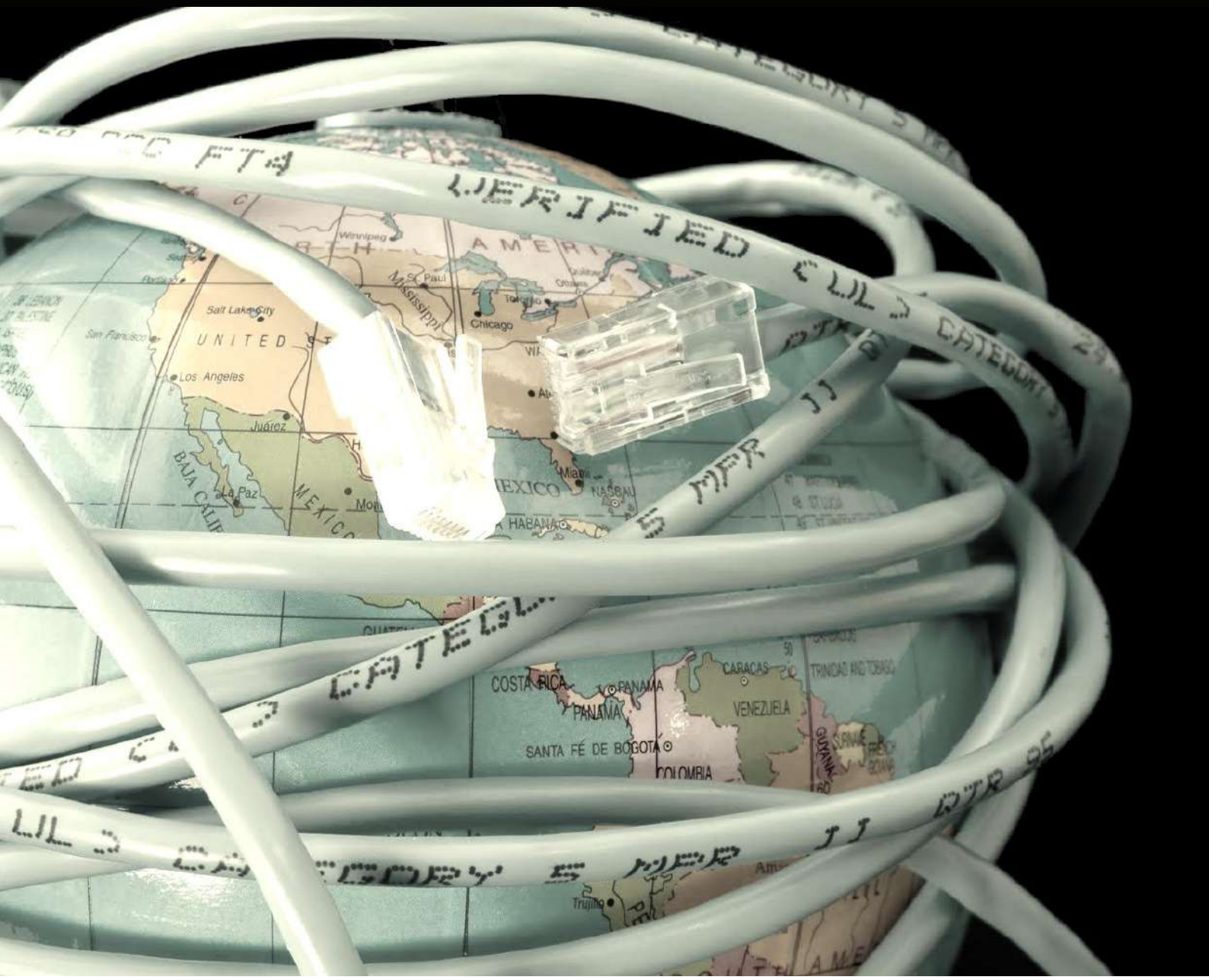
SEGURIDAD EN INTERNET DE LAS COSAS

Estado del arte



Documento Público

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-CV ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2014 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana para la prevención, detección y respuesta antes incidentes de seguridad en las TICs.

Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana

http://www.csirtcv.gva.es/

https://www.facebook.com/csirtcv

https://twitter.com/csirtcv

Licencia de uso

Este documento es de dominio público bajo licencia Creative Commons Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Imagen de portada de LOSINPUN, compartida en flickr con licencia Creative Commons (by-nc-sa).

Índice de contenido

1. Introducción a IoT

El término "*Internet de las cosas*" (Internet of things, en adelante IoT) es una expresión en auge que hace referencia a objetos comunes que con el avance de la tecnología se están interconectando a Internet. El término IoT se introdujo cuando el número de dispositivos fue mayor que el número de personas conectadas a Internet, entre 2008 y 2009. Hoy en día es habitual que la mayor parte de ciudadanos dispongan de un *smartphone*, una *tablet* o un equipo portátil. Esto hace que se tenga acceso permanente a Internet sin importar el lugar donde se encuentre el usuario. Asimismo, casi un 70% de los hogares españoles[1] disponen de Internet. Según el informe del ONTSI, en el tercer trimestre de 2013 los dispositivos que más han aumentado son las *tablets* (28,5 % de los hogares), las televisiones (78,6 %) y los ordenadores portátiles (62,5 %).

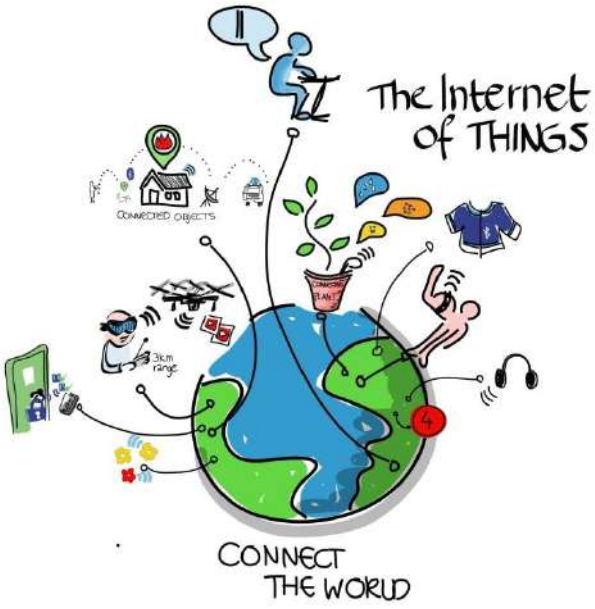


Ilustración 1: "Internet of Things" by Wilgengebroed on Flickr - Licensed under CC via Wikimedia Commons

Como se ha comentado anteriormente, el término IoT va mucho más allá, y engloba objetos comunes que hasta ahora no disponían de conectividad. Con esta evolución, algunos elementos como neveras, hornos, lavadoras, coches, relojes, televisores y un largo etcétera disponen ya de conexión a Internet. La conectividad de estos elementos permite, entre otras muchas cosas, controlar el objeto de forma remota a través de otro dispositivo o una aplicación a través de Internet. Además permite recibir información externa como puede ser el caso de una

[1] Datos de 2013 según el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información – http://www.ontsi.red.es/ontsi/sites/default/files/informe_anual_la_sociedad_en_red_2013_ed._2014.pdf

nevera que informa en tiempo real de la climatología en cualquier ciudad, o que se pueda consultar a través de una pantalla incorporada en la misma la caducidad de los productos, consultar el correo electrónico o leer las últimas noticias. Son algunas funciones de las que dispone este tipo de dispositivo, además de las funcionalidades habituales de cada uno. Hasta ahora Internet era una herramienta de trabajo, de consulta de información y de comunicación. Mediante esta nueva forma de interacción, hacemos que Internet sea una parte necesaria en las tareas comunes y cotidianas de la vida. Además del término IoT también se llega a denominar este fenómeno como "*Internet del Todo*" (*Internet of Everything*). La tendencia es que siga evolucionando y aumentando exponencialmente.

Un ejemplo de la expansión de esta unión de la tecnología con la vida real es la domótica. Durante *el boom inmobiliario* las casas de nuevas construcción empezaron a disponer de este tipo de sistema, que venía preinstalado en el domicilio. La domótica permite que muchas familias en su vida diaria realicen de forma remota y/o automática acciones como encender la calefacción, abrir y cerrar persianas, encender y apagar las luces, controlar el acceso al domicilio, y un largo etcétera. Hoy en día los estudios indican que hay numerosos hogares utilizando este sistema interconectado también a Internet, y se espera que sigan en aumento.

Algunos de los dispositivos más conocidos que están liderando la expansión de *IoT* son los llamados *wearables*. Son pequeños dispositivos que una persona puede llevar puestos y que pueden capturar información de ciertas actividades que realiza. Además, pueden proporcionar otro tipo de información al usuario como puede ser la hora, el tiempo o incluso las notificaciones que se reciben en él mismo o en un teléfono móvil enlazado. Un ejemplo claro de un dispositivo *wearable* son los relojes que disponen GPS que geoposiciona al usuario, además de disponer de acelerómetro, pulsómetro, etc. Algunos de estos relojes además de sincronizar la actividad con otros dispositivos o redes sociales, son capaces de recibir correos, mensajes, e incluso llamadas, por lo que en la mayoría de ocasiones la información es almacenada en la nube. Otros ejemplos de *wearables* son gafas (como es el caso de las famosas Google Glass), sensores incorporados en la ropa o zapatillas (como es el caso de las Nike+), localizadores incorporados en llaves, y se espera que en un

futuro no muy lejano haya biosensores destinados a medir variables médicas como glucosa o colesterol.

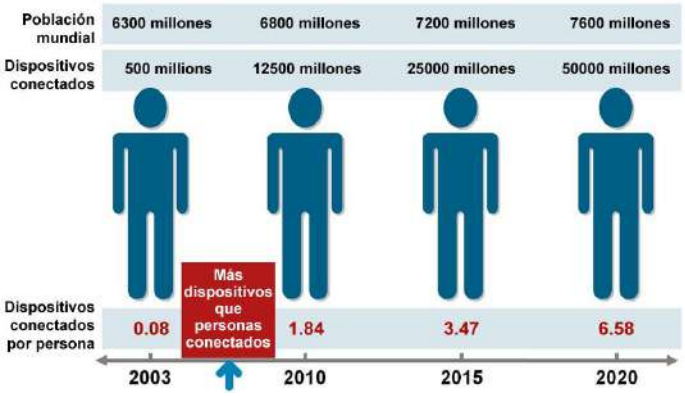


Ilustración 2: Fuente: IBSG de Cisco. Abril de 2011

Internet ha sido y sigue siendo una revolución y su llegada a dispositivos de uso cotidiano IoT va a generar grandes cambios y, si cabe, generar más necesidad de disponer de estos tipos de dispositivos y, en consecuencia, de mayor conectividad a Internet. De esta forma, el tráfico que circulará por la red va a aumentar exponencialmente en los próximos años con la expansión de IoT y... ¿quién sabe qué será lo siguiente? Según el IBSG de Cisco, en un estudio de 2011[2], calcularon que en 2020 habrá 50.000 millones de dispositivos conectados a Internet, a una media de 6,58 dispositivos conectados por persona.

[2] Informe: "Internet de las cosas. Como la próxima evolución de Internet lo cambia todo" Fuente: Cisco - http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

2. Alcance y objetivos del informe

En el presente informe se va a realizar un análisis del estado de seguridad en que se encuentran los dispositivos englobados en la categoría de IoT.

La seguridad de la información es un aspecto que está dando cada vez más que hablar, dado que el número de dispositivos conectados a Internet es cada vez mayor, lo que supone un crecimiento en la exposición de datos en la red. A pesar de que en general los dispositivos IoT no parecen dispositivos críticos, son elementos que pueden llegar a serlo si no son utilizados de forma adecuada. Según el informe de Julio de 2014 de HP FORTIFY[3] el 80% de los dispositivos tienen fallos en la autenticación y 6 de cada 10 dispositivos con interfaz de usuario son vulnerables. Estos datos no son muy tranquilizadores, ya que la evolución que se está produciendo es sobre la funcionalidad y tecnología de los dispositivos, pero la seguridad es un aspecto que *a priori* no se está considerando con la importancia que debería. En cambio, la seguridad es un factor que se debería tener en cuenta desde el inicio del diseño de cualquier producto. Para más información y recomendaciones sobre los aspectos que deben tener en cuenta los diseñadores se puede consultar el decálogo OWASP[4]. En cualquier caso, en el apartado de prevención y salvaguardas del presente informe se pueden ver las medidas que como usuarios también deberíamos tomar para mejorar la seguridad en el uso de nuestros dispositivos.

A lo largo del informe vamos a comentar algunos casos reales, pero para comenzar podemos imaginar lo que podría provocar que un tercero malicioso dispusiera de acceso no autorizado al control remoto de un horno o de la caldera de una casa. Lo mismo si consiguiera acceder a una nevera, pudiendo cambiar la temperatura o incluso apagarla. Esto podría provocar grandes perjuicios.

---

3 Informe: "Internet of Things Research Study". Fuente: HP FORTIFY - http://fortifyprotect.com/HP_IoT_Research_Study.pdf

4 Web: "OWASP Internet of Things Top Ten Project". Fuente: OWASP - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014

Hasta el momento nos hemos centrado en entornos domésticos, pero IoT también engloba dispositivos utilizados en el entorno empresarial. Imaginad por un momento lo que supondría perder el control de una máquina de aire acondicionado de un centro de proceso de datos de una empresa, o de la nevera de un restaurante, o de las puertas de acceso a un comercio. Cualquiera de estos ejemplos podría provocar graves pérdidas a la organización afectada. La conectividad de estos dispositivos también entra en el espectro de IoT.

Estos son algunos ejemplos de elementos que van evolucionando, adquiriendo conexión a Internet y que si no disponen de las medidas de seguridad adecuadas pueden suponer un riesgo considerable de seguridad, afectando a hogares, oficinas, y por extensión a las personas que se alojen en ellas.

En este informe de análisis de las IoT no se pretende ser catastrofista, sino **ser y hacer conscientes de lo que es ya una realidad así como la problemática y las recomendaciones de seguridad que se requieren para que su uso sea un avance global y no un retroceso en la seguridad, confidencialidad y libertad de las personas.**

Por ello se van a detallar los riesgos a los que estamos expuestos, los vectores de ataque a estos dispositivos y las medidas de seguridad que desde CSIRT-CV recomendamos.

Desde CSIRT-CV esperamos que este informe resulte atractivo y sea de utilidad para conocer esta nueva realidad y situación tecnológica.

Los objetivos del presente informe son los siguientes:

- **Informar** sobre el significado de IoT **y dar a conocer** la situación en la que se encuentra la evolución de este término y los dispositivos que se pueden encontrar.

- Evidenciar la **falta de seguridad** en muchos de los dispositivos conectados actualmente a Internet que hasta hace poco tiempo no disponían de esta característica, lo que aumenta sus funcionalidades pero a su vez incrementa los **factores de riesgo** que afectan a la seguridad y la privacidad.

- Detallar posibles **vectores de ataque** que se pueden utilizar para comprometer la seguridad de un dispositivo conectado a Internet, como pueden ser los casos mencionados anteriormente.

- Dar a conocer las **medidas de protección** recomendadas para los dispositivos que estén conectados a Internet y concienciar en la necesidad de protegerlos para garantizar la privacidad de la información.

3. Riesgos asociados

En este apartado vamos a analizar los riesgos asociados a la evolución de IoT. Los riesgos varían en función de la criticidad del dispositivo ya sea por la función que realizan o por la dependencia que se tenga del mismo. En cualquier caso, vamos a analizar algunos de los riesgos más comunes y las áreas que pueden verse afectadas ante la materialización de una amenaza. Más adelante nos centraremos en riesgos que pueden ser propios de determinados dispositivos.

La materialización de las amenazas a las que están expuestos nuestros dispositivos puede afectar a la **accesibilidad** del dispositivo, a la **integridad** de la información que contiene y a la **identidad** del usuario que la posee ya que puede provocar una suplantación de identidad. Y no nos quedamos ahí, ya que la **disponibilidad** quizá sea uno de los aspectos que más problemas puede generar, principalmente si hablamos por ejemplo de entornos industriales donde una parada del servicio debido a un ataque de denegación de servicio (DoS) entre otros, puede provocar grandes pérdidas. Otro factor a tener en cuenta y directamente relacionado con la información es la **confidencialidad** de los datos, que se debe garantizar tanto a la información almacenada en el dispositivo como a la transmitida en las comunicaciones que éste realice, más si son a través de Internet. Todos estos factores son considerados riesgos asociados a IoT.

Para determinar el nivel riesgo que produce la materialización de estas amenazas vamos a concretar algunas situaciones que se pueden producir en determinados dispositivos.

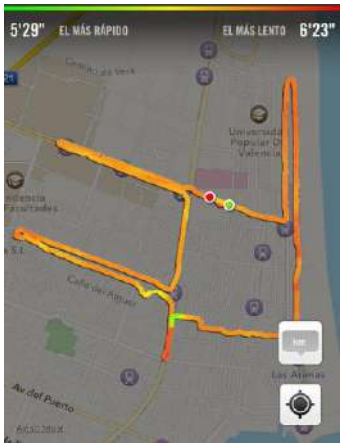


Ilustración 3: Nike+ Running GPS for iPhone

- Posicionamiento GPS. Como hemos comentado anteriormente, los *wearables* son dispositivos que un usuario lleva puestos. Por lo general, estos van conectados a Internet por lo que pueden ser fácilmente geoposicionados en todo momento (algunos incluso incluyen módulos GPS dedicados a ello). Esto hace que la localización del usuario quede

registrada en algún sitio web y, en función de la configuración de privacidad pueda estar al alcance de cualquiera. Esta situación se produce también al usar un *smartphone* si no sabemos qué aplicaciones tienen acceso a la localización. Para ampliar información sobre este riesgo, en CSIRT-CV hemos realizado una campaña sobre el uso seguro de los dispositivos *wearables*[5].

- Robo de información. Como se ha comentando, en los dispositivos que conectamos a Internet cada vez almacenamos más información. En muchos casos, y dada la nueva mentalidad de la nube (o *cloud*), podemos acceder a esa información desde otros dispositivos a través de Internet, desde aplicaciones móviles o desde entornos web donde para acceder disponemos de un usuario y una contraseña. En caso de que un tercero pudiera acceder, dispondría de información que podría vulnerar nuestra privacidad.

En cualquier caso el robo de información puede no producirse debido a una debilidad en el acceso, ya que como los dispositivos *wearables* son cada vez más pequeños, la facilidad de perderlos también es un riesgo que puede facilitar a cualquier persona acceso directo a nuestra información.

El uso de aplicaciones en dispositivos conectados a Internet puede hacer pública cierta información, como es el caso de las aplicaciones de salud y vida sana que pueden publicar la posición GPS, las calorías quemadas durante la carrera, la edad, la altura, el peso, los kilómetros recorridos,... y todo ello en ¡tiempo real!

- Control y uso malintencionado de los dispositivos. Otro de los riesgos al que nos enfrentamos en esta nueva era son los ataques que pueden llegar a tomar el control de los dispositivos que utilizamos. Dispositivos que después de un ataque aprovechando una posible vulnerabilidad son controlados por terceros de forma remota. Vamos a imaginarnos por un momento que un atacante consiguiese controlar nuestro frigorífico, nuestro horno, nuestra

[5] Campaña Uso seguro de dispositivos *wearables* – Fuente: CSIRT-CV - http://www.csirtcv.gva.es/es/paginas/seguridad-para-llevar-protege-tus-wearables.html

lavadora, o incluso como ya ha ocurrido[6], nuestro coche. El uso no legítimo de alguno de estos dispositivos puede afectar a la seguridad e integridad física de sus usuarios.

Los riesgos que se han mencionado en este apartado del informe no son aspectos tan remotos o lejanos como pueden parecer, ya que la probabilidad de que se materialicen es considerablemente alta si no se aplican las salvaguardas adecuadas.

Aunque quizá pensemos que estas situaciones ocurren en entornos personales y de ámbito reducido, debemos tener en cuenta, como ya hemos mencionado también, que IoT ha llegado también a los entornos profesionales e industriales. En estos entornos además de los dispositivos que podemos encontrar y utilizar en cualquier hogar, hay Infraestructuras Críticas monitorizadas en tiempo real por sistemas complejos, llamados sistemas **SCADA** (*Supervisory Control And Data Acquisition;* Supervisión, Control y Adquisición de Datos) ampliamente utilizados. Los sistemas SCADA, como parte de IoT, están integrando los sensores de las redes con Internet de modo que estos puedan ser monitorizados y controlados de forma remota. En algunos sistemas SCADA incluso se gestionan flujos de datos recibidos de subestaciones (UTR, Unidades Terminales Remotas) como es el caso de sistemas de control de tráfico, sistemas de transporte o sistemas de distribución de agua entre otros. De esta forma recolectan y gestionan información recibida por sensores y la transmiten al sistema central. Asimismo se está extendiendo también el uso de redes de sensores inalámbricas (*Wireless Sensor Networks*, en adelante WSNs). Estos son dispositivos que transmiten los datos al sistema SCADA de forma inalámbrica. Por tanto es evidente el riesgo que corren estas infraestructuras al utilizar sensores inalámbricos para el intercambio de información y control de los sistemas, que aumenta considerablemente si está conectado a Internet. Es obvio que la seguridad en los sistemas SCADA es un aspecto que debe estar en constante

[6] Artículo: "'Hackers' chinos logran vulnerar la seguridad del coche Tesla" Fuente: elconfidencial.com - http://www.elconfidencial.com/tecnologia/2014-07-21/hackers-chinos-logran-vulnerar-la-seguridad-del-coche-tesla_165313/

mantenimiento y control ya que detrás de estas redes hay Infraestructuras Críticas como sistemas de energía, de transporte, de agua, de salud, etcétera, que afectar a seres humanos.

Para finalizar este apartado, la comunicación inalámbrica sea quizá uno de los riesgos a los que más expuestos nos encontremos puesto que en redes domésticas lo más generalizado es disponer de una **red Wifi** y, si esta red es insegura se convierte en una puerta de acceso a nuestra red y por tanto a todos nuestros dispositivos conectados a ésta (como pueden ser el horno, la lavadora, la calefacción,…). Por tanto debemos asegurarnos que los accesos a la misma sean legítimos.

4. Vectores de ataque a las IoT

Cuando se trata de identificar brechas de seguridad para dispositivos IoT, se deben tener en cuenta los posibles vectores aplicables a sistemas digitales, así como a los propios ordenadores personales (en adelante PCs). En este aspecto, es fundamental tener en cuenta las particularidades de los dispositivos IoT respecto a los demás.

En general **se trata de dispositivos empotrados, que son menos complejos que por ejemplo un ordenador personal**, dado que están diseñados con una funcionalidad particular y no con un propósito general. Este hecho hace que se trate de **sistemas más heterogéneos** puesto que **los fabricantes implementan sus propias soluciones, descartando en muchos casos un operativo global o común como sucede con los PCs o *Smartphones***.

El caso en el que estos dispositivos empleen un sistema operativo de uso común como Windows, Android, Linux, etc. **es más sencillo mantener actualizaciones de seguridad** ya que es el propio proveedor de software el que se dedica a prepararlas y desplegarlas. Sin embargo, **en la mayoría de los sistemas IoT es el propio fabricante de hardware el que se encarga del mantenimiento de su software**, y en muchos casos no disponen de la experiencia y recursos para poder dar una respuesta aceptable ante posibles brechas de seguridad.

Como se ha comentado, en muchos casos se emplean **sistemas empotrados** y en la mayoría de los casos **estos dispositivos no se diseñaron inicialmente para estar conectados a la red**, lo cual provoca que **potencialmente sean más vulnerables.** Algo similar está sucediendo con los sistemas de control industrial (SCADA), que originalmente se diseñaron para situarse en redes aisladas y actualmente se empiezan a conectar a Internet. Su **exposición sin las medidas adecuadas supone un elevado riesgo**.

En muchos casos, **el problema no está en las capacidades del dispositivo**, **sino en las decisiones tomadas en las configuraciones por**

defecto de los mismos. En general, los dispositivos IoT no disponen de una entrada o salida de datos amigables como las de un PC, y tienen que **facilitar acceso a sus interfaces de administración mediante otros medios más opacos y menos amigables para el usuario medio**. Alrededor de este problema surge el concepto de *Security by Default* (en adelante SbD), que se traduce en la necesidad **de establecer una configuración por defecto lo más segura posible para un dispositivo en su fabricación**.

Por desgracia, **en la mayoría de los casos esto no es así.** Los fabricantes suelen establecer una **solución intermedia o baja**, que no requiera elevados conocimientos del usuario ni la configuración del dispositivo para su funcionamiento. Con esto, **se busca mejorar la experiencia del usuario y posiblemente dar una "buena" imagen de marca y producto**. Este hecho es un **arma de doble filo**, ya que no es frecuente que **los usuarios tengan conocimiento de las posibilidades de configuración de seguridad de su dispositivo**, así que los dispositivos posiblemente mantengan una configuración potencialmente insegura.

Otra de las principales debilidades de estos dispositivos es su ubicación física ya que pueden ser desde televisores, dispositivos wearables, sensores en redes de detección de incendios, sistemas domóticos, actuadores luminosos de tráfico, etc. Este hecho hace que sean **más difíciles de proteger**, ya que esta situación **puede permitir un sencillo acceso físico a ellos**, lo que entraña uno de los riesgos más graves de cara a su seguridad. Los dispositivos IoT, adicionalmente a los riesgos de seguridad habituales sobre la disponibilidad, integridad y confidencialidad de la información, abarcan **actuadores o componentes que pueden realizar cambios en el "mundo real"** y como es lógico, **este tipo de acciones pueden afectar a la seguridad y la salud de las personas**.

4.1. Deficiencias de la seguridad en la transmisión de datos

En este apartado nos centraremos sobre las deficiencias fundamentales que se pueden aprovechar en un ataque relacionadas con la transmisión de datos, dado que estos dispositivos están eminentemente enfocados al envío de

información entre dispositivos o hacia Internet. Uno de las medidas fundamentales a emprender será la protección de la información en tránsito.

Analizando el entorno en el que nos encontramos, es fácil comprender la **importancia de la seguridad en las comunicaciones para este tipo de dispositivos**. En la mayoría de los casos, **los sistemas distribuidos que forman requieren un elevado uso de canales de comunicación**, bien sea empleando redes cableadas, inalámbricas o cualquier otro medio de transmisión. Sea como sea, **todas estas comunicaciones, especialmente las que se propagan por medios inalámbricos o por redes públicas son sensibles de sufrir ataques a la confidencialidad en las comunicaciones.**

Cuando los dispositivos o implementaciones no garanticen un **nivel aceptable de seguridad en la identificación, privacidad, e integridad en las comunicaciones** realizadas, es muy probable que estas deficiencias puedan ser **aprovechadas por un atacante remoto para comprometer la información intercambiada**. Esta información puede incluir **datos privados o de carácter personal**, o bien puede tratarse de datos técnicos que se puedan emplear para realizar otro tipo de ataques que por ejemplo, faciliten el control del dispositivo.

Si no se protege adecuadamente el canal de comunicación mediante el cifrado de datos, puede ser sencillo para un intruso realizar **ataques de tipo *Man In The Middle***. Este tipo de ataques se basan en que el atacante puede capturar el tráfico del cliente, rectificarlo para aparentar ser él el originador del mismo y remitirlo al servidor legítimo, de modo que actúa como un punto intermedio en las comunicaciones, invisible tanto para el origen como para el destino del tráfico. Así **puede obtener toda la información que desee incluso modificarla para alterar el comportamiento o funcionamiento de cualquiera de los dos extremos**.

Un escenario para ilustrar esta situación podría ser el siguiente: pongamos que disponemos de nuestro nuevo y flamante coche conectado, y éste nos facilita datos de posición, velocidad, estado, etc. a través de un servicio en la nube que mantiene el fabricante. Imaginemos que existen deficiencias en el mecanismo de intercambio de información entre el propio coche y el servicio en Internet. Un atacante podría interceptar la comunicación enviada por el propio vehículo y hacerla llegar en su estado original o modificada al servidor del fabricante. ¿Cuáles podrían ser las implicaciones de esta situación? La primera a tener en cuenta podría ser que el atacante podría conocer sin problemas toda la información que el vehículo enviara al servicio *online*, como por ejemplo el estado del motor y nivel de líquidos, así como la posición GPS, por la que sabría cuando estamos en nuestro domicilio. El segundo factor a tener en cuenta es que también sería capaz de dar las mismas órdenes que pudiera dar el usuario, como por ejemplo abrir o cerrar las puertas del vehículo, encender o apagar las luces, hacer sonar el claxon, encender o apagar la climatización, etc.[7] Todo esto dependería de las funcionalidades que tuviese implementadas el vehículo.

4.2. Deficiencias en la seguridad de la plataforma software

Uno de los vectores de ataque más frecuentes tanto en este ámbito como en general, es el **aprovechamiento de vulnerabilidades de software.**

El primero de los vectores de ataque a considerar es el propio **sistema operativo.** En cierto tipo de dispositivos se utilizan versiones ajustadas de sistemas operativos de uso común (Windows XP, Android, Línux, etc.) de forma que se abaratan los costes de fabricación. Este hecho, evidentemente, supone un riesgo de seguridad, ya que **cuando se detectan vulnerabilidades sobre dichas plataformas son explotables sobre todos los dispositivos que las instalan**, facilitando a los potenciales atacantes una puerta de entrada para infinidad de dispositivos.

[7] Informe: "I Estudio anual de coches conectados". Fuente: iabspain - http://www.iabspain.net/wp-content/uploads/downloads/2014/07/Informe-coches-conectados-2014.pdf

Otro vector de ataque incluso más habitual que el anterior son las **interfaces web**, de uso muy frecuente en dispositivos IoT, ya que éstos normalmente son de tamaño reducido y no disponen de monitor, teclado o dispositivos apuntadores, permitiendo su administración desde otro dispositivo habilitado. Adicionalmente, es importante destacar que **es común que estas interfaces web se publiquen directamente a Internet** para facilitar la administración del dispositivo desde la red. Del mismo modo que con los sistemas operativos, es habitual que se empleen plataformas web comunes, de modo que **cuando se identifican vulnerabilidades de seguridad afectarán a todos los dispositivos que las implementen**.

Otra característica común a una gran cantidad de dispositivos es el **uso de servicios en la nube.** En este caso dichas aplicaciones suponen otro vector de ataque, ya que si existen **deficiencias en la gestión o actualización de este tipo de plataformas** se podrá **acceder a la información que puedan almacenar;** así como dependiendo del servicio que se preste, incluso **tomar el control del dispositivo** IoT.

En algunos dispositivos como las *Smart TV* se pueden **descargar e instalar aplicaciones de terceros sobre el propio dispositivo** que amplían su funcionalidad, al igual que sucede con los *smartphones,* las cuales normalmente se obtienen de repositorios de aplicaciones o *markets* que mantienen los propios fabricantes. En estos casos **se pueden emplear estas aplicaciones como puerta de entrada** para tomar el control del dispositivo, así como para **obtener información**. Este tipo de ataque se puede perpetrar de dos formas posibles; la primera sería **explotando vulnerabilidades identificadas en el software**, y la segunda podría ser **descargando aplicaciones maliciosas**, bien sea desde una fuente oficial que no analice suficientemente la seguridad de las aplicaciones que incorpora, o bien desde un canal no oficial de aplicaciones.

Por último, está muy de moda emplear **aplicaciones móviles** que se instalan en nuestro *smartphone* para cualquier tipo de gestión, bien sea obtener datos o controlar el dispositivo. Debido a ello, las aplicaciones móviles también **pueden ser objetivo de ataques**, ya sea **aprovechando vulnerabilidades o deficiencias en su implementación**, o mediante el **desarrollo de aplicaciones maliciosas que emulen el comportamiento y aspecto** de las legítimas para obtener acceso a los dispositivos IoT.

Para ilustrar la problemática que entraña la explotación de este tipo de vectores de ataque, consideremos el siguiente escenario: Supongamos que disponemos de un sistema domótico en nuestra vivienda. Los sistemas actuales permiten una gran cantidad de opciones, como controlar hornos, neveras, sistemas de climatización, actuadores que pueden cortar el suministro de gas o agua de la vivienda, sistemas de persianas, encender o apagar luces de la vivienda, etc. En estos casos, es habitual que se facilite acceso a estas aplicaciones mediante software en cualquier dispositivo digital, incluso en algunos casos mediante servidores intermedios como servicios en la nube. Cualquier posible deficiencia en el software empleado por los propios dispositivos IoT, *apps* móviles o el servicio *cloud* podría comprometer la información facilitada, así como permitir a un potencial atacante manipular a su antojo todos los dispositivos actuadores que se han mencionado con anterioridad. Este hecho podría permitirle accionar un horno, apagar la nevera o el congelador de la vivienda, encender todas las luces de la misma, manipular la climatización, etc.

4.3. Deficiencias en la seguridad de la funcionalidad y configuración

Otro punto fundamental en la seguridad de cualquier sistema es su propia funcionalidad. En muchas ocasiones, bien los desarrolladores (configuración por defecto) o los propios usuarios no mantienen un criterio alineado con la seguridad en la implementación o configuración de la funcionalidad de un servicio. En este aspecto, el panorama en el mundo de IoT es semejante, ya que la mayoría de los dispositivos no siguen una política adecuada de SbD.

Como consecuencia de este hecho, **la mayoría de dispositivos habilitan muchas de sus funcionalidades en sus configuraciones por defecto**, normalmente muchas más de las que emplea el usuario. Hay que ser conscientes de que **cada uno de estos servicios habilitados pueden suponer una brecha de seguridad** en la actualidad o en un futuro si no se actualizan o gestionan adecuadamente.

Daremos un ejemplo concreto para ilustrar esta situación. En primer lugar, pensaremos en un *router* de acceso a Internet, como el que se puede encontrar en cualquier vivienda. En muchos casos, este tipo de dispositivos facilitan acceso a su interfaz de administración con distintos protocolos: ***HTTP***, ***SSH, TELNET***, etc. Es habitual que se habiliten por defecto todos los protocolos; sin embargo, cada usuario usará como mucho uno en la vida del dispositivo. El resto estará habilitado sin su conocimiento y pueden suponer una potencial brecha de seguridad. Otra situación habitual es el caso de los *routers* con cifrado *WEP* que instalaban diversos proveedores de servicio en España en los que se descubrió que, basándose en el nombre y codificación del *SSID* del punto de acceso *Wifi*, se podía obtener la clave de acceso a la red (como si el uso de *WEP* no fuera suficientemente inseguro). En estos casos, se pueden encontrar **brechas de seguridad dependiendo de si los servicios están adecuadamente protegidos**, por ejemplo empleando autenticación en el acceso a los mismos, cifrado y validando correctamente el destino de la información antes de realizar cualquier envío. En caso de que no se cumplan dichas premisas estos servicios serán vulnerables a distintos tipos de ataques.

4.4. Deficiencias en la seguridad del hardware

El último punto a tratar, hace referencia a los vectores de ataque debidos a posibles vulnerabilidades en la implementación del *hardware*. Aunque en la mayoría de las ocasiones suelen ser de las vulnerabilidades menos frecuentes,

normalmente cuando se producen tienen una criticidad alta y son con mucho las más difíciles de subsanar.

Destacar en este caso, que **las vulnerabilidades o brechas de seguridad ya existían antes de considerar el término IoT**, ya que **la mayoría de ellas eran explotables sin necesidad de que el dispositivo estuviera conectado a Internet**; sin embargo, **consideramos oportuno incluirlo** en el presente informe dado que es una de las vías de entrada más habituales.

Cierto tipo de dispositivos de toma de datos se suelen encontrar **dispersos en grandes áreas,** lo que dificulta en gran medida la aplicación de controles de seguridad física que puedan mitigar sus riesgos. En este ecosistema, el **acceso físico al dispositivo** suele ser **más sencillo** que en el caso de grandes sistemas guardados a cal y canto en centros de proceso de datos.

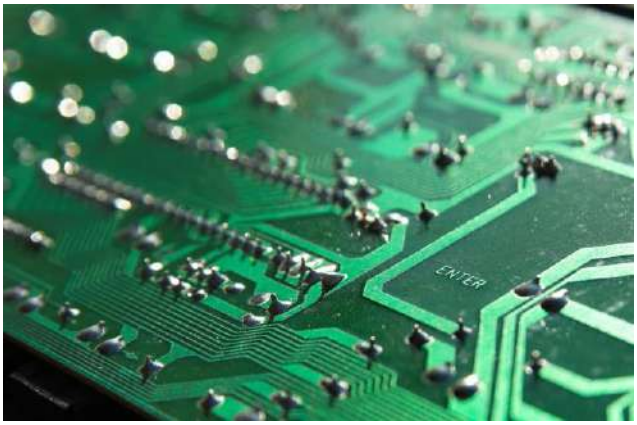
Los **ataques contra *hardware*** se basan fundamentalmente en **entender la estructura y realizar un análisis de comportamiento del dispositivo a atacar**, basándose en sus capacidades. Se emplean este tipo de ataques **cuando la seguridad *software* es robusta** o en **sistemas localizados en redes aisladas** o **bien protegidas de un acceso público** vía Internet. Un ejemplo de este tipo de situaciones podrían ser ataques a componentes de la red eléctrica o a sistemas de control de tráfico.

Cabe destacar que para realizar este tipo de ataques, **se suele requerir el uso de equipamiento especializado**. Dependiendo del equipo que se disponga se podrán realizar distintos tipos de ataque desde monitorización de interfaces hasta ingeniería inversa y manipulación de componentes internos.

L**a aplicación de medidas de seguridad dependerá en gran medida de la criticidad del dispositivo considerada por el fabricante**, su **uso previsto y la criticidad de los datos** que gestione. En un dispositivo *wearable* por ejemplo, que únicamente gestione notificaciones de uso mediante un *Smartphone,* no se encontrarán gran cantidad de estas contramedidas, sin embargo, en un sistema criptográfico como un *Hardware Security Module* (*HSM*) o en sistemas industriales sí que cabría esperarlas.

Una técnica de ataque habitual en este aspecto es el **acceso directo a**

componentes de almacenamiento tanto volátil (memoria) **como no volátil** (disco duro, memoria flash). De este modo, **dependiendo del diseño del dispositivo** será más o menos sencillo el acceso a memoria, así como dependiendo de si dispone de las protecciones implementadas en los datos será fácil acceder a la información en disco del mismo.



En general, el **acceso a la memoria volátil protegida del dispositivo** en caliente es un riesgo considerable, ya que fácilmente se pueda acceder a claves criptográficas, credenciales de acceso o información sensible almacenadas en la misma.

Por otra parte, el **almacenamiento no volátil** es quizá el **componente más sensible a ataques de este tipo**, ya que se puede desmontar el dispositivo para acceder a los mismos y se podrían extraer sin pérdidas de información. Contra este ataque únicamente existen **dos soluciones** viables. En primer lugar **protecciones físicas contra manipulaciones**, que puedan garantizar la destrucción del soporte en caso que se manipule, y en segundo lugar el **cifrado de la información**.

Otro problema habitual en este tipo de dispositivos es el mal **borrado de información**. En muchas ocasiones, cuando consideramos que la información ha sido eliminada del dispositivo nos encontramos que no ha sido así. Este problema se debe a la naturaleza del soporte y a la estructuración del sistema de archivos. En un proceso normal de borrado se **modifican las tablas de asignación de archivos del sistema de ficheros, estableciendo que el espacio en disco que ocupaba la información eliminada está actualmente disponible para su uso pero sin realizar un borrado efectivo**. Es más, aunque el sistema de borrado tenga en cuenta la sobreescritura del espacio en disco liberado, **existen herramientas que son capaces de reconstruir la información si no se realiza un número mínimo de pasadas en el borrado**. A modo de curiosidad, dependiendo del entorno y de la sensibilidad de los datos, se deberían establecer políticas de

eliminación de información que vayan desde las 7 sobreescrituras hasta las 32 para entornos de muy alta criticidad.

De esta forma pueden darse **situaciones potencialmente peligrosas respecto a la confidencialidad de los datos del dispositivo.** Un ejemplo sería la restauración de los datos de fábrica de un dispositivo para su reutilización o venta; una eliminación insegura podría facilitar el acceso a la información de dicho dispositivo al nuevo propietario. Esta situación se ha producido recientemente con *smartphones* que instalan un operativo concreto.

Otro ejemplo podrían ser los sistemas de control y asistencia de tráfico. Todos nosotros hemos visto más de una vez paneles informativos digitales en las vías, o paneles para el control de uso de carriles, sistemas de control de túneles, redes de semáforos de ciudades, etc. Estos sistemas en general tienen un alto rango de distribución, ya que deben mantener señales, semáforos e indicadores en distancias muy amplias, fácilmente de decenas de kilómetros, por lo que existen subestaciones de control distribuidas por toda el área facilitando en gran medida la posibilidad de acceso físico a las mismas ya que en la mayoría de las ocasiones los terminales están protegidos por un cajetín que puede ser forzado sin demasiada dificultad. En el supuesto que un atacante pudiera acceder al sistema y aprovechar vulnerabilidades en el hardware, es posible que pudiera tomar el control de semáforos o señalización de carriles en vías de alta ocupación, pudiendo manipular el sistema a su voluntad.

4.5. Deficiencias en la cultura de seguridad de los usuarios

El último punto a tener en cuenta dentro de vectores de ataque a IoT es un clásico y es **el producido por el propio usuario y su experiencia**. Por desgracia en muchas ocasiones, a pesar de que los sistemas estén bien configurados y bastionados, **una negligencia de un usuario podría comprometer el servicio**.

Desde CSIRT-CV sabemos que éste es un tema tratado hasta la saciedad, pero como sucede en la mayoría de los casos, consideramos que **es uno de los fundamentales vectores de ataque a explotar para obtener el acceso a**

un sistema ya que todos están destinados a ser usados por personas.

El principal ataque que se puede llevar a cabo es la denominada **Ingeniería Social** (*Social Engineering*). Se basa en una **manipulación psicológica de los usuarios, empleándolos como vía de acceso a los sistemas mediante acciones de engaño o estafa**. Empleándola, los atacantes se aprovechan del desconocimiento o la ignorancia para obtener la información necesaria para alcanzar su fin.

Dado que la mayoría de sistemas y servicios en la red se protegen mediante el uso de nombres de usuario y contraseñas, el objetivo habitual es intentar obtener este tipo de credenciales mediante estafas por cualquier vía, habitualmente correo electrónico. La mayoría conocemos casos de *phishing*, que **normalmente se envían de forma masiva y poco personalizada, centrados en la obtención de credenciales de acceso a servicios de correo electrónico o acceso a banca *online***. Sin embargo, cuando se trata de un ataque algo más elaborado es habitual realizar una **investigación previa de la víctima en Internet** consultando fuentes públicas, realizando actividades de recolección de información. **Cuanto más descuidada o incauta sea la víctima al publicar o facilitar su información en la red, más fácil le resultará al atacante perpetrar un ataque más preciso**, y en consecuencia con una mayor probabilidad de éxito.

Supongamos una situación en que un potencial atacante que deseara acceder a los sistemas de videovigilancia de una vivienda o una oficina. Para ello, podría comunicarse con el propietario o responsable del sistema haciéndose pasar por el proveedor de servicios de mantenimiento de la videovigilancia. Mediante esa estafa es posible que el usuario le pudiera dar acceso remoto o físico al propio sistema. Este hecho por ejemplo le podría facilitar información del propio sistema de videovigilancia para poder realizar un robo, incluso capacidades para desactivarlo o borrar sus huellas. Otra posibilidad sería que

el atacante empleara el acceso al dispositivo de videovigilancia para poder saltar a otros servicios en la red o para obtener información de cualquiera de ellos. La última de las posibilidades consideradas podría ser que el atacante empleara el acceso al dispositivo para realizar espionaje, y así aprender o obtener beneficio directo de las imágenes capturadas por el sistema.

Como se ha comentado con anterioridad, los ataques de Ingeniería Social se pueden realizar **desde una forma sencilla hasta ataques sumamente elaborados y dirigidos**. Evidentemente, **el esfuerzo que dedique el atacante dependerá del beneficio que pueda obtener o sus intereses**. Los ataques más elaborados estarán dirigidos a objetivos de mayor provecho, generalmente las empresas o administraciones públicas.

5. Recopilación de incidentes

En este apartado vamos a presentar alguno de los incidentes más relevantes que se han publicado hasta la fecha de elaboración del presente informe.

En este primer caso un investigador de la empresa *Proofpoint* detectó **entre diciembre de 2013 y enero de 2014 el envío de una campaña de correo malicioso**. Según podemos leer en su propio artículo[8] empezaron las investigaciones para saber qué tipo de dispositivos formaban las *botnet* que estaban enviando una determinada campaña de *SPAM*. Cuando comenzaron con el análisis, rápidamente evidenciaron que **alrededor de un 25% del correo malicioso enviado** no se había producido por dispositivos convencionales, como PCs o portátiles, sino que se habían enviado **desde dispositivos que resultaron estar dentro del conjunto de IoT**. Entre estos dispositivos, pudieron establecer que se envió *SPAM* desde *routers* domésticos, centros multimedia, *Smart TV* y alguna nevera. Tras este incidente se acuñó el término *Thingbotnet* (Botnet[9] de las Cosas).

Durante su análisis, pudieron determinar que **gran parte de los dispositivos compartían soluciones software comunes**, como por ejemplo el uso de sistemas empotrados basados en *Linux* o servidores web ligeros basados en *Apache*. **Este hecho denota las deficiencias en la gestión de seguridad de este tipo de dispositivos**.

Proofpoint se cuestiona la seguridad de estos dispositivos, especialmente dentro de una **red doméstica**, que cuenta con menores mecanismos de seguridad y control que una red corporativa. Del mismo modo, consideran que si en este momento **las *Botnet* suponen una de las amenazas más**

[8] Artículo: "Proofpoint Research: Internet of Things (IoT) Cyber Attack Security" Fuente: Proofpoint - http://www.proofpoint.com/products/targeted-attack-protection/internet-of-things.php

[9] Botnet – Fuente: Wikipedia - http://es.wikipedia.org/wiki/Botnet

importantes en la red, las **"*Botnet* de las Cosas" pueden empeorar considerablemente la situación**, teniendo en cuenta el número de dispositivos conectados y las condiciones especiales asociadas a la seguridad de los mismos.

Resulta muy interesante el siguiente artículo[10] que fue publicado por un investigador en el portal *Securelist* propiedad de *Kaspersky Lab*. Antes del experimento, **actualizó a la última versión del *firmware* todos sus dispositivos**, dándose cuenta que algunos no tenían soporte desde hacía años o de las dificultades para actualizarlos (un verdadero escollo para un usuario medio – según comenta el investigador). Su objetivo era saber **cuán seguros eran los dispositivos IoT conectados en su red doméstica**, como su *Smart TV* o su impresora. En el informe indica: "tenemos que entender que **CUALQUIER DISPOSITIVO vulnerable que conectemos a la red puede ser un trampolín para un atacante**". Existe software malicioso que es invisible a los usuarios y en ocasiones estos atacantes se dejan puertas traseras abiertas que el usuario desconoce.

Securelist nos quiere hacer ver con este artículo de investigación que **cada uno de los elementos conectados a la red es fundamental de cara a proteger al resto**, ya que el fallo de cualquiera de ellos puede comprometer por completo la seguridad de la red. La investigación no solo se queda en la seguridad que un usuario puede aplicar en un dispositivo, sino la conciencia de seguridad que desarrolladores y fabricantes deben conocer y aplicar en sus productos.

[10] Artículo: "IoT: How I hacked my home." Fuente: Securelist - http://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/

Repasamos a continuación un conjunto de casos destacables:

El primero se refiere al del conocido ***Tesla*[11], que pudo ser controlado de forma remota por un atacante**. *Tesla* es un modelo de coche pionero en el campo de los eléctricos, que además destaca por su conectividad, funcionalidad y acceso a Internet. Otro caso con menor impacto fue el caso de unas **bombillas que podían ser controladas desde la red doméstica e incluso desde Internet**. En este caso[12], un usuario explica cómo pudo tomar el control de este dispositivo a través de la red, controlando toda su funcionalidad sin ser un usuario autorizado.

Es posible que pensemos que los posibles ataques que se pueden realizar son complejos y que no están al alcance de cualquiera. Esto no es así en todos los casos. En agosto de 2014 se dio a conocer una **vulnerabilidad en un dispositivo *wearable* de uso muy difundido, el reloj *Pebble***[13]. El reloj *Pebble* es un *smartwacth* que se puede enlazar a un *smartphone*, mostrando por su pantalla las notificaciones recibidas. La vulnerabilidad podía provocar **condiciones de denegación de servicio, así como en algunos casos borrar la memoria del dispositivo** (aplicaciones, configuraciones, notas, mensajes, etc.). El ataque únicamente consistía en enviar 1500 mensajes de Whatsapp al dispositivo en un periodo de 5 segundos.

11 Artículo: "Chinese hackers take command of Tesla Model S" Fuente: CNET - http://www.cnet.com/news/chinese-hackers-take-command-of-tesla-model-s/

12 Artículo: "Hacking into Internet Connected Light Bulbs" Fuente: Context - http://contextis.co.uk/resources/blog/hacking-internet-connected-light-bulbs/

13 Artículo: "Remote Attack Coud Format Your Pebble Smartwatch Easily" Fuente: The Hacker News - http://thehackernews.com/2014/08/remote-attack-could-damage-your-pebble.html

Otro caso preocupante es el que se identificó en 2013 respecto a ***Karotz***, denominado como "*smart rabbit*". Básicamente es un conejo interactivo que tiene acceso a Internet y que permite controlarlo por voz, más o menos como los asistentes de voz de los *smartphones* actuales. Es importante destacar que el dispositivo se diseñó pensando en interactuar con niños e incorpora, como es lógico, micrófono y cámara. En este caso se descubrieron vulnerabilidades que se dieron a conocer en una ponencia dentro de la conferencia *Black Hat 2013* en Estados Unidos. Estas vulnerabilidades podían llegar a **permitir a un atacante tomar el control del dispositivo, pudiendo obtener por ejemplo imagen y audio en tiempo real del mismo**. En la misma ponencia, se puso en evidencia la seguridad de muchos dispositivos IoT[14].

[14] Ponencia "Home Invasion 2.0: Attacking Network-Connected Embedded Devices" Fuente: BlackHat - https://media.blackhat.com/us-13/US-13-Crowley-Home-Invasion-2-0-WP.pdf

6. Prevención y salvaguardas

Una vez analizado el estado del arte respecto a IoT, el siguiente paso será, **dentro de nuestras posibilidades, garantizar un uso seguro de las mismas**. **Se pueden aplicar una serie de medidas de seguridad que ayuden a mitigar en la medida de lo posible los riesgos de seguridad derivados del uso de estos dispositivos**.

Para afrontar esto, se va a dividir en una serie de partes en los que se abordarán los puntos de atención de la seguridad en IoT y las posibles salvaguardas aplicables.

6.1. Control de interfaces de acceso

Como se ha comentado, en la mayoría de casos, este tipo de dispositivos incorporan funciones de conectividad a la red para la gestión, control o intercambio de datos; sin embargo, no suelen disponer de interfaces directas con el usuario, como teclados o pantallas. En estos casos una solución es implementar una interfaz web que permita configurar todos los parámetros o acciones del dispositivo desde cualquier otro dispositivo remoto, bien sea un PC, una *tablet*, un móvil, o cualquier otro dispositivo capacitado.

Se debe poder controlar el acceso al dispositivo, más aún si dicha interfaz está publicada directamente a Internet. **En muchos de los casos estas interfaces no disponen de mecanismos de autenticación**, o en caso de emplearlos vienen configurados con las credenciales de acceso por defecto, facilitadas públicamente por el fabricante.

En caso de que este tipo de interfaces empleen autenticación es fundamental que **se sustituyan las credenciales de acceso por defecto por unas generadas por nosotros** con la mayor complejidad posible. Tomando esta

medida complicaremos en gran medida el trabajo a los ciberdelincuentes que quieran controlar nuestro dispositivo. Las contraseñas empleadas deberán seguir unas sencillas normas, como tener una longitud de un mínimo de 7 caracteres, emplear mayúsculas, minúsculas, números y algún símbolo especial.

Si la interfaz no emplea autenticación y además no permite que se habilite, en ningún caso se debe poder acceder a ésta a través de Internet sin la aplicación de medidas de control de acceso adicionales.

Otro punto fundamental en el uso de este tipo de interfaces es el cifrado. Una interfaz web implementa cifrado cuando se hace uso del protocolo *HTTPS* (se denota cuando en la barra de direcciones del navegador web se emplea *https://* delante de la ruta, así como se suele mostrar un candado en la conexión). **En caso de no emplearse una conexión cifrada se desaconseja publicar la interfaz de administración o conexión directamente a Internet.** Por ejemplo, supongamos que dejamos abierto el acceso al *router* de nuestra vivienda a través de Internet. Si la conexión no va cifrada cualquier persona conectada a nuestra misma red **podría capturar nuestras credenciales de acceso al servicio sin dificultades, ya que viajarían en claro por Internet**.

En este caso, **si se requiere el acceso al dispositivo desde fuera de nuestra vivienda**, **recomendamos implementar un acceso alternativo** al mismo, como por ejemplo emplear un servicio de ***Virtual Private Network*** **(en adelante VPN)**, que nos facilitará acceso a la red local de nuestra casa con total seguridad, ya que emplea cifrado y autenticación en las comunicaciones.

6.2. Actualización del dispositivo

En muchas ocasiones, e independientemente de la configuración que pueda realizar el usuario, la propia implementación del dispositivo está afectada por diversas vulnerabilidades de seguridad que pueden comprometerlo.

Para mitigar este riesgo, se recomienda **mantener el dispositivo actualizado con la última versión de *software* o *firmware* facilitada por el fabricante**. A este respecto, se consideran dos opciones. La primera de ellas, cuando el dispositivo lo permita, será configurar el dispositivo para que instale de forma automática dichas actualizaciones, o al menos reporte de su disponibilidad. La segunda será, obviamente si el dispositivo no permite una gestión de actualizaciones automatizada, que seamos nosotros mismos los que comprobemos e instalemos las actualizaciones periódicamente.

Por desgracia, **existen fabricantes que no llevan un ritmo fluido de actualizaciones, o que ni siquiera publican actualizaciones de seguridad**. Una buena práctica será adquirir dispositivos de fabricantes que ofrezcan un buen servicio post-venta, como suele ser el caso de fabricantes de renombre internacional. En cualquier caso para salir de dudas, se recomienda revisar los recursos del fabricante o directamente consultarle para asegurar que se va a dar un soporte adecuado al dispositivo.

En caso de que ya dispongamos del dispositivo y **no disponga de soporte**, o se trate de un soporte muy discontinuado, la recomendación será **mantener el dispositivo oculto dentro de nuestra red local sin que se publique directamente a Internet**, e implementar medios alternativos de acceso a dicha red que ofrezcan una conexión segura (VPN) si se requiere el acceso remoto, como se ha comentado con anterioridad.

6.3. Configuración segura de la red local

El primero de los puntos a tratar, que no es ni mucho menos específico o propio del uso de IoT, es la adecuada securización o bastionado de la red, con la implementación de un cortafuegos que rechace por defecto las conexiones entrantes desde Internet y solo permita iniciar conexiones desde dispositivos conectados desde el interior de nuestra red. Partiendo de esta base, podremos habilitar los accesos externos estrictamente necesarios, teniendo en cuenta nuestras necesidades y los potenciales riesgos de seguridad. Dicho esto,

seguimos con los consejos propios del tipo de dispositivos que nos ocupa en este informe.

Muy habitualmente, **los fabricantes de los dispositivos habilitan múltiples puertos de acceso o gestión** (cuando nos referimos a puertos, de una forma muy simplificada hacemos referencia a distintas "funcionalidades de red" asignadas al mismo dispositivo). Cuando se configura el acceso a un dispositivo de estas características a Internet, **se debe controlar que únicamente se permita el acceso a los puertos estrictamente necesarios**, de este modo se reducirán los riesgos de seguridad sustancialmente. Es fundamental tener claro el concepto, ya que en muchas ocasiones estos dispositivos no permiten especificar, y facilitan el acceso al dispositivo completo, de modo que se permitiría el acceso remoto a todos sus puertos. **Para realizar una configuración adecuada, se recomienda emplear reglas de *NAT* o de *Port Forwarding*** (Redirección de Puertos), dependiendo de las capacidades o características de tu *router*. Esta configuración la permiten prácticamente la totalidad de *routers* del mercado.

Un método simplificado para implementar una red *Wifi* es el uso de ***Wifi Protected Setup*** (en adelante *WPS*). Este protocolo implementado en 2007 por la *Wi-fi Alliance*, **facilita a los usuarios una implementación sencilla de una red inalámbrica segura**. Es importante destacar que ***WPS* no es un mecanismo de seguridad en sí, sino un proceso asistente para implementar una red inalámbrica con *WPA2***, pensado para minimizar la intervención del usuario en entornos domésticos o redes profesionales de pequeñas dimensiones. Sin embargo, hace un par de años, **se identificó una vulnerabilidad en el protocolo que podría permitir acceso a la red por un usuario malintencionado en unas pocas horas**, para lo cual ya existen herramientas automatizadas. La mayoría de los dispositivos que lo implementan suelen llevarlo activo por defecto. Aunque no tengamos la certeza de si nuestro *router* es o no vulnerable, **recomendamos a todos los efectos desactivar el protocolo** en el mismo. Para ello os remitimos a la documentación del fabricante para realizar la configuración.

Recientemente, y para facilitar a los usuarios la administración de su red doméstica, se ha comenzado a emplear el protocolo ***Universal Plug and Play* (en adelante *UPnP*).** Este protocolo está diseñado para facilitar la interconexión automática de dispositivos en la red. Una de sus funcionalidades más destacadas es **automatizar la apertura de puertos a Internet que los dispositivos conectados a la red local puedan necesitar**. Esta práctica desde luego que es muy cómoda, sin embargo no tiene por qué ser segura. Por defecto, **es posible que los dispositivos soliciten acceso remoto a puertos que no consideremos oportunos o lo que es peor, que puedan suponer un riesgo importante de seguridad**. A este respecto, y a pesar de que puede que no sea lo más cómodo, **recomendamos deshabilitar (en la medida de lo posible) dicho protocolo** dentro de nuestro *router*.

NOTA IMPORTANTE: Se aconseja verificar la funcionalidad de los servicios una vez desactivado, ya que es posible que existan dispositivos que lo requieran para su funcionamiento. En estos casos se aconseja intentar configurar el dispositivo manualmente, habilitando excepciones. También es posible que el propio dispositivo de red permita la configuración de UPnP o de los puertos que emplea, puede ser una buena alternativa revisarlo.

6.4. Identificación y control del uso de servicios en la nube o *cloud services*

Un riesgo a tener en cuenta con dispositivos IoT es el de que **nuestros datos pueden acabar en Internet mediante el acceso a servicios en la nube o *cloud services***. En este caso, no es necesario que se abran puertos al exterior, ya que con únicamente un acceso a Internet normal el dispositivo podrá enviar información a sitios públicos en Internet. No nos alarmemos, en muchas ocasiones es lo que esperamos del dispositivo. Sin embargo, es fundamental que tengamos constancia de las medidas de seguridad que aplica el dispositivo y el sitio que recibe nuestros datos, así como de la política de privacidad que aplica sobre los mismos.

Otro caso común es que **el dispositivo pueda ser gestionado externamente empleando un servicio web prestado por el propio fabricante**. En este caso, el usuario deberá acceder al servicio en la nube, el cual conectará y gestionará nuestro dispositivo, o bien nos permitirá acceder a información o datos relacionados con el mismo (usualmente capturados por el mismo dispositivo). En estos casos, se deben seguir buenas prácticas en el uso de contraseñas, como se ha comentado con anterioridad. También es lógico requerir que se establezca una conexión cifrada con el servicio mediante el empleo de protocolo *HTTPS*.

6.5. Uso de aplicaciones móviles para dispositivos IoT

En la actualidad, el **control de los dispositivos IoT** es muy habitual que se realice con **aplicaciones para *smartphones***. Normalmente la aplicación facilita un acceso intuitivo y práctico para controlar y monitorizar nuestro dispositivo, sin embargo, se deben tener en cuenta ciertos **requerimientos de seguridad** a la hora de emplear este tipo de *apps*.

Como suele suceder en general con las *apps* móviles, un punto prioritario a tener en cuenta es el punto de descarga de la misma. Es fundamental **descargar la aplicación desde un punto de descarga de confianza**. Si se realiza la descarga desde un *market* no oficial, **es posible que la aplicación pueda estar modificada** incluyendo **funcionalidades maliciosas** que puedan comprometer nuestra información personal o el propio dispositivo, dependiendo de sus capacidades.

Cuando se instale una de estas *apps*, también **se deben tener en cuenta los permisos que solicita** para funcionar. Por ejemplo, si instalamos una aplicación que nos permite controlar las luces de nuestra casa, es posible que

requiera acceso a la red, sin embargo no es lógico que nos solicite acceso a nuestros contactos o mensajes. Cuando identifiquemos uno de estos casos se recomienda, en primer lugar **denegar el acceso a la información que no consideremos estrictamente imprescindible,** y en segundo lugar **comprobar exhaustivamente si la fuente desde la que la hemos obtenido es confiable**.

6.6. Buenas prácticas y cultura de seguridad

Sea cual sea el ámbito de aplicación, los sistemas de información están preparados y diseñados para interactuar o prestar servicios a personas. Este hecho hace que además de los propios sistemas, **las personas puedan ser objetivos de ataques con el fin de acceder a un sistema informático**.

Teniendo en cuenta que **se suele asociar el eslabón más débil de la seguridad con el entorno de usuario**, es obvio que son un vector potencial de ataque y uno de los más empleados en la actualidad.

A este respecto, es fundamental que los usuarios **sepan reconocer una estafa o *phishing***, de modo que no sean víctimas fáciles. Por defecto, se debe **desconfiar de cualquier comunicación desde una fuente desconocida**, sea cual sea el medio por el que se reciba (correo electrónico, llamada telefónica, visita presencial, etc.). Por tanto se debe solicitar una identificación inequívoca en caso de una visita presencial o bien contactar por un medio alternativo con el proveedor o cliente al que supuestamente representa.

Por norma, **un administrador de un servicio nunca pedirá al usuario sus credenciales de acceso**, y menos por medios como correo electrónico o acceso a formularios web sin cifrado (que no comiencen por *https://* en la barra de nuestro navegador). Hay que entender que los administradores tienen acceso al listado completo de usuarios, siendo de su potestad dar el alta o baja de usuarios, así como gestionarlos. Cuando se reciba una solicitud en estos términos se debe desconfiar y validar en todos los casos la fuente de la misma.

Para minimizar el impacto en caso de sufrir una posible estafa, se recomienda

mantener credenciales de acceso diferentes para cada uno de los servicios de los que seamos usuarios (correo, banca *online*, redes sociales, etc.). Ya que en caso de que se faciliten es fácil extrapolar las mismas a otros servicios, y de ese modo el atacante obtendría más información fácilmente. Otra buena solución será, siempre que el servicio lo permita, optar por **habilitar autenticación por dos factores**, de modo que aunque se comprometieran las credenciales de acceso al servicio, no se vería comprometido al requerirse un segundo factor de autenticación, como por ejemplo un mensaje *SMS* al móvil.

Además de la precaución, la **formación y la concienciación** son la principal salvaguarda en estos casos, ya que otorgan al usuario la capacidad de identificar las estafas y reaccionar adecuadamente contra ellas. Por desgracia, la ingeniería social es una de las técnicas más empleadas en la actualidad y cada vez se diseñan técnicas más elaboradas y complejas que resultan mucho más difíciles de identificar para cualquiera. A este respecto, CSIRT-CV realiza y mantiene campañas de concienciación y cursos para facilitar cultura de seguridad de los usuarios[15].

[15] Campañas de Concienciación CSIRT-CV - http://www.csirtcv.gva.es/es/paginas/campañ-de-concienciación.html

Cursos de Formación CSIRT-CV - http://www.csirtcv.gva.es/es/paginas/formación.html

Guías e Informes CSIRT-CV - http://www.csirtcv.gva.es/es/paginas/descargas-informes-csirt-cv.html

7. Conclusiones

Con el presente informe desde CSIRT-CV hemos querido dar a conocer el estado del arte del término Internet de las Cosas. IoT hace referencia a aquellos "objetos" que hasta hace poco tiempo no tenían conexión a Internet o que recientemente se han incorporado con necesidades de conectividad. Como hemos visto, el número de dispositivos que cada uno de nosotros disponemos con conexión a Internet va en aumento y se espera que siga creciendo en los próximos años, especialmente los *wearables* aunque están surgiendo nuevos tipos y clases.

A lo largo del informe se ha ido enfatizando la importancia de que esta evolución deba notarse también en las medidas de seguridad que se aplican, tanto a nivel de producto como a nivel de usuario. A todos nos preocupan las amenazas de seguridad, la privacidad de nuestros datos y nuestra propia integridad física.

En términos generales se debe tener en cuenta la protección en la medida de lo posible de nuestro dispositivo (configuración del mismo, protección de acceso, información almacenada, cifrado, localización,...) y de nuestra red (cifrado *WPA2*, dispositivos conectados, puertos abiertos y *UPnP, WPS*,…).

En el ámbito corporativo IoT también supone un avance y a la vez un reto para las empresas ya que a pesar de la evolución y las ventajas que puede aportar, existe una elevada preocupación por las amenazas de seguridad que conlleva. Como podemos ver en la Ilustración 2, hay

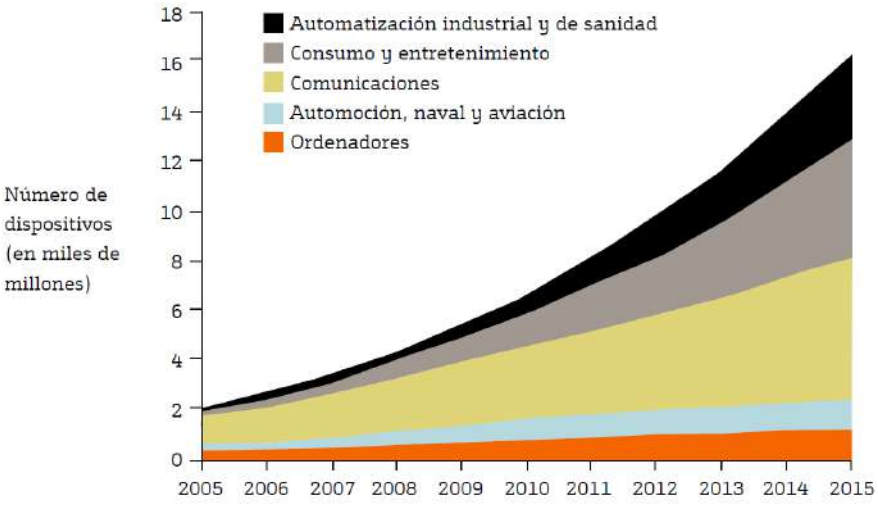


Ilustración 2: Dispositivos que se comunican por una red mundial.
Fuente: *Rise of the Embedded Internet*, White Paper Intel® Embedded Processors, 2009.

Fuente: Fundación Bankinter

sectores en los que esta revolución ha comenzado aunque todavía la previsión es de crecimiento exponencial en este aspecto.

Del mismo modo, la previsión de adopción de IoT en los diferentes sectores industriales se prevé abordar mayoritariamente en un plazo inferior a 5 años.

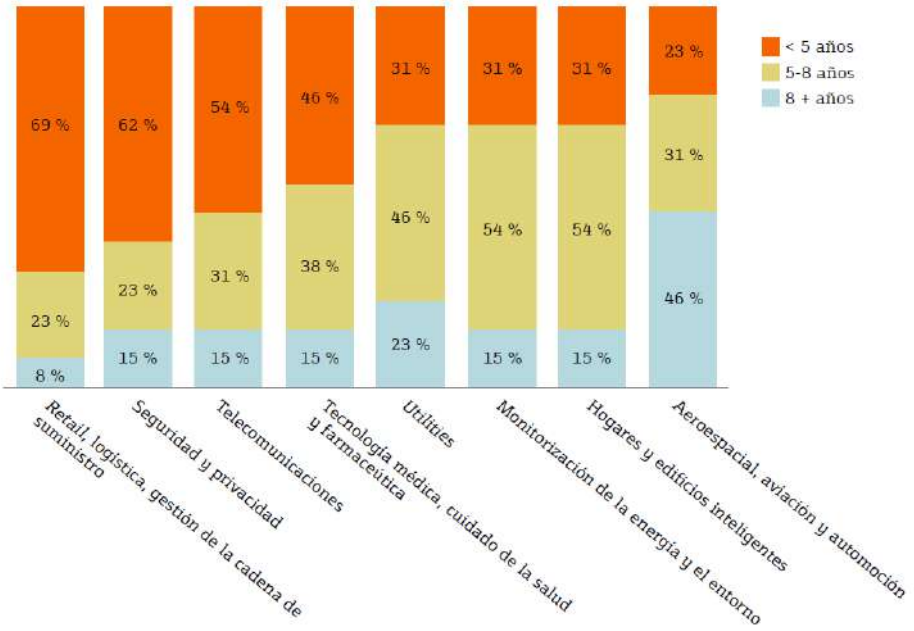
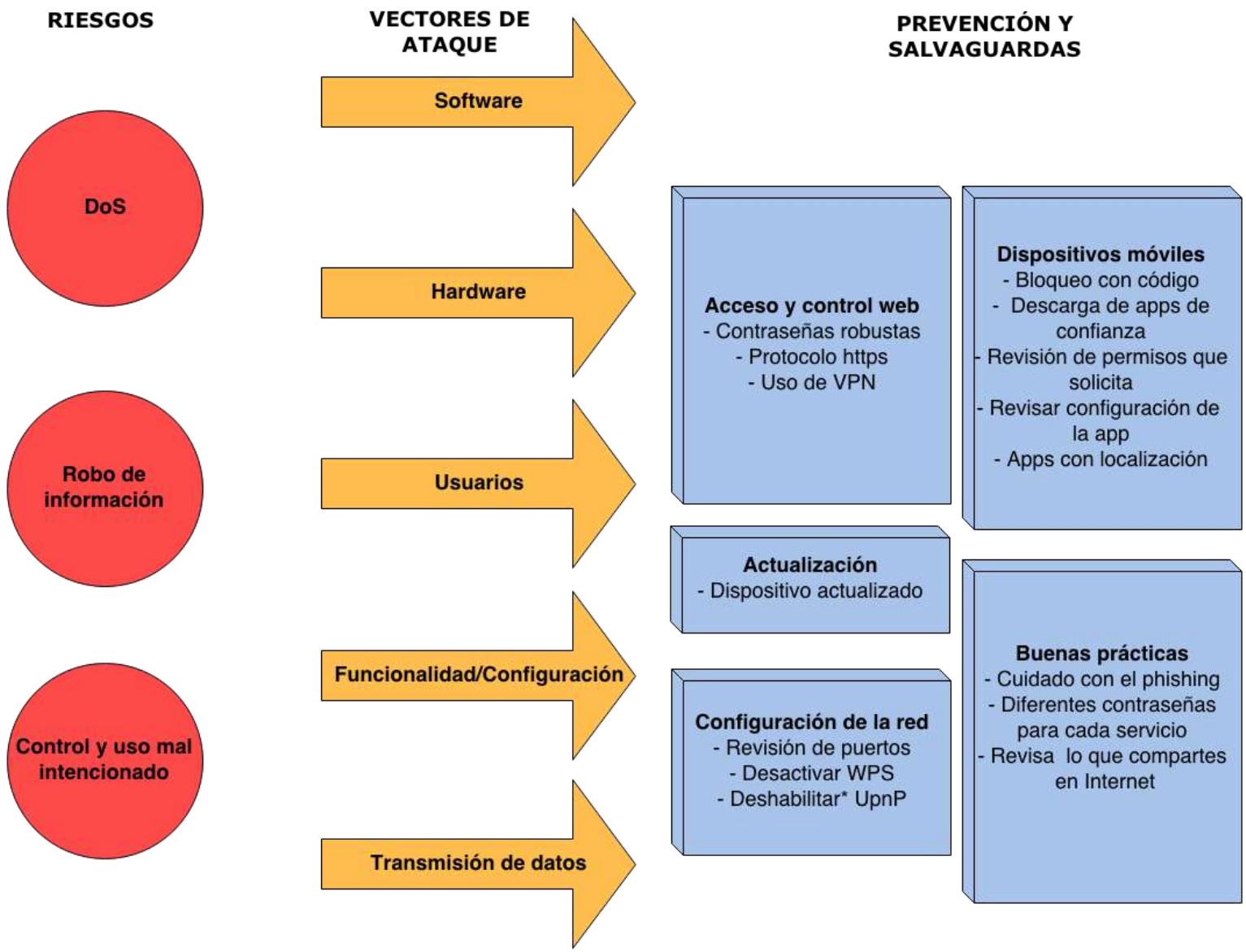


Ilustración 3: Velocidad de adopción del Internet de las Cosas en las distintas industrias.
Fuente: Elaboración propia.

Fuente: Fundación Bankinter

En el siguiente esquema queremos reflejar a modo de resumen lo expuesto en el informe, para que nos ayude a entender la importancia de las salvaguardas en los dispositivos que utilizamos.

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana



Desde CSIRT-CV queremos destacar que para que exista confianza en el uso de las nuevas tecnologías y se adopten sin recelo, es imprescindible que su uso sea seguro y que tengamos garantías de que cumplen con nuestras expectativas de privacidad, integridad y disponibilidad. En el caso de los dispositivos IoT es necesaria la participación de todas las partes (desde el desarrollo del producto e implementación del mismo hasta el usuario final que lo configura y hace uso del dispositivo) para que se ocupen y preocupen por la seguridad y apliquen las medidas que en cada caso sean necesarias. La tecnología debe ser evolución en todos los aspectos y no un retroceso en seguridad y privacidad de sus usuarios.


CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana