Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema
Internet de las cosas (IoT)

Título
Soluciones tecnológicas, de regulación y gobierno para los desafíos de IoT

Autor: **Diego Alberto Wydler**
Tutora: **Graciela Pataro**

Año de presentación: **2018**
Cohorte 2017

Declaración jurada de origen de los contenidos

Por este medio, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se responsabiliza de que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Diego Alberto Wydler

DNI: 24.800.088

Resumen

“Conectar a todo y a todos” es la propuesta de Internet de la Cosas (*Internet of Things,* IoT por sus siglas en inglés *o IdC en español*), y bajo este principio, avanza desde principios de siglo una revolución tecnológica que augura, entre otros beneficios, la optimización en el uso de los recursos, un aumento marcado en la productividad y un mayor bienestar para la sociedad en su conjunto.

Sin embargo, junto a estos beneficios, surgen numerosos factores negativos que abarcan desde la preocupación por cómo es afectada la privacidad de las personas hasta fallas críticas de seguridad que ponen en peligro no solo a los sistemas de información sino incluso a la integridad física de los usuarios.

El presente trabajo enumera los desafíos y problemáticas que enfrenta Internet de las Cosas y describe diversas soluciones que se han propuesto para resolverlos, mencionando aspectos de seguridad, privacidad, ética, regulación y gobierno.

Finalmente presenta conclusiones incluyendo la evaluación de la aplicación de algunas de las soluciones mencionadas y proponiendo posibles caminos a seguir con el objetivo de asegurar la confianza en IoT.

Palabras clave

Internet de las cosas, IoT, IdC, seguridad IoT, privacidad IoT, confianza, gobierno, ética, regulación.

Índice General

Declaración jurada de origen de los contenidos i

Resumen ii

Nómina de Abreviaturas vi

Introducción 1

1 – Desafíos y problemáticas de IoT 3

1.1 - Seguridad 3

1.1.1 – Restricciones físicas y comportamiento del usuario 3

1.1.2 – Manejo de contraseñas 4

1.1.3 – Heterogeneidad, contexto y pruebas 5

1.1.4 – Escalabilidad y medición de la reputación 6

1.2 – Privacidad 6

1.2.1 – La paradoja de la privacidad y el consentimiento 6

1.2.2 – Fusión de sensores 7

1.2.3 – Anonimización y re-identificación 8

1.2.4 – Privacidad en ciudades inteligentes 8

1.3 - Ética 9

1.3.1 – Ética en las TI 9

1.3.2 – Discriminación a partir de fusión de sensores y Big Data 10

1.3.3 – Delegación de la autonomía y grieta digital 11

1.4 - Regulación, gobierno y estándares 11

1.4.1 – Las dificultadas para gobernar y regular IoT 11

1.4.2 – Falta de estándares y certificaciones 12

1.4.3 – Aplicación de leyes y regulaciones existentes 13

2 – Propuestas de Seguridad y administración de la confianza en IoT 14

2.1 - Edge Computing 14

2.2 – Autenticación, autorización y confianza con EC 16

2.3 - Inteligencia artificial contra los ataques masivos 18
2.3.1 – Swarm Intelligence 18
2.3.2 – Expectativas y advertencias 19
2.4 - Blockchain para seguridad y reputación en IoT 20
2.4.1 – Adaptación para IoT 20
2.4.2 – En busca de un modelo optimizado 23
2.5- Herramientas y dispositivos para el usuario final 24
2.5.1 – El problema de la “fatiga de la seguridad”. 24
2.5.2 – Security-by-design 24
2.5.3 – Estableciendo el nivel de seguridad 25
2.5.4 – Dispositivos encargados de la seguridad 27
2.5.5 – Seguridad en Wi-Fi y WPA3 28
3 – Propuestas para Privacidad, Ética y Gobierno 30
3.1 – Privacidad 30
3.1.1 – Privacy-by-Design 30
3.1.2 – GDPR 32
3.1.3 – Consentimiento en IoT y ciudades inteligentes 33
4.2 - Ética 35
4.2.1 – Educación para la demanda de ética 35
4.2.2 – ¿Ethics-by-design? 36
4.3 – Gobierno, Marcos y Estándares 37
4.3.1 – Marcos para la búsqueda de un gobierno global 37
4.3.2 – Los primeros estándares de IoT 38
Conclusiones 41
Glosario 44
Definiciones de IoT: 44
Confianza y términos relacionados: 44

Tecnologías: 45
Redes: 45
Seguridad: 46
Referencias..... 47

Nómina de Abreviaturas

ETSI: *European Telecommunications Standards Institute*, Instituto Europeo de Normas de Telecomunicaciones

GDPR: *General Data Protection Regulation*, Reglamento General de Protección de Datos (Comisión Europea)

HTTP: *Hypertext transfer protocol,* Protocolo de transferencia de hipertexto

ICANN: *Internet Corporation for Assigned Names and Numbers,* Corporación de Internet para la Asignación de Nombres y Números

IEC: *International Electrotechnical Commission*, Comisión Electrotécnica Internacional

IEEE: *Institute of Electrical and Electronics Engineers*, Instituto de Ingeniería Eléctrica y Electrónica

IERC: *IoT European Research Cluster,* Grupo de Investigación Europeo sobre IoT

IETF: *Internet Engineering Task Force*, Grupo de Trabajo de Ingeniería de Internet

IoT/IdC: *Internet of Things*, Internet de la Cosas

ISO: *International Organization for Standardization*, Organización Internacional de Normalización

NIST: *National Institute of Standards and Technology*, Instituto Nacional de Estándares y Tecnología (Estados Unidos)

PBD: *Privacy-By-Design*, Privacidad desde el diseño

PKI: *Public Key Infrastructure,* Infraestructura de clave pública

TI: Tecnologías de la Información

W3C: *World Wide Web Consortium,* Consorcio WWW

WPA: *Wi-Fi Protected Access*, Acceso Inalámbrico Protegido

Introducción

El avance tan avasallante de Internet de la Cosas ha mantenido por un tiempo en segundo plano a la necesidad de generar confianza en sus componentes. Confiar significa, en el caso de IoT, en primer lugar que las personas perciban que los sistemas proveen niveles aceptables de seguridad y privacidad. Lo mismo puede decirse de los proveedores de servicios, las ciudades y las empresas. Si no están convencidos de que los sistemas IoT son confiables no estarán dispuestos a invertir en ellos o a adoptar soluciones IoT a gran escala. [1, p. 187]

Los desafíos por enfrentar para lograr confianza son considerables.

En el presente trabajo, por un lado, se mencionan numerosos incidentes de seguridad sucedidos recientemente que han hecho tambalear la confianza en IoT, al demostrar que las amenazas sobre la seguridad podrían derribar sistemas enteros y afectar el funcionamiento de servicios críticos en un mundo hiperconectado.

Por otro lado, la evidencia de la manipulación de los datos de las personas obtenidos con o sin el consentimiento de estas hace pensar que se corre el riesgo de que la promesa de “conectar a todos y a todo” derive en la práctica, en “revelar todo de todos” [2, p. 91] y dispara diversos cuestionamientos en relación a comportamientos éticos y la necesidad de regulación efectiva.

No es el propósito del presente trabajo extenderse en la descripción de los dispositivos de IoT y sus características, excepto cuando estos estén involucrados en alguna de las problemáticas o cuando sean parte de alguna solución. Tampoco realizar un catálogo de los múltiples beneficios que IoT provee actualmente o que pueda traer en el futuro, tanto para consumidores, empresas y gobiernos, excepto cuando sea en contraposición a los desafíos generados. Intentar abarcar ambos temas superaría el alcance del trabajo y

por otra parte los mismos están documentados extensivamente en cientos de artículos, libros e informes sobre IoT.

El objetivo del trabajo es establecer claramente los desafíos y problemáticas que enfrenta IoT y avanzar en mostrar soluciones que se hayan propuesto para resolverlos. Para eso se ha dividido en tres capítulos:

En el primero se analizan los desafíos y problemáticas de IoT, mencionando aspectos de seguridad, privacidad, ética, regulación y gobierno.

En los capítulos segundo y tercero se realiza una selección de soluciones que han sido propuestas para afrontar las problemáticas, haciendo hincapié en aquellas que pueden ser utilizadas para resolver el problema de la confianza.

Se incluyen temas de candente actualidad como *Edge Computing*, Inteligencia Artificial y *BlockChain* aplicados a IoT, además de tres muy recientes lanzamientos: la nueva normativa europea para privacidad GDPR que entró en vigor en mayo de 2018, WPA3 para asegurar conexiones *Wi-Fi* lanzado en junio de 2018 y el nuevo estándar de referencia de IoT, el ISO/IEC 30141:2018 publicado en agosto de 2018.

1 – Desafíos y problemáticas de IoT

1.1 - Seguridad

No es sorprendente que Gartner haya identificado a la seguridad como el área más importante dentro del desarrollo de IoT para los años 2017 y 2018, explicando que “IoT introduce un amplio rango de nuevos riesgos y desafíos de seguridad no solo para los dispositivos IoT en sí mismos sino también para sus plataformas, sistemas operativos, comunicaciones y sistemas a los que están conectados” [3].

1.1.1 – Restricciones físicas y comportamiento del usuario

Algunos de estos desafíos de seguridad tienen que ver con las particularidades de las “cosas” de IOT ya que un gran número de dispositivos, especialmente los diseñados para ser utilizados en “hogares inteligentes” o también los *wearables* que pueden obtenerse en tiendas minoristas, poseen procesadores simples y utilizan sistemas operativos básicos que no soportan mecanismos de seguridad complejas. Muchos de ellos deben ser necesariamente pequeños y consumir la menor cantidad de energía posible.

Estas restricciones afectan tanto a la posibilidad de autenticación de los dispositivos como a la seguridad de los datos transmitidos, impidiendo el uso de métodos criptográficos seguros para el intercambio de claves y el cifrado de los flujos de información. Otra característica de muchos dispositivos IoT es que no pueden ser arreglados ni mejorados luego de su venta. Tampoco es contemplada la forma de recibir y aplicar actualizaciones de *firmware* en forma automática.

Adicionalmente la gran mayoría de los dispositivos para el hogar inteligente son fabricados o ensamblados por compañías de productos para el consumidor (*consumer-good companies*) más que por compañías generadoras de hardware o software. Las primeras integran los componentes de estas últimas sin verificar su seguridad, la interoperabilidad entre ellos y la compatibilidad con otros dispositivos. [2]. No puede sorprender entonces que un reciente estudio de la universidad israelí Ben

Gurion [4] sobre este tipo de dispositivos mostró que 14 de los 16 analizados tenían graves fallas de seguridad.

Estas limitaciones y debilidades se contraponen con los hallazgos que indican que nueve de cada diez consumidores entrevistados esperan que la seguridad de IoT se provea como un estándar, en vez de ser algo por lo que deban preocuparse o que deban considerar ellos mismos. Más aún, el 54% de los consumidores ya cuenta con algún dispositivo IoT y sin embargo solo el 14% dice conocer algo sobre la seguridad de esos dispositivos y solo el 45% ha cambiado la contraseña por defecto en todos sus dispositivos [5].

1.1.2 – Manejo de contraseñas

El manejo de contraseñas es en IoT un tema especialmente preocupante. Analicemos por ejemplo el incidente de seguridad más conocido hasta el momento, la interrupción de servicios del proveedor de DNS Dyn provocada a través de un ataque distribuido de denegación de servicio (*DDOS*) generado por millones de dispositivos IoT infectados por el *botnet* Mirai, y que impidió el acceso a los servicios de miles de sitios de Internet, entre ellos 85 de los más grandes incluyendo Twitter, Netflix, Amazon y Paypal, en octubre de 2016.

Más allá de los aspectos técnicos del ataque DDOS sobre servicios de DNS, el aspecto facilitador del problema fue la pobre configuración de contraseñas de los dispositivos IoT que utilizaban componentes del fabricante chino Xiongmai y que permitió la intrusión en los mismos y su posterior infección con Mirai. [6]

Lamentablemente aún en el caso en que los usuarios tuvieran la concientización y la voluntad necesaria para intentar modificar sus contraseñas por algunas más robustas o diferentes a las que son configuradas por defecto, un gran número de dispositivos no facilita realizar dicha operación dado que no cuentan con una interfaz con el usuario o no aplican políticas razonables de contraseña. Sin dejar de mencionar a los que directamente ni siquiera proveen esa opción.

1.1.3 – Heterogeneidad, contexto y pruebas

La interacción entre sistemas y dispositivos heterogéneos es más la norma que la excepción en los sistemas de IoT y, por lo tanto, es extremadamente difícil mantener bajo control a los diferentes componentes de los sistemas. A esto se le suma una dificultad adicional que es el contexto en que funcionan las “cosas”, ya que la automatización de las tecnologías para la seguridad y la privacidad definidas para un contexto específico puede comportarse en forma incorrecta en un contexto diferente o no planificado con la consecuencia de generar vulnerabilidades.

Una demostración de esta dificultad son por ejemplo los incidentes sucedidos en pruebas con vehículos autónomos de Tesla y Uber durante 2017 y 2018, directamente relacionados con problemas de seguridad y confiabilidad de los algoritmos utilizados cuando actuaban en situaciones o contextos no previstos, y que han puesto en un compás de espera aún indeterminado el lanzamiento en forma masiva de estos dispositivos.

La relación entre los dispositivos informáticos y el ambiente físico se encuentra muy presente en IoT. En muchos casos estos sistemas ciber-físicos proveen servicios que impactan directamente en la seguridad de las personas, como por ejemplo en infraestructuras críticas de energía y telecomunicaciones. El desafío en estos casos es “determinar el riesgo relacionado con la implementación de sistemas y dispositivos IoT en esas infraestructuras y la transferencia de vulnerabilidades afectando la seguridad y privacidad de los usuarios” [7, p. 20].

El mismo dinamismo de la tecnología en el caso de IoT dificulta de algún modo la aplicación de mayores niveles de seguridad. La necesidad de liberar los productos en forma rápida para satisfacer las demandas del mercado y superar a otros competidores conspira contra la aplicación de mejores medidas de seguridad, algo que objetivamente encarece y enlentece la producción. Una vez terminado el producto, la necesidad es realizar lanzamientos rápidos, habitualmente sin la adecuada prueba. Desafortunadamente, aun en los casos en los que se contempla un período de prueba razonable para un producto específico, las particularidades de

IoT, en especial la heterogeneidad, hacen que no haya una verdadera noción consensuada de cómo probar redes de cosas.

1.1.4 – Escalabilidad y medición de la reputación

Potenciando todos los anteriores desafíos se encuentra una característica intrínseca de IoT: la necesidad de escalabilidad.

IoT propone integrar a las redes más dispositivos que cualquier otra tecnología. Esto sumado a que los sensores tienen un rol vital en IoT como generadores de información, determina que el gran número de fuentes y la alta frecuencia de envío de información presenten desafíos especiales en relación con el volumen de datos a procesar, filtrar y proteger [8]. Y por otra parte, hace más vulnerables a los sistemas a ataques masivos que intentan interrumpir el servicio o robar información al proveer más vectores de ataque y dificultar el monitoreo y mitigación.

La escalabilidad genera también nuevos desafíos en relación con una precisa medición de la reputación: los sistemas deberán poder medir y utilizar la reputación para, al momento de fusionar grandes cantidades de información de diferentes fuentes, tomar las decisiones correctas de acuerdo con la confiabilidad de la información recibida.

Contrariamente a las estrategias tradicionales que consideraban la reputación únicamente a partir de la confiabilidad de la información, para IoT otros parámetros deben ser considerados y deben poder ser medidos, como por ejemplo confiabilidad de la comunicación, aspectos de seguridad y privacidad y de compatibilidad entre diferentes dispositivos. Este conjunto de mediciones provee un valor mucho más certero y confiable de la reputación de un dispositivo IoT, pero hace mucho más compleja su medición y actualización. [1]

1.2 – Privacidad

1.2.1 – La paradoja de la privacidad y el consentimiento

Mientras que la necesidad de proveer seguridad en los sistemas resulta en la mayoría de los casos evidente, la problemática de privacidad

suele ser más difusa, especialmente para los consumidores. Aún en aquellos que se declaran preocupados por la privacidad, como por ejemplo el 54% de los poseedores de dispositivos IoT que dicen temer que sus datos personales puedan ser comprometidos [5], se suele verificar lo que es comúnmente llamado la “paradoja de la privacidad”. Esta consiste en que, a pesar de mostrarse preocupados por el tema, los consumidores prestan poca o ninguna atención a los términos y condiciones relacionados con la seguridad, aceptándolos sin entenderlos o directamente sin leerlos. [9]

Un problema clave con respecto a la privacidad en IoT es que los dispositivos son diseñados explícitamente para recolectar información al mismo tiempo que pasan desapercibidos y se integran con naturalidad a la experiencia del usuario. Contrariamente, cuando compartimos información en el mundo digital online, por ejemplo, en Facebook o Google, estamos al menos mínimamente conscientes de ingresar al dominio de esa plataforma e incluso usualmente tenemos la oportunidad, aunque sea una vez, de dar o retener el consentimiento a la recolección de datos. En IoT esa consciencia y esa oportunidad de dar consentimiento están predominantemente ausentes por definición. Este problema es ya de por si grave en dispositivos domésticos pero como veremos más adelante, se hace mucho peor en espacios públicos o ciudades inteligentes. [10]

1.2.2 – Fusión de sensores

Uno de los principales beneficios de IoT, la generación de una cantidad y variedad de información como nunca antes estuvo disponible, provista por los sensores incluidos en los dispositivos, puede ser ampliado y optimizado utilizando una técnica llamada fusión de información de sensores (*sensor fusion*). Desafortunadamente, este es también uno de los mayores desafíos en relación con la privacidad.

Por medio de la fusión de sensores los datos obtenidos de un sensor, que vistos individualmente no parecen ser motivo de preocupación, cuando se agregan a los producidos por otros sensores y se sincronizan dentro del

Big Data, empiezan a proveer una variedad de información mucho más compleja y detallada de lo que pudiera haberse previsto.

Muchas compañías comerciales están aplicando técnicas de *Big Data* a información obtenida por IoT para producir inferencias sobre el comportamiento de los consumidores. Por lo tanto, a partir de la fusión de sensores y de su posterior proceso, “información aparentemente inocua compartida para un cierto propósito puede ser utilizada para inferir actividades y comportamientos que el individuo no tenía intención de compartir” [11].

1.2.3 – Anonimización y re-identificación

En principio una solución simple a este problema pareciera ser anonimizar los datos. Habitualmente muchos proveedores de productos para el consumidor aplican esta estrategia, prometiendo a los usuarios que su información solo va a ser compartida con otros luego de ser anonimizada.

Sin embargo, aquí surge un problema habitualmente no contemplado cuando los datos se encuentran aislados, pero que es crítico cuando pueden ser combinados desde distintas fuentes. Es nuevamente la fusión de sensores lo que permite que, al combinarse datos completamente anonimizados, utilizando potentes algoritmos, finalmente pueda inferirse casi con certeza al individuo generador de la información.

Por ejemplo, investigadores del MIT analizaron información de 1,5 millones de usuarios de teléfonos celulares en Europa por 15 meses y encontraron que era relativamente fácil extraer información completa de ubicación perteneciente a un único individuo a partir de un set de datos anonimizado. Para ilustrar el problema mostraron que para hacerlo solo requerían poder localizar a ese usuario en un área cercana a alguna de las antenas transmisoras en cuatro ocasiones el mismo año. Con solo cuatro puntos conocidos, los investigadores pudieron re-identificar al 95% de los usuarios del set de datos. [12]

1.2.4 – Privacidad en ciudades inteligentes

No hay dudas que todos estos problemas se aplican, y en verdad se magnifican, al introducirse el concepto de las ciudades inteligentes (*Smart*

cities). La fusión de sensores es aquí fundamental para proveer beneficios como la optimización de recursos y la provisión de seguridad. Pero a los problemas de privacidad mencionados anteriormente se suma una cuestión particular, que es la propiedad de los datos (*data ownership*) relacionado con el tipo de financiamiento de los proyectos de las ciudades inteligentes.

El financiamiento de las ciudades inteligentes tiende a ser del tipo Participación Público Privada (PPP, *Public-Private Partnership*). Este tipo de arreglos lleva a preguntarnos quien resulta dueño de la información que se produce y procesa en la ciudad inteligente. Dado que el poder de vigilancia, de policía y de respuesta a emergencias son funciones históricamente monopolizadas por el estado, los ciudadanos podrían esperar que los datos sensitivos relacionados con estas tareas sean retenidos por el estado también. Sin embargo, en una ciudad con arreglos del tipo PPP la probabilidad de que la información sea manipulada y quede en manos privadas, por lo menos parcialmente, es muy grande. Incluso, en un caso extremo, una ciudad inteligente puede convertirse en el feudo de información de un monopolio tecnológico o de telecomunicaciones. [10, pp. 7-8]

Otra característica de las ciudades inteligentes es la difusa división del espacio público y el privado. Lo que tradicionalmente era considerado espacio público, las calles, plazas, rutas y transporte ahora se encuentra cubierto por sensores operados por empresas privadas y generando información que será almacenada en bases de datos también privadas. Por otro lado, todo lo que sucede en la privacidad del hogar, una vez que cada dispositivo esté conectado a la red, está a un paso de ser observado, fusionado y analizado en el *Big Data*. Por lo tanto, la distinción “Privado vs. Público”, a nivel del procesamiento y propiedad de los datos pierde su relevancia tradicional.

1.3 - Ética

1.3.1 – Ética en las TI

Una búsqueda en Internet acerca de la problemática de seguridad, y en menor medida de privacidad, en IoT devolverá con toda seguridad cientos

de artículos. Sin embargo, es mucho más difícil encontrar menciones a la necesidad de fomentar y exigir comportamientos éticos en la industria. Esto sucede a pesar de que muchas decisiones que involucran seguridad y privacidad podrían ser optimizadas si fueran evaluadas en primer lugar por criterios éticos. Al fin y al cabo, debería ser evidente que si el diseño y la fabricación de dispositivos, la provisión de servicios y el mismo gobierno de la tecnología no se realizan de acuerdo con normas éticas universalmente aceptadas, es muy difícil que pueda confiarse en que se cumplan otras características.

A diferencia del campo de las ciencias de la vida o biológicas, en el campo de la tecnología informática no había surgido, hasta recientemente, una necesidad de institucionalizar el acercamiento a la ética. Solo en los últimos tiempos se ha buscado un rol específico para la misma, en los sectores con un nivel percibido de intrusión más elevado, como por ejemplo la robótica y los dispositivos autónomos. Está siendo ampliamente reconocido que las tecnologías informáticas, cuando funcionan como habilitadores tecnológicos y especialmente cuando interactúan con otros campos de la tecnología, introducen profundas preocupaciones relacionadas con la ética ya que pueden tener el potencial de reformular muchas capacidades y habilidades humanas en maneras que son solo parcialmente pronosticables y muchas veces poco controlables. [7]

1.3.2 – Discriminación a partir de fusión de sensores y Big Data

IoT, por su parte, no hace más que magnificar los desafíos relativos al conocimiento y control individual de los procesos tecnológicos y de las consecuencias para la sociedad, emergentes de las acciones realizadas a través de la tecnología. Por ejemplo, uno de los más claros beneficios que brinda IoT en conjunto con la fusión de sensores y *Big Data*, la posibilidad de diferenciar a los consumidores con más precisión que nunca antes, también puede generar nuevas formas de discriminación. Y en muchos casos esta discriminación sería mucho más difícil de detectar que en otros contextos.

Empleadores, aseguradoras y vendedores por nombrar solo a algunos interesados, podrían utilizar los millones de datos generados por

IoT, agregados en el *Big Data* y convenientemente analizados para realizar inferencias sobre los individuos y aplicar discriminación en base a nivel social y económico y, avanzando un poco más, en base a etnicidad, edad y género, incluso en formas tan sutiles que serían prácticamente indetectables. [2]

1.3.3 – Delegación de la autonomía y grieta digital

Y en campos donde IoT promete grandes beneficios, por ejemplo, en el cuidado de adultos mayores, se advierten dilemas éticos relacionados con la delegación de la autonomía humana y el aislamiento. Con el avance de IoT y su masificación, voluntariamente o no las personas deberán confiar en los dispositivos para realizar las tareas para las cuales la tecnología esté para ayudarle. Esa delegación sumada a la ubicuidad de IoT y a la capacidad de pasar desapercibidos de la mayor parte de los dispositivos contribuyen a crear una situación en la que “si son advertidos estos artefactos actuarán en nombre del usuario, pero si no son advertidos los dispositivos podrán actuar a favor de los intereses e intención de los desarrolladores”. [7, p. 21]

Otro aspecto relacionado con la ética e IoT, es también el de la grieta digital *(digital divide).* Tradicionalmente esta se refería a la diferencia de oportunidades en el acceso a las tecnologías que determina que aquellos que no puedan capacitarse y adaptarse a las mismas, progresivamente se vuelven más inhábiles y excluidos. Con la irrupción de IoT y otras tecnologías relacionadas puede comenzar a darse una nueva situación en donde únicamente un grupo privilegiado, por conocimientos o por su posición favorecida, puede protegerse de los abusos y elegir entre las opciones tecnológicas o incluso sustraerse a su influencia de ser necesario. [7]

1.4 - Regulación, gobierno y estándares

1.4.1 – Las dificultadas para gobernar y regular IoT

Uno de los primeros inconvenientes que se advierten al comenzar a abordar la temática de Internet de la Cosas es la falta de una definición

concreta, única y consensuada a nivel global. Esta dificultad, que a primera vista puede parecer poco relevante, nos adelanta, sin embargo, la complejidad inherente para alcanzar consensos sobre diferentes aspectos de gobierno, regulación y estándares en IoT.

Para sistemas que se consideran críticos a nivel seguridad, tanto la regulación como algún tipo de gobierno son usualmente aceptados y aun esperados. Sin embargo, esas tecnologías han evolucionado más lentamente, requirieron en general una mayor inversión que IoT y sus componentes son habitualmente más homogéneos, por lo que desarrollar regulaciones para IoT ha sido hasta el momento muy dificultoso. Mientras que la tecnología que habilita a IoT es global y evoluciona a cada momento las regulaciones son mayormente locales y avanzan a paso lento y dificultoso [1, p. 215].

A su vez, el gobierno está considerado como una espada de doble filo, “porque por un lado puede ofrecer estabilidad y soporte a las decisiones, pero también puede ser excesivo y resultar en un ambiente sobre controlado”. [7, pp. 13-14]. Por lo tanto, un desafío adicional es determinar cómo aplicar regulación y gobierno a IoT, sin afectar a la creatividad y dinamismo de la industria.

1.4.2 – Falta de estándares y certificaciones

Lo mismo puede decirse del desarrollo de estándares propios y certificaciones. Al ser IoT una tecnología relativamente nueva hasta muy recientemente no contaba con estándares aceptados globalmente, ni certificaciones reconocidas.

En el capítulo sobre soluciones se mencionan varios proyectos financiados por los gobiernos para generar nuevos estándares para IoT y el reciente lanzamiento de un estándar ISO/IEC, sin embargo, hasta el momento en general se suelen aplicar estándares tomados de otras tecnologías sobre las que se basa IoT, como es el caso de redes de información. Y también, como ha sucedido con otras tecnologías emergentes, “la comunidad de IoT tiende mucho más a utilizar estándares de facto que prescriptivos” [8, p. 17].

1.4.3 – Aplicación de leyes y regulaciones existentes

En su estudio sobre Regulación de Internet de la Cosas [2], Peppet menciona los problemas de la falta de preparación de las leyes actuales de Estados Unidos para enfrentar los desafíos de IoT y los relaciona principalmente con las problemáticas de discriminación, privacidad y consentimiento. En la sección anterior de ética ya hemos introducido el concepto de discriminación y los problemas relacionados con la posibilidad de una diferenciación extrema de los usuarios que sea indetectable y difícilmente abarcable por las actuales leyes antidiscriminación.

Con respecto a privacidad Peppet advierte que las leyes y regulaciones aun cuando existan pueden ser difíciles de adaptar a las características y nuevos desafíos de IoT. Veamos un ejemplo que menciona en relación con una problemática ya mencionada de privacidad y el manejo de datos personales: Hasta el momento la gran mayoría de las leyes distinguen un cierto tipo de información como “información personal para la identificación” (IPI), usualmente definida por el nombre del individuo, el domicilio, número de identificación impositivo y teléfono, separándola de cualquier otra información presumiblemente no utilizable para revelar la identidad.

La transferencia y uso de este último tipo de información, la que en principio no es utilizable para revelar identidad, no se encuentra entonces limitada, ni su seguridad protegida al no ser considerada IPI. Sin embargo, el concepto ya explicado de la relativa facilidad de re-identificación con la asistencia de la fusión de sensores y de algoritmos especialmente diseñados para tal fin, significaría que toda la información generada por IoT podría ser considerada como IPI. Lo que conlleva tanto un problema práctico como también de redefinición de las leyes actuales de protección de los datos personales.

2 – Propuestas de Seguridad y administración de la confianza en IoT

Por las ya mencionadas características particulares de IoT especialmente las relacionadas con escalabilidad y heterogeneidad las soluciones que pretendan proveer confianza y ser efectivas en asegurar IoT no pueden ser unidimensionales, sino que deben tener en cuenta el contexto y las particularidades de la tecnología, por un lado las relacionadas con la escasez de recursos computacionales y la necesidad de baja latencia que demandan las conexiones en tiempo real y, por otro lado las amenazas de ataques masivos que superen la capacidad de monitoreo y mitigación tradicionales.

Veremos que para enfrentar el primer grupo de desafíos la mayor parte de las soluciones más recientes se apoya en *Edge Computing* y que para enfrentar los ataques masivos se proponen soluciones de inteligencia artificial.

2.1 - Edge Computing

Edge Computing (EC) [13] es un concepto vital para dar soporte y seguridad a IoT y se basa en la idea de traer el procesamiento de la información cerca de donde se genera, transmitiéndola a la nube solo cuando sea necesario.

Un ejemplo claro es un automóvil autónomo: toda la información recabada por los miles de sensores con que está equipado es procesada por la computadora local del vehículo, que toma decisiones en tiempo real en base a la misma. Esta misma computadora o uno de sus subcomponentes tienen habitualmente la función de puerta de enlace y solo envía y recibe de la nube y de otros dispositivos la información relevante.

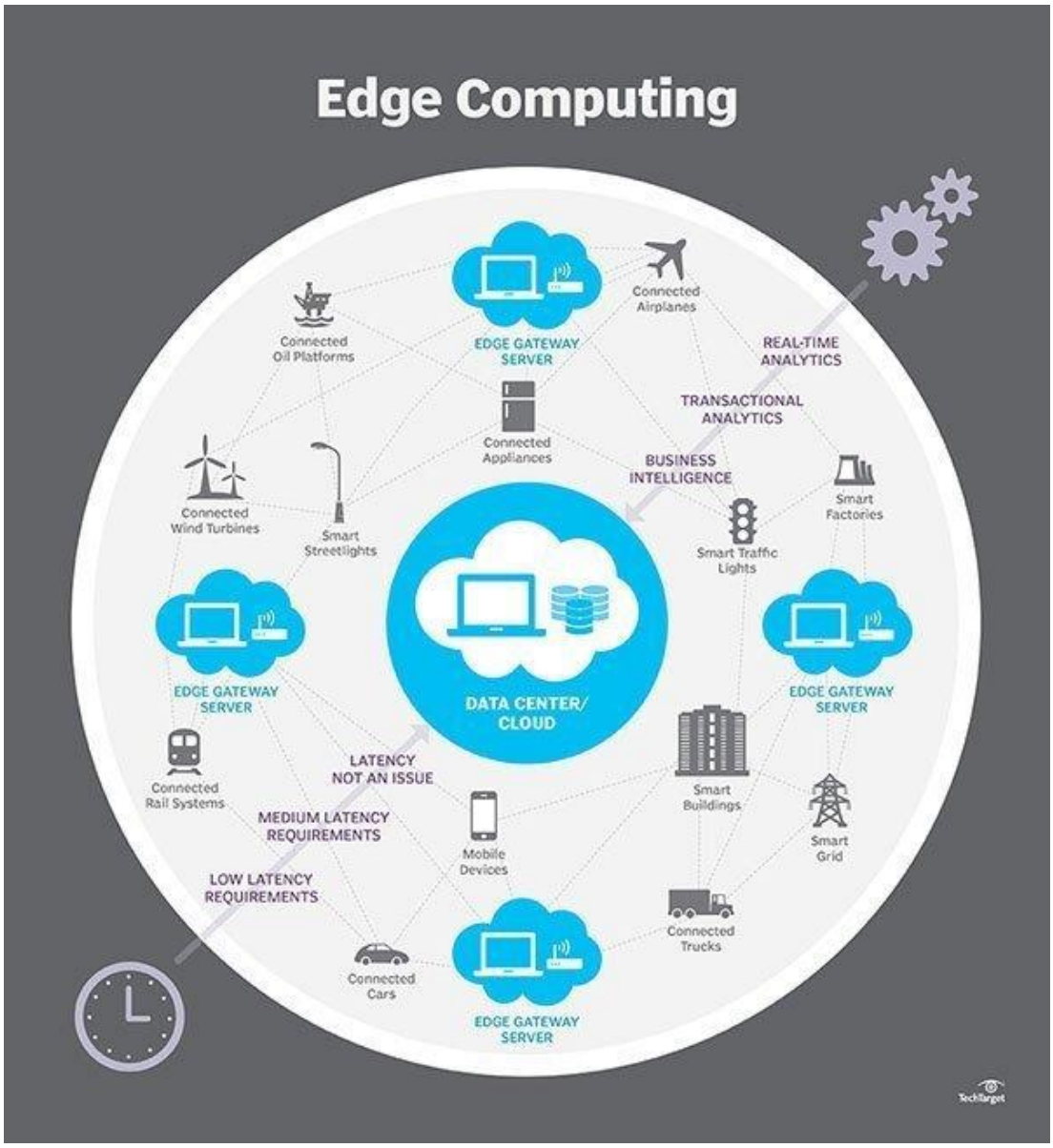


Figura 1 – El tipo y objetivo de procesamiento de la información y los requerimientos de latencia determinan cuando es conveniente transferir la información a la nube o procesarla en el "Edge" [13]

En un entorno IoT *Edge Computing*[1] provee las siguientes ventajas en términos de seguridad [14, p. 30]:

1. la proximidad de EC permite interacción en tiempo real con los dispositivos IoT, con menor necesidad de utilización de recursos, latencia predecible y sincronización asegurada.

[1] De ahora en más se la referencia como "EC"

2. EC permite reducir la carga y cuellos de botella sobre las redes al limitar la transferencia de datos a la nube.
3. EC tiene más información del contexto en relación con la seguridad, sirviendo mejor a entidades heterogéneas.

Por otra parte, y ya más en relación con la privacidad, la información sensible y privada puede mantenerse en el *Edge* en vez de ser enviada a la nube.

Los mismos grandes jugadores que dominan la computación en la nube (Amazon, Microsoft y Google) se han lanzado a conquistar EC previendo invertir miles de millones de dólares para extender su influencia desde la nube hacia los dispositivos Edge.

Por el lado del hardware, HP planea invertir cuatro mil millones de dólares en EC en los próximos años y ya presentó sus primeros equipos Edge Systems [2] que permiten a instalaciones industriales contar con procesamiento de nivel datacenter y administrar inteligentemente los dispositivos conectados localmente sin depender de una conectividad remota permanente. [15]

2.2 – Autenticación, autorización y confianza con EC

Existen numerosas propuestas para brindar seguridad y confianza a IoT utilizando EC, por ejemplo, la arquitectura de red llamada Auth [14, p. 30], que utiliza autenticación y autorización en entidades locales y que puede ser implementada en dispositivos *Edge* de todo tipo. Auth provee servicios de autorización a entidades registradas localmente (en este caso dispositivos IoT) mientras mantiene relaciones de confianza con otras entidades Auth globales.

[2] https://www.hpe.com/us/en/servers/edgeline-iot-systems.html

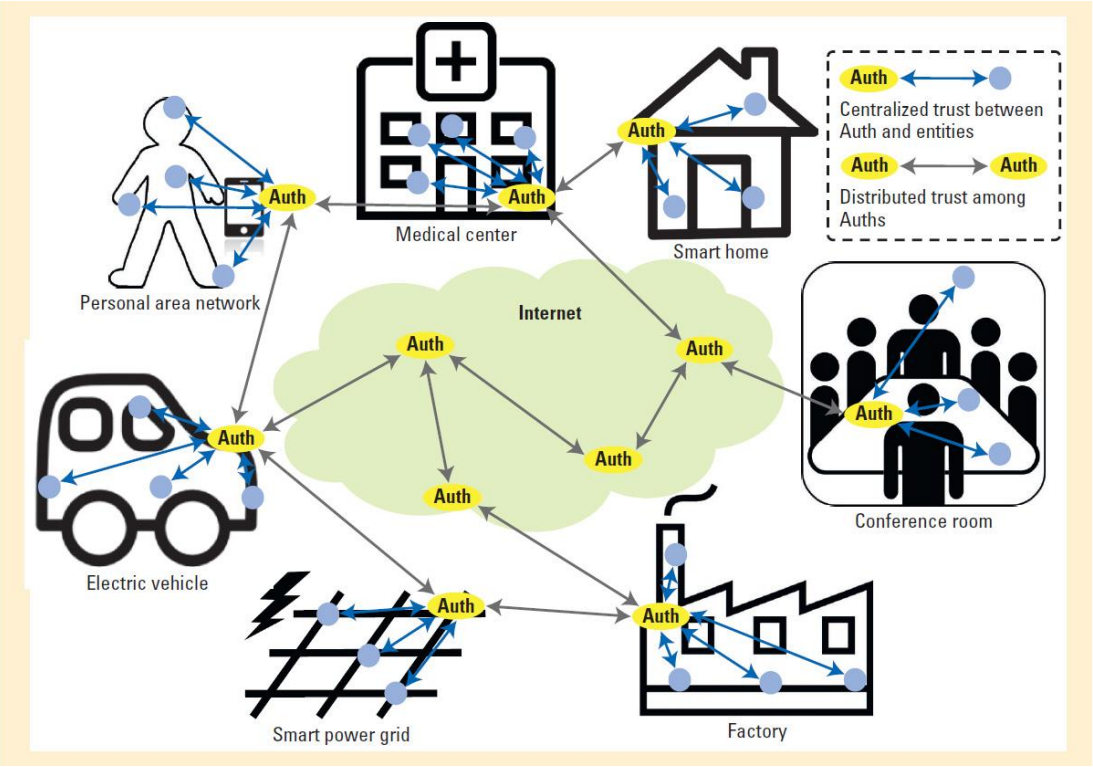


Figura 2 – El esquema localmente centralizado, globalmente distribuido de Auth [14]

La entidad administradora local de Auth administra las credenciales y políticas de accesos asignadas a cada entidad local registrada en su base de datos y distribuye claves de sesión válidas únicamente para cada distinto tipo de acceso. Permite a los dispositivos con limitación de recursos mantener las claves de sesión en cache reduciendo la necesidad de operaciones criptográficas que consumen procesamiento y energía.

La relación de confianza de Auth está distribuida globalmente. La comunicación entre entidades utiliza HTTPS basado en certificados administrados de una forma que es similar a la de Open PGP, confiando en otras entidades Auth para firmar los certificados. A diferencia de PKI, Auth no requiere un nombre de dominio o una dirección fija de red para los certificados, lo que habilita a dispositivos Edge sin esas características a utilizar Auth. Manejar la confianza en forma distribuida hace al sistema más robusto, limitando el impacto de ataques aun cuando alguna entidad haya sido comprometida. También es posible continuar funcionando localmente aun cuando sea necesario desconectar por cualquier razón el ambiente local de Internet, una de las ventajas de EC.

Según los autores: “Los esquemas de seguridad basados únicamente en la confianza centralizada pueden convertirse en un único punto de falla además de no aprovechar los dispositivos de tipo *Edge* cada vez más numerosos. Por otro lado, una solución completamente distribuida no sería práctica debido a la sobrecarga sobre cada dispositivo individual de IoT, especialmente aquellos con restricción de recursos.” [14, p. 32] Por lo tanto, se propone un esquema de infraestructura de autenticación y autorización localmente centralizado y globalmente distribuido, lo que es obtenible implementando entidades *Edge* de autorización local soportadas por la confianza globalmente distribuida entre otras entidades.

2.3 - Inteligencia artificial contra los ataques masivos

El siguiente gran desafío por enfrentar es el que se genera debido a que las aplicaciones y servicios basados en IoT e interconectados a gran escala, son vulnerables a ataques masivos que intentan interrumpir el servicio o robar información. Para poder combatir estos ataques masivos, en donde formas de monitoreo y mitigación tradicionales son de aplicación difícil o imposible, una alternativa son las soluciones de seguridad basadas en la inteligencia artificial.

2.3.1 – Swarm Intelligence

Por ejemplo, la llamada “Inteligencia del enjambre” (*Swarm Intelligence*)[3] es una de estas áreas de investigación tecnológica, que puede inspirar el diseño de nuevas soluciones para las problemáticas de seguridad de IoT. La IE es particularmente importante teniendo en cuenta las restricciones ya mencionadas de la mayoría de los dispositivos de IoT incluyendo memoria, recursos computacionales y conectividad limitadas.

La IE es un subcampo de la inteligencia artificial, estudia la inteligencia emergente de un grupo de agentes basado en el comportamiento social que puede ser observado en la naturaleza, como en colonias de hormigas, bandadas de aves, cardúmenes de peces o enjambres de abejas, donde un número de individuos con capacidades propias limitadas son capaces en conjunto de producir soluciones

[3] De ahora en más se la referencia como “IE”

inteligentes para problemas complejos. La reacción de estos grupos ante amenazas es uno de los ejemplos más concretos y para el cual IoT puede inspirarse.

Aunque la mayoría de los dispositivos IoT tengan capacidad limitada para implementar medidas de seguridad es claro que un grupo de objetos IoT tendrá más recursos colectivos para procesar una mayor cantidad de información, de forma tal de prevenir, detectar y reaccionar antes amenazas y a su vez tomar decisiones basadas en la información obtenida. La idea es proveer a los dispositivos de mecanismos a través de los cuales los recursos e inteligencia individuales puedan agruparse y auto protegerse. [1]

El uso de la IE puede extenderse a la auto-optimización, de forma que los objetos agrupados puedan cooperar y compartir recursos eficientemente. Esto significa que sus capacidades pueden ser usadas en muchas aplicaciones de IoT, como la localización del nodo óptimo, control de cobertura óptima y una gran cantidad de ruteos inteligentes. Se relaciona también con la disyuntiva de local-distribuido-centralizado mencionado anteriormente para *Edge Computing*, de forma que agrupaciones locales de objetos más simples se ocupan de los problemas distribuyendo la inteligencia localmente y transfiriendo a una inteligencia central problemas más complejos.

La auto-recuperación y la tolerancia a fallas basada en IE implica que el grupo puede generar automáticamente alternativas de transporte de datos, para evitar que un ataque genere la pérdida de datos o impida su transmisión.

2.3.2 – Expectativas y advertencias

En los últimos estudios conocidos en el ámbito corporativo, las respuestas de encargados de seguridad en diferentes industrias muestran que los ataques masivos son la mayor preocupación: en 2018 el 82% (cuando era 76% en 2017) estima que en los próximos dos años sucederá algún incidente relacionado a *DDOS* y dispositivos IoT y el 94% considera que puede ser de dimensiones “catastróficas” [16]. Esto demuestra que

poder implementar soluciones de inteligencia artificial que permitan contrarrestarlas será sin duda cada vez más demandado.

Numerosos proveedores se han lanzado a producir soluciones de Inteligencia Artificial para dispositivos, plataformas y servicios de EC como por ejemplo el fabricante de chips NVIDIA, que en 2017 lanzó su módulo de AI Edge Jetson TX2 [4] para dispositivos IoT que asegura "redefinir las posibilidades de la extensión de inteligencia artificial avanzada desde la nube hasta el *Edge*" [17].

De todos modos, hay que destacar que tanto la Inteligencia de Enjambre como otras aplicaciones de inteligencia artificial para IoT son relativamente recientes y algunos investigadores han advertido contra la tendencia de una adopción masiva sin analizar posibles debilidades en relación con la seguridad. En particular las que puedan generar intrusiones en los sistemas que de una forma maliciosa intenten causar adaptaciones y reacciones inesperadas en grupos de dispositivos. Es decir, existe el riesgo de que IE pueda combatir con éxito los ataques masivos externos, pero sucumba ante una manipulación interna que logre modificar en forma maliciosa los comportamientos adaptativos del grupo. [18]

2.4 - Blockchain para seguridad y reputación en IoT

Si hay en la actualidad alguna tecnología que genere aún más expectativas que IoT esa es claramente el *Blockchain*. El *Blockchain*, relacionado originalmente con las criptomonedas, encuentra en los últimos tiempos numerosas aplicaciones para asegurar la confianza entre partes.

2.4.1 – Adaptación para IoT

El *BlockChain* [5] utiliza un mecanismo de consensos para incluir y validar nuevas transacciones, necesario para impedir que se agreguen bloques ilegítimos, y el más común es el *Proof-of-Work* utilizado por ejemplo por las dos cripto-monedas más populares: Bitcoin y Ethereum.

[4] https://devblogs.nvidia.com/jetson-tx2-delivers-twice-intelligence-edge/
[5] De ahora en más se lo referencia como "BC"

Este método, a pesar de ser sumamente efectivo para impedir alteraciones al BC, tiene dos problemas que son inherentes al tipo de trabajo matemático que requiere para su resolución. El primero es la cantidad de energía que insume la alta utilización de los recursos computacionales, no solo por el "minero" que logra agregar un nuevo bloque, sino por todos los que "compiten" simultáneamente realizando los mismos cálculos. El segundo es la alta latencia requerida para confirmar cada transacción y agregarla al BC.

Es por eso por lo que los trabajos que proponen al BC como solución a algunas de las problemáticas de IoT reemplazan al Proof-of-Work por otra forma de consenso o validación para el ingreso de nuevas transacciones.

Una de estas propuestas es la presentada en "Blockchain for IoT security and privacy" de 2017 [19] que además de eliminar al Proof-of-Work como herramienta de consenso también propone la utilización de los conceptos de *Edge computing* para solucionar otro problema que plantea *Blockchain* para los sistemas IoT: la baja adaptación a la escalabilidad que representa distribuir las transacciones y los bloques a toda la red.

En esta solución los objetos están agrupados en *clusters* y cada grupo tiene designado un *Cluster Head*[6] (CH). Cada CH, que puede ser un *gateway* con suficiente potencia computacional o un dispositivo separado, mantiene un *Blockchain* público para llevar registro de las transacciones tanto entrantes como salientes y actúa como "minero" local.

[6] De ahora en más se lo referencia como "CH".

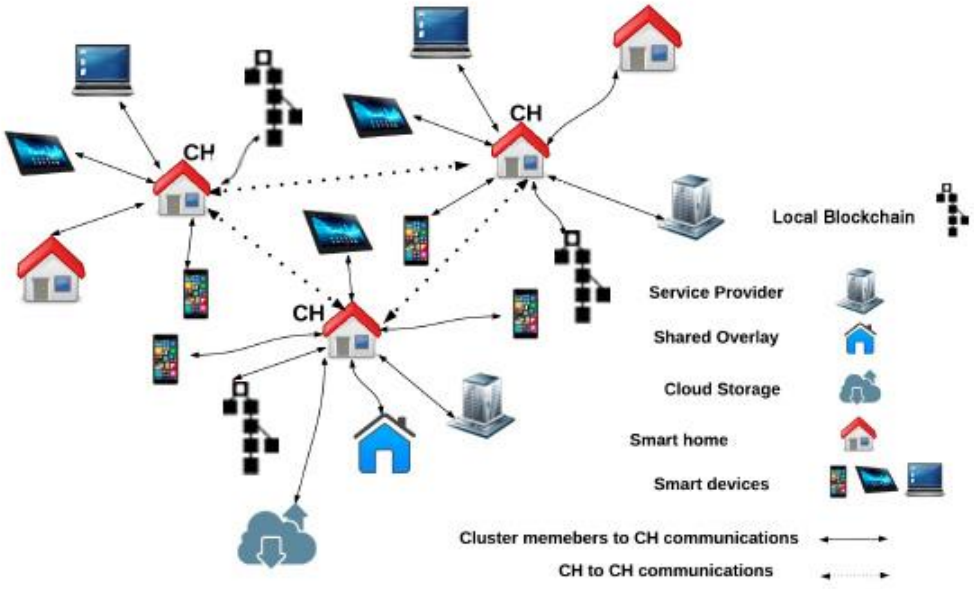
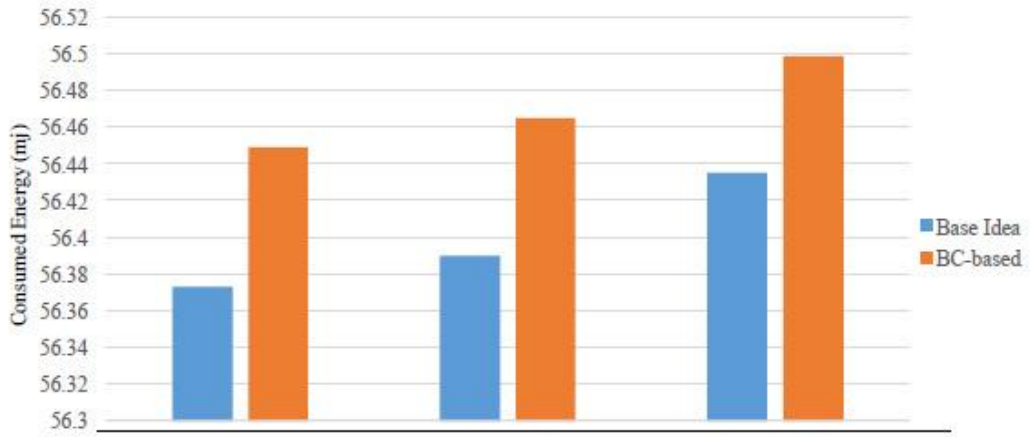


Figura 3 – Diagrama de la estructura propuesta (adaptada de Dorri et al. [19])

Luego de generar una transacción de tipo “génesis” para agregar dispositivos, y en forma similar a la solución presentada en 2.4, el CH realiza la autenticación y autorización local asignando claves compartidas a los objetos para que puedan interactuar directamente entre ellos dentro del *cluster*. Todas las transacciones hacia afuera y hacia adentro del *cluster* son analizadas por el CH e ingresadas al BC y se utiliza confianza distribuida entre los CH, que obtienen su reputación a través de la verificación de las transacciones ingresadas en los BC que están disponibles para toda la red.

Aunque es efectivo como forma de calcular la reputación de las entidades y asegurar las transacciones, desafortunadamente analizando los cálculos de los propios autores, se advierte que el *overhead* generado por la verificación de las transacciones, aun para este BC “liviano”, lo hace difícilmente aplicable para un gran número de dispositivos con capacidades de procesamiento limitado.



	Access			Store-Query			Store-Period		
	CPU	Tx	Lx	CPU	Tx	Lx	CPU	Tx	Lx
Base Idea	0.0103	0.0102	56.3489	0.0117	0.0357	56.3393	0.0121	0.0549	56.3645
BC-based	0.0127	0.0834	56.3496	0.0132	0.1106	56.3379	0.0133	0.1166	56.3657

Figura 4 – El *overhead* a nivel energético propuesto por esta solución no es trivial para muchos dispositivos IoT con limitaciones de consumo energético. [19]

2.4.2 – En busca de un modelo optimizado

Es por eso por lo que una presentación posterior [20] los mismos autores proponen un sistema optimizado que permite reducir el *overhead* que genera la verificación de los bloques de transacciones.

Se propone que la proporción de transacciones a ser verificadas cambie como una función del número de bloques previamente verificados exitosamente para un cierto CH. Una cierta cantidad mínima de transacciones deben continuar siendo verificadas aún en el caso de máxima confianza para protegerse ante el caso de que un CH haya sido comprometido recientemente.

El BC aplicado de esta forma resuelve muchas de las problemáticas de IoT incluyendo autenticación, autorización y medición de la reputación, e incluso protege contra la utilización de dispositivos infectados dentro del *cluster* para realizar ataques de *DDOS* ya que, aún en el caso en que estuvieran infectados, el CH no permitiría el paso de transacciones no verificadas hacia el exterior del *cluster*.

El mayor problema aun sin solución para esta propuesta es un ataque de denegación de servicios a nivel de *clusters*, ya que el intento de conexión

por parte de múltiples CH maliciosos puede generar un bloqueo al superarse la capacidad de verificación de las transacciones.

2.5- Herramientas y dispositivos para el usuario final

2.5.1 – El problema de la “fatiga de la seguridad”.

Antes de avanzar con las soluciones concretas de esta sección es preciso introducir un debate que intenta determinar si resulta útil y factible capacitar a los usuarios para que pueda tomar decisiones inteligentes y realizar acciones con respecto a la seguridad o si solo debe ponerse el foco en lograr que las empresas incluyan a la seguridad en sus procesos de desarrollo y provean al mercado productos probados, de simple configuración y actualizables en forma automática. Apoyando esta última postura se encuentran estudios como el del 2016 del NIST [21] que demuestran que la mayoría de los usuarios promedio de sistemas de información sufre lo que se denomina “fatiga de la seguridad”.

Esta sensación surge cuando los usuarios comienzan a sentirse sobrepasados y bombardeados por las constantes alertas y recomendaciones de seguridad. Al sentir que se les demanda tomar más decisiones relacionadas con la seguridad de las que pueden manejar comienzan a experimentar esta fatiga de seguridad, que los lleva finalmente a albergar sentimientos de resignación y pérdida de control. Estas reacciones los puede llevar tanto a evitar tomar decisiones como a elegir las opciones más fáciles dentro de un grupo de alternativas y a comportarse impulsivamente, por lo que terminan ignorando completamente las políticas y recomendaciones de seguridad.

2.5.2 – Security-by-design

Teniendo en cuenta lo anterior sería ideal que las herramientas o soluciones de seguridad disponibles para el consumidor le demandaran la menor cantidad de esfuerzo y que pudieran ser utilizadas por usuarios con la mínima capacitación. Al fin y al cabo, como se mencionó en el primer capítulo los estudios más recientes indican que **“**nueve de cada diez consumidores entrevistados, esperan que la seguridad de IoT se provea

como un estándar, en vez de ser algo por lo que deban preocuparse o que deban considerar ellos mismos" [5].

Idealmente, según esta corriente de pensamiento, debería asegurarse que la industria incluya "seguridad por diseño" (*security-by-design*) en las soluciones IoT desde la fase de concepto y sea integrada a nivel de hardware, firmware, software y servicio, sin contar con que el usuario pueda o quiera aplicar otras medidas por sí mismo.

A su vez, "las aplicaciones IoT deberían embeber mecanismos para monitorear continuamente la seguridad y mantenerse por delante de las amenazas que supone el interactuar con otros dispositivos y ambientes", actualizándose en forma autónoma. La confianza de los usuarios solo se obtendrá entonces cuando se perciba que los sistemas cuentan con la capacidad de proveer seguridad, protejan la privacidad y puedan responder en forma autónoma a incidentes. [1, p. 97]

2.5.3 – Estableciendo el nivel de seguridad

Sin embargo, aunque no se les exija mayor capacitación o atención, podría ser útil para los usuarios poder verificar el nivel de seguridad de los dispositivos IoT antes de comprarlos. En ese sentido, en su tesis de Maestría en Seguridad Informática de la Universidad de Buenos Aires [22] Diana Fernández Sánchez propone un diseño lógico de una aplicación para definir el nivel de seguridad de un dispositivo IoT.

El objetivo de la aplicación es facilitar "a los usuarios el diagnóstico de problemas típicos de seguridad para alertar a las entidades responsables, sin la necesidad de contar con conocimientos profundos sobre el tema".

La aplicación, en primer lugar, en base a un número de serie del dispositivo IoT ingresado por el usuario o una combinación de parámetros de búsqueda, consulta con una base datos de vulnerabilidades conocidas públicamente (SHODAN[7]).

Luego, utilizando los datos obtenidos, realiza una serie de pruebas para encontrar factores que puedan comprometer la seguridad del

[7] https://www.shodan.io/

dispositivo. Entre otros, verifica la utilización de credenciales por defecto, comunicaciones no cifradas y puertos abiertos innecesariamente utilizando scripts en lenguaje de programación Python y utilidades de la distribución Security Onion de Linux [8].

Finalmente realiza un escaneo de vulnerabilidades del portal de gestión de dispositivo utilizando el escáner VEGA además de cotejar las mismas en motores de búsqueda públicos.

Aunque la aplicación descripta sin duda sería útil para encontrar fallas conocidas una vez que se ha logrado identificar al dispositivo, podría ser criticada por adolecer de dos problemas de usabilidad. Por un lado, para la enorme mayoría de los usuarios no expertos será muy difícil realizar exitosamente una búsqueda de un producto genérico en SHODAN utilizando la interfaz que propone la aplicación (figura 5), un sitio que además requiere registrarse para utilizar eficazmente su API.

Figura 5 – Interfaz propuesta de la aplicación para definir el nivel de seguridad de un dispositivo IoT [22]

Por otro lado, el análisis y comprensión de los resultados de este tipo de búsquedas puede resultar dificultoso y frustrante para quienes no estén familiarizados con el léxico de seguridad. En resumen, podría ser reorientada exitosamente al usuario experto, que desee unificar en una sola

[8] https://securityonion.net/

aplicación una multiplicidad de búsquedas de seguridad sobre el dispositivo IoT. Más aún si fuera agregada la funcionalidad de almacenar los datos de los dispositivos encontrados y alertar al usuario si se descubrieran vulnerabilidades en forma posterior relacionadas con esos dispositivos..

Para facilitarle al usuario la tarea de elegir productos IoT seguros, existen propuestas de informar el nivel de seguridad de los dispositivos utilizando rótulos con categorías, como sucede actualmente con las especificaciones de consumo de energía o con los rótulos nutricionales. Por ejemplo, se podría graduar de la A a la F el nivel de seguridad y obligar a mostrar la calificación alcanzada por el producto prominentemente como se hace en el caso del consumo de la energía con los electrodomésticos.

En una propuesta similar el Instituto de Estándares Británico (BSI) y la compañía Digital Catapult [1] definieron una especificación que indica al consumidor la seguridad y la privacidad de los dispositivos a través de una serie de íconos similares a los utilizados para las advertencias nutricionales.

El desafío para este tipo de soluciones es seleccionar a nivel global o regional qué organización será la que evalúe los productos y en base a qué estándar.

2.5.4 – Dispositivos encargados de la seguridad

Avanzando un poco más en facilitarle el control de la seguridad al usuario final, o incluso relevarlo de tener que realizar dicho control, se encuentra disponible en el mercado un gran número de dispositivos, que pueden utilizarse como puerta de enlace de la conexión a internet del hogar o como complemento de esta, y se encargan de la protección de la red y los dispositivos IoT conectados. Entre los más populares podemos nombrar a F-Secure Sense [9], Dojo by Bullguard [10] , Bit-Defender BOX2 [11] y CUJO [12]. Estos dispositivos, como mínimo, filtran el tráfico de internet, monitorean a todos los dispositivos conectados, mantienen una base de datos de

[9] https://www.f-secure.com/en/web/home_global/sense
[10] https://dojo.bullguard.com/
[11] https://www.bitdefender.com/box/
[12] https://www.getcujo.com/

amenazas actualizada en forma permanente y alertan al usuario de cualquier anomalía.

Cada uno ofrece características adicionales de protección de la seguridad y privacidad. En todos los casos intentan que la configuración inicial sea mínima y que las notificaciones y alertas básicas sean de fácil comprensión para el usuario final. Para los usuarios con un nivel mayor de conocimiento todos estos equipos proveen aplicaciones para teléfonos inteligentes, desde las cuales se puede monitorear y configurar la actividad de la red y los dispositivos.

2.5.5 – Seguridad en Wi-Fi y WPA3

Como puede advertirse, muchas de estas soluciones se utilizan en conjunto con la puerta de enlace a Internet, que habitualmente en un hogar es el *router Wi-Fi*. Es por eso por lo que debe asegurarse que las características de seguridad de estos mismos equipos y también su configuración no expongan alguna vulnerabilidad que pueda ser explotada para tomar control de la red interna.

Casi todas las problemáticas de seguridad de los dispositivos IoT se aplican también a los *router Wi-Fi*. Los usuarios suelen utilizar contraseñas débiles o no modificar las ingresadas por defecto por el personal del proveedor de servicio que, en la mayoría de los casos, por lo menos en Argentina, suelen ser el número de identificación del cliente o su número de documento con alguna ligera modificación. Sumado a debilidades inherentes a WPA2 que permiten interceptar las claves encriptadas, esto facilita enormemente los ataques de diccionario offline.

A su vez, el usuario final usualmente no tiene el conocimiento o disposición para instalar actualizaciones ante la detección de vulnerabilidades conocidas como la que afecta a dispositivos que utilizan el protocolo de seguridad WPA2 revelada 2017 [23] y que permite, en redes Wi-Fi no emparchadas, descifrar datos previamente encriptados, y en casos extremos, tomar el control de la red, con una técnica de reinstalación de claves.

Para proveer soluciones a algunos de estos problemas el 25 de junio de 2018 la Wi-Fi Alliance anunció el lanzamiento de WPA3 [24]. Además de solucionar vulnerabilidades conocidas de WPA2, las dos características principales en relación a IoT son las siguientes: el nuevo WPA3-Personal toma en cuenta y remedia la tendencia de los usuarios a utilizar contraseñas débiles, agregando protocolos de conexión con clave segura entre dispositivos para proteger contra los intentos de adivinación de claves por terceros, eliminando de esta forma los ataques de diccionario comunes en WPA2. A su vez introduce el programa Easy Connect, que reduce la complejidad de conectar dispositivos IoT Wi-Fi con interfaces limitadas o inexistentes mientras mantiene altos estándares de seguridad. Su objetivo es asegurar que los usuarios “reciban una experiencia positiva al mismo tiempo que permanecen conectados en forma segura a pesar de los cambios que puedan suceder en el ámbito de la seguridad”.

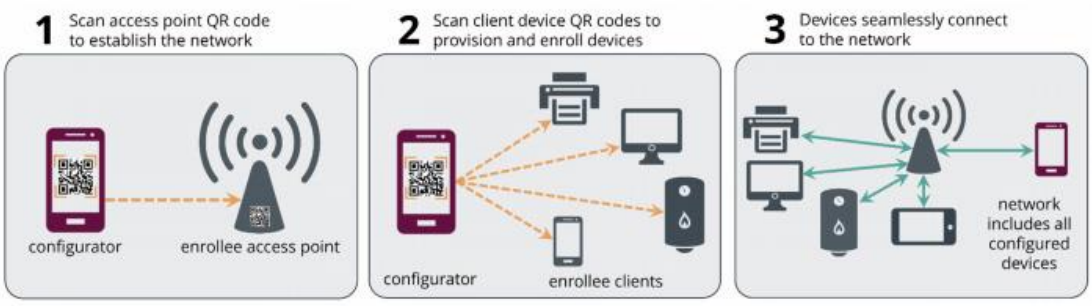


Figura 6 – Diagrama del proceso de conexión de dispositivos “Easy Connect” de WPA3 [25]

3 – Propuestas para Privacidad, Ética y Gobierno

3.1 – Privacidad

3.1.1 – Privacy-by-Design

Tal como la necesidad de introducir seguridad desde el diseño (*security-by-design*) ha ido ganando consenso en el ambiente de IoT, a partir de la evidencia de la problemática de privacidad ha surgido el concepto de privacidad desde el diseño[13] (*privacy-by-design*, PBD) para los dispositivos IoT. Este término fue originalmente acuñado por Ann Cavoukian, Comisionada de Información y Privacidad de la provincia canadiense de Ontario a finales del siglo pasado y cuenta con siete principios fundamental genéricos [26]. Su aplicación práctica incluye las siguientes medidas principales [10, p. 27] :

- ✓ restringir al mínimo necesario la cantidad de información que recaban las aplicaciones;
- ✓ encriptar todos los flujos de datos;
- ✓ restringir los tiempos de retención de la información;
- ✓ anonimizar la información personal;
- ✓ incluir notificaciones de privacidad de forma amigable para el usuario en los momentos apropiados y
- ✓ proveer opciones de configuración de privacidad simples y en lenguaje claro.

Es notorio que, en casi toda la literatura sobre el tema, se encuentra la advertencia de que la introducción de los principios de PBD, aunque necesaria y bien intencionada, no ha logrado en la práctica proteger la privacidad de los usuarios y que la confianza en el manejo de los datos realizado por la industria en el ámbito de IoT no ha hecho más que disminuir.

[13] De ahora en más se referencia como “PBD”

Estudios recientes sobre la percepción del consumidor indican que más del 60% incluye la filtración de datos personales a terceros a través de dispositivos y proveedores de servicio IoT como una de las principales preocupaciones [5].

El fracaso de PBD para generar mayor confianza en la privacidad en IoT se debe principalmente a las siguientes razones:

1. Por la renuencia lisa y llana de las empresas en aplicarla efectivamente. Hay que tener en cuenta que “el modelo de servicio a IoT es mayormente el de una multiplicidad de proveedores de servicio que lo ofrecen en un modo *Freemium* al recolectar datos personales y cuyo mayor ingreso es generado por la explotación por terceras partes de los datos personales para publicidad” [1, p. 200], por lo tanto medidas como la restricción tanto de la recolección como de la retención van directamente en contra de sus modelos comerciales.
2. Por la falta de verificación efectiva de la inclusión de las medidas de PBD y de sanciones a los proveedores que no cumplan con las mismas. Una herramienta válida a este efecto son las Evaluaciones de Impacto sobre la Privacidad (*Privacy Impact Assesments*, PIA) que deberían utilizarse para verificar el cumplimiento de los principios PBD y que son definidas por diferentes normativas, e incluso con el nombre de “Evaluaciones de protección de datos, DPIA” en la novedosa norma europea GDPR, que se describe a continuación. Sin embargo, hasta el momento continúa siendo limitado el consenso sobre cuando hay que llevarlas a cabo, con qué alcance y qué sanciones les cabrían a aquellos que no las realicen o no logren superarlas exitosamente.
3. Por los distintos aspectos que hacen que, aun cuando realmente se apliquen los principios de PBD, estos sean menos eficaces de lo esperado. Por ejemplo, cuando los datos son anonimizados para proteger la identidad de los usuarios, su efecto protector de la identidad se diluye debido a la ya explicada facilidad con que los mismos pueden ser re identificados utilizando técnicas de Fusión de sensores y Big Data. Las notificaciones de privacidad, por muy claras

y pertinentes que sean, chocan tanto con la “Fatiga de seguridad” y la “Paradoja de la Privacidad” mencionadas en capítulos anterior; es decir, cuantas más notificaciones se incluyen menos atención les presta el usuario.

3.1.2 – GDPR

Para suplir estas falencias, que están relacionadas no solo con IoT sino con la protección de la privacidad en todo el universo de tecnologías de información, es que se vienen debatiendo otras soluciones complementarias. Por ejemplo, la normativa europea GDPR [27], siglas en inglés de *General Data Protection Regulation* (Regulación General de Protección de Datos), largamente esperada y discutida en el seno de la Comisión Europea, finalmente aprobada en 2016 y que entró en vigor en mayo de 2018, combina elementos de PBD, pero a su vez implementa fuertes multas sobre las organizaciones que infrinjan las normas. Estas multas son realmente significativas ya que pueden representar hasta el 4% de los ingresos para las grandes corporaciones.

Una de las disposiciones más notables de la GDPR es el Artículo 33 o “requisito obligatorio de notificación de filtración de datos (*data breach)”*. Este artículo establece que, en el caso de una filtración de datos personales, los controladores de datos deberán notificar a la autoridad supervisora correspondiente "sin demoras indebidas y cuando sea posible, a más tardar 72 horas después de haberse dado cuenta del incidente". Además, requiere que se realice una investigación y se provea un mínimo de datos incluyendo la estimación del impacto y las medidas de mitigación tomadas. [28]

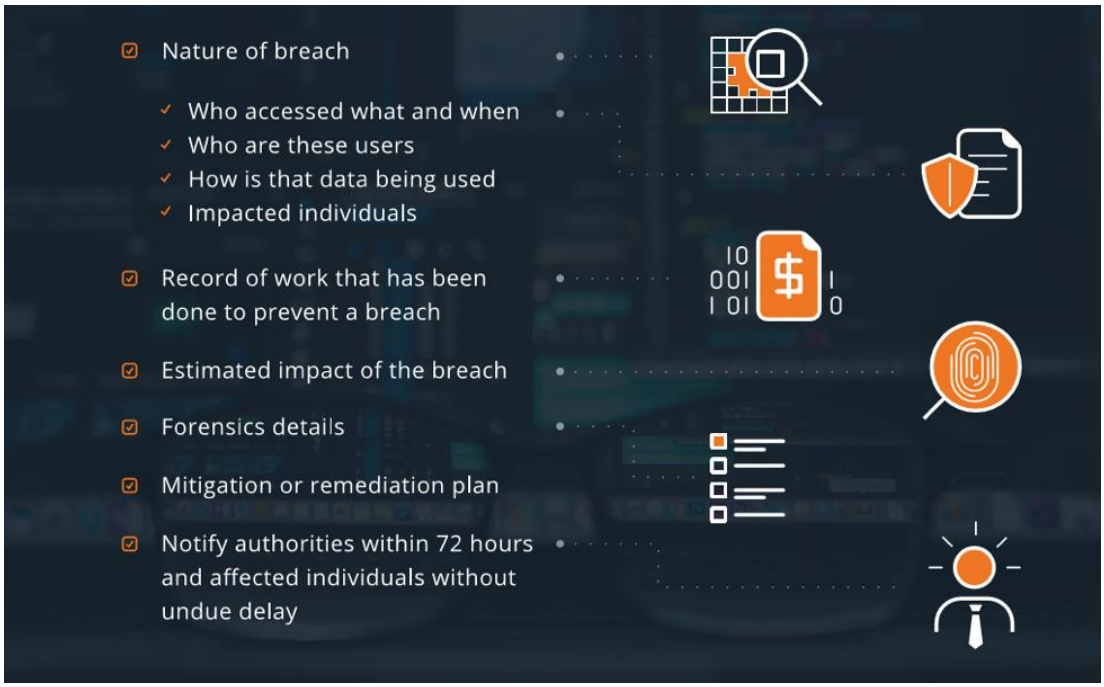


Figura 7 – GDPR Articulo 33: Requerimientos mínimos de información ante una filtración de datos. [28]

Además de la transparencia, que se refiere a las advertencias al usuario y a la posibilidad de configuración de la privacidad, ya mencionadas en PBD, dos principios adicionales que debe implementar cualquier esquema de privacidad de acuerdo con GDPR son**:**

- Posibilidad de Borrado (derecho al olvido): Los recolectores de la información deben ser el punto de entrada de pedidos de borrado de información y deben informar de los mismos a terceras partes; y
- Consentimiento: El consentimiento valido debe ser explícito para la información recolectada y el propósito de dicha recolección debe ser mencionado. Los recolectores de la información deben poder tanto recibir el consentimiento del usuario y como dar la posibilidad de que el mismo sea retirado [1].

3.1.3 – Consentimiento en IoT y ciudades inteligentes

Las formas de dar consentimiento y como mejorarlas han sido objeto de estudio desde mucho antes de la aparición de IoT, por ejemplo, en relación con la aceptación de condiciones de privacidad en sitios de Internet.

Sin embargo, dada la inusitada cantidad de datos que pueden recolectarse en IoT a través de sensores, y su posible combinación con técnicas Big Data, el tema ha cobrado renovada actualidad. Pueden mencionarse por ejemplo proyectos como *Consent Receipt* [1, p. 202] que propone una herramienta que mantiene el registro de consentimiento dado por el usuario, definiendo el alcance de este tanto para el recolector de los datos como para cualquier tercero al que se le dé acceso, y permitiendo también su revocamiento. Esta solución también permite a las autoridades regulatorias realizar auditorías de forma de relacionar los datos transferidos con el consentimiento dado por usuario y de esta forma llevar a cabo evaluaciones de protección de datos efectivas tal como requiere GDPR.

Desafortunadamente la irrupción de las ciudades inteligentes inhabilita muchas de las formas tradicionales de dar consentimiento. Quien ingrese por una autopista a una de estas ciudades con su vehículo inteligente o simplemente transite por un espacio público monitoreado difícilmente podrá prestar atención a advertencias de privacidad ni dar consentimiento para el uso de los datos generados por una multiplicidad de sensores y obtenidos en tiempo real por los proveedores de servicio.

Para esos casos existen propuestas de tipo Pre-Consentimiento, de acuerdo con las cuales el consentimiento no se da necesariamente al momento de usar un producto o servicio, sino que está relacionado con el individuo y esa información es recordada y transferida entre los sistemas inteligentes y se utiliza al momento de realizar alguna elección. Este tipo de solución es más fácil de implementar en hogares inteligentes donde un solo dispositivo, posiblemente alguno de los mencionados en la sección anterior sobre seguridad, “puede aprender las preferencias del usuario y ser el encargado de recordar la configuración de privacidad y aplicarla a cualquier nuevo usuario o dispositivo que se conecte a la red” [10, p. 33].

La temática del consentimiento no escapa al debate sobre la utilidad de empoderar al usuario en contraposición a regular y sancionar a la industria. Existe una corriente de pensamiento que sostiene que la noción de que el consentimiento como legitimador del proceso de datos simplemente

no funciona y que “se ha demostrado que una mayoría de los usuarios no tienen los recursos, oportunidades, conocimiento y motivación para dar un consentimiento significativo en el mundo online actual.” Sin embargo, ese consentimiento, dado habitualmente al hacer clic en el botón o enlace ¨Acepto” a páginas y páginas de condiciones que no se han entendido cabalmente o siquiera leído, luego se utiliza para validar la recolección y el análisis de datos [10, p. 33].

4.2 - Ética

4.2.1 – Educación para la demanda de ética

Existe consenso en las distintas publicaciones consultadas que mencionan esta temática [7] [10] [29], especialmente las relacionadas con la Unión Europea, en que para que la ética sea demandada, debe educarse al consumidor, al desarrollador y al emprendedor. Es decir, hay una relación directa entre la existencia y demanda de comportamientos éticos, y su inclusión dentro de los programas educativos. La expectativa es que estas acciones educativas puedan derivar en la “creación de productos éticos, de forma que esos valores éticos puedan ser trasladados a la preferencia en el mercado, donde diferentes productos puedan competir para ganarse la confianza del consumidor” [7, p. 32].

Incluso, este enfoque va más allá de la educación, ya que propone integrar al ciudadano al debate e, idealmente, la toma de decisiones sobre la tecnología, en contraposición al modelo en el cual solo intervienen los inversores, desarrolladores y vendedores. En resumen, que las personas que utilizan las tecnologías deberían tener voz sobre qué valores y qué normas sociales son embebidas en sus programas y funciones y de esta forma “poder influir en la forma en que desean vivir en el futuro y en qué legado se dejará para las próximas generaciones”. [7, p. 33]

Con relación a IoT, avanzar en esta propuesta significa también educar y concientizar a los usuarios en su relación con la tecnología para evitar que acepten pasiva y mecánicamente sus acciones y decisiones. Por un lado, evitar que las soluciones de IoT redunden en un mayor aislamiento

social y en una desensibilización acerca de los aspectos morales de las relaciones humanas en ambientes no-virtuales. Y por otro, evitar que la delegación de actividades en la tecnología derive en una delegación total y cuasi obligatoria de la autonomía humana a los dispositivos IoT.

4.2.2 – ¿Ethics-by-design?

Adelantándonos a la temática de gobierno y la regulación a las empresas, existen propuestas tendientes a incluir una combinación de acercamientos tecnológicos y normativos, agregando al proceso productivo algo que, parafraseando a *security* o *privacy-by-design,* pueda llamarse "*ethics-by-design*". Esto significaría embeber los conceptos éticos en todo el ciclo de desarrollo de la tecnología, desde el más temprano diseño hasta su implementación, uso y disposición final. De esta forma, la unión de soluciones técnicas con comportamientos "humanos" generadores de confianza, sumados a la educación, debería dar lugar a relaciones con la tecnología más robustas y confiables. Para los impulsores de estas normas "una integración de las dimensiones humanas y tecnológicas en el gobierno de IoT es no solo más legítima (ética y democráticamente) sino incluso más efectiva" [29] que otras soluciones.

Sin embargo, para otros analistas estos procesos son demasiado lentos, y aunque necesarios, no pueden reemplazar la aplicación en el corto plazo de leyes más concretas. Tal como muchos investigadores sugieren que no se debe esperar que el consentimiento sea efectivo para brindar privacidad, estiman que no es esperable que las empresas actúen en forma ética en contra de sus propios intereses comerciales aun cuando los consumidores puedan esperar que lo hagan.

Especialmente en los Estados Unidos, una corriente de pensamiento considera que en el ámbito corporativo solo surge el debate sobre la ética cuando las organizaciones entran en pánico por alguna filtración sobre sus actividades que les genera una crisis de confianza con sus consumidores como en el caso de Facebook / Cambridge Analytica [30] o las revelaciones de Snowden. En otras palabras, para estos analistas, la creación de nuevas

leyes no debe necesariamente incluir a la ética ya que consideran que es básicamente no imponible (*unenforceable*) por medio de la regulación [10].

4.3 – Gobierno, Marcos y Estándares

4.3.1 – Marcos para la búsqueda de un gobierno global

El concepto de Gobierno global ya ha sido aplicado exitosamente a numerosas tecnologías de información, por ejemplo, en el caso de Internet donde organizaciones como IETF, ICANN, IEEE y W3C son cada una responsable de regular y controlar áreas específicas. Sería un paso lógico extender este concepto al gobierno de IoT. La dificultad reside en el gran número de sistemas y dispositivos de IoT y su heterogeneidad, lo que requiere soluciones más complejas que las aplicadas para otras tecnologías. Por esta causa no se ha logrado aún un consenso sobre cómo implementar un gobierno global y efectivo que ofrezca por un lado estabilidad y soporte a las decisiones sin resultar en un ambiente sobre controlado.

Para suplir en parte esta carencia, recientemente han surgido a ambos lados del Atlántico marcos (*frameworks*) generados a partir del consenso de múltiples partes interesadas, que definen una serie de principios estratégicos necesarios para generar confianza en IoT, incluyendo casi todas las problemáticas mencionadas en el presente trabajo.

Un ejemplo de este tipo de marcos es el “IOT Security & Privacy Trust Framework” de la Online Trust Alliance [31], que en su versión 2.5 de 2017 establece sus múltiples objetivos:

- permitir realizar evaluaciones de riesgo,
- destacar los productos y servicios que cumplan con los estándares y
- servir como base de programas de certificación IoT futuros.

Un marco destacado cuyo desarrollo fue financiado por la Unión Europea es el HLA (High Level Achitecture) para IoT [7, p. 245] producido por la AIOTI (Alianza para la innovación en IoT) [32] que se focaliza en dar soporte a la interoperabilidad en sistemas IoT complejos y avanzar en la

identificación y definición de estándares que permitan reducir la complejidad y facilitar la convergencia de las arquitecturas.

4.3.2 – Los primeros estándares de IoT

El desafío de la interoperabilidad conduce a la necesidad de desarrollar estándares que puedan ser aplicados en IoT. Uno de los primeros grupos creados por la Unión Europea para apoyar el desarrollo de la estandarización en IoT es el ETSI STF 505 [7, p. 240] cuyos objetivos son:

- Analizar el estatus actual de estandarización de IoT;
- Apalancar la relación entre organizaciones e industria en relación con la estandarización;
- Apoyar la divulgación de forma de mantener una comunidad global de interesados e involucrados en la estandarización de IoT.

Este grupo presentó en 2016 el que hasta el presente es el estudio [33] más completo sobre los estándares referidos a IoT a nivel global con las siguientes conclusiones: Las iniciativas coexistentes para la estandarización mantenían 329 estándares diferentes en desarrollo, incluyendo alternativas institucionales (ITU, ISO/IEC, W3C, IEEE, etc.) y de la misma industria (Industrial Internet Consortium, Open Connectivity Foundation, etc.). Más del 70% de estos estándares se focalizaban en solo tres áreas: Conectividad, Integración y Arquitectura IoT. Se detectaron numerosos *gaps* tanto por la falta de cobertura de ciertas áreas, la duplicación y también por detalles técnicos no contemplados especialmente en las áreas de seguridad y privacidad.

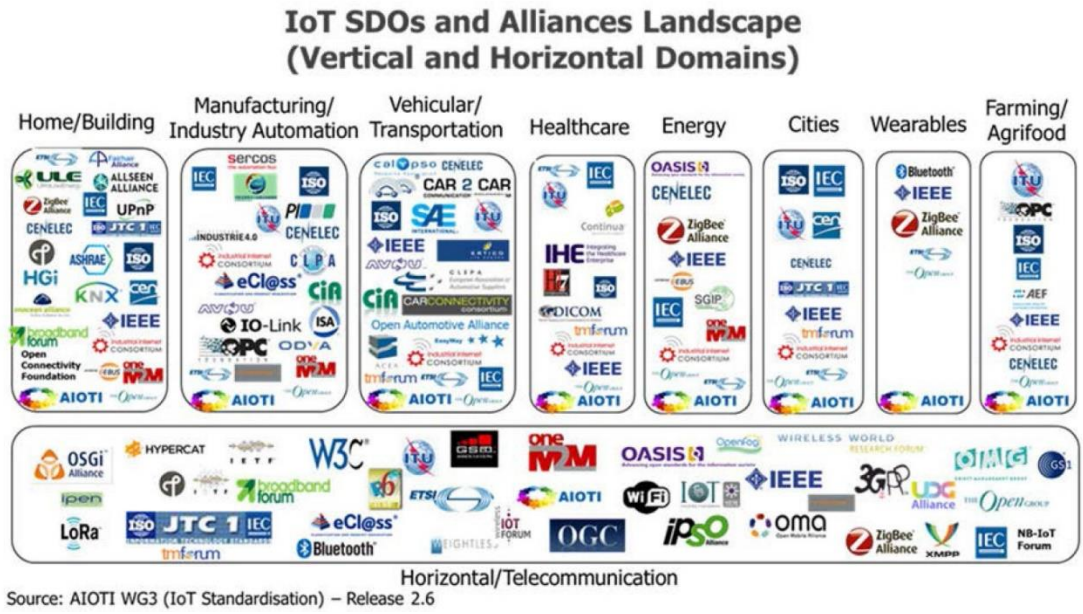


Figura 8 – Una vista de la multiplicidad de estándares aplicables a IoT. [32]

De los proyectos mencionados en el estudio de ETSI, se destacan dos por su alcance, por la envergadura de las organizaciones que los auspician y por haber tenido novedades muy recientemente. En primer lugar, el IEEE P2143 [34], cuyo borrador fue aprobado en la última reunión de grupos de trabajo en septiembre 2018. Esta norma pretende definir un marco de arquitectura para IoT y un modelo de referencia que facilite las relaciones entre varios dominios verticales, por ejemplo, transporte, cuidado de la salud, etc. La norma además reutiliza los estándares aplicables vigentes e identifica proyectos planificados o en curso que puedan superponerse.

Finalmente, ISO/IEC 30141:2018 [35], publicada en agosto de 2018, que proporciona una arquitectura de referencia de IoT utilizando un vocabulario común, diseños reutilizables y mejores prácticas de la industria. Aplica un enfoque de arriba hacia abajo, comenzando con la recopilación de las características más importantes de IoT, luego las abstrae en un modelo conceptual IoT genérico y finalmente las descompone desde el modelo de referencia a cinco vistas de arquitectura (vista funcional, vista del sistema, vista del usuario, vista de información y vista de comunicación).

El objetivo de la norma es que puede servir en forma directa como base para desarrollar aplicaciones específicas de IoT. Por otro lado, hace

foco en la obtención de confianza en IoT dedicándole el capítulo más significativo.

Llamativamente esta última norma se basa mayormente en el trabajo desarrollado por el instituto de investigación sobre IoT Wuxi (*Wuxi IoT Research Institute*), de la ciudad homónima de China [36], lo que viene a romper definitivamente con la hegemonía de Estados Unidos y Europa como generadores de políticas y normas. Incluso los grupos de trabajo fueron liderados por investigadores coreanos [37]. Esto no debería sorprender dada las enormes inversiones gubernamentales chinas y coreanas en desarrollo de IoT. Es muy posible entonces que en el futuro para obtener novedades de gobierno y estándares de IoT, y ya no solo el último *wearable*, haya que observar más a oriente.

Conclusiones

Al analizar las problemáticas y desafíos de IoT y las múltiples soluciones propuestas se hace evidente que la batalla por hacer más confiable a la tecnología se libra ahora mismo en varios campos y que para algunos aspectos es posible ser relativamente optimista acerca de las perspectivas a mediano plazo.

Con respecto a la seguridad, por un lado, la inversión realizada por los estados y las grandes empresas del sector para asegurar las redes sumada a la aplicación estratégica de conceptos de Inteligencia Artificial y otros avances promete en un futuro cercano dejar a su mayor amenaza, los ataques de denegación de servicio, como un mal recuerdo.

También los distintos métodos para calcular la reputación y distribuir la confianza basados en Edge Computing como los que utilizan las soluciones mencionadas hacen su aporte a asegurar tanto el ambiente local como en la interacción entre sistemas y dispositivos heterogéneos.

Por otro lado, dado que la investigación sobre *BlockChain* está en su apogeo, esencialmente por sus posibles aplicaciones a distintos procedimientos financieros y de provisión de confianza entre partes como por ejemplo a través de contratos inteligentes, es esperable que en el mediano plazo continúen proponiéndose soluciones similares a las planteadas en el segundo capítulo de Propuestas de Seguridad y administración de la confianza, pero que hagan aún más eficiente y seguro su uso para IoT.

A nivel del usuario final, las buenas noticias provienen del desarrollo de herramientas que lo relevan de tener que interiorizarse de la seguridad de las “cosas”. El lanzamiento de WPA3 es una excelente novedad teniendo en cuenta que la mayor parte de los dispositivos IoT a nivel hogareño se conectan a través de Wi-Fi. Y los productos que aseguran todo el perímetro informático del hogar inteligente probablemente se volverán cada vez más comunes, eficientes y económicos.

Un aspecto que aún no se encuentra resuelto es el de la información al consumidor al momento de adquirir un dispositivo IoT. En el presente trabajo se propone que tal como existe una calificación para el consumo de energía, se desarrolle una calificación de nivel de seguridad de los productos y que la misma sea provista por uno o varios organismos reconocidos global o localmente. De esta forma también las empresas que fabrican dispositivos con fallas de seguridad serán castigadas con bajas calificaciones.

La publicación de normas y estándares específicos de IoT, que ya se encuentra sucediendo, por supuesto ayudará a basar dichas calificaciones en parámetros reconocidos y a proveer un marco de referencia integral a las compañías fabricantes y proveedoras de servicios.

A nivel de privacidad, por el contrario, es más difícil encontrar soluciones concretas y el panorama a corto plazo se presenta mucho menos definido. Nos encontramos con que una vez que los datos de usuario han sido obtenidos por las empresas, su uso y resguardo son muy difíciles de controlar. Al fin y al cabo, como indica Edwards [10, p. 14] “la historia de las corporaciones de Internet demuestra que casi todas las compañías cuentan con obtener la mayor cantidad de información personal posible gracias a la falta de transparencia en sus políticas de privacidad y a la ignorancia o inercia del consumidor”.

Solo en casos de incidentes que toman estado público o cuando ciertas maniobras son delatadas desde el interior de estas organizaciones, pueden intervenir los organismos de control y muchas veces con limitaciones dadas por la inadecuación de las leyes y regulaciones. Las fuertes multas establecidas y la obligación de hacer público cualquier incidente relacionado con la privacidad que establece GDPR intentan dar una solución parcial a estos problemas, pero evidentemente aún hay mucho camino por recorrer.

Idealmente sería la incorporación de comportamientos éticos lo que proveería una solución para estos temas que no son eminentemente técnicos. Pero como fue explicado anteriormente esto requiere un proceso habitualmente lento y no siempre exitoso de educación, tanto del consumidor

para que demande dichos comportamientos, como de los profesionales para que los incorporen en sus actividades.

Una asignatura pendiente de investigación es entonces encontrar la forma de llevar a la industria a embeber efectivamente conceptos de ética y privacidad desde la concepción misma de los productos y servicios, de forma que, sumados a las soluciones de seguridad mencionadas anteriormente, se pueda obtener finalmente y para beneficio de toda la sociedad una IoT realmente confiable.

Figura 9 – Algunos atributos y características deseables de una IoT confiable (Adaptación propia en base a Shindler et al. [29])

Glosario

Definiciones de IoT:

De IEEE: Provee la definición base: “Una red de cosas, cada una provista de sensores, que se encuentran conectadas a internet”.

De ITU: Agrega en su definición de 2005 la palabra “ubicua”[14] cuando se refiere a la red de IoT.

De IETF: Avanza sobre el concepto de “cosas” para, además de indicar que pueden ser físicas o virtuales, establecer que dichas cosas deben estar identificadas al menos por un identificador único con la capacidad de ser direccionado y verificado por otras entidades.

De IERC: Provee en su reporte de 2014 sobre IoT una de las definiciones más abarcadoras: “Una infraestructura de red dinámica y global con capacidades de autoconfiguración, basada en protocolos de comunicación estandarizados e interoperables, donde cosas físicas y virtuales poseen identidades y atributos, utilizan interfaces inteligentes y están integrados a la red informática” [38]

Confianza y términos relacionados:

Confianza: Se define como la esperanza que una entidad tiene, de que otra entidad funcione o se comporte de la forma esperada. Se considera subjetiva.

Confiabilidad: Se describe como la probabilidad de que una entidad se comporte de una forma determinada. Se entiende objetiva, medible y comparable.

Reputación: Estimador de la confiabilidad de una entidad de acuerdo con los criterios de otra u otras entidades. Habitualmente será la reputación el valor utilizado en los sistemas IoT para definir, en base a las métricas conjuntas de otras múltiples entidades, si una entidad es confiable o no.

[14] El termino ubicuo, *ubiquitous*, que proviene del latín *ubiquo*: “que está en todos lados”, es importante ya que define a la red de IoT como disponible en todos lados y todo el tiempo, y también porque trae aparejado el concepto de que, por esa misma razón, eventualmente puede pasar inadvertida para los usuarios.

Tecnologías:

Big Data: Conjunto de datos de tal volumen que permiten a aplicaciones informáticas especializadas realizar análisis complejos de forma de extraer patrones y otra información valiosa.

BlockChain: Registro en el cual se almacenan transacciones agrupadas en bloques, y el *hash* combinado de esas transacciones también se almacena, de forma que cada bloque guarda el *hash* combinado del bloque anterior. Esto crea una cadena de bloques relacionados y criptográficamente asegurados contra la manipulación retrospectiva. [39]

Criptomonedas: Medio digital de intercambio que utiliza a la criptografía para asegurar las transacciones.

Edge Computing: Paradigma de tecnología distribuida en el cual la información que se genera en el cliente es procesada en la periferia de la red, tan cerca de la fuente como sea posible.

Freemium: Modelo de negocio en el cual el usuario utiliza gratuitamente un producto o servicio, generando ingresos para el proveedor a través de publicidad o venta de datos personales. Contracción en inglés de las dos palabras: "free" y "premium"

***Wearable*:** Objeto de uso diario incorporado a la ropa o como complemento del cuerpo humano y al que se le ha incorporado capacidad de procesamiento y conectividad.

Redes:

***Cluster*:** Conjunto o conglomerado de dispositivos unidos entre sí por una red informática, habitualmente administrados y conectados a Internet u otros *clusters* a través de un dispositivo gerenciador o *Cluster Head*.

DNS (Domain Name Service): El sistema de nombres de dominio es un sistema de nomenclatura jerárquico descentralizado que asocia información, incluyendo la dirección IP real, con los nombres de dominio asignados.

Gateway (*puerta de enlace*): Dispositivo que actúa de interfaz de conexión entre otros dispositivos y hacia el exterior de la red informática.

Latencia: Suma de retardos temporales dentro de una red producidos por la demora en la propagación y transmisión de paquetes.

***Overhead*:** Tiempo computacional extra que una determinada operación puede requerir si se le añade una funcionalidad.

Seguridad:

Ataque *DDOS* (*Distributed Denial Of Service*): Ataque distribuido a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Botnet: Conjunto o red de ordenadores o bots, que se ejecutan de manera autónoma y automática habitualmente para realizar ataques DDOS sobre otros sistemas o redes.

Firmware: Programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

PGP: Pretty **G**ood **P**rivacy es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet, en particular por correo electrónico, mediante el uso de criptografía de clave pública.

PKI: La infraestructura de clave pública es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten proteger la información y asegurar las transacciones a través de operaciones criptográficas.

Referencias

[1] O. Vermesa y P. Friess, Internet of Things: Connecting the Physical, Digital and Virtual Worlds, Gistrup, Denmark: River Publishers, 2016. Disponible: http://www.internet-of-things-research.eu/pdf/Digitising_the_Industry_IoT_IERC_2016_Cluster_eBook_978-87-93379-82-4_P_Web.pdf [Último acceso: 14 10 2018]

[2] S. Peppet, «Regulating the Internet of Things: First steps towards managing discrimination, privacy, security and consent.,» *Texas Law Review,* vol. 93, nº 85, pp. 86-178, 2014. Disponible: https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf [Último acceso: 14 10 2018]

[3] Gartner, «Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018,» 2016. [En línea]. Disponible: https://gartner.com/newsroom/id/3221818. [Último acceso: 6 3 2018].

[4] Ben-Gurion University, «Off-the-Shelf Smart Devices Found Easy to Hack,» 14 05 2018. [En línea]. Disponible: http://in.bgu.ac.il/en/pages/news/offshelf_smart.aspx. [Último acceso: 24 08 2018].

[5] Gemalto, «The State of IoT Security – Global Survey Report - October 2017,» 2017. [En línea]. Disponible: https://www.gemalto.com/brochures-site/download-site/Documents/documentgating/iot-security-report.pdf. [Último acceso: 23 08 2018].

[6] D. Lewis, «The ddos attack against DYN: One year later,» 23 10 2017. [En línea]. Disponible: https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later. [Último acceso: 17 08 2018].

[7] European Research Cluster on the Internet of Things, «Internet of

Things: Governance, Privacy and Security Issues,» European Commision, 2015. Disponible: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf [Último acceso: 17 08 2018]

[8] I. Bojanova y J. Voas, «Trusting the Internet of Things,» *IT Professional,* vol. 19, nº 5, pp. 16-19, 2017. Disponible: https://www.computer.org/csdl/mags/it/2017/05/index.html [Último acceso: 14 10 2018]

[9] R. Arnold, A. Hillebrand y M. Waldburger, «Personal Data and Privacy: An Study for Ofcom,» WIK-Consult, Bad Honnef, Alemania, 2015. Disponible: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/67088/personal_data_and_privacy.pdf [Último acceso: 14 10 2018]

[10] L. Edwards, «Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective,» CREATe, Glasgow, 2015. Disponible: https://www.create.ac.uk/publications/privacy-security-and-data-protection-in-smart-cities-a-critical-eu-law-perspective/ [Último acceso: 21 10 2018]

[11] Raij, Andrew et al., «Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors,» *Proceedings of the Sigchi Conference on Human Factors in Computing Systems,* p. 11, 2011. Disponible: https://www.researchgate.net/publication/221518517_Privacy_risks_emerging_from_the_adoption_of_innocuous_wearable_sensors_in_the_mobile_environment [Último acceso: 21 10 2018]

[12] de Monjoye et al., «Unique in the Crowd: The privacy bounds of Human Mobility,» *Scientific Reports,* vol. 3, nº 4, p. 4, 2013. [En línea]. Disponible: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607247/ [Último acceso: 21 10 2018]

[13] M. Rouse y E. Mixon, «Edge Computing,» 08 2016. [En línea]. Disponible: https://searchdatacenter.techtarget.com/definition/edge-

computing. [Último acceso: 21 10 2018].

[14] H. Kim y E. Lee, «Authentication and Authorization for the Internet of Things,» *IT Professional,* vol. 19, nº 5, pp. 27-33, 2017. Disponible: https://www.computer.org/csdl/mags/it/2017/05/index.html [Último acceso: 14 10 2018]

[15] CB Insights, «What Is Edge Computing?,» 08 08 2018. [En línea]. Disponible: https://www.cbinsights.com/research/what-is-edge-computing/. [Último acceso: 10 09 2019].

[16] Ponemon Institute LLC, «Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk,» 03 2018. [En línea]. Disponible: https://sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf. [Último acceso: 27 08 2018].

[17] B. Butler, «What is edge computing and how it's changing the network,» Network World, 21 09 2017. [En línea]. Disponible: https://www.networkworld.com/article/3224893/internet-of-things/what-is-edge-computing-and-how-it-s-changing-the-network.html. [Último acceso: 10 09 2018].

[18] M. Vahidalizadehdizaj, L. Tao y J. Jadav, «Security Challenges In Swarm Intelligence,» IEEE 6th International Conference on Computing, Communication and Networking Technologies, New York, 2017. [En línea]. Disponible: https://www.researchgate.net/publication/293176049_Security_Challenges_In_Swarm_Intelligence [Último acceso: 10 09 2018].

[19] A. Dorri, S. Kanhere, R. Jurdak y P. Gauravaram, «Blockchain for IoT security and privacy: The case study of a smart home,» de *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*, Kona, HI, 2017. [En línea]. Disponible: https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_and_Privacy_The_Case_Study_of_a_Smart_Home

[Último acceso: 10 09 2018].

[20] A. Dorri, S. Kanhere y R. Jurdak, «Towards an optimized Blockchain for IoT,» de *Proceedings of the 2nd ACM/IEEE Conference on Internet Of Things*, Pittsburg, PA, 2017. [En línea]. Disponible: https://ieeexplore.ieee.org/document/7946872 [Último acceso: 10 09 2018].

[21] NIST, «Security Fatigue,» 04 10 2016. [En línea]. Disponible: https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly. [Último acceso: 11 09 2018].

[22] D. Fernández Sánchez, *Diseño lógico de una aplicación para determinar el nivel de seguridad de un dispositivo IoT,* Buenos Aires: Tesis de maestria en Seguridad Informática, 2017.

[23] M. Vanhoef, «Key Reinstallation Attacks,» 2017. [En línea]. Disponible: https://www.krackattacks.com/. [Último acceso: 14 10 2018].

[24] Wi-Fi Alliance, «Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security,» 26 06 2018. [En línea]. Disponible: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security . [Último acceso: 12 09 2019].

[25] Redact, «WPA3 Wi-Fi security announced after more than a decade of WPA2,» 26 16 2018. [En línea]. Disponible: https://medium.com/redact/wpa3-wi-fi-security-announced-after-more-than-a-decade-of-wpa2-7ca1fb00e036. [Último acceso: 22 10 2018].

[26] A. Cavoukian, «Privacy by Design: The 7 Foundational Principles,» 01 2011. [En línea]. Disponible: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. [Último acceso: 14 10 2018].

[27] Trunomi, «The EU General Data Protection Regulation (GDPR),» 05 2018. [En línea]. Disponible: https://eugdpr.org/. [Último acceso: 18 10

2018].

[28] S. Ryan, «Understanding the GDPR Data Breach Reporting Timeline,» 16 05 2018. [En línea]. Disponible: https://www.imperva.com/blog/2018/05/72-hours-understanding-the-gdpr-data-breach-reporting-timeline/. [Último acceso: 22 10 2010].

[29] Schindler, Rebecca et al., Europe's policy options for a dynamic and trustworthy development of the Internet of Things, Cambridge: Rand, 2013. Disponible: https://www.rand.org/pubs/research_reports/RR356.html [Último acceso: 22 10 2010].

[30] C. Cadwalladr y E. Graham-Harrison, «50 million Facebook profiles harvested for Cambridge Analytica in major data breach,» 18 03 2018. [En línea]. Disponible: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. [Último acceso: 21 10 2018].

[31] Online Trust Alliance, «IoT Security & Privacy Trust Framework v2.5,» 14 10 2017. [En línea]. Disponible: https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf. [Último acceso: 18 10 2018].

[32] AITOI, «AIOTI Alianza para la innovación en IoT,» 05 10 2018. [En línea]. Disponible: http://www.aioti.eu. [Último acceso: 16 10 2018].

[33] J. Koss, «ETSI Specialist task force STF 505 -IOT,» 11 2016. [En línea]. Disponible: https://docbox.etsi.org/Workshop/2016/201611_M2MIoTWS/00_WORKSHOP/ZZ_CONCLUSION/STF505_Koss.pdf. [Último acceso: 15 10 2018].

[34] IEEE Standards Association, «P2413 - Standard for an Architectural Framework for the Internet of Things (IoT),» 09 2016. [En línea]. Disponible: http://grouper.ieee.org/groups/2413/Intro-to-IEEE-

P2413.pdf. [Último acceso: 18 10 2018].

[35] International Organization for Standardization, «ISO/IEC 30141:2018 Internet of Things (IoT) -- Reference Architecture,» 08 2018. [En línea]. Disponible: https://www.iso.org/standard/65695.html?browse=tc. [Último acceso: 13 09 2018].

[36] W. Zhou, «ISO chooses China's IoT standards,» 11 07 2018. [En línea]. Disponible: http://www.chinadaily.com.cn/m/jiangsu/wuxi/2018-07/11/content_36556927.htm. [Último acceso: 14 10 2018].

[37] iEC, «Why the IoT needs standardization,» 01 2017. [En línea]. Disponible: https://iecetech.org/Technical-Committees/2017-01/Why-the-IoT-needs-standardization. [Último acceso: 14 09 2018].

[38] R. Minerva, A. Biru y D. Rotondi, «Towards a Definition of the Internet of Things (IoT),» IEEE, Turín, 2015. [En línea]. Disponible: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf [Último acceso: 26 07 2018].

[39] R. Beck, «Beyond Bitcoin: The Rise of the Blockchain world,» *IEEE Computing Edge,* vol. 4, nº 4, pp. 26-30, 2018. [En línea]. Disponible: https://www.computer.org/csdl/mags/co/2018/02/mco2018020054.pdf [Último acceso: 14 10 2018].