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

Maestría en Seguridad Informática

Tesis de Maestría

Tema
Internet de las Cosas (IoT)

Título
Seguridad y privacidad para el consumidor de IoT

Autor: **Diego Alberto Wydler**
Directora de Tesis: **Graciela Pataro**

Año de presentación: **2020**
Cohorte 2018

Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable 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

La seguridad y privacidad de la información generan numerosos desafíos para IoT, pero mientras que a nivel corporativo e industrial los expertos en seguridad informática pueden valerse de distintos mecanismos conocidos de defensa y mitigación, no es mucho lo que puede hacer el consumidor, que se ve restringido por sus limitados conocimientos, por configuraciones de seguridad poco amigables y por la falta de advertencias sobre privacidad, entre otros obstáculos.

Como posible solución a estos problemas esta tesis evalúa distintas propuestas para informar el nivel de seguridad y privacidad de los dispositivos IoT utilizando diferentes tipos de rótulo, tal como sucede actualmente con las especificaciones de consumo de energía o con los rótulos nutricionales. A su vez, analiza esquemas de certificación y validación de dispositivos IoT puestos en práctica o en estudio en diferentes países.

El objetivo principal de la tesis es establecer las características de un sistema de información y certificación de dispositivos IoT que proteja y provea confianza al consumidor y, a su vez, incentive a las empresas fabricantes y proveedoras de servicios a mejorar la seguridad y privacidad de los dispositivos.

Palabras clave

Internet de las cosas, IoT, seguridad IoT, privacidad IoT, información al consumidor, certificación IOT, rotulado IoT.

Índice

Introducción

Al momento de la compra de un dispositivo IoT, el consumidor se encuentra con numerosas opciones de productos de similares características. Sin embargo, no cuenta con suficientes mecanismos que le ayuden a tomar una decisión informada para proteger su seguridad y la privacidad de su información.

Cada uno de estos dispositivos IoT menciona en forma prominente desde sus embalajes los beneficios y ventajas tecnológicas que provee su uso. Sin embargo, las referencias a temas de seguridad o privacidad suelen brillar por su ausencia. Tampoco se encuentran, en su mayoría, indicaciones de que hayan sido certificados u homologados por organismos oficiales o confiables.

Por otra parte, al no estar presente esta información y, por lo tanto, no representar un argumento de compra, las empresas fabricantes no encuentran incentivos para mejorar la seguridad y privacidad de los dispositivos, prefiriendo competir por la atención del consumidor tanto por precio, reduciendo los costos, uno de los cuales es evidentemente la provisión de mayor seguridad, como por características técnicas, para lo cual apuran los lanzamientos, muchas veces sin realizar la cantidad de pruebas recomendadas en relación con la seguridad.

Al conectar el dispositivo en su ambiente hogareño y realizar el primer uso del mismo, el usuario encuentra que las configuraciones de seguridad suelen ser, o extremadamente básicas, o demasiado avanzadas y poco claras, al menos para aquellos sin conocimientos en el tema. Las advertencias y condiciones de privacidad habitualmente deben ser buscadas en el fondo del sitio web del proveedor, e incluso redactadas de forma de desanimar hasta a los más avezados expertos en temas legales.

Todas estas limitaciones y debilidades se contraponen con los hallazgos de diferentes estudios mencionados en la tesis, que indican que nueve de cada diez consumidores entrevistados esperan que la seguridad y privacidad de IoT se provea como un estándar, en vez de ser algo por lo que deban preocuparse o que deban considerar ellos mismos. Peor aún, el usuario de múltiples dispositivos y aplicaciones sufre habitualmente de lo que se ha dado en llamar **"fatiga de la seguridad"**, sensación que surge cuando los usuarios comienzan a sentirse sobrepasados y bombardeados por las constantes alertas y recomendaciones de seguridad, y los lleva tanto a evitar tomar decisiones como a comportarse impulsivamente, por lo que terminan ignorando completamente las políticas y recomendaciones de seguridad.

Es por todo esto que es vital establecer con urgencia mecanismos que ayuden a proteger la seguridad y la privacidad de los usuarios de IoT desde el momento de la compra y posibiliten al consumidor elegir dichos dispositivos con suficiente confianza.

Como posible solución a estos problemas esta tesis evalúa distintas propuestas para informar el nivel de seguridad y privacidad de los dispositivos IoT utilizando diferentes tipos de rótulo, tal como sucede actualmente con las especificaciones de consumo de energía o con los rótulos nutricionales. A su vez, analiza los desafíos que plantean dichos sistemas de rotulado y los esquemas de certificación y validación de dispositivos IoT.

El objetivo de la tesis es lograr describir las características de un sistema de información y certificación de dispositivos IoT para el consumidor, factible de ser implementado en nuestro país y la región, que incluya adecuadas mediciones y definiciones acerca de qué y cómo informar, y que provea información precisa al consumidor de IoT sobre seguridad y privacidad al momento de la compra, a la vez que incentiva a las empresas fabricantes y proveedoras de servicios a mejorar la seguridad y privacidad de los dispositivos.

1. Características del consumidor de IoT

1.1 Mercado, dispositivos y particularidades

Generalmente el mercado de IoT puede ser dividido en dos grandes segmentos: el mercado orientado al consumidor y el mercado orientado a los negocios o la industria tal como se muestra en la ilustración siguiente.

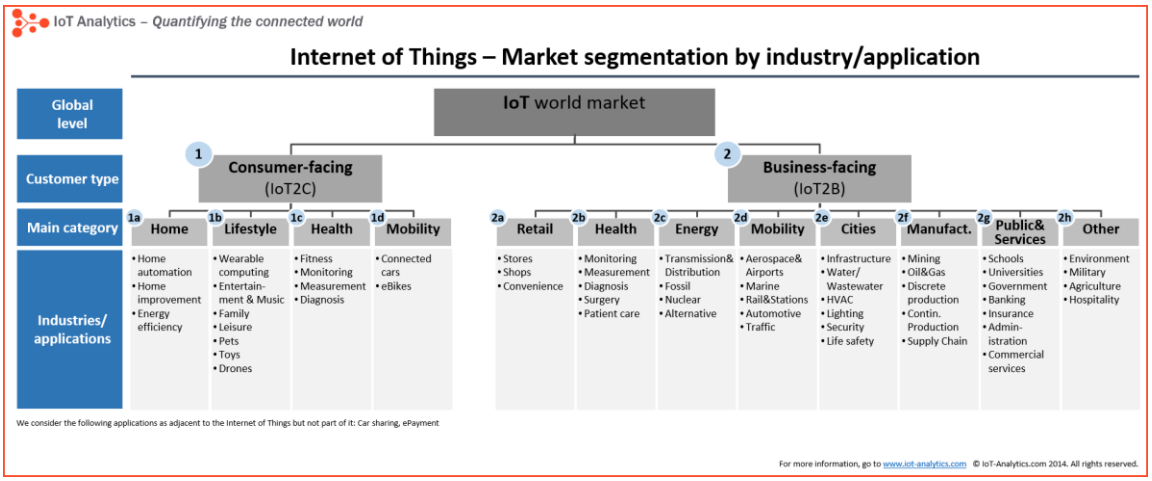


Ilustración 1 – La aplicaciones orientadas al consumidor en la segmentación del mercado IoT [1]

Las principales categorías dentro del mercado orientado al consumidor, identificado por siglas en inglés como IoT2C (*IoT to Consumer*) o CIoT (*Consumer IoT*), son las siguientes [2]:

Hogar: En esta área son populares los dispositivos de control de temperatura, luminosidad y seguridad del hogar. A su vez, entran dentro de esta categoría los artefactos tradicionales como refrigeradores y cocinas, a los que se les ha dotado de capacidad de procesamiento y de conexión a la red.

Estilo de vida: Esta categoría incluye a dispositivos como relojes inteligentes, juguetes y asistentes personales.

Salud: Incluye tanto a los dispositivos utilizados por deportistas como a sensores profesionales para monitorear en forma remota a pacientes.

Movilidad: Los automotores actuales, y hasta algunas bicicletas, están equipados con todo tipo de sensores y dispositivos que pueden conectarse a las redes para proveer seguridad y asistencia.

Veamos las diferencias entre el mercado de negocios o industrial y el orientado al consumidor que determinan características especiales de este último y lo hacen más vulnerable a los desafíos de seguridad y privacidad.

Con relación a la privacidad, a diferencia del mercado industrial o de negocios, en los cuales la información recolectada por los dispositivos IoT está orientada mayormente a la mejora de los procesos, el mercado para al consumidor declama el objetivo de mejorar y dar soporte a la vida personal del usuario. Esta es una de las causas por las cuales la amenaza a la privacidad es mayor en el mercado del consumidor, ya que para cumplir su objetivo los sensores de los dispositivos IoT deben recolectar necesariamente grandes cantidad de información personal, en muchos casos sensible con respecto a la protección de la privacidad.

Con respecto a la seguridad, en el mercado orientado al consumidor los desafíos están determinados en primer lugar por las particularidades de las "cosas", ya que un gran número de estos dispositivos, especialmente los diseñados para ser utilizados en "hogares inteligentes" o también los *wearables*[1], 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 de los dispositivos IoT para el consumidor es que no pueden ser arreglados ni mejorados luego de su venta. En muchos casos tampoco es contemplada la

[1] La tecnología ponible o vestible (del inglés wearable technology), tecnología corporal, ropa tecnológica, ropa inteligente, o electrónica textil, son dispositivos electrónicos inteligentes incorporados a la vestimenta o usados corporalmente como implantes o accesorios que pueden actuar como extensión del cuerpo o mente del usuario. https://es.wikipedia.org/wiki/Tecnolog%C3%ADa_vestible (consultada 27/11/2020)

forma de recibir y aplicar actualizaciones de *firmware* en forma automática. [3]

Estas debilidades intrínsecas del mercado orientado al consumidor 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. Al mismo tiempo solo 48% de las empresas creen que la seguridad sea una consideración importante para el consumidor, y un minúsculo 14% lo ve como una obligación ética. Mientras tanto las empresas y proveedores de servicio continúan ampliando la oferta de IoT y el 54% de los consumidores ya cuenta con al menos un dispositivo. 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 [3].

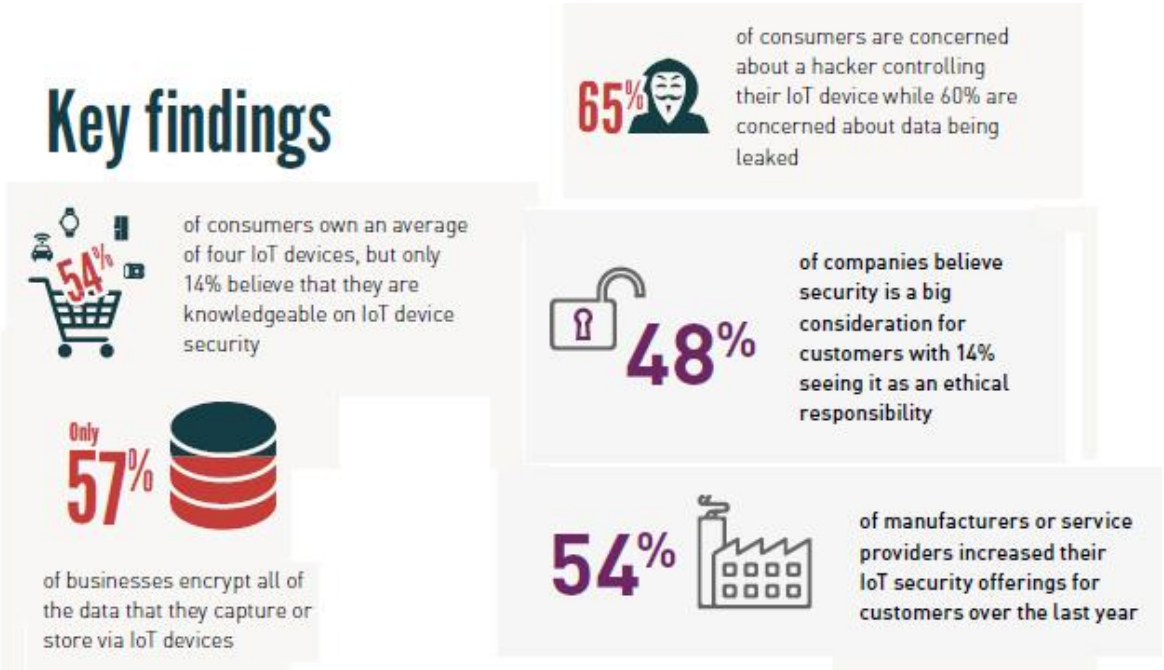


Ilustración 2: Elaboración propia en base a Key Findings de IoT-Security-Reports-Gemalto- 2017-2018 [3]

1.2 Dos enemigos: la “fatiga de la seguridad” y la “paradoja de la privacidad”

A primera vista una de las posibles soluciones para los enfrentar los desafíos planteados por el mercado de IoT orientado al consumidor sería mejorar la capacitación de los consumidores en temas de seguridad y privacidad de la información. Se presenta entonces el debate sobre si resulta útil y factible esforzarse en capacitar a los usuarios para que puedan realizar acciones y tomar decisiones informadas con respecto a la seguridad de sus dispositivos o si debe ponerse el foco en avanzar en procesos de certificación y rotulación que alivien a los usuarios de, al menos parte de, esa responsabilidad. Apoyando esta última postura se encuentran estudios como el del 2016 del NIST [4] que demuestran que la mayoría de los usuarios 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, que los lleva finalmente a albergar sentimientos de resignación y pérdida de control. Estas reacciones los pueden 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 en muchos casos terminan definiendo la compra de productos por cualquier otra característica diferente a la seguridad e ignorando completamente las recomendaciones y advertencias sobre el tema. [3]

Estudios recientes [5] han comprobado y cuantificado el efecto de la fatiga de la seguridad en la intención de seguir las recomendaciones de seguridad por parte de los usuarios e incluso han demostrado que el efecto negativo es superior a lo anticipado en trabajos anteriores.

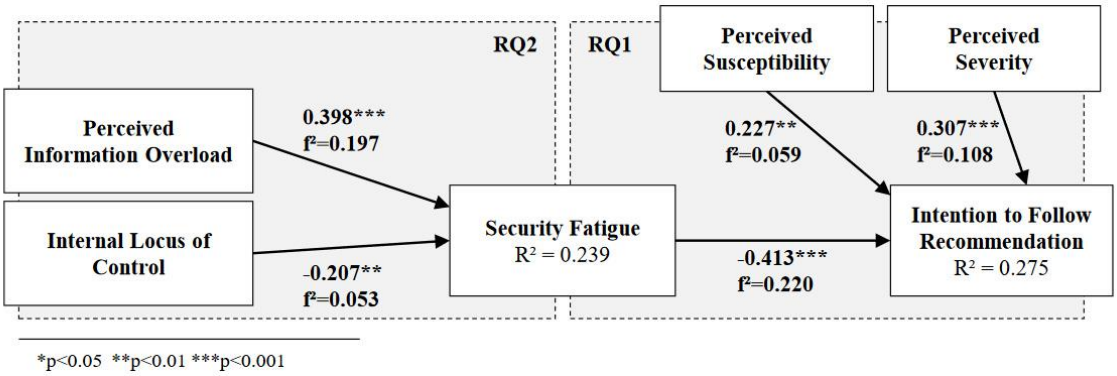


Ilustración 3: La relación entre las causas de la fatiga de la seguridad y su efecto en el comportamiento del usuario de acuerdo al estudio "Cause and effect of Security fatigue". [5]

Por otro lado, en relación con la privacidad, el desafío está planteado por otra característica que afecta a muchos 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, 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, no pudiendo prescindir de los beneficios que ofrece la tecnología, prestan poca o ninguna atención a las opciones provistas y a los términos y condiciones relacionados con la privacidad, aceptándolos sin entenderlos o directamente sin leerlos. [6]

Teniendo en cuenta lo anterior sería ideal que las opciones o soluciones de seguridad y privacidad disponibles para el consumidor le demandaran la menor cantidad de esfuerzo y que pudieran ser comprendidas y utilizadas por usuarios con la mínima capacitación. Por lo tanto cualquier esquema de rotulado deberá tener en cuenta estas características y convertirse en un aliado en la tarea de aligerar la carga sobre el consumidor: es decir poder proveer mayor confianza en los dispositivos IoT adquiridos sin exigirle más acciones, a menos que sean requeridas por él mismo.

Idealmente, en realidad, debería poder asegurarse que la industria incluya "seguridad por diseño" (*security-by-design*) y "privacidad por diseño"

(*privacy-by-design*[2]) en las soluciones IoT desde la fase de concepto y ambas sean integradas 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, de acuerdo a estar idea, “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 obtendría 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. [7]

Veremos a continuación porqué esto no sucede en la actualidad y porqué hay pocos incentivos para que las empresas dediquen esfuerzos a mejorar la seguridad y privacidad de los dispositivos IoT.

1.3 Fabricantes y proveedores de servicios: asimetrías y falta de incentivos.

En la actualidad 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 suelen integran los componentes de estas últimas sin verificar su seguridad, la interoperabilidad entre ellos y la compatibilidad con otros dispositivos. [8].

. 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

[2] Enfoque desarrollado inicialmente por Ann Cavoukian, formalizado en 1995 y actualizado en 2009 (https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf accedido 27/11/2020)

enlentece la producción. Una vez terminado el producto, la necesidad es realizar lanzamientos rápidos, habitualmente sin la adecuada prueba. Desafortunadamente, aún 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 [3].

Sumado a lo anterior, la falta de información y advertencias sobre seguridad y privacidad en los embalajes de los productos, y la ausencia de certificación, homologación o regulación por parte de organizaciones gubernamentales o privadas deriva en una falta de incentivo para las empresas fabricantes y proveedoras de servicios para mejorar la seguridad y privacidad de los dispositivos.

La falta de incentivos es acompañada por otro problema que podría llamarse de “asimetría” de la información entre los fabricantes y consumidores. Estas asimetrías se deben a la falta de información precisa y accesible sobre la seguridad real de los diferentes productos lo que hace muy difícil al consumidor, y también a los vendedores, establecer la seguridad que ofrecen éstos. Por ejemplo, una investigación reciente abarcó la revisión de 270 dispositivos IoT para establecer cuanto podían determinar los consumidores acerca de su seguridad antes de la compra. Los investigadores encontraron que en la inmensa mayoría de los casos muy poca o ninguna información estaba disponible [9].

Para el consumidor es casi imposible saber las capacidades exactas de los productos IoT que va a “invitar” a sumarse a su vida. Mucho menos si las compañías fabricantes y proveedoras de servicios cumplen con buenas prácticas y son responsables con el manejo de datos. Por lo tanto se inclina a preferir otros atributos del producto antes que la seguridad y privacidad.

Esto se extiende incluso a *reviewers* y *testers*[3] profesionales, que junto con organizaciones de defensa del consumidor han estado luchando con la forma de probar los productos IoT. Es claro también que si la forma de

[3] Podrían traducirse como “revisores” y “probadores” de productos.

comportarse de un producto puede cambiar del día a la noche entonces los métodos tradicionales de prueba son inadecuados por naturaleza. [10]

Todas estas asimetrías se manifiestan en decisiones de compra poco informadas por parte del consumidor y son aprovechadas por los potenciales atacantes debido a la proliferación de dispositivos conectados que son inseguros. Peor aún, dichos atacantes conocen la forma de obtener detalles acerca de las vulnerabilidades de los productos, que pueden encontrarse a veces abiertamente en internet, en su versión “oscura” (*dark web*) o eventualmente por propia experimentación.

2. Desafíos de Seguridad y Privacidad para el consumidor de IoT

En el trabajo anterior del autor “Soluciones tecnológicas, de regulación y gobierno para los desafíos de IoT” [3] se mencionan numerosos desafíos con respecto a la Seguridad y Privacidad de IoT en general y muchos de estos son directamente aplicables a la situación del consumidor. En las secciones siguientes se resumen las principales amenazas que plantean los dispositivos IoT específicamente para el consumidor:

2.1 Vigilancia

Espías, delincuentes, e incluso agencias gubernamentales en nombre de la seguridad nacional, pueden utilizar dispositivos comprometidos para activar micrófonos o cámaras sin la autorización ni conocimiento del usuario.

En algunos casos, espiar requiere sencillamente interceptar las comunicaciones no encriptadas que emiten dispositivos inseguros, tales como juguetes “inteligentes”. Un ejemplo muy conocido es el de la muñeca Cayla en 2017, prohibida luego en varios países de la Unión Europea, que no solo transmitía localmente datos de voz de los niños de forma insegura, sino que era utilizada por el proveedor de servicio para grabar y almacenar esa información sin permiso. [11] En el último capítulo de la tesis se menciona nuevamente este caso en relación con cómo detectar y medir las vulnerabilidades de un dispositivo y poder calificarlo.

Ilustración 4: Noticias como la de la muñeca *hackeada* Cayla no ayudan a ganar la confianza del consumidor. [4]

El incidente de los televisores Samsung comprometidos por personal de la CIA y la NSA para activar de forma inadvertida micrófonos y cámaras es un ejemplo más avanzado de esta amenaza, tal como fue evidenciado por documentos filtrados por Wikileaks en 2017, entre los cuales pudieron incluso obtenerse las instrucciones desarrolladas en cooperación con el servicio de inteligencia Británica MI5 para realizar este tipo de intrusiones. [12]

Aunque el nivel de sofisticación para realizar estas últimas acciones es bastante alto, los usuarios perciben una amenaza potencial aun mayor a la real. Y las investigaciones sugieren que “aún la percepción de que exista una posibilidad remota de vigilancia tiene un efecto de auto-censura en los individuos y erosiona la confianza en IoT”. [13]

2.2 Integridad física:

Cuando los problemas de seguridad digital avanzan sobre el mundo físico la integridad física del usuario puede ser comprometida. Esto se pone de manifiesto, por ejemplo, cuando la transmisión de un automóvil puede ser manipulada remotamente o cuando los sensores de dispositivos *wearables* que capturan la ubicación física de personas expuestas políticamente (PEP) pueden ser comprometidos por posibles atacantes.

[4] Captura de pantalla de https://www.mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112

Ya a partir del año 2010 se encuentran referencias comprobables de que los sistemas conectados de los vehículos podían ser comprometidos a distancia y una vez obtenido en control llevarlos a realizar maniobras que ponen en peligro real tanto a la integridad física del conductor como a los peatones o conductores circundantes. [14]

Incluso en las filtraciones de Wikileaks mencionadas en el punto anterior se incluye la denuncia de que la CIA y la NSA intentaron extender sus actividades de espionaje y control remoto de dispositivos a los automóviles conectados, convirtiendo a estos en posibles vehículos para “asesinatos prácticamente indetectables”. [15]

2.3 Venta de información

Los dispositivos IoT, a través de sus sensores, recaban gran cantidad de información personal de los usuarios. Parte de esta información es habitualmente vendida por el proveedor de servicios a otras corporaciones con o sin el consentimiento del usuario. En su defensa los proveedores alegan que dicha información es previamente 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.

Por medio de la fusión de sensores los datos obtenidos por 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. Esto permite que, al combinarse datos completamente anonimizados, utilizando potentes algoritmos, finalmente pueda inferirse casi con certeza al individuo generador de la información. [3]

Muchas compañías comerciales están aplicando técnicas de *Big Data* a información obtenida por IoT por dispositivos hogareños 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" [16].

2.4 Delegación de la autonomía y dependencia

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 ayudarles. El riesgo de dicha delegación es que la ubicuidad de IoT y 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" [17] o proveedores de servicios.

La dependencia en los dispositivos IoT puede ser difícil de advertir. Por ejemplo muchos productos utilizan tecnología en la nube para su control y no cuentan con métodos de configuración manual. Por ejemplo, si los servicios de Amazon AWS o Microsoft Azure cayeran, algo que se espera que suceda raramente, pero que no es imposible, numerosos dispositivos IoT perderían la capacidad de conectarse a través de IFTTT[5], un servicio web utilizado para programar comportamientos simples de objetos conectados. Es posible entonces que si estos servicios no se encuentran disponibles, algo tan vital como la calefacción o la iluminación de una casa dejen de funcionar. [10]

[5] "If This, Then That" o en español SIEEE (Si [ocurre] esto, entonces [haz] eso)

Ilustración 5: ¿Si AWS dejara de funcionar las rosas se secarían? [6]

Las actualizaciones de software de los dispositivos son habitualmente una ventaja. Sin embargo el usuario no puede estar seguro de que una actualización pueda cambiar el comportamiento esperado por el dispositivo IoT, modifique configuraciones de seguridad o privacidad o simplemente deje al dispositivo inutilizable.

La funcionalidad de los dispositivos IoT, de los que se dependa para realizar distintas tareas, puede ser reducida o discontinuada por falta de soporte o incluso por decisiones estratégicas. Es el caso de dispositivos que podrían funcionar correctamente si fueran actualizados o si pudieran ser operados por un tercer proveedor, pero por falta de ese soporte se convierten en basura electrónica.

2.6 Otros desafíos para el consumidor

Algunos de los productos que pueden alojar dispositivos IoT, por ejemplo, una vivienda o un automóvil son susceptibles de ser revendidos. Los usuarios no quieren que sus datos personales almacenados, o los algoritmos entrenados con esos datos caigan en manos desconocidas. Sin embargo, es muy difícil para el usuario determinar si ha podido eliminar sus datos registrados tanto en los dispositivos como en los almacenamientos externos de los proveedores de servicio.

Otro de los beneficios que brinda IoT en conjunto con la fusión de sensores y *Big Data* es la posibilidad de diferenciar a los consumidores con

[6] Captura de pantalla de http://wikipage.rainmachine.com/index.php?title=File:Ifttt-amazon-echo-rainmachine-3.png

más precisión que nunca antes y con la que también pueden generarse nuevas formas de discriminación. Empleadores, aseguradoras y vendedores por nombrar solo a algunos interesados, podrían utilizar los millones de datos de los consumidores 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. [8]

2.7 Hacia la protección del consumidor

El reconocimiento de estas problemáticas ha llevado a los gobiernos a introducir regulaciones y a apoyar iniciativas de certificación y desarrollo de estándares para enfrentar los desafíos de seguridad y privacidad en IoT.

Un avance importante en este sentido fue la aprobación en 2016 y la entrada en vigencia a partir de mayo de 2018 de la normativa europea GDPR (Regulación General de Protección de Datos), largamente esperada y debatida en el seno de la Comisión Europea, que implementa fuertes multas sobre las organizaciones que infrinjan las normas de privacidad. También la reciente publicación de normas y estándares específicos sobre seguridad en IoT, que apuntan a proveer un marco de referencia integral a las compañías fabricantes y proveedoras de servicios. [3]

Sin embargo, estos avances aún no han tenido un impacto real en la protección del usuario final al momento de tomar una decisión de compra y durante la vida útil del producto.

Es por eso que numerosos gobiernos y organizaciones han propuesto medidas específicas para mejorar esta situación. Una de las recomendaciones principales en que coinciden casi todas estas iniciativas es la de implementar un sistema de rotulado en relación a los riesgos de seguridad y privacidad de los productos IoT.

Como primer ejemplo podemos tomar el de la iniciativa de un sistema de rotulado global de la Comisión Europea con su “IoT Confiable”, dentro de

la propuesta de un Mercado Común Digital, en la cual se indica: “Uno de los desafíos de IoT con respecto a las políticas de la Comisión es reforzar la confianza y la seguridad al mismo tiempo que la protección de los datos personales y la privacidad. Una de las posibles soluciones a este desafío sería el desarrollo de una etiqueta “IoT Confiable” que proveería a los consumidores de IoT información acerca de los niveles de seguridad y privacidad de los productos. Esta etiqueta “IoT Confiable” podría ser similar a las utilizadas en actualmente para indicar la eficiencia energética en los electrodomésticos vendidos en la Unión Europea” [18]

Un segundo ejemplo de estas iniciativas es el del NIST, a través del reporte de la Comisión para mejorar la ciberseguridad nacional de Estados Unidos, que adopta esta perspectiva y refuerza muchos de los argumentos ya mencionados anteriormente en esta tesis indicando que la solución ideal para los desafíos de IoT “es que todos los dispositivos puedan ser considerados ‘seguros para la venta’. Pero hasta que eso pueda cumplirse las compañías deben proveer suficiente información para permitir a los consumidores tomar decisiones informadas e inteligentes en relación a la seguridad al adquirir productos y servicios de tecnología. Un objetivo adicional de este esfuerzo debería ser convertir a la ciberseguridad en un diferenciador de mercado”. [19]

En concreto, el NIST vehiculiza esta recomendación como Ítem de Acción 3.1.1 del reporte de la siguiente manera: “Para mejorar las decisiones de compra de los consumidores, una organización independiente debería desarrollar el equivalente a las “etiquetas nutricionales” de ciberseguridad para productos y servicios tecnológicos, idealmente relacionado con un sistema de calificación entendible e imparcial de evaluación por tercera partes que los consumidores comprendan intuitivamente y en el que puedan confiar” [19]

El objetivo de estos esquemas entonces es doble: en primer lugar que le facilite al consumidor realizar una decisión informada al comprar productos IoT y le advierta de potenciales riesgos, y en segundo lugar que la implementación de dicho marco incentive a las empresas fabricantes o ensambladoras a aplicar mejoras de seguridad y privacidad desde el diseño

de forma de obtener mejores resultados en las mediciones o eventualmente poder certificar u homologar los productos, y de esta forma destacarse entre la competencia.

3. Alternativas de información al consumidor

Una vez establecida la necesidad de proveer al consumidor un sistema de rotulado con respecto a seguridad y privacidad de dispositivos IoT el siguiente paso no es trivial ya que deberá definirse por un lado, qué información proveer y de qué forma, y por otro, qué y cómo se mide y quién lo hace para nutrir al sistema de rotulado. Los dos primeros aspectos se analizarán en el presente capitulo, los últimos en el siguiente, en conjunto con la temática de certificación y homologación de IoT.

Las decisiones que se tomen en relación a la forma y cantidad de información deberán ser las que permitan lograr el mayor impacto posible con el esquema de rotulado. Los desafíos son variados y los aspectos a considerar tan disímiles como los de diseño, que conduzcan a encontrar un formato que sea fácilmente distinguible y comprensible para el usuario, como los de índole económica, que permiten determinar cuánto valora el consumidor la seguridad en relación con otros atributos del producto.

3.1 Tipos de rotulado y propuestas para IoT

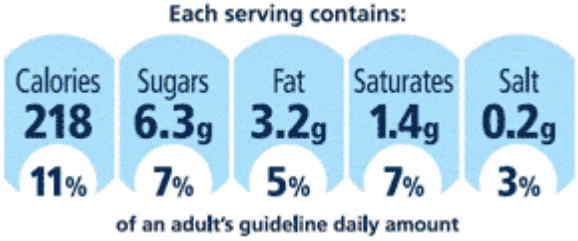
Las etiquetas habitualmente utilizadas en sistemas de rotulado de productos, no solo tecnológicos, pueden agruparse en tres tipos:

1. Sellos de aprobación: Son binarios e indican si un producto ha sido certificado u homologado. La ventaja de este tipo de rotulado es claramente su simplicidad. Su efectividad depende fuertemente de la confianza en la entidad que provee la aprobación. Aunque habitualmente son los preferidos por los consumidores, están asociados a resultados no intencionales como la falsa sensación de seguridad.

Ilustración 6: Sello de aprobación utilizado para indicar conformidad con los estándares de la Unión Europea. [7]

2. Etiquetas de información: Comunican información sobre características del producto en relación a una serie de aspectos o dimensiones. Pueden ser solo gráficas (ilustración 7) o incluir información adicional (ilustración 8) Su principal ventaja es que permiten advertir o informar fácilmente sobre diferentes aspectos seleccionados. Sin embargo, suelen las menos comprendidas por los consumidores con menos conocimiento de los aspectos relevados.

Ilustración 7: Etiqueta informativa de derecho de reproducción y uso Creative Commons. [10]



[7] El sello CE (conformidad con los estándares europeos) es provisto por numerosas empresas y cuerpos certificantes autorizados. La imagen corresponde al sello provisto por IQS: https://iqs-ltd.com/ce-mark/

Ilustración 8: Etiqueta nutricional con información adicional. [20]

3. Etiquetas de calificación o graduada: Comunican la calificación del producto a través de un esquema de niveles predefinidos, representados habitualmente por colores o letras. Estas etiquetas facilitan la comparación entre productos similares y permiten obtener dicha información de un vistazo. En la mayoría de los estudios mostraron tener un mayor impacto en el comportamiento del consumidor y ser comprendidas más fácilmente pero requieren un proceso de evaluación mucho más complejo que los otros dos tipos de etiqueta.

Ilustración 9: Etiqueta de calificación Nutriscore, en uso en la Unión Europea para productos alimenticios. [8]

En el capítulo anterior hemos mencionado dos recomendaciones para implementar un sistema de rotulado para IoT, las del NIST en Estados Unidos y la de la Comisión Europea. La mayoría de los gobiernos que han divulgado informes sobre seguridad y privacidad en IoT han coincidido en las mismas recomendaciones, especialmente en lo que refiere a IoT para el consumidor, tal como puede advertirse en los siguientes ejemplos:

Australia: "… se espera que un proceso de auditoría conduzca a la utilización de un sello de confianza como un símbolo público calificado de conformidad con las mejores prácticas. " IoT Security Guideline – IoT Alliance Australia – 2017 [21]

[8] Imagen de etiqueta adaptada de https://www.distribuicaohoje.com/destaques/portugueses-consideram-nutri-score-como-sistema-de-rotulagem-mais-eficaz/

Países Bajos: “… mejorar el nivel de conocimiento del consumidor IoT a través de un sistema de rotulado que informe a los usuarios el nivel de seguridad…” Recommendation on the cybersecurity of the Internet of Things (IoT) - Dutch Cyber Security Council – 2018 [2]

Reino Unido: “… crear un sistema de rotulado para consumidores de productos IoT para asistir las decisiones de compra y facilitar la confianza en los desarrolladores que adhieran…“ Government's regulatory proposals regarding consumer Internet of Things (IoT) security – UK Department of Digital and Culture – 2020 [22]

A pesar de estas múltiples recomendaciones, a fines de 2020 aún no hay sistemas de rótulos para IoT que hayan sido aplicado en forma extendida, y son muy pocos los sistemas concretos que están implementados, en desarrollo o que han sido propuestos por entidades gubernamentales y privadas.

El primer sello de aprobación disponible para IoT fue el creado en el Reino Unido por el Instituto de Estándares (BSI *British Standards Institute* por sus siglas en inglés), que a su vez ofrece la certificación CE (conformidad con los estándares europeos) entre otras. Al momento de la redacción de esta tesis se encuentra en la última etapa de las pruebas piloto el IoT BSI Kitemark, un sello de aprobación “desarrollado para proveer a los fabricantes una forma de demostrar que aplican medidas para asegurar la seguridad de sus productos una vez conectados a internet”. [23]

Ilustración 10: El sello de aprobación para IOT creado por el BSI. [23]

Nuevamente en el Reino Unido, se encuentra en estudio la aplicación de etiquetas de advertencia e información para IoT. Entre 2018 y 2020 el

Departamento de Cultura, Medios y Digital de dicho país, en el marco del proyecto de regulación concerniente a la seguridad para el consumidor de IoT, realizó una consulta muy amplia incluyendo a fabricantes, proveedores de servicio, desarrolladores, grupos de consumidores, académicos y expertos técnicos acerca de opciones para asegurar que todos los productos vendidos en el Reino Unido cumplan con los lineamientos de seguridad establecidos con el objetivo de proteger la seguridad y privacidad del consumidor. Algunos de los resultados de esta consulta fueron publicados en febrero 2020 y entre ellos se incluyeron los diseños de un sistema de rotulado que se muestran en la ilustración 11.

Estas etiquetas de información se destacan por incluir no solo íconos positivos sino también negativos en los casos en que no se cumplan con las guías recomendadas por la autoridad certificante. [22]

Ilustración 11: Algunos de los rótulos de información propuestos por el gobierno británico. [22]

A pesar de ser el Reino Unido, el pionero en Europa en iniciar estudios y prototipos para un sistema de etiquetado para IoT, fue Finlandia en noviembre de 2019 el primer país Europeo en lanzar un sistema de certificación y rotulado de productos conectados e inteligentes. El programa se creó a fines de 2018 y en tiempo record logró completar estudios, un plan piloto y finalmente la estructura para la inspección y certificación de productos a cargo del laboratorio del Centro de Cyber-Seguridad Nacional,

dependiente de la Agencia de Transporte y Comunicaciones de Finlandia (TRAFICOM). [24]

Ilustración 12: La etiqueta provista a los dispositivos IoT aprobados en Finlandia. [24]

La etiqueta provista por el sistema finlandés es una combinación de sello de aprobación con un segundo nivel de información accesible a través de un código QR[9].

Finalmente, una de las últimas novedades en relación a sistemas de rotulados para IoT fue el lanzamiento en octubre 2020 del "programa de rotulado de ciberseguridad para IoT" en Singapur. En una primera etapa incluye a los *routers* Wi-Fi y a los *hubs* de hogares inteligentes, pero se espera extenderlo a todos los productos IoT en el mediano plazo. El primero en Asia y la zona del Pacífico e inicialmente voluntario, el programa tiene cuatro niveles, los dos primeros de autoevaluación y los dos más altos requiriendo validación por terceras partes. Las etiquetas propuestas son del tipo sello de aprobación, pero contienen la graduación que indica a qué nivel de validación ha llegado el producto. [25]

Ilustración 13: Las etiquetas a aplicar por el nuevo programa de rotulado para IoT de Singapur [25]

[9] Del inglés *Quick Response Code*: Código de respuesta rápida, es un código de barras matricial.

Con respecto a entidades certificantes privadas, la oferta es aún más reducida: realizando una búsqueda rápida de estos servicios en internet, a fines de 2020, solo se pudieron encontrar dos servicios: el de la empresa francesa Digital.security, que ofrece el programa IQS de rotulado de productos "IoT Certificado como seguro" [26] y el de Underwriters Laboratories (UL), un histórico proveedor de certificaciones en Estados Unidos, de verificación del nivel de seguridad como parte de su programa "IoT Security Rating" [27]. Esta última empresa, a pesar de proveer cientos de certificaciones de productos anualmente, al momento de la redacción de esta tesis ha otorgado certificación de IoT a un solo producto. [10]

Ilustración 14: Los sellos de certificación ofrecidos por la compañía UL [27]

3.2 Desafíos de los sistemas de rotulado

Uno de los principales problemas que pueden generar los sistemas de rotulado es la "**falsa sensación de seguridad**". Es decir, que los consumidores entiendan que un dispositivo será inmune a los atacantes o estará completamente libre de vulnerabilidades solo por haber obtenido una alta calificación de seguridad o mostrar un ícono de certificación. Una consecuencia de esta falsa sensación de seguridad podría ser también que

[10] https://verify.ul.com/verifications/365

ante la materialización de alguna amenaza sobre los productos calificados o certificados los consumidores pierdan completamente la confianza en el esquema de rotulado.

Para evitar este problema sería necesario advertir al consumidor que en todos los casos existe un riesgo al conectar los dispositivos a internet y que deben tomarse todas las precauciones posibles para protegerse incluyendo revisar las recomendaciones y advertencias de seguridad y privacidad. [28]

Otro desafío importante es que el personal de venta entienda el significado de los rótulos y pueda transmitirlo a los consumidores. Los responsables de los puntos de venta deberían comprender que el sistema de rotulado establece una referencia y por lo tanto estimula buenas prácticas y eleva el nivel de la industria beneficiando al consumidor y estimulando las ventas de productos IoT.

En ese punto resulta de vital importancia la capacitación y concientización del personal de venta. Si el propio vendedor no está convencido de la importancia de la seguridad y la privacidad como un argumento para la venta difícilmente pueda acompañar el círculo virtuoso que pretende establecer el sistema de rotulado.

El éxito de un Sistema de rotulado también depende de cuan fácil es entenderlo, sin sobre-simplificarlo. Es clave lograr el balance correcto entre accesibilidad y densidad de información. Idealmente incluso el rotulo debería dar a primera vista el nivel de confianza y permitir luego obtener más información detallada a demanda. [10]

Lograr el balance adecuado, sin embargo, no es tan sencillo como parecería a primera vista, como se demuestra en el siguiente caso:

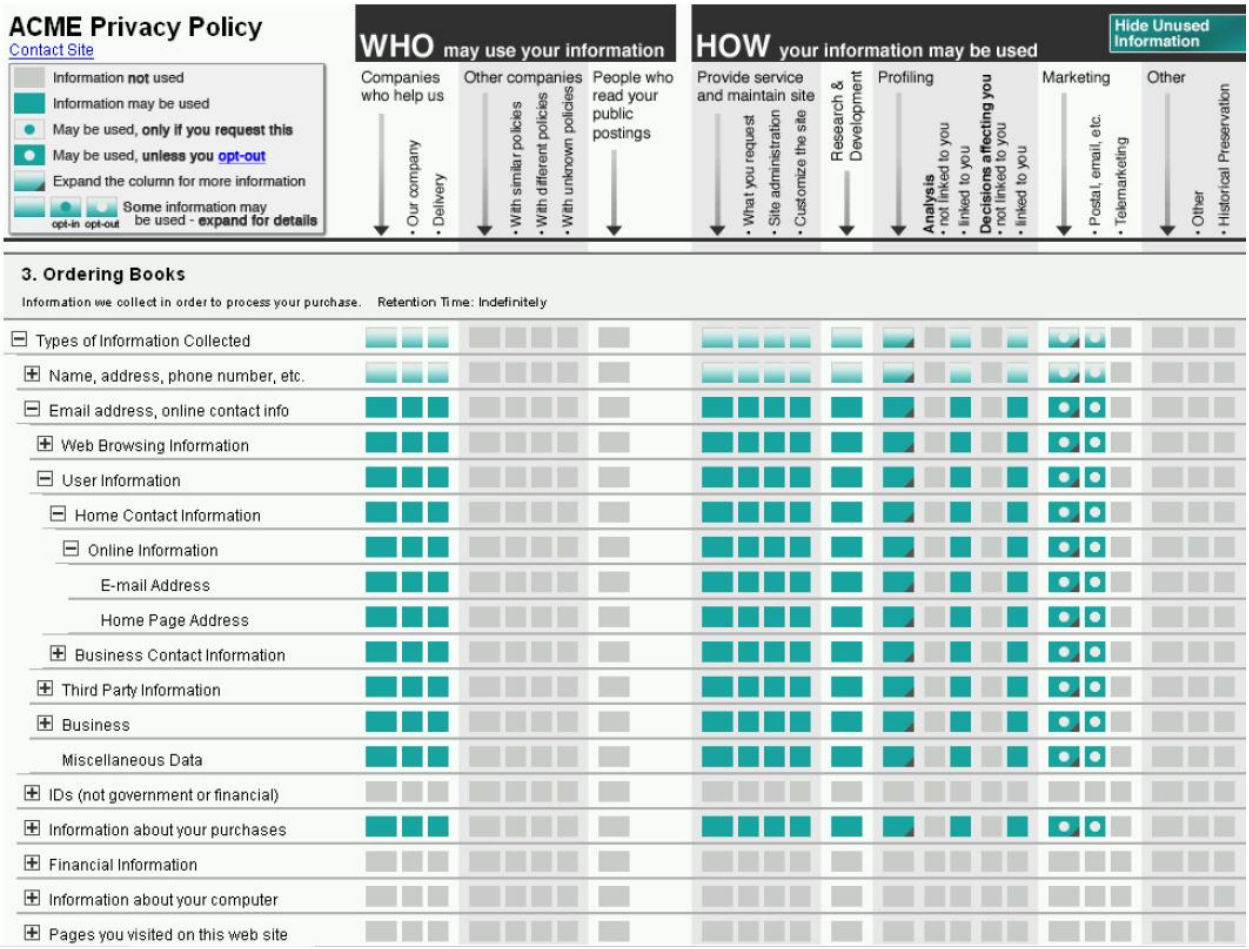


Ilustración 15: el modelo original de información de privacidad en base a las recomendaciones P3P de la WC3. [2]

El modelo anterior es una de las primeras propuestas para mostrar al usuario información sobre privacidad y está basado en las recomendaciones de la World Wide Web Consortium (WC3) para mostrar las opciones de privacidad de los sitios web [29]. Este sistema basado en P3P (Platform for Privacy Preferences) permite a los sitios web representar sus políticas de seguridad en XML y publicarlas sin la necesidad de un software especial. El resultado, del lado del cliente, es una grilla como la presentada en la ilustración que es indudablemente completa y precisa.

Sin embargo, su desarrollo y los estudios realizados sobre el mismo son una valiosa lección para IoT. A pesar de que dicha grilla representa fielmente las opciones de privacidad, distintos estudios han mostrado que no es eficaz como medio de transmitirlas al usuario. Más aun, “los participantes que utilizaron la grilla no pudieron contestar mejor ni más rápido las

consultas sobre el entendimiento de las políticas de seguridad que los participantes que utilizaron leguaje natural. Incluso las medidas de satisfacción de los usuarios mostraron que realmente la grilla les desagradaba.”

No solo la gran cantidad de opciones disponible era una llamada a que los usuarios sufrieran la “paradoja de la privacidad” mencionada anteriormente, sino que muchos de ellos no comprendían los múltiples símbolos ni las posibilidades de expansión necesarias para obtener información importante. [2]

Son reconocidos los estudios de Kelley et al. [30] para adaptar las recomendaciones P3P a un formato más amigable para el usuario. Luego de varias iteraciones, que incluyeron estudios de laboratorio con usuarios, llegaron a presentar algunas opciones de lo que llamaron “etiqueta nutricional de privacidad”. Esta etiqueta elimina las sub-categorías del modelo anterior, concentrando la información en nueve categorías principales que se encuentran a la vista, simplificando también los rótulos y otras opciones.

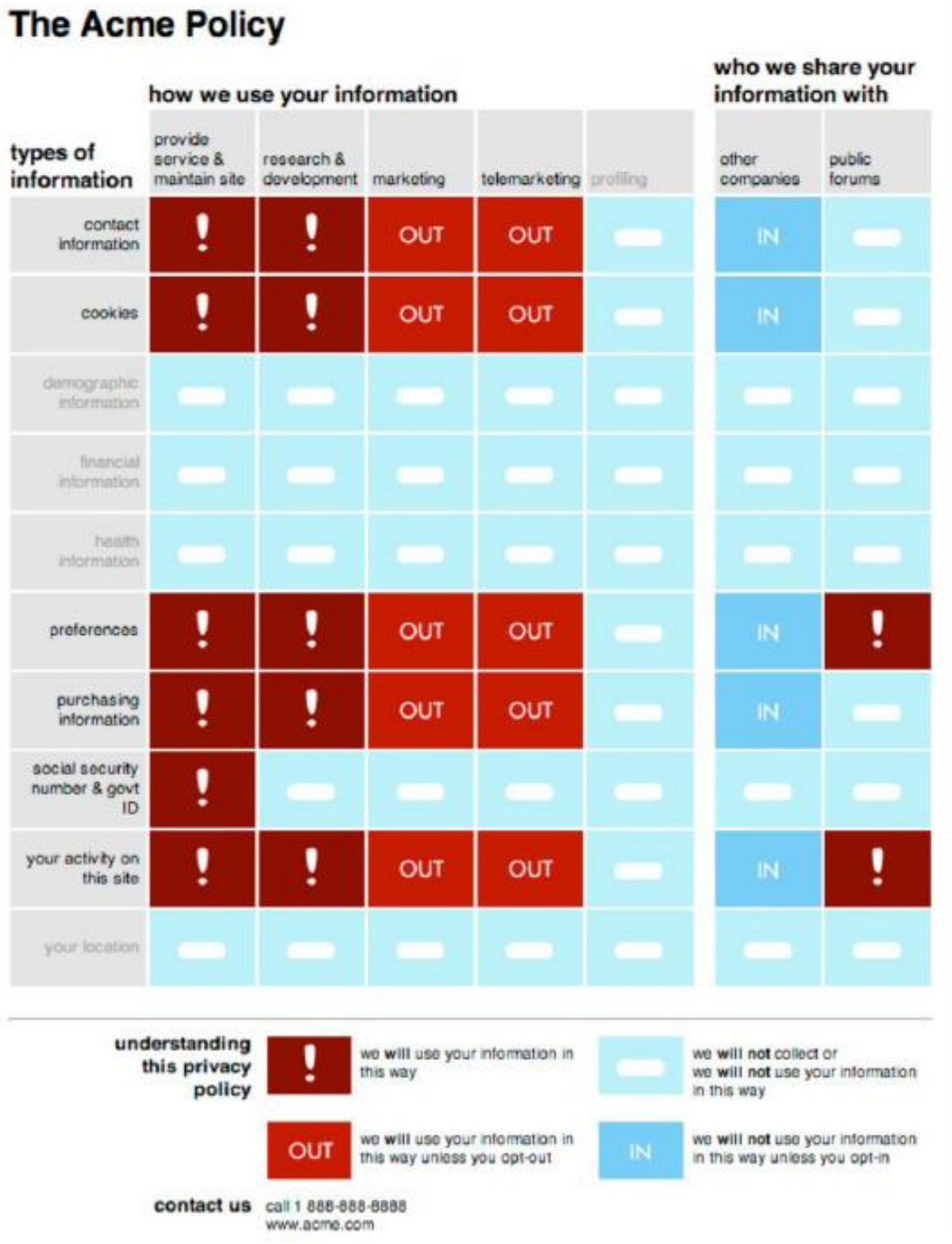


Ilustración 16: Una de las propuestas de "etiquetas nutricionales de privacidad" de Kelley et al. [2]

El resultado es una grilla de comprensión mucho más simple para el consumidor y que, de acuerdo a los resultados de los estudios, resultó más eficiente para transmitir la información de privacidad que el lenguaje natural.

Sin embargo, continúa teniendo dificultades con respecto al exceso de información a procesar por los usuarios y la confusión sobre ciertos términos utilizados. Su aplicación a productos IoT en el embalaje y para permitir la comparación entre varios productos sería claramente muy dificultosa. [2]

Otro desafío para asegurar la eficacia del sistema de rotulado es su relación con el diseño del empaque, ya que uno de los lugares más importantes donde los rótulos se ubicarían sería en las cajas en las que los dispositivos son empacados. Dado que estas cajas ya llevan una serie de rótulos (por ejemplo, de conformidad eléctrica o de reciclaje), para que el sistema de rótulos de seguridad pueda influir en las decisiones de compra del consumidor, será importante que las etiquetas sean diseñadas y posicionadas de una forma que el consumidor pueda y quiera prestarle atención. En algunos casos el uso de etiquetas autoadhesivas puede ser evaluado. [28]

Finalmente, otro inconveniente a salvar al plantear el objetivo de modelar el comportamiento de los consumidores es la falta de entendimiento de cuánto valoran estos a la seguridad y privacidad entre otros atributos de los productos de IoT y cuánto estarían dispuestos a pagar por un producto seguro.

Esta medida, la disposición a pagar (*willingness to pay*, WTP por sus siglas en inglés) identifica la máxima cantidad que un consumidor pagará por un producto y es útil para estimar cuanto está dispuesto a pagar el consumidor por un producto que a través de un esquema de rotulado transmite mayor seguridad. [28]

3.3 Dos modelos ya establecidos: Información nutricional y energética

Los sistemas de rotulado de productos tanto para la información nutricional como para la información de consumo energético existen desde hace varias décadas. A diferencia de otras áreas, entre ellas la de productos de tecnología, se cuenta con numerosos estudios que analizan sus ventajas

y desventajas en relación a su eficacia para afectar el comportamiento del consumidor.

Uno de los primeros comparativos para cualquier tipo de rotulado para el consumidor es el de la información nutricional, y el rotulado IoT no es la excepción. En numerosos estudios y recomendaciones, como la anteriormente mencionada del NIST, se habla incluso de Etiquetas de Seguridad (y/o Privacidad) Nutricionales para establecer la comparación.

Hasta hace poco tiempo en la mayoría de los países era obligatorio incluir solamente una tabla de información nutricional en los productos, pero recientemente se han sumado iniciativas y legislación para incluir rótulos fácilmente legibles y comprensibles por el consumidor en el frente de los embalajes. Estos rótulos, se dividen entre las etiquetas de información, con advertencias sobre el contenido poco saludable y las etiquetas de calificación o graduadas tipo Nutri-Score de la comunidad europea.

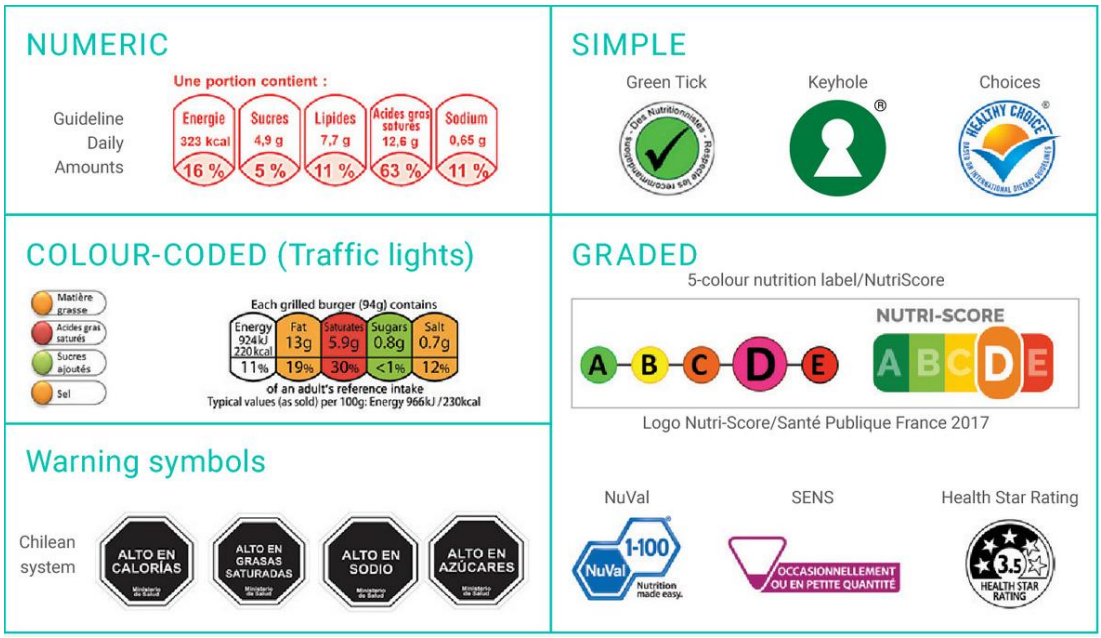


Ilustración 17: Variedad de etiquetas de información nutricional utilizadas alrededor del mundo. [11]

[11] Captura de pantalla de https://www.semanticscholar.org/paper/Development-of-a-new-front-of-pack-nutrition-label-Julià-Hercberg

Haciendo una analogía con IoT, en vez de advertencias sobre el contenido calórico o de sodio incluidos en productos alimenticios, en los productos IoT, siguiendo estos principios, se podría incluir advertencias sobre la capacidad de capturar video o grabar audio por parte de los sensores del producto en cuestión. Es decir que las etiquetas de los dispositivos conectados deberían advertir de las capacidades de hardware, especialmente de los sensores, que pudieran ser relevantes para el consumidor. [10]

Los objetivos de los sistemas de rotulado de información nutricional son básicamente los mismos que se perseguirían en el caso de IoT, es decir: dar al consumidor la posibilidad de realizar mejores decisiones de compra, incentivar a los fabricantes a mejorar los productos haciéndolos más saludables y finalmente permitir a los gobiernos promover el cambio sin impactar directamente en la libertad de la industria alimenticia de producir todo tipo de alimentos. [20]

Este último punto es especialmente importante para su aplicación a desarrollos tecnológicos e IoT en particular, dado que en estas áreas, el gobierno es 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”. [17]. Por lo tanto, la aplicación de los sistemas de rotulado ayudaría hasta cierto punto a aplicar medidas de regulación a IoT, sin afectar a la creatividad y dinamismo de la industria.

Siendo que se utilizan desde hace décadas se podría pensar que las etiquetas nutricionales son ampliamente aceptadas y que su uso está libre de controversias. Sin embargo, la reciente aprobación en el Senado de la República Argentina de la ley de etiquetado frontal de alimentos dejó en evidencia las divergentes opiniones de muchos especialistas sobre dicho tipo de etiquetado, aplicado con mayor y menor éxito en otros países. [31]

Algunos de los problemas que muestran los sistemas de rotulado nutricional son los siguientes. En primer lugar, la coexistencia de muchos tipos de etiquetas confunde a los consumidores. Es deseable que, como se

ha logrado con otras áreas como la de eficiencia energética desarrollada a continuación, se logre una cierta estandarización de los sistemas de rotulado y que los mismos sean ampliamente aceptados. El siguiente problema es el del poco tiempo que tiene el consumidor para realizar elecciones al momento la compra que reduce la cantidad de tiempo que pueden dedicarle a analizar la información provista por los rótulos, aunque esto podría no ser relevante para la compra de IoT ya que no se espera que el consumidor deba realizar sucesivas elecciones de productos en corto tiempo. Finalmente, los sellos de aprobación suelen sobre-simplificar las elecciones, es decir el consumidor suele caer en la tentación de encasillar los productos en buenos y malos, sin distinguir las diferencias entre ellos.

Con respecto a los sistemas de etiquetado para la información energética, existe mucha menos variedad. Casi todos los rótulos utilizados son variantes de la etiqueta de energía de la Unión Europea que es del tipo calificado o graduado, e indica la eficiencia energética en un rango tradicionalmente de la letra A a la G, reforzado por colores.

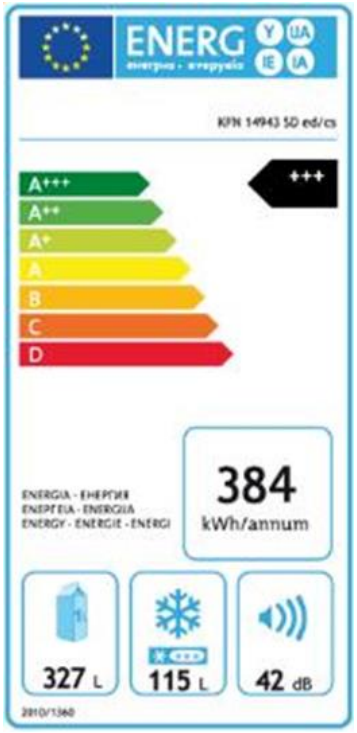


Ilustración 18 – Etiqueta de eficiencia energética de la Unión Europea. [20]

Se suele acompañar dicha calificación de eficiencia con información adicional en recuadros incluyendo otros datos que se consideran importantes para el consumidor al momento de realizar la compra. Dicha información se representa en etiquetas de información en combinación con la etiqueta graduada principal.

Los objetivos de este sistema, que son similares a los mencionados para el sistema de rotulado nutricional, se han cumplido con creces y ha incentivado a las empresas productoras a esforzarse en mejorar la eficiencia energética e invertir en investigación y desarrollo en ese campo. Los estudios demuestran que la presencia de la etiqueta en un lugar prominente hace que los consumidores presten más atención a la eficiencia energética y se estima que gracias a la aplicación del sistema para 2020 se habrán ahorrado aproximadamente 175 Mtep (millones de toneladas equivalentes de petróleo) que equivale al consumo de energía anual de un país como Italia. [20]

La etiqueta de eficiencia energética, sin embargo, tiene problemas particulares que han sido creados por su propia evolución. La mayor eficiencia lograda por muchos productos de ciertas categorías desde la instauración del sistema de rotulado en 1995 hizo que una década más tarde la mayoría de esos productos calificaran en el nivel A. Se debatió por entonces entre dos alternativas: modificar los límites de cada nivel de la graduación para distribuir de mejor manera los productos o agregar nuevas categorías por sobre la A. Finalmente se decidió por la segunda alternativa y en 2010, para cierto tipo de electrodomésticos se incluyeron nuevas categorías A+ a A+++ para simbolizar mayor eficiencia.

Esta decisión sin embargo ha sido poco beneficiosa para dirigir las elecciones de consumidor: en primer lugar, porque los consumidores no perciben la diferencia entre A y A+++ de la misma forma que entre A y G. Por lo tanto, la mayoría se contenta aún con los equipos que cumplen la categoría A, sin comprender que para algunas categorías de productos ese nivel ya representa una eficiencia regular. Por otro lado, ha llevado a confundir a los consumidores al momento de realizar compras de productos de diferentes categorías o incluso de las mismas cuando no se utiliza

exactamente la misma graduación. Este es un error del que otros sistemas de rotulados graduados, como el que podría aplicarse para IoT, deberían aprender.

Otro problema del sistema de rotulado de eficiencia energética es la combinación de etiquetas graduadas con informacionales. Se ha comprobado que los consumidores dan mucha más importancia a la información principal (la graduada) y muchas veces no advierten o no entienden la información adicional, que habitualmente indica el consumo total del producto entre otros datos relevantes. Una consecuencia de dicho problema es que los consumidores están dispuestos a pagar más por productos de mayor eficiencia energética, sin embargo esto no se traduce necesariamente en mejores elecciones, ya que en muchos casos la motivación de comprar un producto eficiente no resulta en la compra de uno que consuma menos. Esto ha sido referido como la falacia de la eficiencia energética: la creencia del consumidor de que alta eficiencia energética implica bajo consumo de energía. [20]

3.4 Estudios sobre el impacto en el consumidor

En los capítulos anteriores ya se han mencionado algunos estudios sobre el impacto de los sistemas de rotulado en las decisiones del consumidor y se ha destacado que hay numerosa bibliografía acerca de los utilizados para información nutricional y energética. Aunque son útiles como un indicador preliminar, estos resultados no deberían extrapolarse directamente a la situación de proveer información sobre seguridad y privacidad de productos conectados a internet.

También se explicó que los sistemas de rotulado de IoT reales aún se encuentran en una fase piloto o han sido implementados solo muy recientemente. Por lo tanto aún no hay estudios sobre el efecto de esos sistemas en las decisiones de los consumidores. Los estudios que se mencionan a continuación se realizaron a partir de etiquetas ficticias, pero que coinciden con los tres tipos mencionados al principio del capítulo, en situaciones hipotéticas explorando las preferencias indicadas de los usuarios

y obteniendo conclusiones relevantes para ser aplicadas a los diseños de los sistemas de rotulado IoT. Estos estudios son muy recientes, dos realizados en el Reino Unido y otro en Estados Unidos entre enero de 2019 y enero de 2020.

El primer estudio “Resultados de la encuesta sobre etiquetado de seguridad IoT para el consumidor” [32], encargado por el gobierno del Reino Unido como parte de la investigación para el programa de etiquetado de información mencionado en capitulo anterior, fue realizado por la compañía Harris Interactive a principios de 2019 sobre más de 8000 casos, siendo el de base más extendida hasta el momento.

Para el estudio el Departamento de Cultura, Medios y Digital definió una serie de cuatro tipos de etiquetas de información y requirió investigar varias cuestiones, entre ellas: ¿Cuán importante consideraban los consumidores la información de seguridad?, ¿Cuál de las etiquetas era preferida por los consumidores? y ¿Cuánto estaban dispuestos a pagar los consumidores por un producto que contara con una etiqueta?

La consulta a los consumidores incluyó dos etapas: en la primera se les exhibió solamente una de las cuatro etiquetas para conocer su efectividad evitando cualquier sesgo causado por el conocimiento de las otras; en la segunda se les exhibieron todas las etiquetas para obtener un ranking de preferencias.

	Shield with Text Underneath	Shield with Text Inside	Icons with Text Underneath	Full Lozenge
				
Label Abbreviation	**Label 1**	**Label 2**	**Label 3**	**Label 4**
Smart TV	404	405	412	406
Wearable Device	403	407	403	409
Smart Toy	405	406	403	403
Smart Thermostat	404	402	407	403

Ilustración 19: Dispositivos, etiquetas y distribución de los participantes (número en la intersección) tal como fueron definidas para estudio de Harris Interactive. [32]

Los resultados de este estudio no solo son relevantes en cuanto al diseño de un sistema de rotulado para IoT sino que respaldan numerosas hipótesis de otros trabajos sobre las preferencias del consumidor. Por ejemplo, entre los hallazgos se destaca que el 72% de los consumidores esperaba que la seguridad estuviera provista como un estándar en los dispositivos mientras que otro 19% directamente no comprendía la relevancia de la seguridad. La privacidad no logró mejores resultados: entre las diez primeras características buscadas por los consumidores en un dispositivo IoT se ubicó en el puesto siete siendo mencionada como una de las cuatro más importante por solo 32% de los participantes como puede verse en la ilustración 20.

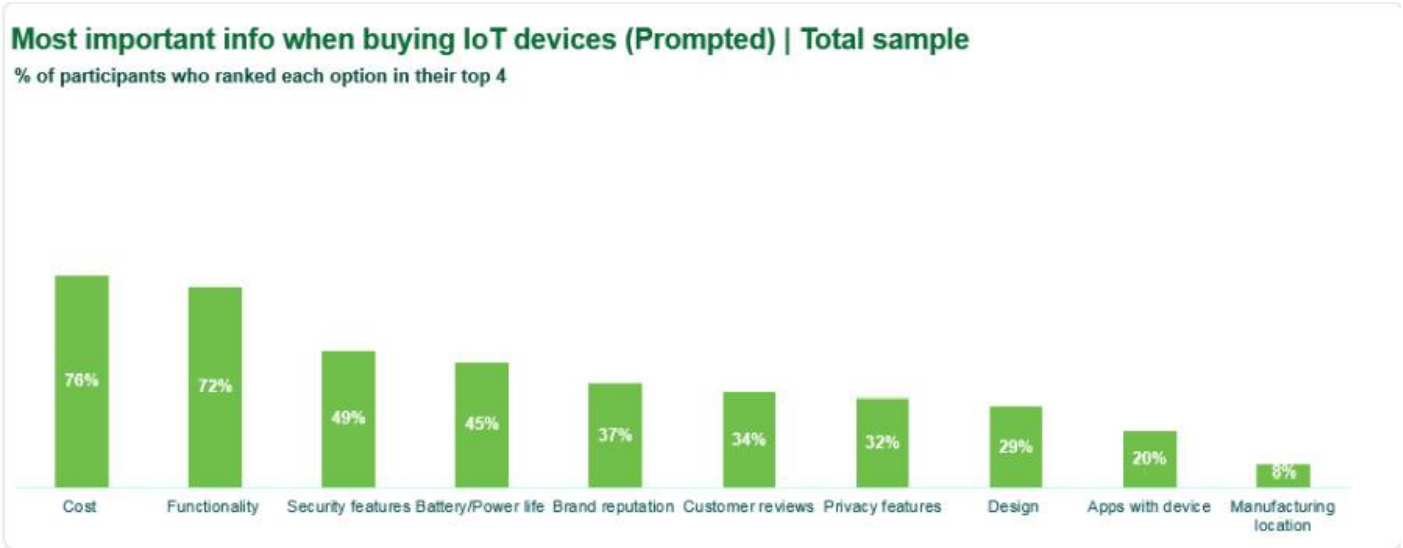


Ilustración 20: La seguridad, y aún más la privacidad, se ubicaron bastante por debajo del costo y la funcionalidad en las prioridades de los consumidores. [32]

Otro hallazgo importante es el que determina qué hacen los consumidores con los dispositivos que ya no usan. Las acciones más elegidas fueron por lejos “dar a un familiar/amigo”, “quedárselo” o “revenderlo”, lo que, tal como fue mencionado en el capítulo 2 en la sección de otros desafíos para el consumidor, los expone tanto a transferir inadvertidamente sus datos a terceras personas como a continuar utilizando y conectando a la red dispositivos fuera de su período de soporte o con conocidas fallas que no han sido remediadas.

Ya con relación a las etiquetas presentadas y su influencia en el comportamiento del consumidor, los resultados indican que el 73% de los participantes expresaron que consideraban importante incluir un sistema de rotulado y, dependiendo de la etiqueta presentada, entre el 49% y el 54% se mostró dispuesto a cambiar su elección de dispositivo en base a los expresado en las etiquetas.

De las cuatro etiquetas propuestas el estudio concluye que la más efectiva es la de los iconos separados con texto explicativo debajo y tal recomendación fue la que utilizó el gobierno británico para su propuesta de sistema de rotulado para IoT mencionada en la sección 3.1. (Ilustración 11). Esta etiqueta fue la que mejor logró transmitir la información deseada y resultó más clara para los consumidores.

Finalmente, el estudio se refiere a la disposición a pagar. En primer lugar se encontró, quizás como era de esperarse, que la disposición a pagar un adicional fue mayor para los productos más baratos, aun cuando la percepción de la importancia de la seguridad fuera prácticamente la misma para todos los productos. En segundo lugar, realizando un promedio sobre todas las etiquetas y todos los productos se obtuvo que hasta 59% de los participantes estaban dispuestos a pagar un 5% más pero solo el 40% de ellos un 10% más sobre el precio de un producto tal como se muestra en la ilustración 21. De todas formas, estos últimos resultados y su metodología de obtención, fueron cuestionados por otros estudios, como se mostrará a continuación.

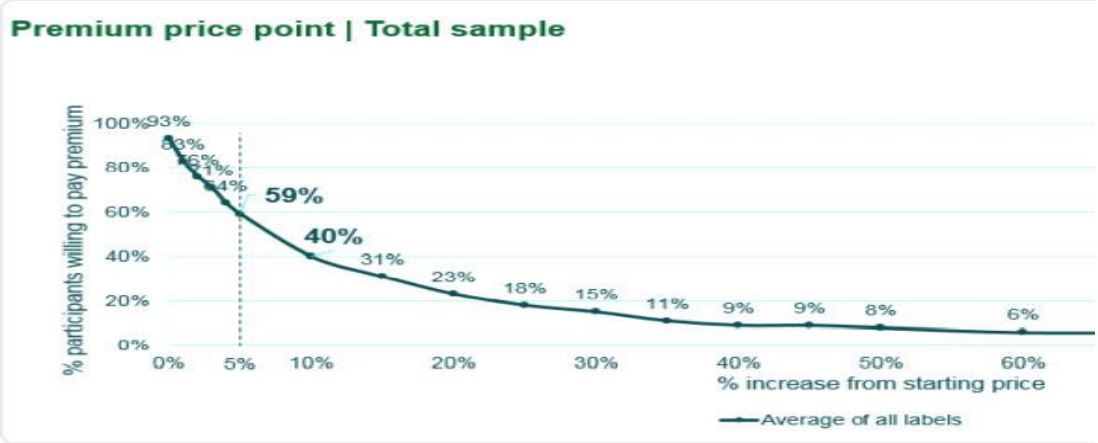


Ilustración 21: La disposición de los consumidores a pagar por mayor seguridad y privacidad de acuerdo al estudio de Harris Interactive. [32]

El estudio de Harris Interactive, aunque es muy completo en relación al comportamiento del consumidor, adolece de una limitación con respecto a la selección del tipo de rotulado y es haber propuesto únicamente etiquetas del tipo informativo. Para determinar qué tipo de rotulado es el más efectivo para IoT debemos consultar un segundo estudio: “El impacto del rotulado de seguridad IoT en las elecciones del consumidor y su disposición a pagar” [28], también realizado en el Reino Unido en 2019.

El estudio, que abarcó a 3000 participantes, analizó las siguientes cuestiones:

1. ¿Cuál es el tipo de sistema de rotulado IoT que tiene el mayor impacto en las decisiones de compra del consumidor?
2. ¿Cuánto están dispuestos a pagar los consumidores por la seguridad de un dispositivo IoT?
3. ¿Hasta qué punto perciben los consumidores que una etiqueta de seguridad asegura que un dispositivo es inmune al *hacking*?

Como puede advertirse, la última pregunta intenta averiguar cuanto afecta al consumidor una posible “falsa sensación de seguridad”, que como fue mencionado en el capítulo 3.2 es unos de los desafíos de los sistemas de rotulado.

Los tipos de rotulado presentados a los participantes fueron los mencionados en el capítulo 3.1, es decir: una etiqueta graduada basada en la de eficiencia energética de la Unión Europea, etiquetas de información con combinación de íconos y texto explicativo, y un sello de aprobación utilizando el logo de *secured-by-design*[12], representados como se muestra en la ilustración 22.

[12] Un logo reconocido en el Reino Unido que representa la aprobación de la seguridad física de las construcciones. https://www.securedbydesign.com/

Ilustración 22: Los tipos de rotulado presentados a los consumidores en el estudio sobre impacto (elaboración propia en base a [28]**)**

El estudio utilizó un método de experimento de elección discreta (*DCE Discrete-Choice Experiment*) que permite cuantificar la importancia relativa que los consumidores asignan a los atributos de los productos, como por ejemplo, funcionalidad y precio. Su objetivo fue estudiar el impacto potencial de los sistemas de rotulado en la decisión de los participantes, luego de controlar la influencia de la funcionalidad y precio del dispositivo.

El uso de este tipo de método de estudio le permitió estimar la disposición a pagar de los participantes por dispositivos que tuvieran una etiqueta de seguridad sin necesidad de preguntarles directamente, reduciendo el sesgo que afecta a otras formas de calcular la disposición a pagar. Como conclusión en ese sentido, los participantes, tal como era esperado, estuvieron dispuestos a pagar más por dispositivos con mejores especificaciones de seguridad, demostradas por la etiqueta. Pero en este estudio esta disposición fue superior a lo esperado, variando entre 29 al 40% del precio del producto dependiendo del tipo de dispositivo.

En relación a la elección del tipo de rotulado el estudio establece que los tres ayudarían al consumidor a tomar mejores decisiones al momento de la compra de dispositivos IoT, aunque los participantes expresaron que el

sello binario de aprobación sería menos útil al momento de seleccionar un producto seguro entre varios otros.

Con respecto a la etiqueta graduada, que no fue evaluada en el estudio anterior, es claro que los consumidores se inclinaban en primer lugar a seleccionar un dispositivo con calificación A; sin embargo al sumarse otras características, como precio y funcionalidad, podían incluso bajar hasta el nivel D pero difícilmente al nivel G. El 48% de los participantes indicó que se necesitaría más información acerca de cómo se evalúan los niveles y los riesgos a nivel seguridad y privacidad que plantearía un dispositivo en cada nivel.

Con respecto a la percepción del riesgo, aunque estaba claramente relacionada con el tipo de etiqueta, dado que por ejemplo los participantes estimaron que un dispositivo con grado A (43%) era menos susceptible a ser *hackeado* que uno con grado G (63%), en realidad esto no significa que los consumidores pensaran que esos dispositivos fueran inmunes. En realidad, aun para las etiquetas consideradas más seguras, los participantes estimaron en más de un 40% la probabilidad de que los dispositivos que tuvieran esa etiqueta pudieran ser comprometidos.

Finalmente uno de los estudios más recientes sobre un hipotético sistema de rotulado para IoT es el realizado por investigadores de la Universidad de Carnegie Mellon en Estados Unidos a principios de 2020 [33]. Se destaca por haber realizado varias rondas de consultas a expertos y académicos para luego entrevistar a consumidores, aunque la cantidad de consumidores encuestados – quince - es muy poco significativa en relación a los estudios anteriormente mencionados.

En base a la investigación inicial, que cubrió muchas de las referencias mencionadas anteriormente en esta tesis, y a la opinión de los profesionales entrevistados se desarrolló una propuesta de etiquetado de dos niveles de información vinculados con un código QR.

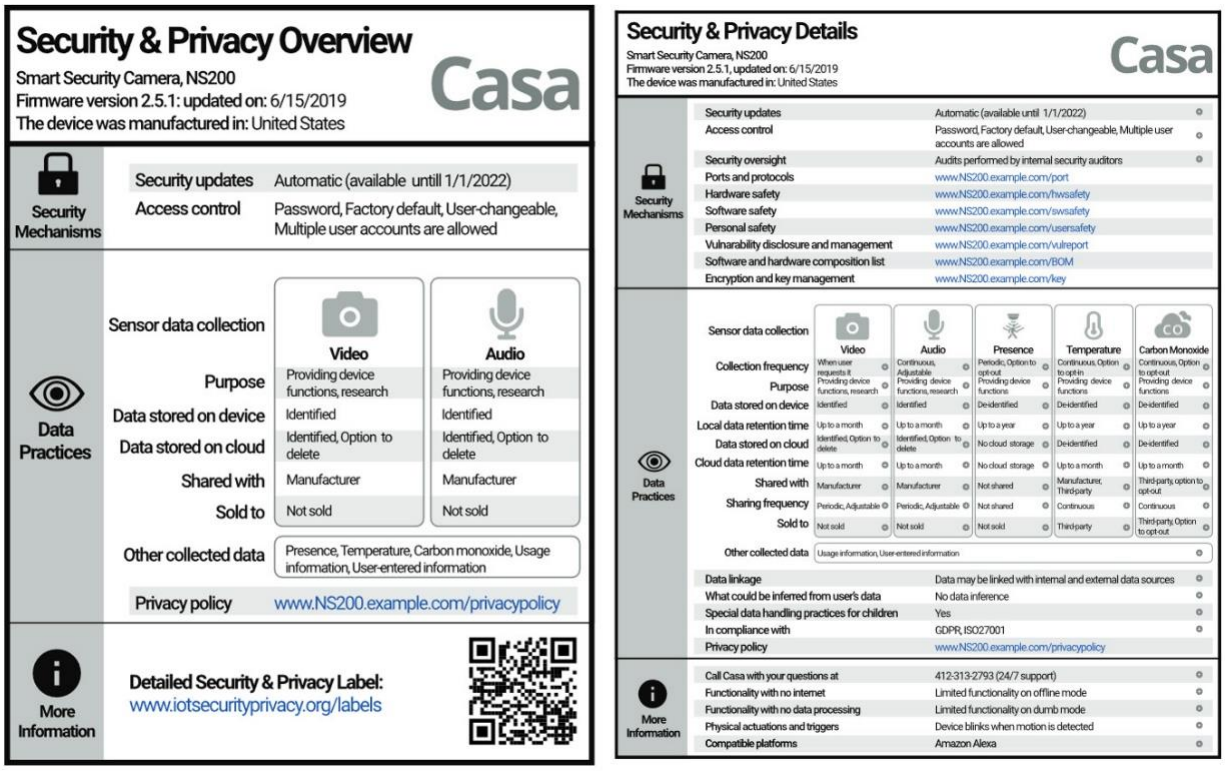


Ilustración 23: La etiqueta con dos niveles de información utilizada en el estudio de Carnegie Mellon [33]

Al ser expuestos a estas propuestas de etiqueta la mayoría de los consumidores encuestados expresó su deseo de contar con un diseño aún más simple del primer nivel cuya información pudiera ser ampliada en la etiqueta de segundo nivel. Muchos de los participantes tuvieron dificultades para asociar la información con el riesgo potencial y con respecto a la información más detallada del segundo nivel casi ninguno pudo utilizarla para establecer o comparar el nivel de seguridad y privacidad de más de un dispositivo. En relación con esto último, el estudio advierte que, aunque la información pueda no ser relevante para el consumidor, su presencia sirve a los expertos para analizar si el producto posee alguna característica cuestionable.

Ilustración 24: Un participante del estudio de la Universidad de Carnegie Melon comparando las etiquetas de dos productos similares. [33]

Otra característica saliente de este estudio es que no pretende quedarse en desarrollar solamente una serie de recomendaciones teóricas, sino que ha sido continuado como un proyecto para proveer a los fabricantes y consumidores de IoT de una herramienta real de rotulado. La última versión de la etiqueta y la información para su implementación junto con una herramienta para generar la etiqueta automáticamente han sido puestas a disposición en www.iotsecurityprivacy.org.

4. Certificación de dispositivos IoT

4.1 Las dificultades para gobernar, regular y definir estándares de 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 [7].

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. Parecería ser 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. [3]

Lo mismo puede decirse del desarrollo de los estándares propios. Al ser IoT una tecnología relativamente nueva, hasta muy recientemente no contaba con estándares aceptados globalmente. Hasta la publicación de los estándares específicos mencionados más adelante, en general se solían 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” [34].

El desafío de la interoperabilidad de IoT condujo a la necesidad de desarrollar estándares que puedan servir como base a programas de certificación. Uno de los primeros grupos creados por la Unión Europea para apoyar el desarrollo de la estandarización en IoT es el ETSI (*European Telecommunications Standards Institute*, Instituto Europeo de Normas de Telecomunicaciones) STF 505 [17].

Este grupo presentó en 2016 uno de los estudios [35] más completos 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.

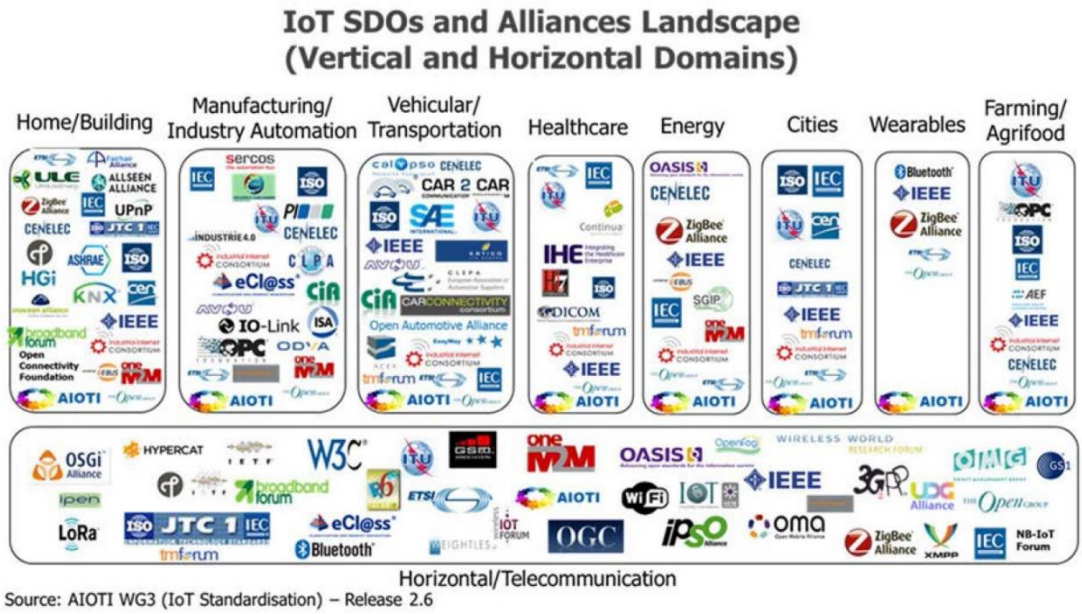


Ilustración 25 – Una vista de la multiplicidad de estándares aplicables a IoT. [36]

De los proyectos mencionados en el estudio de ETSI, se destacaba el de la norma ISO/IEC 30141:2018 [37] en su momento en elaboración y finalmente 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. El objetivo de la norma es que puede servir en forma directa como base tanto para desarrollar aplicaciones específicas de IoT y como para programas de certificación realizados por terceras partes independientes.

Finalmente, el mayor avance para la temática de IoT para el consumidor fue dado por el mismo ETSI, que en febrero de 2019 publicó la especificación 103 645 [38], el primer estándar aplicable globalmente por la industria para el IoT orientado al consumidor. El estándar establece un Código de Practicas muy concreto que puede utilizarse como base para programas de certificación y validación. En la sección 4.3 se mencionan más detalles de su posible utilización.

4.2 El camino hacia la certificación de IoT y sus desafíos

Los desafíos para elegir una forma de certificación están, en primer lugar, relacionados con la gran cantidad de opciones disponibles. Para comenzar existen dos métodos para certificar que un producto o un servicio está de acuerdo con los requerimientos necesarios: el autoevaluado y el evaluado por terceras partes.

En el autoevaluado la organización realiza una revisión de sus propios productos, servicios, procesos y políticas y luego establece su conformidad con los estándares, regulaciones, leyes, buenas prácticas y otros requerimientos externos.

En la evaluación por terceras partes una parte independiente evalúa a la organización que se postula y certifica que se encuentra en conformidad con un grupo predefinido de estándares, regulaciones, leyes, buenas

prácticas y otros requerimientos externos. Este proceso puede ser llevado a cabo por distinto tipo de organizaciones:

1. Organizaciones Gubernamentales: Son organizaciones creadas y administradas por gobiernos como por ejemplo el Programa de Validación del NIST en Estados Unidos, el Europrise Privacy Seal creado por el gobierno alemán y el ya mencionado caso del BSI en el Reino Unido.
2. Organizaciones de la industria: Creadas, respaldadas y mantenidas por la propia industria con o sin fines de lucro. Ejemplos incluyen a ETSI y SAFE-BioPharma.
3. Organizaciones Privado-Públicas: Para estas organizaciones no se puede hacer una clara distinción entre la administración pública y privada. Los ejemplos incluyen a ISO e IEC.
4. Organizaciones privadas: Son entidades con o sin fines de lucro que proveen un sello de calidad. Por ejemplo, TRUSTe o TÜVSÜD.

Al definir qué tipo de certificación utilizar es importante entender el balance a lograr entre la mayor credibilidad (que se traduce en confianza en el producto) y los costos (generados por la burocracia y el proceso mismo de certificación). La autoevaluación es comparativamente fácil y barata de aplicar. La contra es que tiene como inherente un nivel bajo de credibilidad. La certificación por terceras partes tiende a lograr una credibilidad mucho mayor. Pero es más cara y requiere más tiempo y burocracia. [39]

No hay consenso aun sobre cuál de estos acercamientos es el mejor para aplicar a IoT. Es claro que cuanto más baja sea la barrera para implementar la certificación se puede esperar mayor aceptación. Por el contrario, cuanta más alta sea esa barrera, más lento será ese proceso. En casos extremos el costo de la certificación puede ser prohibitivo para pequeñas compañías y en esos casos se corre el riesgo de excluir a estos pequeños pero importantes actores del desarrollo IoT [10]. De esta forma se les impediría poder demostrar que sus productos son seguros, lo que va en contra de los objetivos del sistema de certificación y rotulado ya que le quitaría opciones al consumidor y restaría competitividad al mercado.

Las particularidades de IoT, por ejemplo, la necesidad de interoperabilidad y la cantidad de distintos componentes que forman parte de algunos dispositivos, plantean desafíos adicionales para la certificación.

Esto se debe, a que, para productos de tecnología habitualmente se proponen tres acercamientos posibles: certificar productos, certificar procesos y certificar personas. En IoT definir los límites entre cada dominio es particularmente dificultoso. [40]

Aun entendiendo que para el consumidor de IoT la certificación más significativa será la del producto en sí, para muchos dispositivos no resulta fácil de definir si se tratan de una sola “cosa” o varias. Es claro que productos complejos, como un smartphone, difícilmente puedan certificarse como un todo.

Por otro lado, un ecosistema IoT plantea importantes desafíos para la certificación utilizando a las pruebas tradicionales. El dispositivo IoT y sus funciones locales pueden calificar como seguras, pero en la actualidad es practicante inevitable que utilice servicios de terceros, posiblemente en la nube, para autenticación, monitoreo, o almacenamiento y análisis de información. En particular en relación con la privacidad, los proveedores de estos servicios tienen un rol fundamental al concentrar grandes cantidades de datos de millones de dispositivos.

El riesgo para el consumidor es doble: por un lado, puede realizarse un ataque sobre los proveedores de servicios para intentar sustraer esta información explotando vulnerabilidades de los servicios web o las aplicaciones en la nube. Por otro lado, el mismo proveedor de servicio puede compartir la información con terceras partes sin obtener el consentimiento del usuario. Sin embargo, para las entidades certificantes las vulnerabilidades de los proveedores de servicios son muy difíciles de detectar. Realizar pruebas de penetración en servicios en la nube es casi imposible, por la dificultad de obtener autorización o poder conocer todas las tercerizaciones que suelen implicar estos servicios. [2]

Como desafío adicional, ya se ha mencionado que una de las amenazas para el consumidor de IoT es que una actualización de un

producto pueda realizar cambios en el comportamiento de este o en su configuración de seguridad y privacidad. Si esto sucede podría considerarse si una certificación otorgada al producto en su estado original aún se mantiene o debe actualizarse también. Incluso podría surgir una necesidad de definir un proceso de de-certificación. [40]

4.3 Certificación IoT para el consumidor: ¿Qué y cómo se mide y verifica?

Como se explicó en la sección anterior, la definición de qué debe medirse o validarse para asignar una calificación en un sistema graduado o determinar si un producto es certificado cómo seguro es lo que establecerá la marca que deberán superar los fabricantes de dispositivos y proveedores de servicios. La complejidad y rigurosidad de aplicación de dicha medición estará inseparablemente ligada a la necesidad de poder implementar la certificación o validación a un costo razonable y lograr una aceptación lo suficientemente amplia y rápida para el sistema de rotulado elegido.

Una demostración del desafío que dicha definición implica se encuentra en el derrotero seguido por el proyecto de “Regulación concerniente a la seguridad para el consumidor de IoT” llevado a cabo por el gobierno del Reino Unido entre 2018 y 2020, al que ya hemos mencionado en el capítulo 3.1.

Luego de un estudio que culminó en octubre de 2018, el gobierno publicó un Código de Buenas Prácticas para la seguridad del consumidor de IoT con el objeto de “iniciar y facilitar un cambio positivo en seguridad a lo largo de toda la cadena de producción y venta”. Los 13 ítems a tener en cuenta para cumplir con el código no eran en absolutos extraordinarios y forman parte de las buenas prácticas a verificar por cualquier experto en seguridad de la información. Incluye medidas tan básicas, y claramente necesarias como “facilitar el borrado de información personal”, “validar la entrada de información”, “encriptar la información en tránsito” y “asegurar que la información personal esté protegida“ [41]

Sin embargo, por increíble que parezca, dada su simplicidad y razonabilidad, este código no fue bienvenido por la industria. Las opiniones

negativas recibidas forzaron al gobierno a reconocer “que implementar el código ubicaría una pesada carga sobre los fabricantes […] y esta carga sería sentida más por las pequeñas organizaciones, y puede dañar a la innovación” [22]

Por esa razón en la revisión de febrero de 2020 el gobierno se ha contentado con hacer obligatorios solo tres ítems del listado inicial de trece, e incluso dos de ellos solo parcialmente. El requerimiento ha quedo reducido a su mínima expresión de la siguiente forma:

1. Evitar las contraseñas por defecto: Todas las contraseñas de los dispositivos IoT deben ser únicas y no reconfigurables a un valor default de fábrica.
2. Política de exposición de vulnerabilidades: Proveer un punto de contacto público de forma que investigadores de seguridad puedan reportar incidentes.
3. Mantener el dispositivo actualizado: Los productos informarán explícitamente el tiempo mínimo por el cual el producto recibirá actualizaciones.

Otras iniciativas han preferido evitar este problema, permitiendo a la industria autoevaluarse y haciendo la certificación por terceras partes opcional. Es el caso del sistema implementado en Singapur como puede verse en la ilustración 26: Los fabricantes o proveedores de servicio que deciden autoevaluarse solo pueden obtener los dos niveles iniciales de certificación. Certificantes privados, como el ya mencionado Underwriters Laboratories [27] han seguido la misma práctica, creando distintos niveles de certificación de forma de facilitar el acceso.

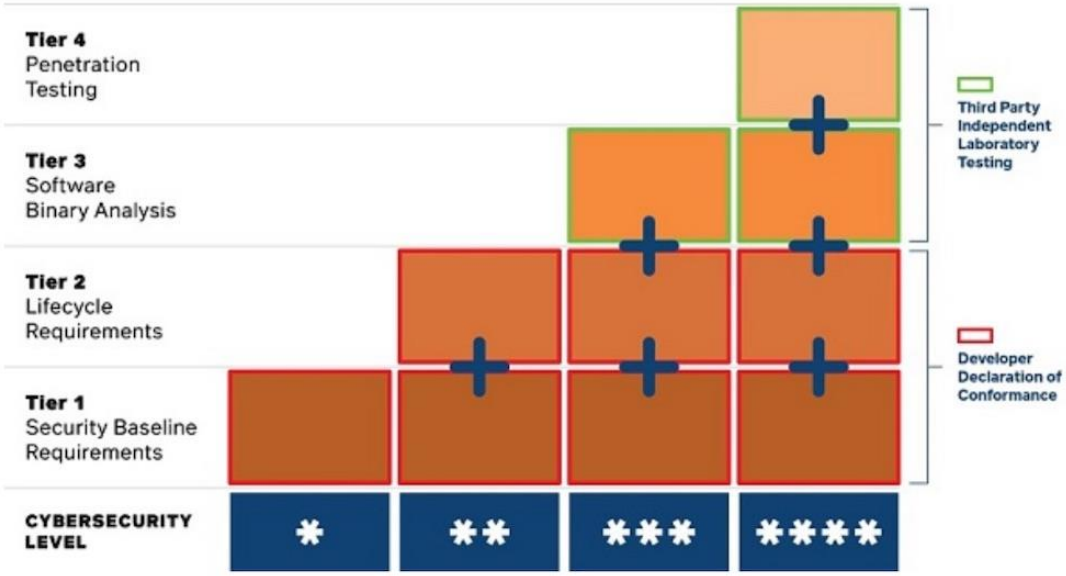


Ilustración 26: El nivel de certificación de seguridad de acuerdo al tipo de medición que acepte realizar el fabricante o proveedor de servicio en el sistema implementado por Singapur. [25]

El riesgo en esos casos es que los fabricantes, al comenzar a certificar sus productos, entiendan que aun el nivel más bajo es percibido por los consumidores como indicativo de un producto seguro, y solo apunten a lograr ese nivel sin preocuparse por mejorar sus prácticas para lograr calificaciones más altas. Por otro lado, quienes están a favor de estas iniciativas, que apuntan a favorecer mayor aceptación, arguyen que la competencia en el mercado empujará a los fabricantes a buscar un mejor nivel de certificación. [33]

Dejando de lado estas dificultades prácticas, y considerando que fuera viable imponer una serie razonable de requisitos para que un dispositivo IoT sea considerado seguro, hay dos fuentes principales que son mencionadas repetidamente en estudios y reportes [2], [10], [21], [22], [27]:

1. OWASP [13] : Una fuente reconocida de guías de seguridad para desarrolladores, fabricantes y proveedores de servicios, provee sus tradicionales *Top 10* de seguridad sobre sitios web desde el año 2004. En los últimos años ha puesto su foco también en IoT convirtiéndose en

[13] acrónimo en inglés de *Open Web Application Security Project*,: ‘Proyecto abierto de seguridad de aplicaciones web”

una fuente reconocida en el ambiente. Su sección *OWASP Internet of Things* [42] no solo contiene el *Top 10 para IoT* sino también proyectos muy completos para validación y prueba de dispositivos IoT. Al momento de la redacción de esta tesis se encuentra en desarrollo la sección sobre regulación y gobierno de IoT. La versión actual de Top 10 para IoT fue desarrollada en 2018 y, si la comparamos con la versión 2014 los principales cambios se refieren a la unificación de la problemática de múltiples interfaces inseguras antes analizadas separadamente (*web*, red, nube, móvil) en una sola Interface del Ecosistema. A la vez se promovió como primer ítem el problema de las contraseñas frágiles o por defecto, algo esperable luego de los ataques globales de denegación de servicio distribuidos (*DDOS*) como el generado por millones de dispositivos IoT infectados por el *botnet* Mirai en 2016 que fueron facilitados por la pobre configuración de contraseñas [43]. Finalmente, aparece listado como novedad en la posición cuarta el problema de los mecanismos de actualización de los dispositivos IoT ya mencionado anteriormente.

OWASP IoT Top 10 2014	OWASP IoT Top 10 2018 Mapping
I1 Insecure Web Interface	I3 Insecure Ecosystem Interfaces
I2 Insufficient Authentication/Authorization	I1 Weak, Guessable, or Hardcoded Passwords I3 Insecure Ecosystem Interfaces I9 Insecure Default Settings
I3 Insecure Network Services	I2 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification	I7 Insecure Data Transfer and Storage
I5 Privacy Concerns	I6 Insufficient Privacy Protection
I6 Insecure Cloud Interface	I3 Insecure Ecosystem Interfaces
I7 Insecure Mobile Interface	I3 Insecure Ecosystem Interfaces
I8 Insufficient Security Configurability	I9 Insecure Default Settings
I9 Insecure Software/Firmware	I4 Lack of Secure Update Mechanism I5 Use of Insecure or Outdated Components
I10 Poor Physical Security	I10 Lack of Physical Hardening

Ilustración 27: El mapeo entre el OWASP *TOP 10* para IOT de 2014 y el actual de 2018 [42]

2. ETSI: La ya mencionada especificación técnica de ETSI (TS 103 645) [38] de febrero de 2019 recomienda trece provisiones para la seguridad de IoT para el consumidor. Cada provisión cuenta con una explicación detallada y en algunos casos con sub-provisiones relacionadas. En el anexo de implementación, que funciona como una validación de cumplimiento, se detallan cuales sub-provisiones pueden considerarse obligatorias y cuales solo recomendadas, una posibilidad que seguramente se incluyó tomando en cuenta la experiencia no del todo positiva del Código de Buenas Prácticas Británico mencionado al comienzo de esta sección y desarrollado en 2018, dado que dicho listado ha servido de base para el de ETSI. [22] Es interesante, por ejemplo, destacar la importancia que se le ha dado al reporte y manejo

de vulnerabilidades (provisión 4.2), intención que ha quedado algo diluida al definirse como obligatorio proveer un punto de contacto (4.2.1) pero no el establecimiento de un tiempo prudencial para la remediación de las vulnerabilidades (4.2.2), ni el establecimiento de un sistema de monitoreo y rectificación durante la vida útil del producto. (4.2.3)

Ilustración 28: Extracto de la tabla de contenidos de ETSI TS 103 645 incluyendo las 13 provisiones de seguridad recomendadas para IoT para el consumidor. [38]

Una vez definido qué es lo que se medirá, el siguiente paso es definir cómo hacerlo y como expresar los resultados. Por ejemplo, para una etiqueta graduada que permita comparar distintos productos los riesgos de seguridad y privacidad deben ser cuantificados de manera consistente. Y para otorgar un sello de aprobación o certificación, en el caso en que la certificación sea provista por terceras partes, debe utilizarse un laboratorio independiente que pueda detectar e intentar explotar las vulnerabilidades de los dispositivos.

Un método muy utilizado para definir vulnerabilidades en software y hardware es el CVSS (Common Vulnerability Scoring System) [44] creado en los años noventa como respuesta a las nuevas amenazas en Internet. CVSS v3.1, la versión actual provee un modelo cuantitativo para medir vulnerabilidades de una manera consistente y factible de ser repetida. El sistema de medición captura las características de una vulnerabilidad y provee una graduación numérica en una escala de cero a diez y una

representación textual de las métricas CVSS utilizadas. A continuación, este método de graduación puede ser traducido a una representación cualitativa como se muestra en la tabla de la ilustración 29.

CVSS Score	Severity rating
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10	Critical

Ilustración 29: Ejemplo de tabla de representación utilizada en el sistema CVSS para cuantificar grados de severidad de vulnerabilidades. [2]

Estas medidas de severidad de vulnerabilidades CVSS pueden ser utilizadas por las organizaciones para proveer una clasificación que podría ser la base para una etiqueta graduada de un producto IoT, volcando la información obtenida en una calculadora como la provista por el NIST[14].

[14] https://nvd.nist.gov/vuln-metrics/cvss

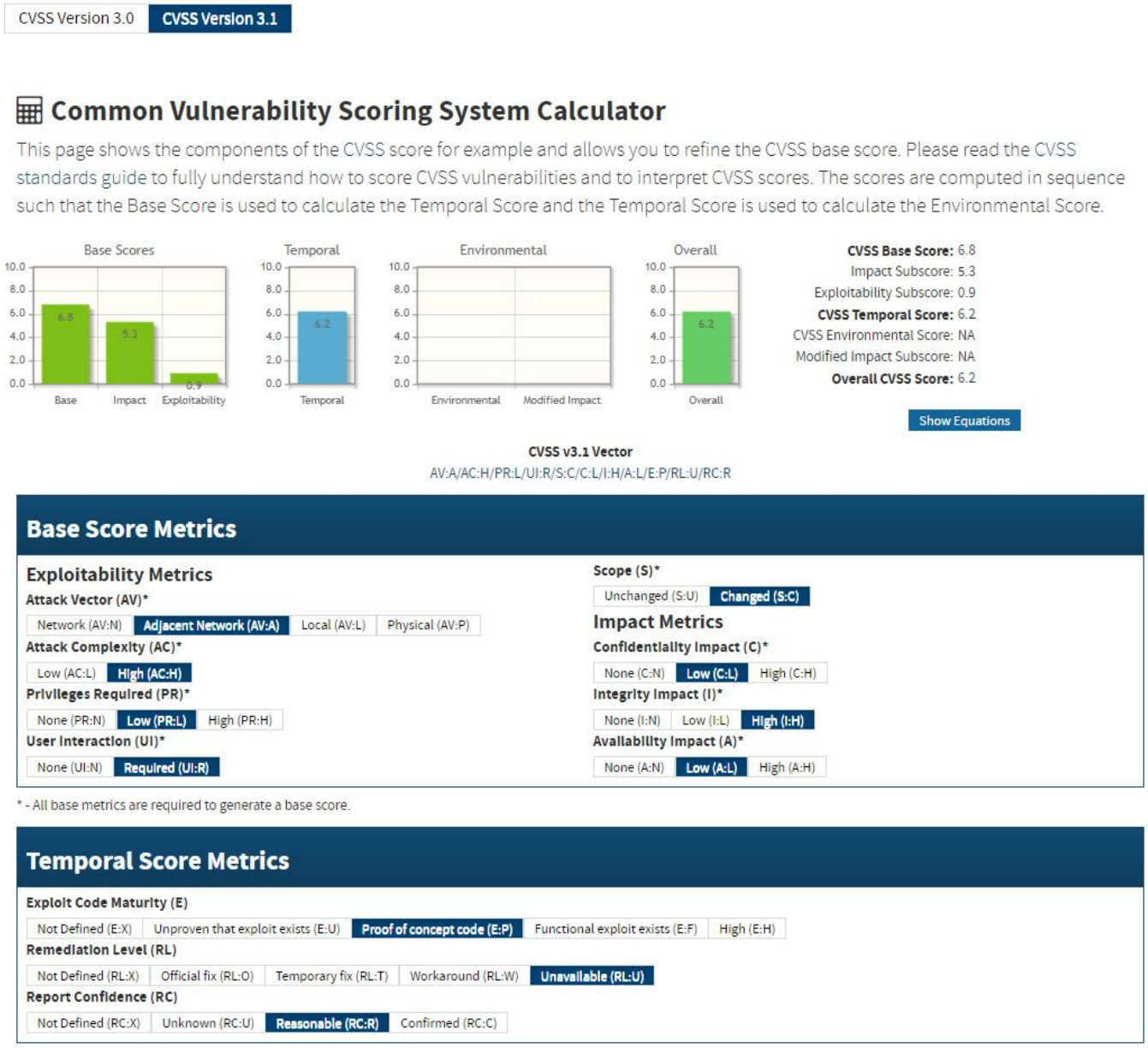


Ilustración 30: Un ejemplo del cálculo de vulnerabilidad de un dispositivo utilizado CVSS con la calculadora del NIST [15]

Por otro lado, el laboratorio a utilizar no necesariamente debe ser extremadamente avanzado. Por ejemplo, para esta tesis se han utilizado datos de análisis de algunos productos IoT incluidos en un estudio realizado en los Países Bajos, entre ellos, tal como fue mencionado en el capítulo 2, la muñeca Cayla de Genesis Toys, que fue la protagonista de una controversia

[15] La etiqueta presentada se obtiene utilizando el vector incluido en el siguiente link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:L/E:P/RL:U/RC:R

por sus fallas de seguridad que llevaron a su retiro de la venta en varios países europeos. [11]

El laboratorio planteado para realizar dichos análisis no requeriría una gran inversión ya que utiliza software de código abierto o de bajo costo (Kali Linux como Sistema Operativo, Killerbee para inspeccionar el tráfico del protocolo Zigbee, WireShark para análisis de tráfico de red) y hardware estándar como servidor, punto de acceso wifi y dispositivo móvil para instalar las aplicaciones. Sin embargo, demuestra ser efectivo para detectar las vulnerabilidades y riesgos para la seguridad y privacidad de dichos dispositivos. [2]

Conclusiones

La situación actual, en la cual por falta de información el consumidor se encuentra a la deriva en el momento de realizar una compra de un dispositivo IoT, lleva a plantearse que cualquier sistema de rotulado e información que se elija será mejor que nada. Sin embargo, los desafíos mencionados en los capítulos precedentes evidencian la necesidad de que dicho sistema logre una aceptación suficientemente masiva y rápida tanto de parte del consumidor como de la industria para lograr que el sistema sea exitoso.

Con respecto a la industria, es claro que los países que cuentan con los fabricantes, sus casas matrices o a los proveedores de servicios dentro de sus fronteras se encuentran con el problema de intentar imponer regulaciones que podrían dejarlos en desventaja frente a competidores de otros países. Para estos países es difícil lograr un balance entre proteger a sus ciudadanos como consumidores de productos IoT, y arriesgarse a impedir la innovación y el desarrollo de sus empresas. En estos casos parecería que el acercamiento más viable es establecer un sistema voluntario y con bajas barreras consensuadas entre gobierno e industria.

La esperanza es que, lanzando un sistema menos restrictivo al comienzo, la misma competencia del mercado lleve a las empresas a subir sus propios estándares de calidad en relación a la seguridad y privacidad.

En países como la Argentina, alejados de los centros de producción, se podría intentar un esquema más estricto y obligatorio. Al fin y al cabo no hay razón para permitir la venta de un producto IoT de origen extranjero con severas fallas de seguridad, tal como no se permite la importación de productos que no cumplan con las reglas de seguridad eléctrica o de eficiencia energética.

Con respecto al consumidor, no importa la ubicación geográfica, el desafío es definir un sistema de rotulado que sea comprensible, aceptado y confiable. Es vital utilizar la información de estudios sobre el comportamiento del consumidor en general y el de productos tecnológicos en particular para

comprender qué tipo de rotulados son los más fácilmente advertidos y cuáles son los preferidos a nivel de comprensión y facilidades de comparación.

Uno de los errores más frecuentes es incluir demasiada información en el sistema de rotulado, más de la que puede procesar un consumidor en el corto tiempo que tiene para comparar y elegir productos. Es por eso que los estudios realizados sobre el impacto en el consumidor de IoT recomiendan separar la información en dos niveles: el primero, más básico e incluido en la etiqueta ubicada en un lugar prominente del embalaje del producto, fácilmente abarcable de un vistazo y de un tipo comprensible para el consumidor. El segundo nivel, más completo, accesible a través de la lectura de códigos QR, que debería contar con información adicional y con datos útiles también para los expertos.

Esta información adicional debería alojarse preferentemente en el sitio web de la entidad certificante, con la inclusión de un punto de contacto actualizado para proveer reportes de vulnerabilidades y de un enlace al sitio web del fabricante. El sitio web de la entidad certificante también debería permitir realizar una búsqueda de productos certificados de forma de poder validar las calificaciones, realizar comparaciones y también recuperar la información de la etiqueta con posterioridad en caso de no contar con el embalaje.

Las etiquetas graduadas son las que mejor se prestan para realizar comparaciones entre los productos, además de relevar al consumidor de intentar definir por sí mismo el nivel de seguridad de un dispositivo analizando la información provista. La posibilidad de utilizar un sistema de colores llamativos sumado a que los consumidores ya están acostumbrados a utilizarlo para eficiencia energética, son dos beneficios adicionales. Sin embargo este formato no es el más elegido en los ejemplos provistos en esta tesis siendo la principal razón que para ser efectivo debería ser obligatorio ya que difícilmente los fabricantes acepten voluntariamente mostrar una etiqueta que indique que sus productos no son seguros.

Las etiquetas de información se muestran útiles para advertir al consumidor de potenciales riesgos o deficiencias de los productos. El uso de

pictogramas en reemplazo de textos o en conjunto con los mismos se recomienda para atraer la atención del consumidor y simplificar la tarea de realizar comparaciones. Cuando se combinan con un sistema graduado el efecto total de la etiqueta se potencia, aunque por lo explicado anteriormente, el consumidor suele prestar más atención a la calificación que a las advertencias o informaciones complementarias.

En la siguiente propuesta de etiqueta se han intentado plasmar todas estas recomendaciones utilizando como base la etiqueta de eficiencia energética en vigencia al momento de la redacción de la tesis en la República Argentina.

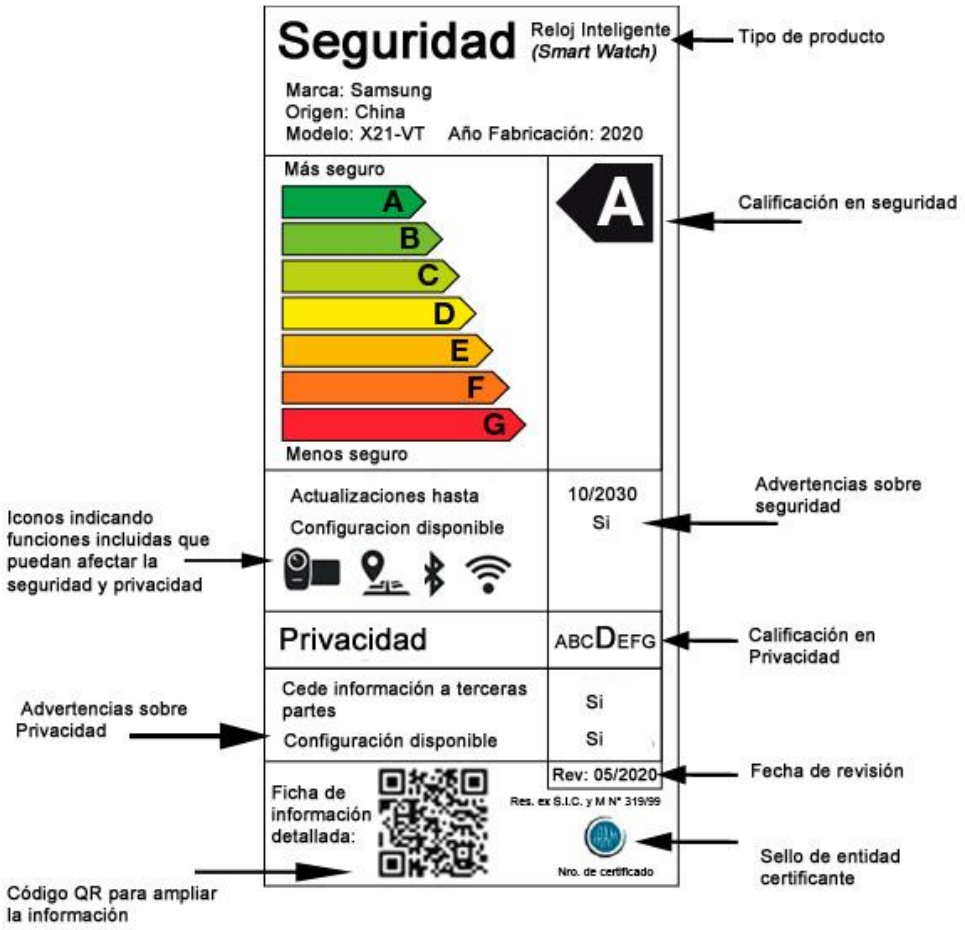


Ilustración 31: Una posible etiqueta de seguridad y privacidad basada en la de eficiencia energética vigente en la República Argentina. Elaboración propia [16]

[16] En base a etiqueta ejemplo disponible en https://www.argentina.gob.ar/economia/energia/eficiencia-energetica/cuidemos-la-energia-en-nuestro-hogar/las-distintas-etiquetas/aire-acondicionado

La etiqueta planteada muestra entonces las siguientes ventajas:

1. El consumidor encuentra la calificación del producto en un formato familiar, claramente decodificable.
2. Los colores y formas utilizados la hacen prominente, destacándose entre otros rótulos, como los de reciclado y de conformidad eléctrica.
3. Permite comparar fácilmente la calificación y otras características de seguridad y privacidad de productos similares
4. No incluye ningún término demasiado técnico. Recordemos que la "fatiga de la seguridad" hace que la utilización de términos *"techie*", que probablemente el consumidor no conozca (como *firmware*, nube, *cookies*, o encriptación), lo afecte negativamente y lo predisponga a ignorar las advertencias.
5. Utiliza íconos reconocibles para destacar funciones incluidas y que pueden representar un riesgo para la seguridad y privacidad.
6. Permite ampliar la información incluida en la etiqueta a través de la lectura de un código QR. Los códigos QR legibles con los teléfonos celulares, una novedad para la mayoría de los consumidores hasta hace unos años, son ahora comunes en nuestro país al utilizarse para realizar pagos o consultas con numerosas aplicaciones, por lo que su utilización no debería representar una barrera para ningún usuario de tecnología.
7. Cuenta con el respaldo de una entidad reconocida que realiza la medición y validación necesaria para establecer los niveles de seguridad y privacidad informados. Este sello es el que finalmente brinda la confianza necesaria a la etiqueta en la precepción del consumidor IoT.

Es de destacar que resulta difícil incluir advertencias de seguridad y privacidad más elaboradas sin afectar el ítem 4. Incluso es posible que algunas de las advertencias, como un icono de Wi-fi para un dispositivo que claramente se conecta a internet o el de una grabadora de video para una

cámara puedan resultar obvios e irrelevantes para los usuarios más avanzados.

Otra dificultad reside en que no hay forma de especificar sucintamente si la configuración de seguridad o privacidad disponible para el usuario es adecuada o no y si, por ejemplo, en el caso de la privacidad logra abarcar toda la información que se comparte con el dispositivo. Sin embargo, se sobreentiende que esto fue verificado por la entidad y se encuentra incluido en la calificación.

En general, resulta más difícil la protección del consumidor en términos de privacidad que de seguridad. Como fue explicado en la sección 4.2 en relación a los desafíos para validar y certificar un ecosistema IoT completo, es prácticamente imposible conocer realmente que es lo que sucede con la información del usuario una vez que es transmitida a los proveedores de servicio en la nube.

Esta dificultad ya fue ampliamente reconocida por los reguladores y es la base de políticas como la implementada por GDPR en Europa, que hace tanto o más hincapié en la aplicación de fuertes multas cuando se descubre una filtración de datos del consumidor que en intentar convencer a los proveedores de servicios de los beneficios de implementar prácticas honestas y éticas en relación a la privacidad.

Como se ha demostrado en el cuerpo de la tesis, para obtener las calificaciones, advertencias y otra información necesaria para producir la etiqueta propuesta no hay dificultad en encontrar una serie de parámetros validados y consensuados que debieran cumplir los dispositivos IoT para ser considerados seguros. A su vez, tampoco es necesario en montar laboratorios excesivamente avanzados para realizar las verificaciones de estos parámetros.

Solo habría que sortear la resistencia de la industria a recibir bajas calificaciones. Es posible que, por esa razón, esta etiqueta deba ser agregada al embalaje luego de ser ingresada al país, posiblemente al mismo tiempo que la estampilla de aduana, lo que requeriría una importante infraestructura para la generación y distribución de etiquetas.

El costo de esta infraestructura se sumaría a los recursos necesarios para el proceso de verificación en sí mismo y para el mantenimiento y actualización de la información alojada en el sitio web de la entidad certificante. Los fondos requeridos podrían ser generados a partir de una mínima tasa agregada a la importación de los productos.

De esta forma, el sistema de rotulado podría iniciar el círculo virtuoso que consiste en proteger a los consumidores de IoT, ayudarlos a realizar mejores elecciones de productos en base a su calificación de seguridad y privacidad, e incentivar a la industria a incluir mejores prácticas en sus procesos de producción y provisión de servicios. Sin dudas sería un aporte importante para lograr, finalmente, una Internet de la Cosas en la que se pueda confiar.

Bibliografía

[1] K. Lueth, "IoT Analytics," 30 10 2014. [Online]. Disponible: https://iot-analytics.com/iot-market-segments-analysis/. [Ultimo acceso 07 06 2020].

[2] R. van Diermen, "The Internet of Things: a privacy label for IoT products in a consumer market," 2018. [Online]. Disponible: https://openaccess.leidenuniv.nl/bitstream/handle/1887/64571/Diermen_R_van_2018_CS.pdf. [Ultimo acceso 09 10 2020].

[3] D. A. Wydler, "Soluciones tecnológicas, de regulación y gobierno para los desafíos de IoT. (Trabajo Final de Posgrado. Universidad de Buenos Aires)," 2018. [Online]. Disponible: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1366_WydlerDA.pdf. [Ultimo acceso 13 10 2019].

[4] NIST, "Security Fatigue," 04 10 2016. [Online]. Disponible: https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly. [Ultimo acceso 11 09 2020].

[5] C. Olt and N. Mesbah, "Weary of Watching out? - Cause and effect of Security fatigue," 14 6 2019. [Online]. Disponible: https://aisel.aisnet.org/ecis2019_rp/3/. [Ultimo acceso 16 11 2020].

[6] R. Arnold, A. Hillebrand and M. Waldburger, "Personal Data and Privacy: An Study for Ofcom," 05 2015. [Online]. Disponible: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/67088/personal_data_and_privacy.pdf. [Ultimo acceso 21 10 2020].

[7] O. Vermesa and 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 2020]

[8] 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 2020]

[9] J. Blythe, N. Sombatruang and S. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?," *Journal of Cybersecurity,* vol. 5, no. 1, pp. 1-10, 2019.

[10] P. Bihr, "A Trustmark for IoT," 2017. [Online]. Disponible: https://thingscon.org/publications/report-a-trustmark-for-iot/. [Ultimo acceso 08 10 2020].

[11] Engadget, "Germany bans creepy doll over privacy concerns," 17 02 2017. [Online]. Disponible: https://www.engadget.com/2017-02-17-germany-bans-my-friend-cayla-doll.html. [Ultimo acceso 10 11 2020].

[12] Forbes, "Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself," 17 3 2017. [Online]. Disponible: https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/?sh=c3d610c4bcd5. [Ultimo acceso 08 11 2020].

[13] J. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal,* vol. 31, no. 1, p. 117, 2016. Disponible:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645 [Ultimo acceso 08 11 2020].

[14] Wired, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," 21 07 2015. [Online]. Disponible: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Ultimo acceso 08 11 2020].

[15] The Washington Post, "WikiLeaks: The CIA is using popular TVs, smartphones and cars to spy on their owners," 03 07 2017. [Online]. Disponible: https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying/. [Ultimo acceso 08 11 2020].

[16] 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 2020]

[17] 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 [Ultimo acceso 28 11 2020]

[18] European Commission, "Internet of Things Privacy & Security Workshop," 13 1 2017. [Online]. Disponible: https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshop. [Ultimo acceso 5 11 2020].

[19] NIST, "Report of the Commision on enhancing National

Cybersecurty," 1 12 2016. [Online]. Disponible: https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf. [Ultimo acceso 1 11 2020].

[20] J. Blythe and S. Johnson, "Rapid evidence assessment on labelling schemes and implications for consumer IoT security," 2018. [Online]. Disponible: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775562/Rapid_evidence_assessment_IoT_security_oct_2018.pdf. [Ultimo acceso 07 10 2020].

[21] IOT Alliance Australia, "Internet of Things Security Guideline," 11 2017. [Online]. Disponible: https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf. [Ultimo acceso 28 11 2020].

[22] Department for Digital, Culture, Media and Sport del Reino Unido, "Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security," 2 2020. [Online]. Disponible: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security. [Ultimo acceso 14 11 2020].

[23] BSI (British Standards Institution), "Testing and certification for IoT connected devices," 2020. [Online]. Disponible: https://www.bsigroup.com/en-GB/industries-and-sectors/internet-of-things/IoT-Assurance-Services/. [Ultimo acceso 1 11 2020].

[24] TRAFICOM - Finnish National Cybersecurity Center, "Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products," 26 11 2019. [Online]. Disponible:

https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label. [Ultimo acceso 2020 11 27].

[25] Data Breach Today, "Singapore Launches IoT Cybersecurity Labelling," 16 10 2020. [Online]. Disponible: https://www.databreachtoday.asia/singapore-launches-iot-cybersecurity-labelling-a-15187. [Ultimo acceso 17 11 2020].

[26] Digital.Security France, "IQS Program," [Online]. Disponible: https://iqs-label.com/. [Ultimo acceso 15 11 2020].

[27] Underwriters Laboratories, "IoT Security Rating," [Online]. Disponible: https://ims.ul.com/IoT-security-rating. [Ultimo acceso 6 12 2020].

[28] S. Johnson, G. Wong, J. Blythe and M. Manning, "The impact of IoT security labelling on consumer product choice and willingness to pay," 24 1 2020. [Online]. Disponible: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800. [Ultimo acceso 6 10 2020].

[29] W3C, "Platform for Privacy Preferences (P3P) Project," [Online]. Disponible: https://www.w3.org/P3P/. [Ultimo acceso 15 11 2020].

[30] P. Kelley, L. Cesca, J. Brescee and L. Cranor, "Standardizing privacy notices: an online study of the nutrition label approach," 1 2010. [Online]. Disponible: https://www.researchgate.net/publication/221515415_Standardizing_privacy_notices_an_online_study_of_the_nutrition_label_approach. [Ultimo acceso 17 11 2020].

[31] Infobae, "Cómo funcionará la ley de etiquetado frontal de alimentos," 30 10 2020. [Online]. Disponible: https://www.infobae.com/tendencias/2020/10/30/como-

funcionara-la-ley-de-etiquetado-frontal-de-alimentos/. [Ultimo acceso 08 11 2020].

[32] Harris Interactive, "Consumer Internet of Things Security Labelling," 3 2019. [Online]. Disponible: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf. [Ultimo acceso 1 12 2020].

[33] E.-N. Pardis, L. Faith Cranor, Y. Agarwal and H. Hibshi, "Ask the Experts: What Should Be on an IoT label" 11 2 2020. [Online]. Disponible: https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-pardis_emami_naeini.pdf. [Ultimo acceso 1 12 2020].

[34] I. Bojanova and 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 2020]

[35] J. Koss, "ETSI Specialist task force STF 505 -IOT," 11 2016. [Online]. Disponible: https://docbox.etsi.org/Workshop/2016/201611_M2MIoTWS/00_WORKSHOP/ZZ_CONCLUSION/STF505_Koss.pdf. [Ultimo acceso 15 10 2020].

[36] AITOI, "AIOTI Alianza para la innovación en IoT," 05 10 2018. [Online]. Disponible: http://www.aioti.eu. [Ultimo acceso 16 10 2020].

[37] International Organization for Standardization, "ISO/IEC 30141:2018 Internet of Things (IoT) -- Reference Architecture," 08 2018. [Online]. Disponible: https://www.iso.org/standard/65695.html?browse=tc. [Ultimo

acceso 13 09 2020].

[38] ETSI, "Technical Specification 103 645," 2 2019. [Online]. Disponible: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf. [Ultimo acceso 15 11 2020].

[39] G. Rosner, "Trustmarks in the Identity Ecosystem: Definitions, Use, and Governance," 23 10 2017. [Online]. Disponible: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3054056. [Ultimo acceso 15 11 2020].

[40] J. Voas and P. Laplante, "IoT's Certification Quagmire," *Computer,* vol. 51, no. 04, pp. 86-89, 2018. Disponible: https://www.computer.org/csdl/magazine/co/2018/04/mco2018040086/13rRUzphDtL. [Ultimo acceso 08 11 2020].

[41] Department for Digital, Culture, Media and Sport del Reino Unido, "Code of Practice for consumer IoT security," 14 10 2018. [Online]. Disponible: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security. [Ultimo acceso 3 12 2020].

[42] OWASP, "OWASP Internet of Things," 2 2020. [Online]. Disponible: https://owasp.org/www-project-internet-of-things/. [Ultimo acceso 5 12 2020].

[43] Forbes, "The DDoS Attack Against Dyn One Year Later," 23 10 2017. [Online]. Disponible: https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later. [Ultimo acceso 5 12 2020].

[44] "Common Vulnerability Scoring System," [Online]. Disponible: https://www.first.org/cvss/ [Ultimo acceso 15 11

2020].