproducción de mensajes	Información; dispositivos IoT; toma de decisiones
Interrupciones	Caída de red	Infraestructura; comunicaciones
	Fallo de dispositivos	Dispositivos IoT
	Fallo del sistema	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend
	Pérdida de servicios de soporte	Todos los activos
Daño/pérdida (activos TI)	Filtrado de datos/información confidencial	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; información

Fallos/averías	Vulnerabilidades de software	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; información
	Fallos de terceros	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; infraestructura; aplicaciones y servicios
Desastre	Desastre natural	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; infraestructura
	Desastres ambientales	Otros dispositivos del ecosistema IoT; plataforma y backend; infraestructura
Ataques físicos	Modificación de dispositivos	Dispositivos IoT; comunicaciones
	Destrucción del dispositivo (sabotaje)	Dispositivos IoT; otros dispositivos del ecosistema IoT; plataforma y backend; infraestructura

Fuente: [61, p. 34]

Investigadores demostraron que es posible un ataque remoto a vehículos, en el que se pudo comprometer sistemas físicos como la dirección y el freno. El ataque remoto usado no requiere modificaciones en el vehículo o interacción física por parte de atacante [34]. En [35] se analizan algunas investigaciones sobre vulnerabilidades en vehículos y el autor reflexiona sobre la necesidad de vehículos más seguros.

Los televisores inteligentes son un objetivo para conseguir secretos personales y organizacionales, ya que son comunes en hogares y oficinas. Estos dispositivos son un objetivo perfecto para vigilancia, ya que cuentan con un cable de alimentación que puede estar todo el tiempo conectado, cuentan con cámara y sensores de voz y puede estar localizado en lugares muy privados [36].

Las cámaras IP también han sido un objetivo importante para los cibercriminales, no solo por lo que pueden observar a través de ellos, sino porque han sido usadas para lanzar ataques más grandes. Estos dispositivos junto con enrutadores y grabadoras de video digital (DVR, por sus siglas en inglés) son usadas para generar ataques de denegación de servicio distribuídos – DDoS. Algunos ataques DDoS se han originado de bots de 145,607 cámaras y DVR, y 25.000 cámaras de circuitos cerrados de televisión [37].

Los juguetes infantiles que cuentan con conexión a internet también son un riesgo para la privacidad. De acuerdo con [38], una muñeca Barbie, presentada como la primera muñeca interactiva, con la capacidad de escuchar al niño y responder a través de la voz, podía ser convertida en un dispositivo de vigilancia para espiar a los niños y escuchar conversaciones sin el conocimiento del propietario, una vez el cibercriminal se haya hecho con el control de la muñeca y anulado las medidas de seguridad incorporadas.

Los monitores de bebes también representan un riesgo para los niños y sus padres. En [39] presentan varios casos de vulneración de la privacidad a través de estos dispositivos; en uno de los casos, un monitor de bebés habilitado con Wi-Fi fue usado para pronunciar improperios sexuales y la frase 'voy a secuestrar a su bebé'.

Los timbres de puertas inteligentes, una vez se tenga acceso físico al dispositivo, se puede robar las credenciales de Wi-Fi permitiendo al atacante adueñarse de la red hogareña, y solo necesitando un destornillador y un teléfono inteligente [40].

En un estudio realizado por *Hewlett-Packard Enterprise* [41] se probaron 10 dispositivos IoT y se concluyó que: seis de cada 10 dispositivos que proporcionan interfaces de usuario eran vulnerables a una gama de problemas tales como *Cross-site scripting* (XSS) persistente y credenciales débiles; el 80% de los dispositivos, junto con sus componentes de aplicaciones en la nube y móviles, no han requerido contraseñas de suficiente complejidad y longitud; el 70% de los dispositivos, junto con su aplicación en la nube y en el móvil, permiten a un atacante identificar cuentas de usuario válidas a través de la enumeración de cuenta y el 70% de los dispositivos utilizan el servicio de red sin cifrar.

La compañía *ForeScout Technologies* realizó una auditoría de seguridad a dispositivos IoT con el fin de investigar los riesgos de seguridad que plantean estos dispositivos en entornos empresariales [42]. En esta auditoría se evaluó siete dispositivos IoT, y sus hallazgos clave fueron: (i) los siete dispositivos IoT pueden ser hackeados en tan sólo tres minutos, y puede tomar días o semanas remediar estos incidentes; (ii) si cualquiera de estos dispositivos se infecta, los ciberdelincuentes pueden plantar puertas traseras para lanzar un ataque DDoS automatizado a través de redes equipos informáticos infectados o *botnet* creadas con dispositivos IoT; y (iii) los ciberdelincuentes pueden aprovechar las técnicas de interferencia o falsificación para hackear sistemas de seguridad empresariales inteligentes, permitiéndoles controlar sensores de movimiento, cerraduras y equipos de vigilancia.

Un dispositivo hackeado se convierte en una puerta de entrada a la red de una organización. El estudio realizado por *Kamkar y ForeScout Technologies* [42] afirma que, una vez que los ciberdelincuentes hackean un dispositivo logran acceder a la red de la organización, y algunas de las acciones que podrían desarrollar son: (i) fisgonear y grabar llamadas a través de teléfonos de voz sobre protocolo de internet (*VoIP – Voice over IP*); (ii) a través de los sistemas de climatización conocidos como HVAC, por sus siglas en inglés *heating, ventilation and air conditioning,* pueden forzar espacios críticos, como las salas de servidores, para sobrecalentar la infraestructura crítica y causar daño físico; (iii) deshabilitar los sistemas de seguridad conectados para permitir robos físicos; (iv) a través de los televisores inteligentes, pueden espiar a través de la cámara y el micrófono; (v) utilizando impresoras conectadas, pueden acceder a información privada de la compañía y del usuario; y (vi) a través de neveras inteligentes pueden obtener credenciales de usuario y utilizar las bombillas inteligentes para extraer credenciales de las redes inalámbricas, y con esta información realizar nuevos ataques.

2.3 Medidas de seguridad deficientes en el diseño y desarrollo de aplicaciones IoT

Los fabricantes y desarrolladores de dispositivos y aplicaciones IoT se apresuran a agregar funciones más recientes y atractivas a sus desarrollos al menor costo posible [43]; y en su apuro por comercializar pasan por alto el diseño y la construcción de la seguridad en el hardware y el software que desarrollan [44].

Una encuesta realizada por *Deloitte* [45] sobre la seguridad en dispositivos médicos indicó que las organizaciones que no participan en la fase de diseño de estos dispositivos tienen problema de seguridad cuando estos se conectan a internet. Esta encuesta también indicó que la gestión de los riesgos cibernéticos de los dispositivos médicos es la principal preocupación que enfrentan los fabricantes, proveedores y reguladores.

El crecimiento en la cantidad de dispositivos IoT y de su capacidad de procesamiento, acompañado del elevado número de vulnerabilidades reportadas y la poca adopción de tecnologías que permitan administrar las actualizaciones de software, permite que estos dispositivos puedan ser utilizados para realizar algún tipo de ataque o acceder a las redes que están conectados [46].

Las malas prácticas y el bajo conocimiento de medidas básicas de seguridad por parte de los usuarios también contribuye con el problema. Al implementar soluciones IoT, los usuarios tienden a dejar la configuración predeterminada de sus dispositivos y el software que los administra; esto deja una puerta abierta para que los atacantes puedan acceder a la red de un consumidor u organización [47].

3. La seguridad, un requisito de calidad de aplicaciones IoT

La calidad de un sistema comienza con una adecuada gestión de los requerimientos funcionales y no funcionales o de calidad. La seguridad es un requisito de calidad, y como tal, es transversal a todo sistema [48-49]. Gestionar la seguridad de un sistema IoT debe comenzar en la fase de análisis y diseño. Considerar la seguridad del sistema en estas fases permite a los desarrolladores tener un panorama más claro sobre qué recursos se deben asegurar y cómo se deben proteger, facilitando tomar mejores decisiones durante la construcción de la aplicación.

Un buen análisis de los requisitos de calidad es fundamental durante el desarrollo del sistema [50-51], porque en esta fase se determinan las características de calidad que debe cumplir, y a partir de allí, se base el diseño, implementación y pruebas a realizar del sistema. Además, si los requisitos de calidad no se gestionan adecuadamente, cualquier cambio en las etapas posteriores de desarrollo supone un costo enorme, aumentando el tiempo de diseño y de implementación [52]. Por esta razón, los requisitos de calidad resultan ser los más costosos y difíciles de corregir una vez se ha implementado el sistema [53-54].

En el proceso de desarrollar un sistema IoT usando métodos tradicionales de desarrollo no requiere un mayor contratiempo para analizar, diseñar, implementar y probar los requisitos funcionales y de calidad del sistema. Pero en un mercado competitivo estos métodos tradicionales no son bien vistos y se recurren al uso de métodos ágiles de desarrollo.

El manifiesto por el desarrollo ágil de software valora más a los individuos e interacciones sobre procesos y herramientas, un software funcional sobre documentación extensiva y la respuesta ante el cambio sobre seguir un plan [55]. Dentro de los 12 principios del manifiesto ágil está que la entrega de software funcional se realiza en periodos cortos de tiempo, entre dos semanas y dos meses, y que el software funcionando es la medida principal de progreso [56]. Esta filosofía puede ser mal interpretada y ser usada como pretexto para no implementar las buenas prácticas o priorizar el desarrollo de los requisitos funcionales, rezagando los requisitos de calidad, como la seguridad.

Los desarrolladores de software que implementan el desarrollo ágil se enfrentan a la dificultad de gestionar el ciclo de vida de un desarrollo seguro, o SDL – *Security Development Lifecycle*, con los plazos cortos de desarrollo que se siguen en estos métodos. Los desarrolladores deben equilibrar la implementación de la seguridad y demás requisitos de calidad con la filosofía del desarrollo ágil.

Una de las contribuciones para armonizar el desarrollo seguro con el desarrollo ágil lo realizó Microsoft al adaptar el ciclo de vida del desarrollo seguro que venían usando en sus productos con los métodos ágiles, el cual denominaron SDL-Agile [57-58]. Para lograr esta adaptación, el SDL-Agile divide el ciclo de desarrollo seguro en tres categorías de requisitos: los requisitos *every-sprint*, que son requisitos tan importantes que deben completarse cada iteración; los requisitos *one-time*, que son requisitos que solo se deben completar una vez por proyecto sin importar cuánto se ejecute; y los requisitos *bucket*, que son requisitos que aún deben completarse con regularidad, pero no son tan importantes como para completar cada sprint [59].

Un efecto de esta categorización es que los equipos pueden omitir temporalmente algunos requisitos de SDL para algunas versiones, y de esta forma, proporcionar la mejor combinación de seguridad, desarrollo de funciones y velocidad de lanzamiento [59]. Además de los requisitos específicos del desarrollo seguro, el SDL-Agile también considera las tareas asociadas con el desarrollo seguro en el marco del trabajo ágil, como son la formación en seguridad, herramientas y automatización, modelado de amenazas, pruebas de software usando la técnica *fuzzing*, el manejador de excepciones en el desarrollo y la revisión final de seguridad.

Otro ejemplo es el *Practical security stories and security tasks for agile development environments* por SAFECode [60] que dispone de contenido adaptado específicamente a las necesidades únicas de arquitectos, desarrolladores y probadores de software que usan metodologías ágiles. Este dispone de 36 historias centradas en la seguridad con tareas de seguridad asociadas; un conjunto de 17 tareas de seguridad operacional que los profesionales ágiles deberían considerar realizar de forma continua; y 12 tareas de seguridad avanzada.

4. Conclusiones

El Internet de las cosas y sus dispositivos se ha convertido en un objetivo muy llamativo para los ciberdelincuentes, los cuales aprovechan los errores de diseño y configuración y la falta de gestión de las tecnologías utilizadas en las aplicaciones IoT para hacerse con el acceso a la infraestructura de tecnologías de información y comunicación (TIC) de las organizaciones.

El panorama de inseguridad en IoT es preocupante, esto debido a cuatro razones: (i) la amplia variedad de amenazas cibernéticas, como *malware* y diferentes tipos de ataques, con una tendencia creciente en la variedad de amenazas y la frecuencia con que estas se materializan; (ii) el gran porcentaje de dispositivos IoT vulnerables que se convierten en puertas de acceso a la información de empresas y ciudadanos; (iii) las medidas de seguridad deficientes en el diseño y desarrollo de aplicaciones y sistemas IoT que son el resultado de las condiciones de mercado, donde se exige ser el desarrollo ágil y conseguir nuevas funcionalidades para lograr posicionar el producto.

El desarrollo seguro de aplicaciones IoT puede llevarse a cabo en armonía con los principios del desarrollo ágil. En este sentido, se pueden orientar esfuerzos de investigación, desarrollo tecnológico y formativo en temas relacionados con la implementación de la ciberseguridad en el desarrollo seguro de aplicaciones IoT. Estos esfuerzos podrían estar representados en *frameworks*, modelos y guías que orienten a los desarrolladores de estas tecnologías en el desarrollo seguro, y la formación de profesionales y capacitación de usuarios para la implementación y uso de soluciones IoT en espacios laborales o personales.

5. Referencias

[1] J. Rueda and J. Talavera Portocarrero, "Similitudes y diferencias entre Redes de Sensores Inalámbricas e Internet de las Cosas: Hacia una postura clarificadora," Rev. Colomb. Comput., vol. 18, no. 2, pp. 58–74, 2017.

[2] J. Tully et al., "The Internet of Things and Related Definitions," 2012.

[3] J. S. Rueda-Rueda, J. A. Manrique, and J. D. Cabrera Cruz, "Internet de las Cosas en las Instituciones de Educación Superior," in Congreso Internacional en Innovación y Apropiación de las Tecnologías de la Información y las Comunicaciones – CIINATIC 2017, 2017, pp. 1–5.

[4] E. Borgia, "The internet of things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, 2014.

[5] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Bus. Horiz., vol. 58, no. 4, pp. 431–440, 2015.

[6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Trans. Ind. Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[8] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, 2015.

[9] S. Supriya and S. Padaki, "Data Security and Privacy Challenges in Adopting Solutions for IOT," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green

Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 410–415.
[10] S. M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015.
[11] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, Jan. 2017.
[12] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," J. Adv. Res., vol. 5, no. 4, pp. 491–497, Jul. 2014.
[13] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Proceedings of the 52nd Annual Design Automation Conference on - DAC '15, 2015, pp. 1–6.
[14] F. Dalipi and S. Y. Yayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016, pp. 63–68.
[15] C. Lee, L. Zappaterra, Kwanghee Choi, and Hyeong-Ah Choi, "Securing smart home: Technologies, security challenges, and security requirements," in 2014 IEEE Conference on Communications and Network Security, 2014, pp. 67–72.
[16] A. D. Thierer, "The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation," SSRN Electron. J., 2014.
[17] J. S. Rueda-Rueda, "Framework conceptual de ciberseguridad para aplicaciones de Internet de las cosas," Universidad Autónoma de Bucaramanga, 2018.
[18] R. Shirey, "Internet Security Glossary, Version 2." 2007.
[19] C. Cimpanu, "Problems Reappear for IoT Device Owners with Discovery of New DDoS Trojan." 2016.
[20] Malware Must Die, "MMD-0058-2016 - Linux/NyaDrop - a linux MIPS IoT bad news." 2016.
[21] K. S. Subramani, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Hardware-Induced Security & Privacy Vulnerabilities in the Internet of Things." 2016.
[22] CNSS, "National Information Assurance (IA) Glossary." Committee on National Security Systems, 2010.
[23] S. Pastrana, J. Rodriguez-Canseco, and A. Calleja, "ArduWorm: A Functional Malware Targeting Arduino Devices."
[24] K. Hayashi, "IoT Worm Used to Mine Cryptocurrency." 2014.
[25] S. Edwards and I. Profetis, "Hajime: Analysis of a decentralized internet worm for IoT devices." 2016.
[26] CyberX, "Radiation IoT Cyber Security Campaign." 2016.
[27] Trend Micro, "Trend Micro Glossary: Ransomware." 2015.
[28] S. Cobb, "RoT: Ransomware of Things." 2017.
[29] S. Cobb, "Jackware: When connected cars meet ransomware." 2016.
[30] U. Schrott, "Austrian hotel experiences 'ransomware of things attack.'" 2017.
[31] RSA, "2016: Current State of Cybercrime." 2016.
[32] E. Caltum and O. Segal, "Exploitation of IoT devices for Launching Mass-Scale Attack Campaigns." 2016.
[33] Symantec, "2019 Internet Security Threat Report," 2019.
[34] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," 2015.
[35] R. Currie, "Developments in Car Hacking," SANS Inst. InfoSec Read. Room, pp. 1–34, 2016.
[36] S. Lee and S. Kim, "Hacking, surveilling, and deceiving victims on Smart TV," 2013.
[37] T. Fox-Brewster, "How Hacked Cameras Are Helping Launch The Biggest Attacks The Internet Has Ever Seen." Forbes, 2016.
[38] S. Gibbs, "Hackers can hijack Wi-Fi Hello Barbie to spy on your children." The Guardian, 2015.
[39] A. Wang, "'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say," The Washington Post, 2018. [Online]. Available: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/.
[40] J. Leyden, "One Ring to pwn them all: IoT doorbell can reveal your Wi-Fi key." The Register, 2016.
[41] Hewlett Packard Enterprise, "Internet Of things research study." 2015.
[42] ForeScout Technologies, "IoT Enterprise Risk Report," 2016.
[43] Avast, "Avast Smart Home Security Report

2019," 2019.
[44] Beyond Security, "Security Testing the Internet of Things: Dynamic testing (Fuzzing) for IoT security," 2018. [Online]. Available: https://www.beyondsecurity.com/blog/security-testing-the-internet-of-things-iot.
[45] Deloitte, "Legacy and Fielded Medical Device Risks Pose Greatest Cybersecurity Challenge to Connected Device Ecosystem," Press releases, 2017. [Online]. Available: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/legacy-fielded-medical-devices-pose-greatest-cybersecurity-challenge-to-IoT-device-ecosystem.html?id=us:2el:3pr:meddevsec:awa:adv:081517.
[46] ESET Latinoamérica, "ESET Security Report. Latinoamérica 2018.," 2018.
[47] C. Point, "Cyber Attack Trends Analysis. Key Insights to Gear up for in 2019," 2019.
[48] K. Adams, Non-functional Requirements in Systems Analysis and Design. Springer, 2015.
[49] NIST, "ISO/IEC 25010:2011 - Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models." 2011.
[50] L. Chung, B. A. Nixon, E. Yu, and J. Mylopoulos, Non-functional Requirements in Software Engineering. Springer Science & Business Media, 2012.
[51] R. R. Maiti and F. J. Mitropoulos, "Prioritizing Non-Functional Requirements in Agile Software Engineering," in Proceedings of the SouthEast Conference, 2017, pp. 212–214.
[52] S. N. Mahalank, K. B. Malagund, and R. M. Banakar, "Non Functional Requirement Analysis in IoT based smart traffic management system," in 2016 International Conference on Computing Communication Control and automation (ICCUBEA), 2016, pp. 1–6.
[53] F. Brooks, "No Silver Bullet: Essence and Accidents of Software Engineering," IEEE Comput., vol. 20, no. 4, pp. 10–19, 1987.
[54] A. M. Davis, Software Requirements: Objects, Functions and States. Prentice-Hall, Inc, 1993.
[55] K. Beck and Otros, "Manifiesto por el Desarrollo Ágil de Software," agilemanifesto.org, 2001. [Online]. Available: https://agilemanifesto.org/iso/es/manifesto.html.
[56] K. Beck and Otros, "Principios del Manifiesto Ágil," agilemanifesto.org, 2001. [Online]. Available: https://agilemanifesto.org/iso/es/principles.html.
[57] B. Sullivan, "Announcing SDL for Agile Development Methodologies," Microsoft, 2009. [Online]. Available: https://www.microsoft.com/security/blog/2009/11/10/announcing-sdl-for-agile-development-methodologies/.
[58] Microsoft, "Microsoft Security Development Lifecycle (SDL)," microsoft.com, 2019. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/.
[59] Microsoft, "Microsoft Security Development Lifecyble. Version 4.1a.," 2009.
[60] SAFECode, "Practical security stories and security tasks for agile development environments," 2012.
[61] ENISA, "Baseline Security Recommendations for IoT," 2017.