Guía sobre Seguridad en Dispositivos IoT

Secretaría de Estado de Seguridad

MINISTERIO DEL INTERIOR
AGOSTO 2023

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS

Guía sobre Seguridad en Dispositivos IoT

Título: Guía sobre Seguridad en Dispositivos IoT

Fecha del documento: Miércoles, 2 de agosto de 2023

Versión: V_1.0

Punto de Contacto: Oficina de Coordinación de Ciberseguridad (OCC)

EJEMPLAR:

Copia 01 de 01 copias.

CONTROL DE VERSIONES:

Fecha	Versión	Cambio	Motivo
28/11/2022	V_0.1	OCC-Servicio Análisis	Creación
16/01/2023	V_0.2	Deloitte	Inclusión casos de uso
27/04/2023	V_0.3	OCC-Servicio Análisis	Correcciones menores
02/08/2023	V_1.0	OCC-Servicio Análisis	Maquetación versión final

Prólogo

Cuando hablamos de tecnología en términos generales, podemos encontrar actualmente un amplio abanico de elementos y dispositivos que resultan sumamente funcionales y eficaces para el desarrollo de nuestra sociedad.

Esto se fundamenta en la necesidad de simplificar tareas y obtener formas de buscar la eficiencia en todo tipo de procesos y actividades para todos los ámbitos de nuestra vida, desde los profesionales hasta los personales. Y es por ello que toda esta tecnología debe ser accesible para todas las personas, permitiendo que todos estos recursos lleguen a todo aquel que lo requiera.

De este modo, cada vez tenemos a nuestra disposición más elementos que requieren unas características más especializadas, y sobre todo que tengan acceso a fuentes de información que les doten de mayores capacidades.

Y es precisamente en este punto donde entran en juego los dispositivos conectados, conformando el denominado Internet de las Cosas (o IoT por sus siglas en inglés), que esencialmente recoge todo aquello que se encuentra interconectado a través de la red de redes, permitiendo el intercambio de información y la realización de ciertas tareas de manera autónoma en la mayoría de las ocasiones. Elementos que anteriormente nos ofrecían una funcionalidad limitada, ahora se encuentran potenciados en gran medida gracias a estas nuevas tecnologías, que además les otorga cierta “inteligencia” a la hora de cumplir sus cometidos.

Pero por desgracia esta apertura tecnológica nos expone a ciertos ataques y vulnerabilidades que debemos tener en consideración, pues su uso puede suponer una oportunidad para aquellos que pretendan realizar acciones ilícitas en contra de nuestros intereses.

El Ministerio del Interior, consciente de la necesidad de protección de los sistemas de información, ha desarrollado esta Guía sobre Seguridad en Dispositivos IoT, en colaboración con Deloitte, que pretende, desde la óptica de colaboración público-privada ofrecer una visión amplia acerca de estos elementos, sus características e impacto en los diferentes sectores, así como la normativa que les es de aplicación y otros puntos de interés relacionados, con el propósito de crear conciencia de seguridad.

Ciertamente, los dispositivos IoT representan el futuro, pero no podemos obviar que, al aumentar su uso en cada vez más aspectos de nuestra sociedad, estamos aumentando también nuestra superficie de ataque, y por tanto nuestra visibilidad como objetivos.

Más allá del trabajo de fabricantes y otros especialistas para ofrecernos soluciones técnicas a estas vulnerabilidades, no debemos olvidar actuar también sobre el propio usuario, que debe conocer las implicaciones de no tomar las debidas precauciones al respecto, tanto a nivel personal como empresarial.

Así pues, les invitamos a realizar una lectura detenida de esta Guía, observando riesgos que quizá aún no haya tenido en consideración y ciertos ataques perpetrados que les puedan aportar nuevas ideas para su protección, y sobre todo les animamos a que consideren todas las ideas que, desde una nueva perspectiva, este documento les pueda ofrecer.

D. Álvaro de Lossada Torres-Quevedo,

Jefe de la Oficina de Coordinación de Ciberseguridad

Glosario

Acrónimos

DoS. *Denial of Service.* Tipo de ataque consistente hacer que los sistemas queden inaccesibles.

IoT. *Internet of the Things.* Es la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes).

IT. *Information Technology.* Conjunto de sistemas y telecomunicaciones empleados para procesar, almacenar y enviar información.

LIFI. *Light Fidelity*. Tecnología inalámbrica que emplea la luz para la transmisión de datos.

NFC. *Near Field Communication.* Tecnología inalámbrica que permite el intercambio de información entre dos dispositivos caracterizada por ser de alta frecuencia y corto alcance.

OT. *Operational Technology.* Conjunto de sistemas informáticos y de comunicaciones empleados en gestionar y controlar las operaciones de sistemas industriales.

WIFI. Wireless Fidelity. Tecnología inalámbrica que permite la conexión inalámbrica a través de ondas de radio entre dispositivos.

Definiciones

Amenaza. Potencial evento que puede causar daños graves en un sistema informático.

Botnet. Es una red de equipos que, infectados, son controlados a distancia por un atacante con el fin de propagar *malware* o llevar a cabo un ataque de denegación de servicio.

Bus de Campo. Es una red de comunicación industrial, de área local, que enlaza los dispositivos de campo con los de control sin necesidad de conectar cada dispositivo individualmente al controlador.

Controlador Lógico Programable (PLC). Dispositivo electrónico empleado en la automatización de procesos. Su función principal es la de controlar los procesos de una o más máquinas en un área local.

Control Supervisor y Adquisición de Datos (SCADA). Software empleado en la monitorización y control de procesos automatizados a distancia.

Edge Computing. Nuevo paradigma de la computación consistente en que el almacenamiento y el procesamiento de los datos se produce lo más cerca posible del dispositivo (edge).

Human-Machine Interface (HMI). Panel que presenta la información recopilada por el proceso automatizado de forma amigable y permite al usuario comunicarse con él.

Malware. Aplicación maliciosa diseñada para infectar equipos con el fin de extraer de los mismos información, denegar su acceso o propagar nuevas infecciones por la red entre otros.

Ransonware. Tipo de *malware* consistente en el cifrado de archivos exigiéndole un pago al afectado para la recuperación de los mismos.

Unidad Terminal Remota (RTU). Dispositivo electrónico cuya función principal es la que interconecta de forma inalámbrica el SCADA con los con los dispositivos de campo. Debido a su capacidad de conexión inalámbrica, se recomiendan para la adquisición y transmisión de datos en zonas geográficas más amplia.

Vulnerabilidad. Debilidad existente en un sistema informático que puede ser explotada por un atacante dando acceso al mismo.

1. Introducción

Hoy en día los dispositivos y otros elementos inteligentes y de comunicación resultan fundamentales en una sociedad moderna como la nuestra. El propósito de estos dispositivos no es otro que el de facilitar muchas de nuestras tareas rutinarias, con el fin de obtener un ahorro de tiempo en su realización.

En particular, el incremento actual de la popularidad de los sistemas IT (del inglés Information Technology o tecnologías de la información) es un hecho bastante evidente, y una muestra de ello es que, en apenas unas décadas, se ha logrado interconectar cualquier parte del mundo de forma totalmente transparente para el usuario.

Por otro lado, el hecho de haber podido establecer un sistema de interconexión a través del globo con el fin de poder comunicarse ha llevado al desarrollo de nuevas tecnologías que se sirven de estos sistemas, como es el caso del IoT (del inglés Internet of Things o Internet de las Cosas).

Un dato importante a tener en cuenta es que los dispositivos IoT presentan diferencias significativas con los IT. Una de las diferencias principales radica en que los entornos IT se forman en base a la propia información tanto en sistemas Cloud (de ahora en adelante nube) como en sistemas On Premise, mientras que el entorno IoT lo componen dispositivos con limites en su capacidad de procesamiento cuya principal tarea es la de enviar datos y gestionar el correcto funcionamiento de las máquinas y procesos que controlan.

Hasta hace unos años se disponía de una clara diferenciación entre los entornos de tecnología de operación (OT del inglés Operation Technology), normalmente asociado al ámbito industrial y los sistemas TI, ya que no estaban conectados entre sí, quedando por lo tanto los dispositivos OT protegidos frente a ciber amenazas externas, limitándolos a ser únicamente vulnerables a acciones directas sobre ellos en caso de que llegase a existir una cercanía física. Sin embargo, el concepto IoT proviene precisamente de la convergencia de estas tecnologías.

Con la progresiva digitalización de los procesos industriales, los dispositivos OT han implementado una conexión con el exterior y con otros dispositivos OT e IT. Es debido a esta conexión que comentábamos anteriormente que surge el termino IoT, brindando nuevas posibilidades en la operación y control en los procesos, pero que presenta nuevos problemas que afrontar relativos a la seguridad, como es el hecho de que se ha estimado que hay entre 15 y 20 años de desfase tecnológico entre la seguridad de los dispositivos OT/IoT respecto a los IT, a lo que se suma la complejidad añadida de contar con gran diversidad de los protocolos IoT, lo que hace que preservar su seguridad suponga un gran reto en los próximos años.

Dentro del ámbito IoT podemos entrar a hablar, por ejemplo, de varios tipos de sensores con gran variedad de funcionalidades como los relativos a la temperatura, humedad, presión, caudal, viscosidad y otros parámetros fisicoquímicos que hoy en día son de gran importancia en procesos de fabricación industrial, donde se precisan mediciones con un alto grado de precisión.

Por ejemplo, el proceso de fabricación de la turbina de un avión, durante cuyo proceso se realizan controles continuos mediante sensores de medición que aseguren que las medidas son exactas y que los materiales poseen las propiedades físicas adecuadas para enfrentarse al medio en el que van a trabajar, sometidos a temperaturas extremas y a altas presiones.

Como se ha mencionado con anterioridad, el IoT persigue optimizar la automatización de ciertos procesos en la sociedad actual planteando un sistema de interconexión total. Este sistema de interconexión busca hacer uso de varios sensores y conectarlos a internet para mejorar su gestión.

Poder disponer de dispositivos de uso cotidiano conectados a Internet es una gran ventaja, pero a su vez debemos tener en cuenta que comparten constantemente información y que, además, la recogen desde otros puntos o elementos cuyas funciones pueden ser de lo más diversas, por lo que es muy difícil establecer una protección específica ante la diversidad de dispositivos existentes. Otros ejemplos diferentes a los ya indicados serían la monitorización del estado de salud del usuario, la gestión de elementos a distancia o el control de elementos físicos como la temperatura, la humedad, etc.

Como toda tecnología emergente, esta deberá contar con expertos que ayuden a mantenerla, desarrollarla y mejorarla, con el fin de adaptarse a los nuevos cambios tecnológicos que se avecinen. Los dispositivos IoT no solo realizan estas funciones de manera pasiva, sino que también disponen de cierta inteligencia a la hora de tratar la información que gestionan, conformando de igual modo un ecosistema con otros elementos a través de una plataforma común.

Nuevamente podemos pensar en multitud de ejemplos de cómo el mundo IoT se está adentrando en nuestras vidas: domótica, seguridad en el hogar, los famosos wearables, dispositivos relacionados con la salud, logística inteligente, smartcities, automatización en los procesos industriales, etcétera. Así que las aplicaciones de estos dispositivos van desde lo concreto y lo personal, hasta la operación de una pluralidad de elementos para la gestión de grandes procesos y servicios.

¿Por qué está de moda el IoT si actualmente su seguridad es débil?

Los dispositivos IoT se han introducido en una gran variedad de sectores, pero lamentablemente no se ha creado una conciencia acerca del estado de su seguridad, bien porque antaño no fuera necesaria como en los entornos industriales o porque no se conocen los potenciales riesgos que pueden presentar. Debido a la rápida evolución de Internet, se ha conseguido hacer realidad la implantación de dispositivos IoT en multitud de ámbitos, conectando los dispositivos a internet y ofreciendo un alto grado de comodidad al usuario. Pero ¿qué ocurre si estos dispositivos no disponen de suficiente protección? Pues que cualquier persona con unos conocimientos básicos puede acceder y por lo tanto no solo comprometer la funcionalidad de los dispositivos IoT sino que el problema se amplía hasta el resto de nuestra red, pudiendo llegar a dispositivos e información realmente importante.

Como podemos ver efectivamente hay muchos usos y todos muy útiles, pero ¿qué pasaría si personas no deseadas acceden a ellos? ¿estaríamos dispuestos a usar estos dispositivos sin implantar medidas de protección? Seguramente la respuesta sea no.

2. Objetivos

Con el presente documento se pretende ofrecer una visión amplia acerca del estado actual de la ciberseguridad en dispositivos IoT, planteando en primer lugar el panorama actual, así como aquella normativa de seguridad existente relacionada con estos entornos, con el fin de obtener una familiarización con las normas y estándares de seguridad más aceptados por la comunidad internacional.

Tras ello, se realizará un acercamiento del uso actual de los dispositivos IoT, presentación de los componentes esenciales que conforman estos dispositivos, las infraestructuras necesarias para que puedan conectarse, para posteriormente profundizar en cuáles son los procesos esenciales de automatización de los dispositivos IoT más representativos y los principales protocolos usados en ellos actualmente.

Analizados los componentes y su arquitectura de interconexión, pasaremos a realizar un acercamiento a los sectores donde más incidencia está teniendo esta tecnología explicando brevemente cada sector, poniendo de relevancia sus particularidades y los riesgos a los que se enfrentan los dispositivos empleados en ellos, exponiendo finalmente casos de ataque exitosos ocurridos en los últimos años o potenciales riesgos.

Por último, se presentarán una serie de recomendaciones y buenas prácticas que puedan servir de guía para mejorar la protección en dichos dispositivos, así como para crear una conciencia del nivel de seguridad que asumimos a la hora de utilizarlos, actuando de una forma más estratégica, segura y responsable con el fin de reducir en la mayor medida posible los riesgos más comunes asociados a esta nueva tecnología disfrutando sus numerosas aplicaciones.

3. Panorama Actual

3.1 IoT en Cifras

Como podemos apreciar en nuestro entorno, el auge de esta nueva tecnología es palpable y se puede ver reflejada en todos los ámbitos de nuestra vida diaria.

Según Statista (2022) , se espera que para este año 2022 la cifra de dispositivos IoT sea superior a los 10.000 millones a nivel mundial llegando, en 2030, a superar la barrera de los 25.000 millones de dispositivos conectados.

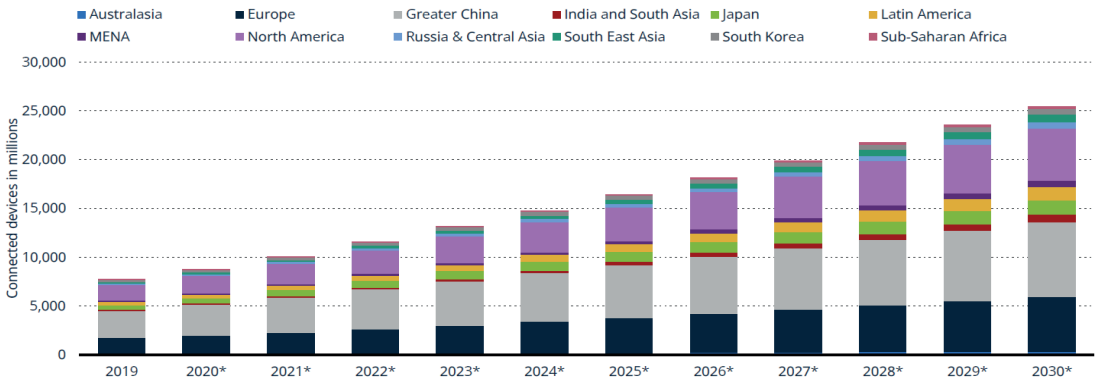


Ilustración 1. Estimación de número de dispositivos IoT conectados. Statista (2022).

Si analizamos las cifras por tipologías de uso podremos apreciar la predominancia de dispositivos enfocados a un uso multimedia (*Consumer Internet & Media Devices*) seguido de los sistemas de red eléctrica inteligentes (*Smart Grid*) y de los vehículos autónomos (*Autonomous Vehicles*).

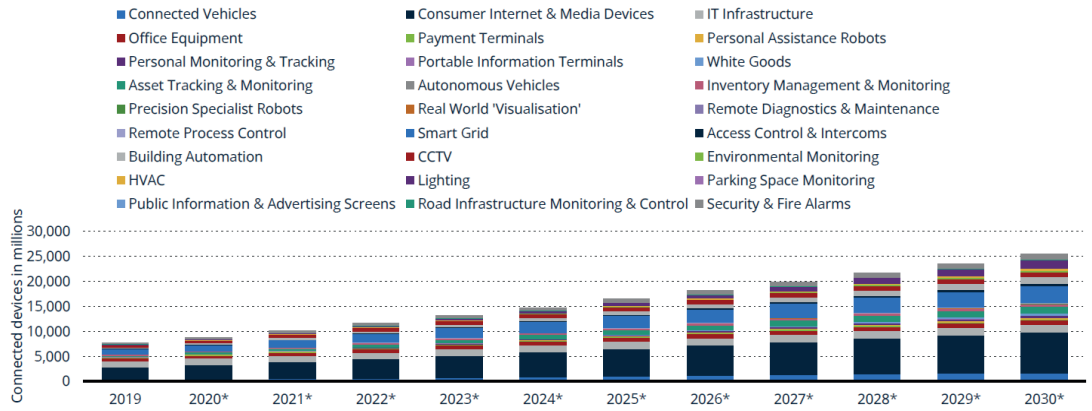


Ilustración 2. Previsión del número de dispositivos IoT conectados agrupados por casos de uso. Fuente: Statista (2022).

Relativo a la tipología de dispositivos conectados mundialmente, en la gráfica mostrada por Statista (2022) podemos apreciar una clara tendencia alcista de las conexiones de dispositivos IoT frente al estancamiento de dispositivos IT en las que se espera que, en 2025, triplique el número de equipos conectados a la red.

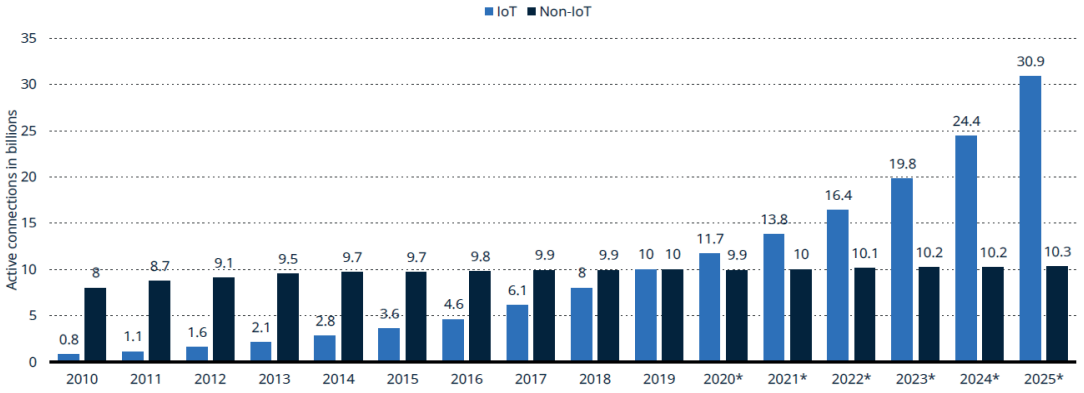


Ilustración 3. Previsión del número de dispositivos IoT y no IoT conectados. Fuente: Statista (2022).

En cuanto al nivel de penetración a nivel europeo del IoT, referido a los principales sectores, vemos una clara predominancia en el sector de automoción (*Automotive*) gracias al despliegue de cada vez más tecnología de sensorización en los vehículos, seguido del sector energético (*Utilities*) y edificios inteligentes (*Smart Buildings*).

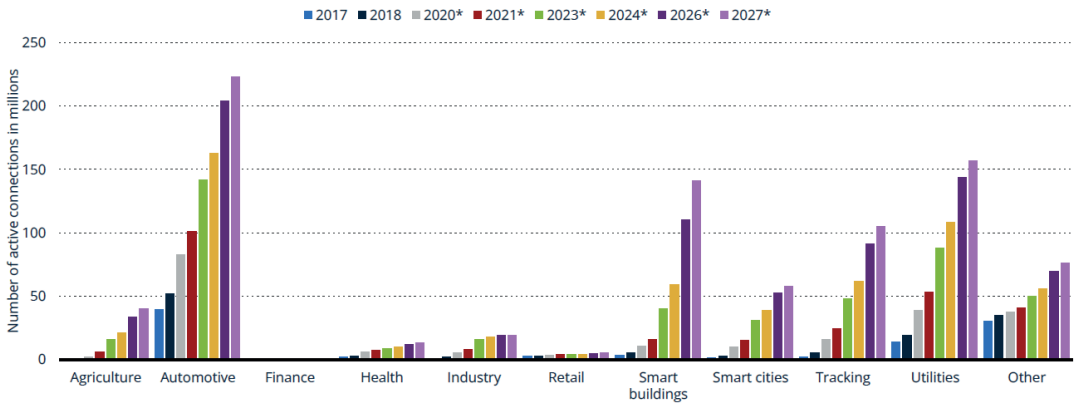


Ilustración 4. Previsión del número de dispositivos IoT conectados agrupados por industria. Fuente: Statista (2022)

En conclusión, los gráficos mostrados sirven para demostrar la evolución acelerada que el IoT está experimentando en numerosos países y sectores. La era de la interconexión entre dispositivos ha llegado, encontrándonos actualmente al inicio de esta nueva ola de innovación que solo el tiempo dirá hasta donde nos puede llevar.

3.2 Normativas aplicables en entornos IoT

El constante auge de estos dispositivos y las múltiples capacidades con las que cuentan han generado una serie de inquietudes a nivel legal. Entre ellas destacamos principalmente la privacidad que dispone el usuario y la protección de datos.

Todo dispositivo IoT es capaz de conectarse a una red recibiendo y enviando datos constantemente, como consecuencia esto facilita la accesibilidad y disponibilidad del dispositivo desde cualquier parte del mundo gracias a la simplicidad de conexión, pero ¿pueden acceder al dispositivo terceras partes ajenas al propietario? La respuesta es rotundamente sí, y no sólo hablamos de un atacante sino de las propias empresas que fabrican los dispositivos, sobre todo a nivel doméstico.

Principalmente se ve afectada la privacidad del usuario en el momento que las empresas que disponen de los datos del dispositivo hacen uso de ellos para fines que el propietario normalmente no aceptaría, por lo que es menester la implantación de marcos jurídicos y tecnológicos aceptados a nivel europeo e internacional, que obliguen a las empresas a contar con una mayor transparencia en sus políticas de privacidad y datos a los que acceden, además de ofrecer entornos seguros.

Con el fin de abordar estas casuísticas a nivel de ciberseguridad se están desarrollando una serie de normativas y estándares que permitirán establecer un gobierno efectivo en este novedoso entorno. No obstante, al tratarse de un entorno poco maduro, la normativa actual específica a este es escasa. Entre la normativa específica a los entornos IoT encontramos la siguiente norma:

- **IEC 30141,** arquitectura de referencia de IoT en el que se establece un marco de control que tiene como objetivo reforzar la seguridad, permitiendo así desplegar sistemas seguros que respeten la privacidad del usuario y minimicen el impacto de un posible ciberataque.

Aunque la normativa específica a entornos IoT sea escasa, existe normativa que afecta directamente a estos entornos. Encontramos las siguientes:

- **Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.** La también llamada Ley de Ciberseguridad 5G diseñada para proteger esta infraestructura y aprobada el pasado 28 de Abril, a través de la cual se definen una serie de medidas técnicas y estratégicas para garantizar la seguridad de las comunicaciones. Esta ley se desarrolló debido a que el avance del IoT está estrechamente relacionada con las comunicaciones ya que, sin ellas, fenómenos como el de la **hiperconectividad**, no llegarán a explotar todo su potencial. Las **redes 5G** son y serán el compañero perfecto de viaje que permitirá las infinitas posibilidades de uso que esta tecnología nos brinda y es por ello que han de regularse.

- **Reglamento General de Protección de Datos 679/2016 y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales 3/2018.** Son las dos normativas de referencia (a nivel europeo y nacional respectivamente) que regulan la problemática relativa a la privacidad en general de los datos del usuario. Cabe hacer mención a los conceptos de privacidad por defecto y desde el diseño los cuales persiguen que los desarrolladores de hardware y software tomen como referencia una serie de principios que garanticen que la creación de sus productos cuente con la implantación de medidas de seguridad enfocadas a la protección de los datos de carácter personal que tratan en sus diferentes fases.

- **Ley 8/2011, de 28 de abril,** por la que se establecen medidas para la protección de las infraestructuras críticas (**Ley PIC**), norma que busca garantizar la protección de infraestructuras catalogadas como críticas, responsables de proveer a la ciudadanía de servicios considerados como esenciales. Esta ley es de aplicación en sectores varios como el energético, nuclear, alimentario, transporte etc.

Asimismo, cabe mencionar aquella normativa y estándares específicos a entornos industriales y energéticos, los cuales se encuentran repletos de dispositivos IoT pudiendo llegar a extrapolarse a dispositivos IoT de otros sectores como el financiero o el de salud. Entre ellos encontramos:

- **NIST SP 800-82,** guía que proporciona las directrices necesarias para securizar sistemas de control industrial (ICS), así como todos los sistemas que lo componen (SCADA, DCS, etc.)

- **ISA/IEC 62443,** un conjunto de normas internacionales que abordan la ciberseguridad de la tecnología operativa en los sistemas de automatización de controles.

Estas y otras normativas se adjuntan, para su conocimiento, en los anexos del presente documento.

4. Desarrollando el ecosistema IoT

4.1 Dispositivos IoT

Definimos un dispositivo IoT como un sistema dotado de conexión a internet y con capacidad proporcionada por una capa de software que le permite medir parámetros físicos o actuar remotamente. Existen gran cantidad de elementos que conforman la familia IoT entre los que destacan los siguientes:

- **Sensores:** Son aquellos elementos capaces de medir una magnitud fisicoquímica. Se podría decir que un sensor busca únicamente determinar cualquier magnitud que queramos cuantificar, como puede ser la temperatura, el ritmo cardíaco, la cantidad de luz, imágenes, la velocidad o distancia y un largo etcétera.

- **Unidad de procesamiento:** El procesamiento de la información que manejan estos dispositivos se realiza en gran medida de manera local, generándose una inteligencia colaborativa potenciada por las capacidades de interconexión con otros dispositivos. Esto requiere de determinados elementos de hardware que doten a cada elemento IoT de cierta autonomía y, por lo tanto, capacidad de procesamiento autónomo suficiente para realizar la labor para la que fue diseñado (*edge computing*).

- **Software:** Tanto el referido al propio dispositivo IoT (interfaz de usuario, sistema operativo y controladores necesarios, actualizaciones y parcheado), como el necesario para generar la plataforma IoT que sustente el ecosistema entre dispositivos.

- **Plataforma IoT:** Relacionado con el punto anterior, una plataforma IoT sustenta los dispositivos interconectados que generan un ecosistema propio, uniendo hardware, puntos de acceso y redes de datos a una aplicación que opera con los mismos. Las plataformas ofrecen, además de esta gestión de dispositivos, el almacenamiento de información y su procesamiento, uso de los actuadores, visualización de datos e informes, herramientas adicionales, etc.

- **Comunicaciones:** Elementos hardware y software que manejen diferentes protocolos de redes inalámbricas, como bluetooth, wifi, red de datos 2G, 3G, 4G o 5G, etc., para la trasmisión y recepción de todos los datos generados por los dispositivos IoT.

- **Actuadores:** Es la manera de conectar con el mundo físico según la información recibida. Si los sensores reciben una información y envían una señal para ser procesada por un dispositivo que añadirá la inteligencia. Este dispositivo inteligente será el que envíe las órdenes pertinentes a los actuadores.

- **Almacenamiento:** Dado a que en los entornos IoT se generan gran cantidad de datos, puede resultar necesario un lugar donde almacenarlos. Suele ser habitual que los propios elementos IoT cuenten con un plan de almacenamiento y servicio propio, local y/o en la nube, en función de las necesidades o de las características de los dispositivos.

4.2 Infraestructura IoT

Las infraestructuras inteligentes son sistemas que hacen uso del Big Data, IoT e IT para gestionar los diferentes dispositivos conectados.

Cuando hablamos en general de internet en los dispositivos IoT, en realidad el término "internet" no sería el más adecuado, sino más bien del tipo de red de conexión a la que se conectan, ya que en ocasiones internet no es la vía principal de transmisión de información.

Existen diferentes tipos de infraestructuras de comunicación que dan cobertura a este aspecto en las Infraestructuras IoT, donde encontramos tecnologías de corto alcance (Bluetooth, LIFI, NFC, fiware u otras radiofrecuencias) o amplio alcance (ultra-wideband, WIFI, 4G o 5G).

Todo este desarrollo de los elementos IoT en nuestra sociedad está potenciado, por tanto, por el incremento de las capacidades de las redes de telecomunicaciones móviles, y especialmente en la implementación de las redes **5G**, que suponen un importante salto cualitativo y cuantitativo respecto a anteriores generaciones.

Pirámide de la Automatización

Así como en IT existe el modelo teórico de referencia OSI, la pirámide de automatización es el modelo de referencia presentado por la ISA-95 y empleado en la Industria 4.0. La Pirámide de Automatización divide y agrupa los distintos procesos, tecnologías y flujos de información que participan en un entorno industrial o productivo automatizado en 5 niveles:

0. **Red de Campo:** Procesos físicos propiamente dichos. Dentro de este primer nivel se encuentran los equipos de campo: los sensores, actuadores, temporizadores y en definitiva cualquier tecnología que forme parte del proceso productivo o industrial.

1. **Red de Control:** Actividades implicadas en el control y manipulación de procesos físicos. Dentro de este segundo nivel se encuentran los dispositivos especializados en el control de la Red de Campo como los Controladores Lógicos Programables (PLCs) o las Unidades de Terminal Remota (RTUs).

2. **Red de Operación y Supervisión:** Actividades de monitorización y supervisión de procesos. Dentro de este tercer nivel se encuentra el Sistema de Control de Supervisión y Adquisición de Datos (SCADA) y los Interfaces Humano-Máquina (HMI).

3. **Red de Manufactura:** Gestión de las actividades y flujo de trabajo necesario para mejorar la eficiencia del proceso. Dentro de este cuarto nivel se encuentra el Sistema de Ejecución de Manufactura (MES).

4. **Red de Administración**: Actividades relacionadas con el negocio, necesarias en una organización industrial. Dentro de este quinto nivel se encuentra el Sistema de Planificación de Recursos Empresariales (ERP).

Ilustración 5. Pirámide de la Automatización según la ISA-95. Fuente: ISA (2018).

La pirámide de la automatización nos permite representar la arquitectura de un sistema IoT en tres niveles bien diferenciados. Esta arquitectura no es ni mucho menos algo estándar y en la que todo el mundo coincida. No obstante, sí que hay cierto consenso en cuanto a los tres niveles establecidos:

- **Edge** o **plano local:** El extremo que incluye sensores y actuadores que interactúan con el mundo tales como puertas de enlace (gateways), concentradores, así como otros nodos IoT que permiten una conexión con los primeros.
- **Red de Comunicaciones:** es el vehículo que conecta los datos desde el plano local al remoto.
- **Nube** o **plano remoto:** Que abarca el conjunto de sistemas que permiten analizar y visualizar los datos en tiempo real (servidores, bases de datos, plataformas, etc.)

Protocolos IoT

Un protocolo de comunicaciones es un conjunto de normas que permite a dos o más equipos entablar, a través de un medio acordado, un intercambio de información. Los protocolos IoT pueden dividirse en dos grandes categorías: **protocolos de transmisión** y **protocolos de acceso a la red.** Gregersen (2020) pone de manifiesto algunos de los protocolos más relevantes en este ámbito. Son los siguientes[1]:

Protocolos IoT orientados al acceso de red

Los protocolos IoT de acceso a la red, conectan dispositivos IoT entre sí y a Internet generado una red. Estos protocolos establecen el medio o vehículo por el cual se va a realizar la comunicación. Entran en esta categoría:

Wi-Fi

El Wi-Fi es un protocolo IoT de uso frecuente que se puede encontrar en edificios de todo tipo: domésticos, comerciales, industriales, públicos etc. Este protocolo ofrece una

1 https://www.nabto.com/guide-iot-protocols-standards/

rápida transferencia de datos y una gran capacidad de procesamiento de datos, además de ser particularmente adecuado dentro de entornos LAN con distancias de corto a medio alcance.

Sin embargo, el gran consumo de energía del Wi-Fi junto con su corto-medio alcance y su baja escalabilidad hacen que se vea limitado para algunos entornos IoT, que empleen dispositivos de baja potencia o que requieran comunicaciones de larga distancia.

Bluetooth

Bluetooth representa una tecnología de comunicación inalámbrica de corto alcance que utiliza ondas de radio de longitud de onda corta y alta frecuencia. En la actualidad, el protocolo Bluetooth tiene dos variantes: el Bluetooth Classic (versión 1.0-3.0) y el Bluetooth Low Energy o BLE (versión 4.0-5.0) destinado a dispositivos de bajo consumo, lo que lo convierte en una opción ideal de comunicación para dispositivos IoT como sensores, medidores de fitness y monitores de salud.

Redes móviles (3G, 4G y 5G)

Muchas de las aplicaciones del IoT usan las redes celulares ya existentes, como 3G, 4G y 5G para la comunicación de datos. Estas representan una de las mejores opciones para implementar en comunicaciones de larga distancia o donde la distancia pueda variar.

Estas redes, gracias a las características que presentan, permiten que el tráfico de datos generado por estos dispositivos pueda ser transportados a gran velocidad y sin que estos se encolen.

Sobre este punto cabe destacar la aportación del 5G dentro del mundo IoT. El 5G permite una conectividad más rápida, estable y segura entre dispositivos que sus predecesores, lo que a su vez permite la elaboración de ecosistemas y redes IoT cada vez más grandes y complejos. La UIT-R define tres grandes áreas en las que englobar las capacidades mejoradas de la 5G. Estas son:

- **Banda Ancha Móvil Mejorada (eMBB):** El 5G ofrece conexiones más rápidas, mayor rendimiento y mayor capacidad. Esto ayuda a la transmisión de datos en zonas de mayor tráfico como estadios, conciertos y ciudades.

- **Comunicaciones Ultra Fiables de Baja Latencia (URLLC):** El 5G permite comunicaciones fiables, robustas e ininterrumpidas entre los diferentes sistemas de una compañía. Esto garantiza el funcionamiento de sistemas, que en caso de fallar o verse interrumpidos impactarían gravemente a la compañía.

- **Comunicaciones Masivas de Tipo Máquina (mMTC):** Se espera que para 2025 el 5G conecte la mayoría de los dispositivos IoT. Dispositivos como drones, coches autónomos o incluso robots dispondrán de una conexión 5G.

Z-Wave

Z-Wave es un protocolo de comunicaciones inalámbricas. Permite el control de dispositivos tales como electrodomésticos similares a través de una red que interconecta a los mismos.

ZigBee

ZigBee al igual que Z-Wave es un protocolo de comunicaciones inalámbricas utilizado principalmente para domótica, que funciona creando una red de área local (LAN) de malla. Igualmente, comparte ciertas similitudes con el Bluetooth, sin embargo, a diferencia de este ZigBee tiene un rango más largo, pero una velocidad de datos más baja.

Matter

Matter es un protocolo de red muy reciente empleado para domótica cuyo objetivo principal es lograr la interoperabilidad entre los dispositivos domésticos inteligentes y las plataformas Smart home de diferentes proveedores. En otras palabras, Matter permite la compatibilidad de los dispositivos domésticos inteligentes con las principales plataformas de Smart home, gracias a su funcionamiento a través de routers de frontera compatibles, evitando el uso de hubs propietarios. Este protocolo también permite a los dispositivos que lo emplean comunicarse con la nube y comunicarse entre sí sin depender de una conexión a Internet.

Protocolos IoT orientados a la transmisión de datos

Los protocolos IoT de transmisión de datos, codifican la información compartida entre dispositivos IoT conectados entre sí y a la red. Estos protocolos establecen el “idioma” con el que se va a realizar la comunicación.

Los protocolos IoT de transmisión de datos se diseñaron para abordar la necesidad de diseñar protocolos seguros y ligeros, que respeten la reducida capacidad de potencia de los dispositivos IoT, conectados a redes de comunicación poco confiables, y la rápida necesidad de transferencia de información y operaciones típica de entornos industriales y automatizados.

A su vez estos protocolos se pueden dividir en: protocolos orientados al IT, que sirven para la comunicación entre los dispositivos IoT e Internet, y protocolos orientados al OT, que sirven para la comunicación con los equipos industriales.

Protocolos basados en la comunicación de dispositivos IoT con la red

Los protocolos de comunicación de dispositivos IoT con la red, son altamente flexibles y están pensados para transmitir cualquier tipo de información. Los protocolos más habituales son:

Message Queuing Telemetry Transport (MQTT)

MQTT es un protocolo ligero de transmisión de datos entre dispositivos IoT que cuenta con un modelo de mensajería publicación-suscriptor y permite un flujo de datos simple entre diferentes dispositivos. A diferencia del modelo cliente-servidor, MQTT divide a los clientes en dos categorías: publicadores y suscriptores. MQTT transmite la información de los publicadores a los suscriptores a través de “brokers” o servidores que actúan como mediadores.

Advanced Message Queing Protocol (AMQP)

Protocolo de código abierto empleado en middleware orientado a mensajes. Es capaz de emplear tanto el modelo de mensajería de petición-respuesta como el modelo publicación-suscriptor.

Constrained Application Protocol (CoAP)

Protocolo diseñado para satisfacer las necesidades de los sistemas IoT basados en HTTP. Se fundamenta en el protocolo UDP que le permite establecer conexiones seguras, permitiendo así la transmisión simultanea de datos.

Protocolos basados en la comunicación industrial

Los protocolos industriales recogen los protocolos utilizados en el telecontrol de los sistemas de supervisión SCADA, encargados de transportar la información o datos desde un dispositivo de control como un RTU, un PLC, un Gateway o un servidor de comunicaciones asociado a un proceso hasta el sistema SCADA propiamente dicho, y los protocolos utilizados en los buses de campo, encargados de reunir la información que se genera en dispositivos de campo (sensores, actuadores) y concentrarla en dispositivos de control para ser procesada. Algunos de los protocolos más comunes serían:

Modbus

Es uno de los más antiguos y más utilizado. En el aspecto de seguridad, el protocolo Modbus en la capa de aplicación carece de autenticación y no permite el cifrado de la información transmitida.

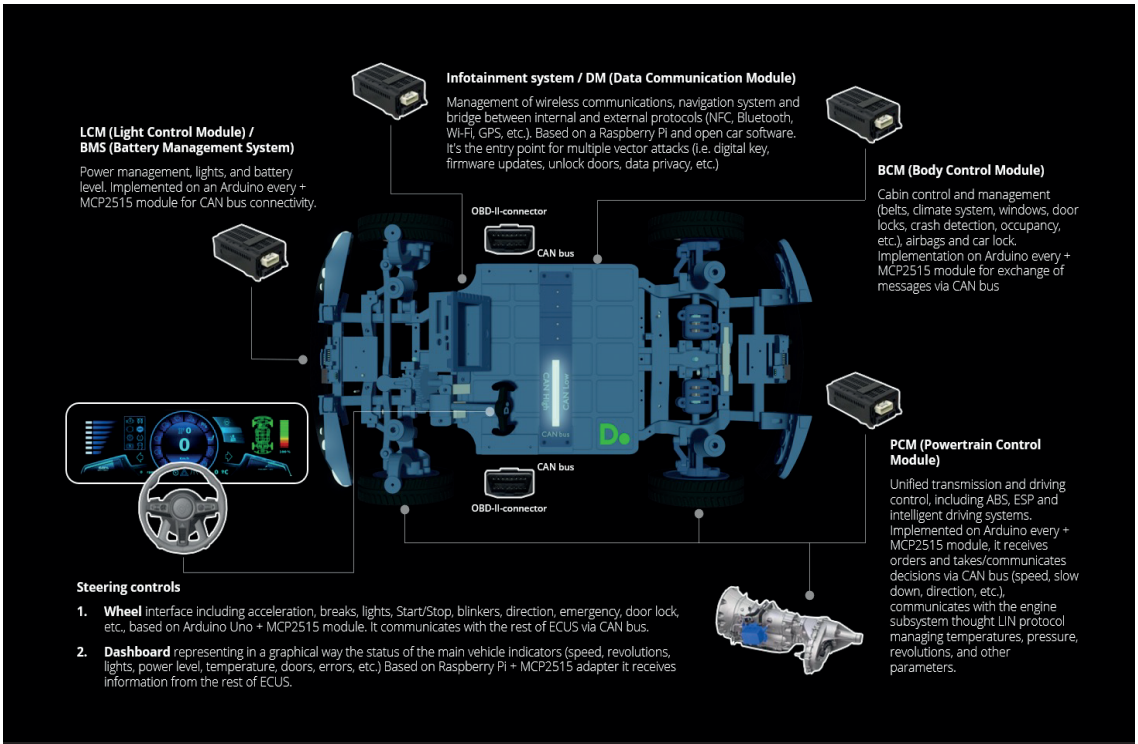


Ilustración 7. Analizando el tráfico CANBUS. Fuente: Deloitte (2022).

DNP3

Se trata de un protocolo de comunicaciones usado sobre todo en el sector eléctrico. Actúa en las capas de enlace, de aplicación y de transporte, y está diseñado para dar prioridad a la disponibilidad, más que a la confidencialidad y la integridad.

IEC104

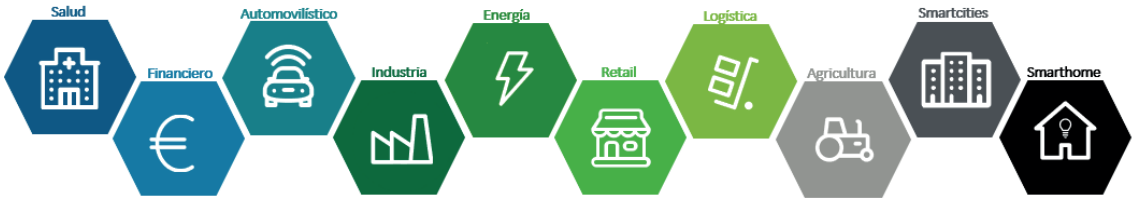
Es un protocolo que se encarga exclusivamente del telecontrol, la monitorización y las comunicaciones con el sistema SCADA. Este protocolo permite a las estaciones de control enviar comandos a dispositivos remotos en una sola dirección, llamada “de control”. Por otro lado, también permite a los dispositivos remotos, también conocidos como estaciones controladas o subestaciones, transmitir los datos recogidos a las estaciones de control, de nuevo en una sola dirección, llamada en este caso “de supervisión”. Al ser dependientes de la estación de control, los dispositivos remotos también reciben el nombre de “esclavos”.

5. Importancia de IoT en sectores esenciales

A continuación, se van a mostrar los principales sectores donde la presencia del uso de dispositivos IoT ha crecido considerablemente.

Ello ha permitido, entre otras cosas, la automatización de diversas tareas lo cual ha repercutido directamente en una mejor gestión de las capacidades existentes.

Cada sector dispondrá de una breve introducción acompañada de las posibles aplicaciones de dispositivos IoT en él, finalizando con posibles casos de uso y/o ciberincidentes ocurridos en sector.



5.1 Salud

La tecnología resulta cada vez más necesaria en la atención médica, ya que permite ofrecer un servicio más personalizado e inteligente, siendo uno de los sectores donde las aplicaciones IoT están teniendo un mayor impacto. Los dispositivos sanitarios interconectados se engloban bajo un término nuevo: Internet de las Cosas Médicas o *IoMT*, por sus siglas en inglés de Internet of *Medical Things*.

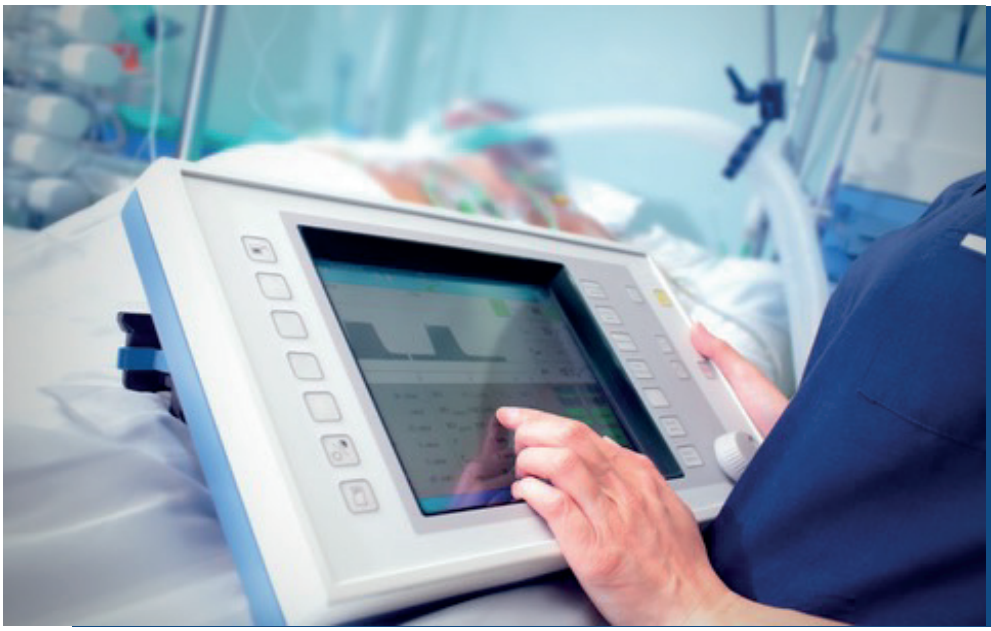


Ilustración 8. Uso de dispositivos IoT en el sector salud. Fuente: Deloitte Insights (2022).

Estos dispositivos ofrecen una disponibilidad en vivo de los datos que recogen en tiempo real (monitorización continua), lo cual agiliza y mejora los tratamientos médicos.

Además, no es necesario que el paciente se encuentre físicamente en el centro sanitario, ya que a través de la telemedicina se pueden ofrecer tratamientos puntuales o realizar el seguimiento diario de una enfermedad. Este punto es de vital importancia, sobre todo en zonas rurales las cuales no disponen de centros, que ven suplida esta carencia, en parte, con la telemedicina y la implantación de sistemas de monitorización continua a los habitantes de las mismas.

De hecho, la situación de pandemia que recientemente ha llevado a escenarios de asilamiento domiciliario ha evidenciado la necesidad de este tipo de servicios especialmente con los pacientes más vulnerables, que demandan una monitorización continua y a distancia, que puede revertir en un sistema de alarmas en tiempo real en caso de que ciertos parámetros de salud alcancen ciertos niveles.

Existe una amplia variedad de dispositivos médicos y cada vez a más de ellos se les está dotando de la capacidad de conectarse a internet y enviar información a los profesionales sanitarios en tiempo real.

Aplicaciones en el sector de la Salud

Las aplicaciones de dispositivos IoMT en el sector de la salud van desde la monitorización del paciente, la telemedicina, los wearables, al uso de drones para la entrega de suministros o la utilización de realidad aumentada en tratamientos de rehabilitación, entre otros.

Un ejemplo de la aplicación de elementos IoMT en el sector salud es la monitorización no invasiva a través de sensores de información fisiológica, como pueden ser audífonos electrónicos o monitores cardíacos o de glucosa.

Igualmente, los dispositivos IoMT también pueden utilizarse para guiar el cuidado de la salud en pacientes que tengan afectada la calidad de vida, a través de elementos biomédicos que recojan no solo esos parámetros fisiológicos a los que hemos hecho mención, sino que también realicen un seguimiento de la actividad y otros cambios vitales relacionados que permitan realizar un tratamiento personalizado.

Más allá del cuidado directo de la salud, pero sin salir de este ámbito, podemos encontrar estos elementos en el control de inventario hospitalario, controlando el registro de suministro y artículos médicos y de farmacia, por ejemplo, a través de etiquetas RFID que se escanean en cada movimiento, vigilando que haya suficiente stock de producto y que las dosis administradas sean las correctas y las reciba el paciente para quien han sido prescritas.

Otro ejemplo puede ser la monitorización de cámaras frigoríficas que aseguren el entorno de conservación óptimo para ciertos medicamentos como las vacunas, intercambio de información clínica, etc.

Esta tecnología aporta muchos beneficios a este sector, como pueden ser:

- Monitorización en tiempo real del estado del paciente y acceso inmediato a la información médica.
- Anticipación en la respuesta ante signos evidentes de ataques o accidentes.
- Seguimiento constante del estado del paciente y posibilidad de ajustar el tratamiento suministrado de forma inmediata.
- Mejora en la eficiencia en el suministro de los recursos médicos.
- Minimización de errores en el diagnóstico de enfermedades gracias al uso de bases de datos compartidas.

Riesgos a los que nos enfrentamos

A pesar de que esta tecnología mejore la calidad de la atención médica, su capacidad para comunicarse a través de internet ha aumentado el riesgo de ciberataques.

Los dispositivos médicos necesitan un mayor nivel de seguridad dado que son vidas humanas las que se ponen en riesgo ante una amenaza, siendo esta también la razón por la que muchos atacantes ponen el foco en el sector sanitario. Ante, por ejemplo, un ataque ransomware los precios que pueden cobrar por datos confidenciales son muy altos dada su importancia.

Ataques perpetrados y casos de uso

¿Alguna vez ha pensado en lo vulnerables que son los marcapasos? Como bien es sabido, años atrás se detectaron fallos de seguridad en dispositivos tan sensibles y con tanta relevancia para la salud de los pacientes tales como marcapasos y desfibriladores. A través de las vulnerabilidades encontradas se pudo comprobar que era posible su hackeo de forma remota.

Un ciberdelincuente solo tendría que modificar el código interno del dispositivo desde su casa para acabar con la vida de un paciente. Las autoridades sanitarias calcularon que podía haber medio millón de dispositivos con este problema.

Otro caso más reciente ha tenido que ver con las las bombas de medicamento a través de las cuales se administran el flujo de los medicamentos y fluidos intravenosos de los pacientes. Su uso adecuado puede ser muy beneficioso, pero ¿qué pasa si un paciente recibe una cantidad insuficiente o excesiva de un medicamento? Supondría un gran riesgo para la vida del paciente.

Empresas especializadas en el sector detectaron ciertas deficiencias en la configuración de las mismas que permitían, al igual que en el caso anterior, acceso remoto a las mismas permitiendo así al atacante poder modificar los parámetros de suministro de la medicación o acceder a datos del paciente entre otros.

5.2 Financiero

Los sectores más corporativos como el sector financiero también deben pasar por grandes evoluciones que incorporen tecnologías IoT. Algunas de ellas no visibles para los consumidores, pero con un gran impacto en la vida de las personas.

Ilustración 9. Monitorización cotización bursátil. Fuente: Deloitte Insights (2022).

Aplicaciones en el sector Financiero

La principal aplicación dentro de este sector se basa en la vigilancia de productos, aplicaciones y locales que conforman la interconexión de la banca entre sí, a través de la fusión de la tecnología de la operación con la de la información.

Otro de los puntos a destacar es el uso de los wearables (pulseras, smartwatches entre otros) con tecnología NFC que permiten al usuario realizar pagos móviles sin necesidad de disponer de su tarjeta de crédito o validar transacciones realizadas a través de otros dispositivos.

Es por esto que cada vez las instituciones van a dedicar una mayor inversión en integrar dispositivos IoT, los cuales ayuden a una mejor optimización y gestión del sistema bancario y financiero.

Riesgos a los que nos enfrentamos

Actualmente hay más de 30.000 millones de dispositivos IoT que transmiten datos a las aplicaciones de aprendizaje automático, Business Intelligence (BI) y análisis. Gran parte de esta actividad se origina en las transacciones financieras, como los registros de transacciones de cuentas, los pagos de hipotecas, las operaciones bursátiles, las puntuaciones de crédito y el análisis del fraude.

Esas son las fuentes más obvias. Pero hay muchos más tipos de datos que se recogen gracias a este tipo de dispositivos, como los recopilados con el acelerómetro de su teléfono que se utilizan para detectar anomalías en sus signos vitales y el comportamiento correlacionado con los patrones de engaño que tienen la capacidad de informar de las predicciones al departamento de fraude de su banco.

Ataques perpetrados y casos de uso

Cobalt es un malware mediante el cual su creador manipulaba los cajeros automáticos de forma remota para poder extraer dinero y obtener así casi 5 millones de euros.

Este ataque constaba de 4 fases:

1. **Desarrollo:** El cibercriminal desarrolló el malware y envió varios correos electrónicos de spear-phishing (correo dirigido a un grupo de usuarios) a los empleados del banco para infectar así sus ordenadores.

2. **Infiltración e infección:** El atacante desplegó el malware por la red interna del banco, infectando los servidores para poder controlar los dispositivos IoT, en este caso cajeros automáticos (ATMs).

3. **Robo de dinero:** El dinero se robaba o extraía del banco de 3 maneras distintas:

    a. Transferencias: El cibercriminal transfería dinero a su cuenta o a cuentas de bancos extranjeros.

    b. Aumento de saldo de cuentas: El cibercriminal aumentaba los saldos de las cuentas en los bancos y los muleros retiraban el dinero a través de los cajeros automáticos.

    c. Controlando ATMs: El cibercriminal enviaba comandos a ATMs específicos para que proporcionaran dinero y así los muleros pueden retirarlo sin necesidad de realizar operación alguna.

4. **Lavado de dinero:** El dinero robado o extraído al banco era usado para la compra de cripto-monedas.

Esta operación fue replicada en ocasiones posteriores por el atacante de forma satisfactoria logrando así aumentar el montante que originariamente había conseguido.

5.3 Automovilístico - Transportes

La industria de la automoción ha iniciado un cambio de paradigma hacia la conexión y la autonomía de vehículos. Los coches inteligentes ya disponibles hoy en día proporcionan características conectadas y de valor añadido tanto para mejorar la experiencia de los usuarios de automóviles como la seguridad del propio automóvil.

Aplicaciones en el sector Automovilístico - Transportes

La automatización de los vehículos ha seguido un proceso gradual, que inicia con la conducción asistida (nivel 1 de automatización), pasando a la conducción parcialmente automática (nivel 2 y 3 de automatización), hasta llegar actualmente a la conducción autónoma. Los automóviles que forman parte de la última categoría pueden clasificarse en dos tipos:

- Automóviles semiautónomos (nivel 4 de automatización): se refiere a automóviles altamente automatizados que son equipados con una multitud de sensores para poder de forma autónoma (es decir, sin ningún tipo de intervención del conductor humano) realizar todas las funciones de conducción en determinadas condiciones (por ejemplo, en un determinado tipo de caminos).
- Automóviles autónomos (nivel 5 de automatización): se refiere a coches totalmente automatizados que, equipados con multitud de sensores, realizan de forma autónoma toda la conducción en todas las condiciones es decir, en cualquier momento y en cualquier camino. Es posible que este tipo de vehículos acaben por eliminar el volante o los pedales de aceleración y frenado en un futuro.

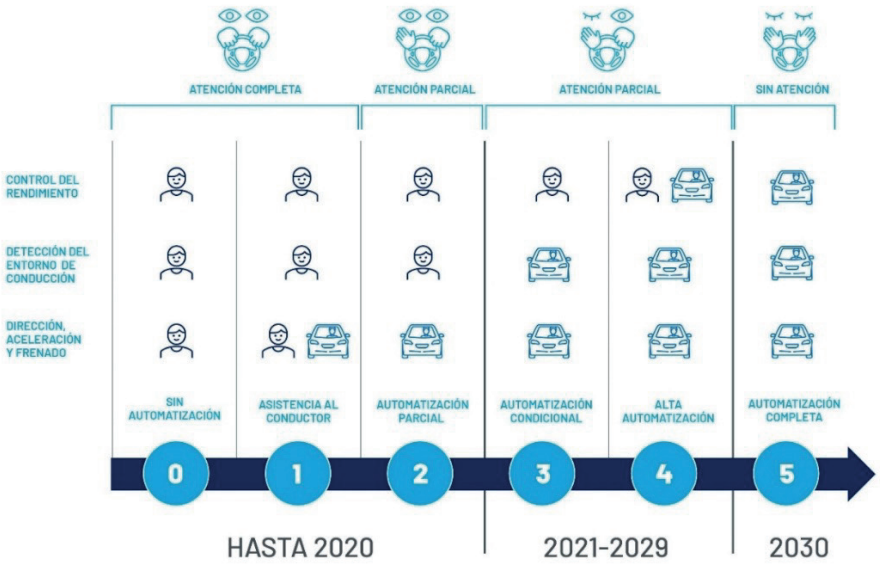


Ilustración 10. Niveles de Conducción Automatizada. EPRS. Fuente: European Commission (2019).

Cada nuevo nivel de automatización supone un incremento en la complejidad y número de conexiones entre el vehículo y dispositivos como sistemas de posicionamiento por satélite, smartphones, servidores, sensores, cámaras o GPS, que trabajan de forma conjunta para hacer que en última instancia el coche asuma todas las funciones de conducción.

ENISA (2019), a través del informe nos muestra la siguiente figura muestra una descripción general de los sistemas y aplicaciones tanto “dentro del vehículo” como “fuera del vehículo” conectados al vehículo durante la conducción autónoma:

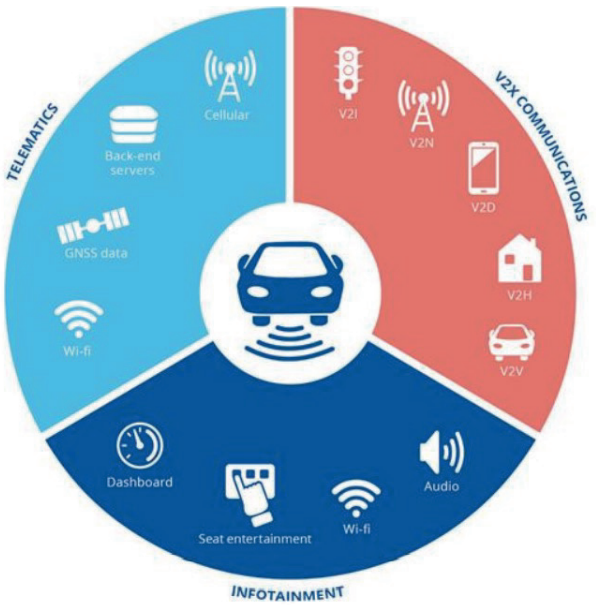


Ilustración 11. Ecosistema de automóviles inteligentes. Fuente: ENISA (2019).

Riesgos a los que nos enfrentamos

Con el surgimiento de los sistemas semiautónomos y automóviles autónomos, que utilizan aprendizaje automático avanzado e inteligencia artificial, los riesgos potenciales y los desafíos de ciberseguridad aumentan. Además, las interfaces de vehículo a vehículo (V2V) y de vehículo a infraestructura/entorno (V2I) necesarias para el despliegue de sistemas de transporte inteligentes y automóviles autónomos, incrementan aún más los riesgos de seguridad, ya que amplían en gran medida la superficie de ataque potencial y los vectores de ataque.

Para habilitar este tipo de comunicaciones, los vehículos están equipados con diferentes sistemas de comunicación inalámbrica no exentos de riesgo, como son: comunicaciones dedicadas de corto alcance (DSRC40), comunicación de luz visible (VLC), comunicación de sensor de imagen (ISC), Bluetooth, WIFI o tecnologías de comunicación móvil, como 3G, 4G y 5G.

Igualmente, los coches autónomos cuentan con puertos USB desde los que el conductor puede conectar dispositivos directamente al vehículo, dispositivos que de encontrarse hackeados le brindarían al hacker el acceso directo al automóvil.

Los ataques dirigidos a coches inteligentes pueden dar lugar a la inmovilización del vehículo, la aceleración involuntaria del vehículo, la alteración de parámetros preprogramados como la presión de los neumáticos o nivel de aceite, accidentes de tráfico, pérdidas financieras, divulgación de datos confidenciales y/o datos personales, e incluso poner en peligro la seguridad de los usuarios de la vía.

En la siguiente figura se muestra el compendio de buenas prácticas a seguir a la hora de securizar los vehículos inteligentes:

Ilustración 12. Buenas prácticas de ciberseguridad en coches inteligentes. Fuente: ENISA (2019).

De acuerdo a la ilustración, los controles recomendados son de 3 tipos:

- Políticas, entre las que no pueden faltar "Seguridad por diseño", "Privacidad por diseño", "Gestión de activos" y "Gestión del riesgo y amenazas".
- Prácticas organizacionales, tales como: Relación con proveedores, Formación, Gestión de la seguridad, o gestión de incidentes.
- Prácticas técnicas: Control de acceso, continuidad de las operaciones, seguridad de la nube entre otras.

Ataques perpetrados y casos de uso

El despliegue de la tecnología en automóviles inteligentes y su cada vez mayor conectividad con el exterior ha dado lugar a la aparición numerosas vulnerabilidades las cuales han sido explotadas consiguiendo así tomar el control remoto del mismo pudiendo arrancar, parar e incluso desviarse de la carretera mientras el usuario conducía el vehículo.

5.4 Industria

En los últimos tiempos los entornos industriales han evolucionado rápidamente gracias a la digitalización y automatización de sus procesos, enlazando el concepto IoT con el de Industria 4.0, que si bien son términos que se refieren a elementos muy parecidos, sí que pueden destacarse ciertas diferencias:

- Los dispositivos IoT se orientan a productos individuales, que recopilan datos como base para otros servicios inteligentes, mientras que el concepto Industria 4.0 engloba

a máquinas mucho más especializadas, conectadas y automatizadas para funcionar de manera autónoma, e incluso interconectarse con otras.

- De igual modo, los dispositivos IoT se dirigen más al tratamiento de personas o a un funcionamiento individual, mientras que en la Industria 4.0 se centra en la producción industrial en conjunto.

Ilustración 13.
Operario industrial. Fuente: Deloitte Insights (2022).

Aplicaciones en el sector Industrial

Según cómo se analice, podría decirse que el uso de IoT está creciendo en los entornos industriales con cierto enfoque propio dirigido a la eficiencia en la producción, dotando de nuevos niveles de sonorización (nuevas capacidades de recibir y enviar datos) e interconexión de todo tipo de dispositivos OT con entornos IT creando en el sector nuevas oportunidades de automatización.

Hasta hace unos años la industria únicamente contaba con elementos de medición que no hacían uso de conexiones ajenas a la propia máquina o al panel de control central y que por lo tanto quedaban exentos de amenazas provenientes del exterior. Sin embargo, aunque la profunda conversión a la Industria 4.0 de los elementos IoT con los OT convirtiéndolos en IIoT (*Industrial Internet of Things*) ha permitido un mejor control de la producción al ofrecer un mayor conocimiento de lo que ocurre en la factoría y una sustancial mejora de la trazabilidad al disponer de más datos, optimizándose la gestión de equipos y el reparto de tareas. Ello permite, para lograr un mantenimiento predictivo de máquinas y sistemas, dejar al descubierto una seguridad desfasada en los dispositivos en relación con los tiempos que corren.

Debemos tomar en consideración que los entornos IT están formados por el intercambio de información tanto en sistemas en la nube como en sistemas físicos. Esto quiere decir que existe una conexión directa a través de internet donde varios equipos informáticos pueden enviar y recibir información entre sí.

Por otra parte, los entornos IoT/OT se orientan hacia dispositivos con capacidad de procesamiento limitada para ofrecer datos y señales, las cuales orquesten el correcto funcionamiento de la maquinaria industrial y de los procesos asociados a este sector, como por ejemplo PLC, dispositivos SCADA o sensores, entre otros.

Llegados a este punto se ha de plantear una cuestión muy importante. Imaginemos que el intercambio de información entre dos máquinas, de las cuales una de ellas dispone de varios dispositivos IoT/OT conectados, se ve afectada por un ciberataque proveniente de la primera máquina y se propaga a la segunda a través de la infraestructura de red.

Puede que alguno o todos los dispositivos OT conectados puedan ser potenciales objetivos para los ciber atacantes al no existir una defensa software como por ejemplo los antivirus en los dispositivos IT. Hasta hace poco tiempo los entornos OT contaban con una gran ventaja ya que no necesitaban en su mayoría interconectarse con los sistemas TI a través de la red, de esta manera estaban protegidos de ataques provenientes del exterior siendo por lo tanto únicamente vulnerables mediante una conexión directa sobre ellos o localizándose en un rango de distancia muy próximo. Por este motivo es por lo que la protección de los dispositivos OT se ha convertido en un objetivo fundamental para las empresas, ya que estos dispositivos pueden convertirse en el objetivo principal de los ciber atacantes.

Retomando el concepto *IIoT* mencionado anteriormente, podemos destacar diversos tipos de sensores, como temperatura, humedad, presión, caudal, viscosidad y otros parámetros fisicoquímicos, haciendo a estos sensores una parte primordial en los procesos de fabricación. Estos sensores son fundamentales debido a que controlan que los valores de las variables en los procesos de fabricación sean correctos tanto en los productos fabricados como en la maquinaria que los fabrica, ya que de no ser así se producirían grandes pérdidas económicas.

Sin embargo, no solo existen sensores en los entornos IoT/IIoT/OT, existen también los llamados *beacons*, que son pequeños dispositivos inalámbricos muy demandados en recintos cerrados en los cuales no es posible establecer una buena conexión GPS capaces de transmitir mensajes y avisos, que informen acerca de la localización de una persona u objeto o su entorno.

Además, si se dota de un sensor a un *beacon* posibilita registrar información detallada acerca de los datos que mida el sensor con el fin de notificar posibles comportamientos anómalos en dispositivo o máquina. Por ejemplo, si se colocara uno de estos sensores en una máquina que trabaja de forma continuad, el *beacon* puede mandar una alerta en tiempo real en el momento que los valores de medición del sensor puedan verse alterados, con el fin de evitar que la máquina se estropee o sufra daños electrónicos.

Se debe tener en cuenta que todas estas tecnologías de conexión anteriormente mencionadas también pueden ser usadas para perpetrar un ataque para acceder a los sistemas de los entornos industriales.

Riesgos a los que nos enfrentamos

Gran parte de los dispositivos IIoT ofrecen la posibilidad de conectarse a otros y extraer información de datos. Sin embargo, surge la pregunta de si estos dispositivos son vulnerables a ciberataques. Se tiene conocimiento de que más de un tercio de las empresas europeas contemplan a los ataques IIoT como una de sus principales preocupaciones en materia de ciberseguridad industrial, teniendo en mente amenazas tan graves como las brechas de datos, ataques a la cadena de suministro o *ransomware* según el informe "*El estado de la ciberseguridad industrial en la era de la digitalización*", realizado por ARC Advisory Group & Kaspersky (2020)[2].

2 https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf

En el citado informe, Grigory Sizov, jefe de la Unidad de Negocios Kaspersky OS de Kaspersky indicaba lo siguiente, “a medida que en las empresas industriales siguen creciendo el número de dispositivos conectados y de sistemas inteligentes implementados, es importante que también se siga incrementado la eficiencia en la protección”. Según Sizov “se debe implantar la protección de los dispositivos desde el inicio de un proyecto, y señala algunas empresas, deberían comenzar ya. El objetivo a perseguir es que los componentes del IIoT sean seguros en su núcleo para eliminar la posibilidad de un ataque”.

Un factor determinante para poder realizar una adecuada gestión del riesgo debe ser el aumento de profesionales en materia de ciberseguridad IoT, ya que recientemente se ha podido observar que varias empresas han involucrado a su personal de TI en iniciativas de protección en sistemas IoT, no siendo este su campo profesional.

Continuaba el informe concluyendo que “hoy en día no todas las organizaciones se sienten preparadas para hacer frente a las amenazas IoT. De hecho, solo el 18% de las empresas europeas ha implantado una vigilancia activa de la red y el tráfico y únicamente el 16% ha introducido la detección de anomalías en la red. Estas soluciones permiten a los equipos de seguridad rastrear las anomalías o la actividad maliciosa en los sistemas IoT”.

Tengamos en mente que los dispositivos IoT e IIoT parten de fábrica con una escasa seguridad ya que no han sido pensados para ser protegidos sino para realizar un control de una función. Entre las mayores amenazas que pueden acabar generando encontramos:

- **Brechas de datos:** Los dispositivos de uso industrial recopilan y envían datos a otros dispositivos conectados a la red de manera que se puedan establecer un vector de ataque si un atacante se conecta a uno de estos dispositivos y por lo tanto accediendo a información.

- **Denegación de servicios (DDoS) y Ataques a la cadena de suministro:** Una cadena es tan fuerte como su escalón más débil. Con esta reflexión se debe tener en cuenta que accediendo a un dispositivo que realice por ejemplo mediciones se puede modificar la medición o alguno de los parámetros que a simple vista no sea perceptible desembocando en pérdida parcial o total en la cadena de suministros provocando cuantiosas pérdidas. También se puede provocar un freno de actividad industrial si se colapsan los sistemas informáticos.

- **Secuestro de datos mediante cifrado:** Recordemos Stunex un famoso ransomware que puso en una situación delicada a miles de empresas, cifrando sus archivos y exigiendo rescates económicos.

Ataques perpetrados y casos de uso

Uno de los ataques más famosos de este sector fue el de la Botnet Mirai el cual, aprovechando la baja seguridad de cámaras de seguridad junto con otros dispositivos similares en una enorme arma DDoS.

Este *malware* poseía una lista con más de 50 combinaciones usuarios y contraseñas comunes, con las cuales se accedía a los mismos. Muchos dispositivos *IoT* se encuentran completa o pobremente protegidos, expuestos a Internet, con contraseñas por defecto o débiles, permitiendo una infección fácil”.

Las combinaciones que el *malware* prueba fueron las siguientes[3]:

root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	root/klv123	Administrator/admin
service/service	supervisor/supervisor	guest/guest
guest/12345	guest/12345	admin1/password
administrator/1234	666666/666666	888888/888888
ubnt/ubnt	root/klv1234	root/Zte521
root/hi3518	root/jvbzd	root/anko
root/zlxx.	root/7ujMko0vizxv	root/7ujMko0admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko0admin
admin/1234	admin/pass	admin/meinsm

Ilustración 14.
Listado de las principales combinaciones de contraseñas empleadas por hackers en Mirai.
Fuente : Cyber Swachhta Kendra (2017).

Como informaba Incibe (2020)[4], a través de su sistema de alerta temprana, "una empresa enfocada al sector de la automatización industrial e IIoT fue víctima de un incidente tipo ransomware Conti. La empresa informó de un ciberataque con esta variedad contra su red TI, que supuso el cifrado y robo de información confidencial corporativa y por la que se llegó a pedir un rescate de 14 millones de dólares".

5.5 Industria

Actualmente el sector energético se encuentra en un proceso de transición ecológica donde se pretende reducir el uso de combustibles fósiles mediante energías limpias, buscando reducir lo máximo e impacto en el medio ambiente y aprovechar la máxima eficiencia de éstas. Para ello se ha de tener en cuenta que la antigüedad de los activos del sector energético juega un papel importante a la hora de asegurar un suministro energético seguro y fiable, por lo que la incorporación de dispositivos IoT puede suponer una gran ventaja ya que mediante análisis de datos recogidos se puede determinar problemas en los equipos de manera temprana evitando daños en cadena.

De esta manera podemos decir que el objetivo del IoT dentro del sector energético es ayudar al sector a evolucionar de una cadena de suministro central y jerárquica a un sistema descentralizado, autónomo y optimizado.

Sin embargo, ¿cómo afectará el IoT al sector energético?

Gracias al IoT el sector energético va a adquirir nuevas mejoras de control y organización a la hora de gestionar la red eléctrica y la seguridad de las instalaciones donde se produce, haciendo que la forma de generación y distribución de la energía alcance mejores niveles de productividad al tener un mayor control gracias al IoT.

3 https://www.csk.gov.in/alerts/mirai.html
4 https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/advantech-victima-incidente-tipo-ransomware-conti

Un claro ejemplo sería disponer de un panel de control donde se pueda controlar en todo momento la información referente a los parques eólicos y los campos solares, con lo que se conseguirá obtener una mayor automatización y eficiencia en estos.

Aplicaciones en el sector energético

El IoT actual que se está incorporando en sector energético está permitiendo los siguientes cambios en este sector:

- Mejoras en la gestión, mantenimiento y monitorización de instalaciones e infraestructuras energéticas, gracias a la realización de análisis preventivos y predictivos.
- Aumento de la fiabilidad del suministro eléctrico al tener una mejor gestión de ésta.
- Mejoras en la eficiencia de las infraestructuras gracias al mayor control y a la automatización de los procesos.
- Integración y gestión de las energías renovables.

Riesgos a los que nos enfrentamos

En los últimos años se han incrementado los ataques dirigidos a el sector energético ya que la indisponibilidad de la electricidad resulta una amenaza vital para el mundo en el que vivimos. Por este motivo es de vital importancia contar con mecanismos que garanticen la resiliencia de las empresas del sector.

Ataques perpetrados y casos de uso

Abajo podemos observar los últimos ciberataques en sistemas de control industrial del sector energético. Este tipo de ciberataques pueden llegar a desencadenar un concepto conocido como **ciberguerra** ya que nos es la primera vez que ocurren acusaciones entre diferentes gobiernos de estar detrás de dichos ataques o incluso se puede llegar a mencionar el concepto de **ciberterrorismo**, ya que por ejemplo dirigir un ataque hacia una central nuclear supone un riesgo crítico.

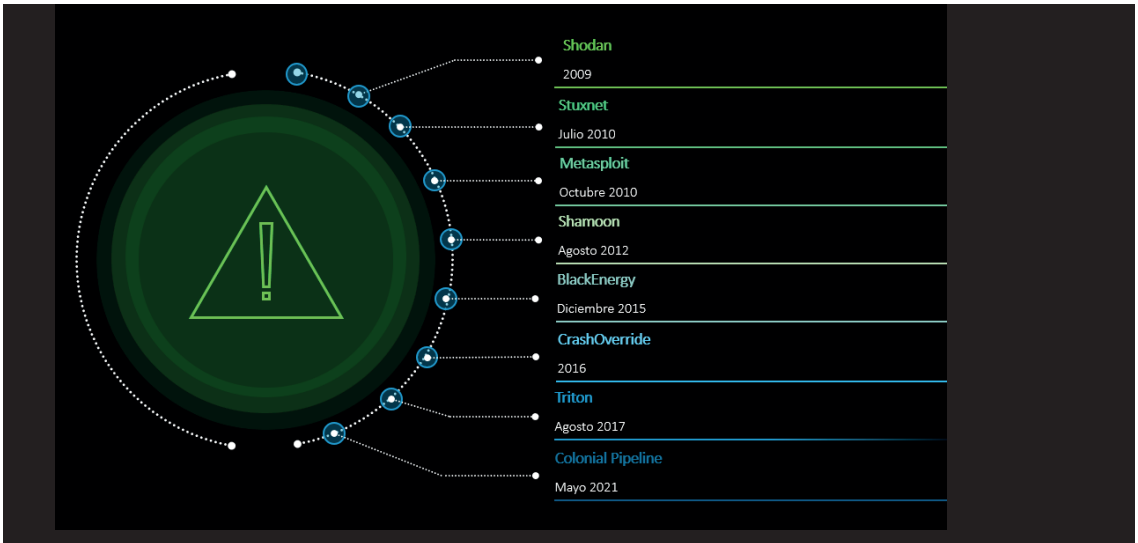


Ilustración 15. Ataques más relevantes de malware ocurridos desde 2009. Fuente: Deloitte (2021).

En enero de 2010, el gusano Stuxnet ordenó a más de 1000 máquinas autodestruirse en una central nuclear. Este ataque se repitió meses después siendo detectado en ese momento debido a que las centrifugadoras usadas para enriquecer uranio estaban fallando. Fue la primera vez que un ataque cibernético logró dañar la infraestructura crítica del mundo.

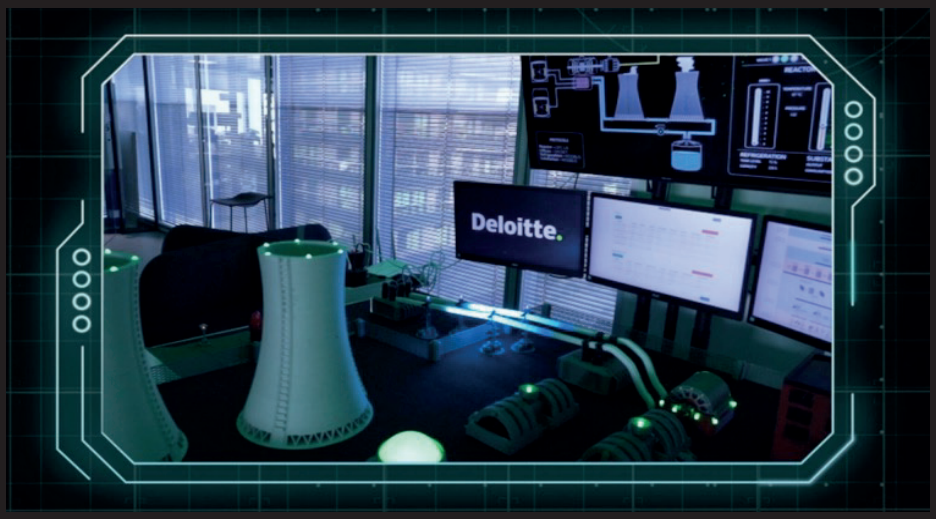


Ilustración 16. Simulación del control infraestructura crítica. Fuente: Deloitte (2021).

Stuxnet, aprovechando las brechas de seguridad del sistema logró acceder a la red central a través de la cual se propagó llegando a la red OT para finalmente tomar el control del sistema.

Como dato adicional se pudo detectar que Stuxnet lazón dos ataques un tanto diferentes. El primero provocó que las centrifugadoras giraran peligrosamente rápido, mientras que el segundo, un mes después, desaceleró las centrifugadoras, repitiéndose en varias ocasiones. El resultado de dicho ataque generó un enorme daño quedando las turbinas del 20% de las máquinas fuera de servicio.

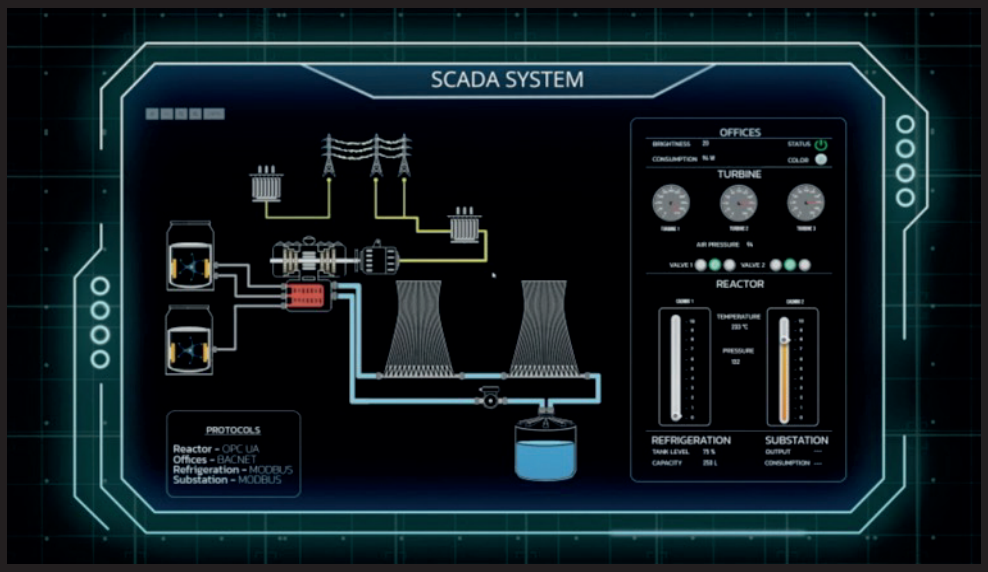


Ilustración 17. Sistemas de control SCADA Infraestructura crítica. Fuente: Deloitte (2021).

El caso del gusano Stuxnet fue un claro ejemplo de que ciertas infraestructuras críticas como es el caso de las centrales nucleares son claro objetivo de los ciberterroristas. Aunque afortunadamente el ataque no derivó en consecuencias mayores como las que hubiese tenido el malograr un sensor de temperatura o el flujo de agua en el reactor lo cual hubiese podido desembocar en un **incidente nuclear**. Por todo esto se debe velar por no solo la protección IT sino que también hay que tener el resto de dispositivos conectados a la red como es el caso de dispositivos IoT.

Otro ejemplo de ciber ataque fue en 2017, donde un grupo de ciber atacantes DragonFly 2.0 vulneró a empresas de energía de Europa y EEUU, provocando que los atacantes tomaran el control de las redes eléctricas habiendo podido comprometer la disponibilidad del suministro eléctrico en diferentes regiones.

DragonFly 2.0 accedió a las interfaces en las que los ingenieros de energía enviaban comandos a los equipos que suministran energía a zonas urbanas. Los primeros ataques se llevaron a cabo en las redes eléctricas de Ucrania en 2015 (Black Energy) y 2016 (Crash Override) causando cortes de suministro.

Los ciberatacantes accedieron mediante **phishing** robando contraseñas de equipos afectados permitiendo de esta manera el acceso remoto a maquinas críticas, obteniendo de esta manera imágenes que mostraban los paneles de control de la red eléctrica con el fin de perpetrar un sabotaje. En este caso podemos ver como los paneles de control que reciben datos de sensores pueden ser críticos a la hora de garantizar la resiliencia en el servicio.

5.6 Retail

En los últimos años el impacto del IoT en el mundo *retail* se ha ido incrementando con el objetivo de obtener una mayor eficiencia en los procesos. Aumentando el número de tecnologías introducidas en las tiendas, permitiendo automatizar ciertos procesos.

Estas tecnologías permiten a las organizaciones disponer de información actualizada en tiempo real, agilizando y optimizando los procesos de reposición y gestión logística.

Según la redacción de Bloomberg (2021)[5] "el tamaño del mercado mundial de IoT en el sector *retail* se valoró en casi 32.000 millones de dólares americanos en 2020 y se espera una tasa de crecimiento anual compuesta (CAGR por sus siglas en inglés) del 11.8% desde 2021 hasta 2028. Cabe destacar el parón de proyectos durante la pandemia COVID, sin embargo, esta situación ha sido utilizada como palanca para potenciar soluciones de pago móvil, robots de limpieza autónomos, cajas de cobro desatendidas con el objetivo de mitigar la propagación del virus. Este crecimiento puede atribuirse a la inclusión de operaciones digitales y en tiendas físicas".

5 https://www.bloomberg.com/press-releases/2021-07-12/retail-logistics-market-size-worth-498-34-billion-by-2028-cagr-11-8-grand-view-research-inc

Ilustración 18. Robot sector retail. Fuente: Deloitte Insights (2022).

Aplicaciones en el sector *retail*

Actualmente las empresas del sector *retail* utilizan los dispositivos IoT principalmente para la gestión del inventario, etiquetado de precios electrónico, gestión desatendida del cobro y para la automatización de la gestión de almacén.

En las zonas abiertas al público las organizaciones pueden a través de etiquetas RFID conocer de forma rápida y sencilla el inventario en estanterías, pudiendo reponer de forma rápida aquellos productos que tienen una mayor demanda. Junto al uso de dispositivos electrónicos de precios permite a las empresas mejorar la identificación de hábitos de consumo y optimizar las campañas de marketing.

Adicionalmente los dispositivos IoT pueden utilizarse para la automatización de la gestión del almacén, reduciendo las mermas y mejorando la visibilidad.

La aplicación de dispositivos IoT no se limita al entorno del almacén o tienda, sino que puede extender a lo largo de toda la cadena de aprovisionamiento con el objetivo de mejorar la trazabilidad de los productos desde su adquisición hasta la reposición.

El IoT ha permitido además establecer un sistema de pago automatizado utilizando dispositivos IoT. Los sistemas de caja automatizados contribuyen a una mayor satisfacción del cliente, lo que se traduce en una mayor afluencia de público. El concepto de tienda IoT está en consonancia con los servicios ofrecidos por empresas líderes en el sector *retail*, lo que facilita a los clientes la elección de artículos y el uso de sistemas de pago automáticos. Actualmente, estas empresas, ponen a disposición sensores de peso en sus tiendas para entender los artículos elegidos por los compradores y así poder realizar el cobro correspondiente sin necesidad de acudir a una caja.

Riesgos a los que nos enfrentamos

El uso de estas tecnologías supone un riesgo para las organizaciones y clientes si no se implementan las medidas mitigatorias adecuadas. De hecho, la utilización de dispositivos con firmware vulnerables o mal configurados dentro de la organización permite que atacantes accedan a segmentos internos de la organización afectando a sistemas críticos

de la misma como puede ser las bases de datos de clientes o los inventarios de stock y precios. Adicionalmente a los incidentes que puedan afectar a la organización, este tipo de dispositivos pueden ser utilizados por los atacantes para generar redes de bots que ataquen a la misma organización o a otras empresas.

Ataques perpetrados y casos de uso

El mundo IoT no solo hace referencia a las últimas tecnologías o dispositivos del mercado, según informaba Thomson (2016)[6] en 2016 pudimos ver como "en más de 25.000 cámaras de CCTV fueron utilizadas para llevar a cabo un ataque DDoS de varios días de duración contra el sitio web de una joyería en Estado Unidos. En este incidente quedó patente como los atacantes utilizaron una red de bots IoT, sino que las cámaras de CCTV instaladas en sus tiendas físicas pueden verse comprometidas y utilizarse en redes de bots de IoT para atacar otros objetivos".

Muy a menudo los dispositivos IoT no reciben el nivel de revisión de seguridad de seguridad que recibe un equipo nuevo, por lo que pueden ser objetivos más fáciles para muchos tipos de ataques

Los ataques por bots en el sector minorista se incrementaron un 13% durante el 2021.

5.7 Logística

Con el paso de los años se ha incrementado notoriamente el envío de mercancías y gestión de estas es por esto que las empresas de transporte y logística (T&L) han adoptado el Internet de las cosas en diversos entornos, desde el transporte marítimo y aéreo hasta el almacenamiento y la entrega de paquetes. Las aplicaciones más importantes incluyen el seguimiento en tiempo real de los envíos, la optimización de las ubicaciones de almacenamiento, o la optimización de rutas.

De hecho, muchos proveedores de logística (empresas que empaquetan, transportan y almacenan bienes) han visto a los usuarios (empresas con productos y mercancías que necesitan ser transportados) renovar sus propias cadenas de suministro.

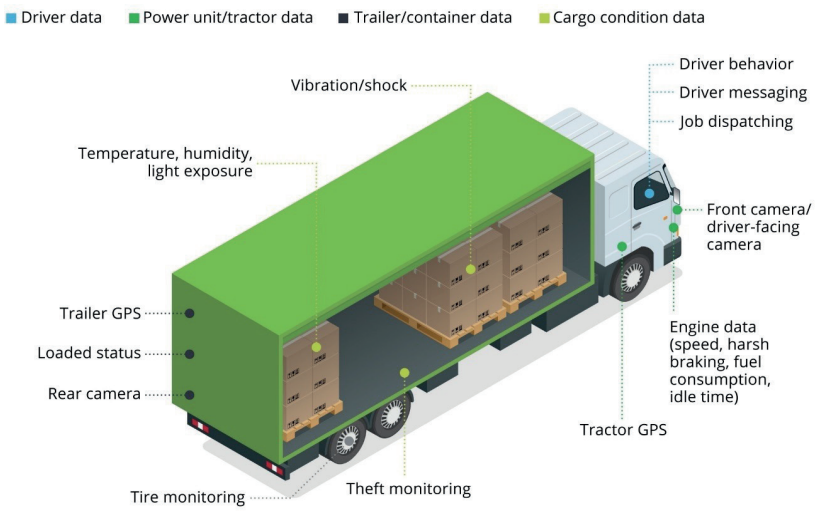


Ilustración 19. Creating IoT ecosystems in transportation. Fuente: Deloitte - R. Ernst et al. (2019).

6 http://www.theregister.co.uk/2016/06/28/25000_compromised_cctv_cameras/

Aplicaciones en el sector Logística

Las aplicaciones comunes de IoT de los proveedores de logística son:

- Detección de capacidad de almacenaje, planificación e informes.
- Optimización de rutas de envíos.
- Gestión de eficiencia energética.
- Detección y resolución eficaz ante de fallos/problemas.

Por el lado de los usuarios de logística, el valor para los clientes está determinado por el tiempo, la seguridad, la trazabilidad y el estado de su carga. Por lo tanto, los casos de uso actuales de IoT se enfocan en mejorar esos factores e incluyen la monitorización del entorno para ajustar la temperatura, la detección y prevención de amenazas (como la apertura no autorizada de contenedores) y la trazabilidad en tiempo real de cada unidad de transporte.

Entre ejemplos de aplicación de la tecnología IoT dentro de este sector encontramos las siguientes:

- Implantación de un sistema que permite guiar vehículos autónomos por instalaciones y fábricas, para el transporte de piezas mecánicas sin necesidad de intervención humana.
- Optimización de rutas de recolección de mercancías.
- Monitorización en tiempo real de las operaciones dentro de varios almacenes durante envíos.
- Implementación de un sistema de tracking de contenedores, plataformas y remolques.
- Instalación de un sistema de automatización y monitorización inteligente, dentro de un centro de grandes dimensiones que procesaba miles de envíos diarios.

Además, estas aplicaciones permiten monitorizar todo tipo de dispositivos, localizar vehículos y conductores, inspeccionar las instalaciones mediante drones o recibir alertas en caso de pérdida o robo de mercancías, todo ello en tiempo real.

Riesgos a los que nos enfrentamos

Se deben considerar los siguientes riesgos, en caso de que el dispositivo IoT se vea comprometido:

- Atascos en el almacén o retrasos en las entregas.
- Alterar o no avisar sobre el mal estado de las mercancías: si está a temperatura adecuada, si ha sufrido golpes o desperfectos, etc.
- Alterar los datos de stock en el almacén lo que puede conllevar a realizar pedidos de mercancía inexistente.

- Información incorrecta sobre dónde se encuentra el pedido y si existe algún tipo de incidencia.

- Información errónea sobre las rutas más eficaces, por ejemplo, si dejan de funcionar los sensores que pueden detectar atascos o accidentes.

En general, todos estos riesgos en caso de materializarse tendrán un impacto negativo en el cliente final, generando para la empresa vendedora pérdidas financieras debidas a una disminución de venta e incluso daño reputacional.

Ataques exitosos

En 2017 numerosas empresas se vieron afectadas por la variante del virus informático "Petya" que atacó de forma masiva a decenas de grandes empresas e instituciones europeas y que fue distribuida a través de un programa de contabilidad.

Se trata de un ransomware que actúa sobre el sistema operativo Windows cifrando el disco duro y, una vez ha infectada una máquina, puede propagarse por el resto de los sistemas conectados a esa misma red.

El impacto del ataque se concentró en los negocios vinculados con contenedores, incluyendo a la principal empresa mundial en transporte marítimo y su división estrella.

La operativa de la compañía quedó temporalmente limitada en lo que se refiere a la gestión de reservas y operaciones relacionadas con las mercancías en los buques. Dos días después del ataque, mientras la compañía luchaba por recuperar de alguna forma la normalidad, los transitarios continuaban trabajando para obtener el despacho de contenedores, pero el virus Petya no sólo perjudicó el sistema de reservas de esta compañía y ralentizó el seguimiento de contenedores, sino que también causó congestión en casi 80 puertos de todo el mundo operados por su filial.

El transportista sólo pudo reanudar las reservas casi tres días después del ataque y lo tuvo que hacer a través de un tercer proveedor".

5.8 Agricultura

Según IAT (2020)[7] se estima que "en el año 2030 la población mundial rondará los 9.000 millones de habitantes. Las necesidades productivas en el sector primario, para poder brindar alimentos a una población creciente, son cada vez mayores. Por ello, el sector de la agricultura se ha visto y se verá obligado a seguir implementando tecnologías y procesos IoT".

Aplicaciones en el sector de agricultura

La aplicación del IoT a la agricultura ha transformado la forma en la que se trabajan los campos, ayudando en la automatización de procesos, ha supuesto un cambio en la manera de trabajar los cultivos y el campo, ayudando a mejorar en la optimización de procesos consiguiendo así una reducción del gasto lo cual nos lleva a un aumento en la rentabilidad de las cosechas.

7 https://iat.es/tecnologias/internet-de-las-cosas-iot/agricultura/

Un claro ejemplo de ello es el suministro de agua para cultivos. En los últimos años, el suministro de agua en los campos se ha realizado a través de tecnología IoT capaz de encender y apagar selectivamente boquillas específicas del sistema de riego en base a la información recogida por sensores los cuales son capaces de medir parámetros como la temperatura, las condiciones del suelo y la humedad. Con la tecnología IoT los agricultores son capaces administrar la cantidad justa de agua a cada zona individual pudiendo llegar a ahorrar grandes cantidades de agua.

Como éste hay muchos ejemplos de soluciones que ofrece el IoT para la agricultura:

- **Tractores y cosechadoras inteligentes,** capaces de operar sin conductor.

- **Tecnología de dosis variable de fertilizantes,** que al igual que la tecnología de irrigación de agua, permite aplicar con la máxima precisión la dosis necesaria de fertilizante, según los datos recogidos por sensores y otros aplicativos.

- **Invernaderos inteligentes** que permiten conservar los cultivos en condiciones óptimas de forma autónoma evitando tener que ser supervisados por personas.

- **Uso de drones para control de enfermedades y plagas,** gracias a su visión panorámica y, junto con la inteligencia artificial (IA) podemos determinar, de forma masiva, el estado de salud de las producciones identificando así aquellos que deban ser tratados para mejorar ésta.

A grandes rasgos, el ***Smart Farming*** o agricultura inteligente es capaz de mejorar la producción de alimentos asegurando su oferta a una población cada vez más numerosa a la vez que es capaz de optimizar el uso de recursos y bienes escasos, como el agua, necesarios para la agricultura y la vida.

Gracias a la agricultura inteligente, países con climatologías extremas como Uganda, económicamente dependientes de la exportación de frutas y hortalizas como Chile o cuya base alimentaria se sostiene sobre alimentos de cultivo como Malasia, son capaces de maximizar su producción haciendo frente a adversidades climáticas y a la escasez de recursos.

Riesgos a los que nos enfrentamos

Actualmente, si un sensor con conexión a internet y a las bocas de riego es hackeado, parámetros como la humedad o nivel de sodio en la tierra pueden ser modificados, haciendo que el sensor envíe la orden de irrigar agua a las bocas de riesgo en base a parámetros erróneos lo que llevaría a que cosechas enteras se perdieran y a que recursos como fertilizantes o agua se malgastaran.

De la misma forma, cualquier tecnología con conexión a internet, sea un invernadero inteligente o un tractor autónomo, es susceptible de verse hackeada y sufrir modificaciones en sus parámetros, poniendo en peligro la disponibilidad de la tecnología y en última instancia la producción de alimentos.

La adopción de la tecnología IoT genera nuevos vectores de ataque cibernéticos en tec-

nología que antiguamente se encontraba segregada y desconectada de Internet. La disponibilidad de la maquinaría operativa dentro del sector agrícola es fundamental para cubrir la alta demanda alimentaría. Si esta tecnología fallara, la escasez y carestía de alimentos serían un hecho a los niveles de producción actuales.

Otro problema al que se enfrenta la tecnología IoT en el ámbito de la agricultura, es la de proporcionar una conexión fiable, capaz de aguantar eventos climáticos como vendavales, diluvios e inundaciones. Al tratarse de un sector en el que se trabaja en amplias extensiones de tierra que cubren varios kilómetros de distancia, se precisa de dispositivos IoT que se comuniquen no solo a través de WIFI, sino también a través de radio frecuencia. Estos dispositivos cuentan con la ventaja de tener un bajo consumo y de no necesitar un mantenimiento muy frecuente. Sin embargo, los mismos presentan un posible vector de ataque, ya que los protocolos de comunicación por radiofrecuencia tienden a ser fácilmente manipulables y filtrables.

Ataques perpetrados y casos de uso

Entre los ataques a empresas agrícolas, su mayoría están relacionado con ataques destinados a modificar la configuración de PLCs y otros dispositivos de control. Con ello, los atacantes buscan interrumpir o incluso detener el funcionamiento de los dispositivos de campo. Dichos ataques, según indica Incident Hub (2022)[8] han llegado a tener impactos de más de $1.000.000.

Otros ataques también habituales, se centran en la introducción de virus como el ransomware en dispositivos de la red de supervisión como servidores HMI, servidores historian, consolas de operador, estaciones de ingeniería, etc. De esta forma, los atacantes buscan corromper la información almacenada y presentada por estos dispositivos, dificultando la supervisión de la red de control y de campo.

En definitiva, las redes y dispositivos objetivo son aquellas que se encuentran hacia la base de la pirámide de la automatización. Esto se debe a que representan el eslabón más vulnerable de la cadena.

5.9 Smartcities / Smart Buildings

Como ya comentamos al inicio del presente documento el sector de las ciudades y de los edificios inteligentes está llamado a ser donde la tecnología IoT tenga un mayor grado de penetración. Esto es en parte debido al alcance de dicho sector y a la gran cantidad de dispositivos e integraciones existentes.

Las funcionalidades que, dentro de este ámbito, el IoT nos ofrece son múltiples, tantas casi como podamos imaginar. Esto se debe a la trasversalidad del mismo, lo cual posibilita que las posibilidades de aplicación se multipliquen.

Ponemos como ejemplo para su desarrollo el exitoso caso del Smart Stadium de Deloitte el cual recoge las principales:

8 https://hub.tisafe.com/

Ilustración 21. Monitorización Smart Stadium. Fuente: Deloitte (2021).

Aplicaciones en el sector de Smartcities

Aparcamientos inteligentes. Funcionalidades como el control de plazas disponibles mediante indicadores visuales, identificación de matrículas o gestión de la recarga eléctrica de vehículos están cada vez más presentes en, por ejemplo, superficies comerciales.

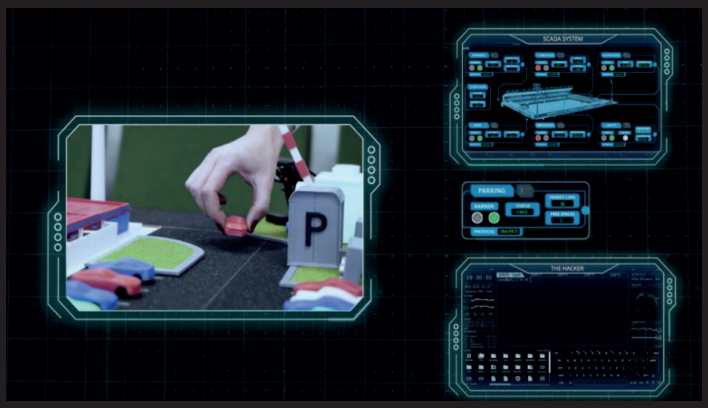


Ilustración 22. Ejemplo de monitorización de aparcamientos inteligentes. Fuente: Deloitte (2021).

Control de accesos. Mediante el control de puertas, tornos, barreras o gestionando tanto credenciales como sistemas biométricos que garantizan que cada persona acceda correctamente donde deba.

Gestión energética. Controlando la iluminación o la climatización de salas conseguimos, además de un mayor ahorro energético, una mayor sensación de confort ambiental.

Gestión de servicios al ciudadano. El tratamiento de aguas o residuos que permitan realizar una gestión eficiente de estos recursos a través del control de calidad del agua, fugas en instalaciones o revisión capacidad de los contenedores de basura para optimizar las rutas de los camiones de recogida de basura.

Mantenimiento. Aplicando sistemas de mantenimiento predictivo o controles de riego en, por ejemplo, parques o cultivos, conseguimos una gestión óptima de los recursos monitorizados.

Seguridad. Sistemas cerrados de televisión (CCTV), alarmas, sistemas de megafonía o alarma antiincendios son algunos de los usos más comunes y con mayor grado de despliegue en nuestro día a día.

Sensorización de ocupación y uso. Durante esta pandemia se ha podido comprobar la necesidad de contar con este tipo de sistemas para controlar los aforos de salas y tiendas entre otros.

Los casos recogidos, como se puede apreciar, los podemos encontrar en cualquier infraestructura que podamos imaginar, en casa, a la hora de ir a comprar, al asistir a un espectáculo.

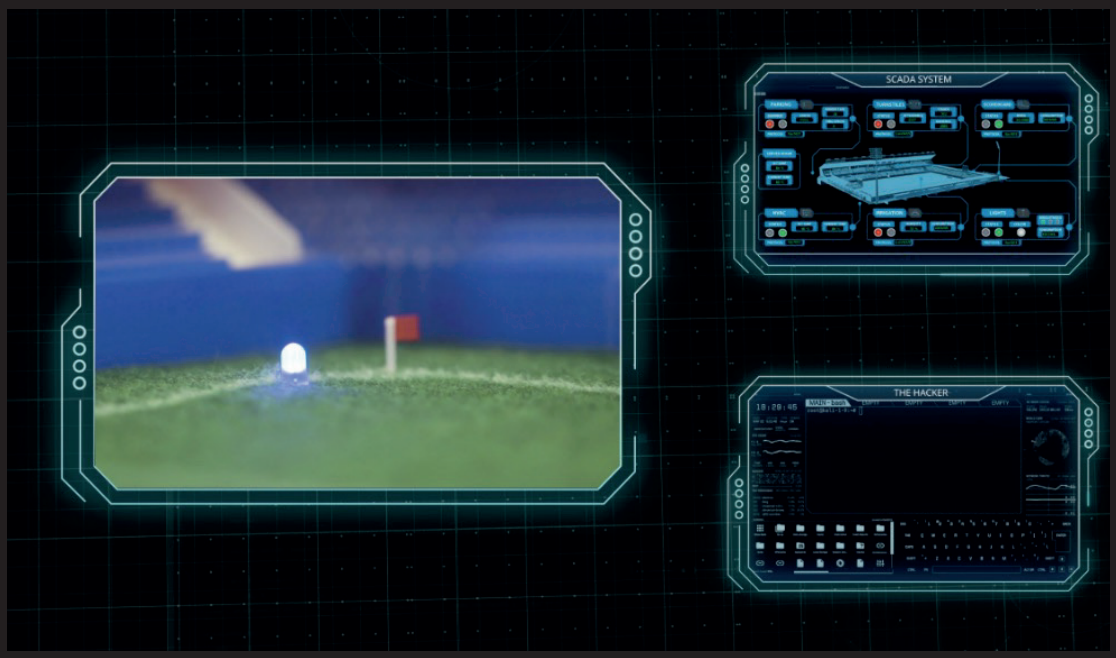


Ilustración 23.Ejemplo de monitorización de sistemas de riego. Fuente: Deloitte (2021).

Servicios inalámbricos. Mediante el uso intensivo de la conectividad podemos conseguir proporcionar información útil al usuario a través de kioscos y paneles informativos o geoposicionamiento entre otras funcionalidades.

Ilustración 24. Ejemplo de monitorización de videomarcadores. Fuente: Deloitte (2021).

Riesgos a los que nos enfrentamos

Las múltiples utilidades que acabamos de ver se convierten, a su vez, en posibles vectores de entrada tanto a los nuevos sistemas (IoT) como a los convencionales (IT/OT) mediante el empleo de técnicas como las de movimiento lateral.

Esta técnica consiste en la explotación de un vector de entrada como puede ser la gestión remota de un aire acondicionado (HVAC) podría llegar a generar una interrupción de un Centro de Procesado de Datos (CPD). Esta infraestructura cuenta con mecanismos de seguridad que, por precaución y en caso de llegar a ciertas temperaturas, procedería a su apagado.

Tomando el control del dispositivo podríamos modificar los parámetros del mismo para elevar la temperatura y conseguir ocasionar una denegación del servicio en el CPD.

Ataques perpetrados y casos de uso.

Al igual que hemos visto a lo largo del documento, múltiples son los ataques que han tenido éxito en los diversos sectores. En éste, no iba a ser menos y entre los más famosos se encuentran el ocurrido en 2018 en un casino de Londres en el que un hacker logró hacerse con sus bases de datos accediendo a través de una pecera decorativa que tenían en sus instalaciones.

Esto fue posible debido a que el sistema de monitorización de la pecera empleado para medir y enviar datos remotamente acerca de la temperatura, estado de los peces, etc., dados los escasos mecanismos de seguridad implantados consiguieron acceder a la red a través de este vector. Una vez dentro, consiguieron su botín y lo extrajeron por el mismo sitio que entraron, subiendo los datos a la nube por el termostato inteligente de la pecera.

En 2013, uno de los edificios inteligentes fue hackeado a través de su sistema inteligente de control del inmueble. Este sistema se encontraba expuesto a internet y era accesible desde buscadores como Shodan. Cabe decir que no encontraron ningún tipo de oposición ya que el sistema no contaba con ningún mecanismo de seguridad que denegara el acceso a los atacantes. A raíz de este caso se detectaron miles de edificios inteligentes en las mismas condiciones que el caso que acabamos de citar.

5.10 Smart Home

Los *Smart Home* o Domótica se puede definir como la integración de tecnología IoT o inteligente en el diseño de una vivienda o un recinto cerrado. La tecnología Smart Home se conecta entre sí y puede ser controlada desde un ordenador, tablet o smartphone que actúe como dispositivo central.

Aparatos como cerraduras inteligentes, luces, televisiones, frigoríficos, termostatos etc. pueden ser controlados y operados en remoto desde un concentrador.

Aplicaciones en el sector de Smart Home

Muchas son las aplicaciones que este sector pueden tener, entre ellas destacamos las siguientes:

Automatización de la vivienda y mejora del confort: La aplicación más evidente de la tecnología Smart Home es la automatización de la vivienda y el mayor confort asociado. La tecnología Smart Home concede a los propietarios de la vivienda el control a distancia y desde sus dispositivos móviles de los aplicativos y dispositivos IoT en su interior. La capacidad de abrir o cerrar las persianas o de encender o apagar la televisión o las luces desde la Tablet o Smartphone, supone una asistencia digital que mejora la comodidad de los propietarios que pueden gestionar su casa a golpe de clic.

Seguridad mejorada: Otra de las aplicaciones más evidentes de los sistemas Smart Home es el reforzamiento de la seguridad de la vivienda. Esta tecnología permite, entre otras funciones, la captación de imágenes en tiempo real de la propiedad, videollamadas con imagen y audio con personas que se encuentren en la puerta o en el perímetro de la vivienda, cerrar ventanas y puertas desde el dispositivo móvil y recibir alertas y notificaciones de dispositivos de seguridad como sensores de detección de intrusión, sensores de monóxido de carbono o alarmas.

Ahorro energético: Una de las aplicaciones más útiles de la tecnología Smart Home es una gestión energética más eficiente. Con esta tecnología, las luces por ejemplo se pueden configurar para encenderse y apagarse según las horas de salida o puesta del sol o en base a la posición y movimiento de las personas en el interior de la vivienda, apagando automáticamente las luces de aquellas zonas en las que no hay nadie y encendiendo aquellas en las que sí que hay gente. Estas funcionalidades se pueden extrapolar a aparatos de climatización como calderas y aires acondicionados.

Riesgos a los que nos enfrentamos

Al igual que en el sector de las *Smartcities* y *Smartbuildings*, el IoT además de abrir un mundo de posibles aplicaciones, abre un mundo de posibles vectores de ataque. El movimiento lateral, la toma de control, el acceso a la red, la exfiltración de credenciales o información personal, la manipulación del tráfico de red enviado desde o para un dispositivo o la ejecución de *malware* son ejemplos de posibles tácticas que un hacker puede desarrollar dentro en un entorno Smart Home.

Si un hacker consigue acceder al sistema a través de un vector de entrada la interoperabilidad de la tecnología IoT le permitiría tener acceso a todos los sistemas. Podría incluso llegar a convertir su ordenador en el dispositivo central a cargo de operar y controlar todos los sistemas Smart Home del hogar y por ejemplo inhibir los sistemas de seguridad de la vivienda.

Ataques perpetrados y casos de uso

El crecimiento exponencial en la adopción de estos dispositivos ha traído consigo el aumento en los ataques sufridos por los mismos. Entre ellos ponemos como ejemplo el caso de un grupo de hackers que aprovechó la explotación de una vulnerabilidad existen-

te en una bombilla inteligente para acceder a la red de un usuario el cual consiguió robar credenciales e información confidencial del usuario atacado. Las conclusiones revelaron que el diseño de la bombilla era inseguro y que la arquitectura de la red de dispositivos contaba con varías vulnerabilidades que permitían el acceso en remoto al producto y la descarga de un archivo con los datos personales de los usuarios necesarios para acceder a sus cuentas y, como resultado, tomar el control de los sistemas domésticos.

Durante las pruebas, los analistas descubrieron que al conectarse a esta bombilla inteligente desde un servidor eran capaces de descargarse un archivo con información sobre las credenciales necesarias para iniciar sesión en la interfaz web que el fabricante ponía a disposición de los usuarios para que pudieran controlar dicho aparato. La información descargada contenía los nombres, contraseñas y números de teléfono de todos los usuarios que se habían conectado anteriormente a la bombilla. Toda esta información se encontraba almacenada sin cifrar dentro de la memoria de la bombilla y conseguirla era tan sencillo como enviar una solicitud legítima al servidor que incluyera el número de serie del dispositivo.

6. Abordando el desafío de la seguridad y la privacidad

Como se ha señalado a lo largo del capítulo anterior, la interconectividad que ofrece el IoT no se encuentra exenta de riesgos.

Esta conexión aumenta el nivel de exposición a amenazas de esta tecnología y supone la aparición de nuevos vectores de ataque. Agentes externos, podrían explotar estos y tomar el control del proceso industrial o de producción en su conjunto, si estos no se encuentran debidamente protegidos.

Las consecuencias de un ataque sobre la tecnología IoT y en especial IIoT son mucho más devastadoras que las que podrían producirse en entornos IT, puesto que ya no solo hablamos del acceso a información, sino al acceso a procesos industriales y tecnologías capaces de interactuar con el medio físico (bombas de insulina, marcapasos, vehículos autónomos, etc.) que de ser modificados podrían, en el peor de los casos, llegar a generar daños físicos a las personas.

Para contrarrestar esta situación y evitar que estos dispositivos sean la puerta de entrada a la organización presentamos una serie de medidas de seguridad para los sistemas IoT:

- **Responsables y segregación de funciones específicos de IoT.** Contar con roles y responsabilidades claramente definidos y diferenciados de la parte de IT se antoja como algo indispensable para realizar un gobierno efectivo en la seguridad de este entorno.

- **Inventario de activos**. Se debe disponer de un inventario completo de equipos que se mantenga actualizado. Los equipos deben de ser clasificados según su criticidad para la prestación del servicio y deben disponer de una guía de bastionado actualizada en la que se recojan las configuraciones generales y buenas prácticas facilitadas por el fabricante.

- **Control de accesos y trazabilidad**. Se debe disponer de medidas de control de accesos lógico con el fin de garantizar que el acceso a un determinado recurso. Medidas como mínimo privilegio, autorización específica y excepcional para la concesión de privilegios y accesos, revisión y revocación de cuentas y segregación de funciones para evitar que la misma persona desempeñe los roles de autorización, uso y control del uso de estos dispositivos, son algunos ejemplos que se deben implementar para un control de accesos adecuado. En estos dispositivos, en los que los usuarios root / admin cuentan con grandes privilegios, se debe hacer un férreo marcaje y, segregar,en la medida de lo posible los permisos que los usuarios deban tener.

- **Segmentación de las redes.** La segmentación entre las redes de control y las redes corporativas garantiza una comunicación controlada y segura entre ambas evitando la propagación de ataques cibernéticos que hayan podido penetrar en alguna de las redes. Desde el punto de vista de la seguridad, la segmentación de la red supone acotar la red en diferentes segmentos con requisitos distintos de seguridad. La segu-

ridad se consigue restringiendo los flujos de información y usuarios entre esas zonas estableciendo controles de entrada y salida. Igualmente, se debe disponer de una arquitectura de red bien integrada y definida que recoja: la ubicación de los equipos de control y dispositivos de campo, los puntos de acceso al sistema, los puntos de interconexión a otros segmentos de la red, etc. esto garantizará que la red esté mejor asegurada, mantenida y monitorizada.

- **Monitorización de los sistemas y detección y registro de incidentes.** Se debe dispo-ner de un sistema de detección y registro de incidentes en tiempo real, acompañado de un procedimiento de gestión de estos.

- **Actualizaciones de seguridad.** Para tratar de garantizar la seguridad de los dispositivos se debe configurar los mismos de manera que no cuenten con claves por defecto y se mantengan actualizados tanto el firmware como el software con el fin de evitar la explotación de posibles vulnerabilidades asociadas a ellos.

- **Cifrado de las comunicaciones**. Como hemos comentado en varios capítulos nos encontramos ante dispositivos que disponen de una conexión a la red por la cual pueden enviar y recibir información. Esta información debe viajar cifrada con el fin de garantizar la confidencialidad de la misma, por lo que es necesario que estos dispositivos puedan trabajar con protocolos de comunicación seguros.

- **Gestión de vulnerabilidades.** Se debe llevar a cabo un plan de gestión de vulnerabilidades que contemple establecer escaneos periódicos de los dispositivos IoT a través de herramientas automáticas de escaneo de vulnerabilidades.

- **Controles sobre dispositivos extraíbles.** Los medios extraíbles representan una de las vías más habituales de infección por malware. Por ello, se debe prohibir el uso de dispositivos extraíbles por defecto dentro de entornos IoT o controlar su utilización cuando lo anterior no sea posible.

- **Controles sobre los equipos y dispositivos móviles que tenga acceso a tecnología IoT.** Se debe limitar el número de equipos con acceso a entornos IoT, además de con-tar con un inventario de todos los equipos junto con una identificación del usuario responsable.

- **Despliegue de gateways controladas por el propietario del activo.** En la medida de lo posible, evitar la conexión de estos dispositivos a servidores externos (del fabricante en la mayoría de los casos) sustituyendo estos por plataformas locales que permitan la integración y posterior explotación de los datos. Ello ayudará a minimizar el riesgo existente al intercambiar datos de forma remota con sistemas que, en algunos casos, tienen dudosa reputación.

7. Conclusiones

Como se ha podido apreciar, la presencia de los dispositivos IoT está cada vez más presente en nuestra sociedad ya sea bien en el ámbito personal o bien en los distintos sectores que nos prestan servicio.

Esta tecnología pese a su simplicidad en cuanto a la forma en la que presenta sus funciones cuenta con una gran arquitectura tanto a nivel de componentes como a nivel de la infraestructura que soporta las conexiones que potencian las características de los dispositivos IoT. Este hecho, a medida que vaya aumentando el despliegue de la red 5G, será cada vez más patente.

La previsión del incremento del número de dispositivos como demuestran diversas fuentes, sumada a la laxitud en las medidas con las que cuentan estos dispositivos - priorizando en muchas ocasiones la funcionalidad a la seguridad – hacen que las probabilidades de sufrir brechas de seguridad aumenten exponencialmente y se extiendan al resto de sistemas (IT y OT). Si alguno de los dispositivos es vulnerable a ataques la fortaleza de la red puede verse comprometida seriamente pudiendo hacer accesibles a el resto de los dispositivos, presentando un punto de especial interés en los ciberatacantes.

Organismos y organizaciones deben trabajar de la mano con el fin de definir estrategias en materia de ciberseguridad que garanticen el uso de esta tecnología en todos los entornos que nos rodean.

Contar con normativas de seguridad que regulen aspectos como la definición de roles y responsabilidades dentro de las organizaciones, la interconexión de estos o las medidas básicas con los que estos dispositivos deben contar se erigen como una piedra angular sobre la que construir un mundo ciberseguro en torno al Internet de las Cosas.

Debemos recordar que, como se comenta en el sector de la ciberseguridad, “somos tan fuertes como nuestro eslabón más débil”. Por este motivo no se debe bajar la guardia y menos con una tecnología tan disruptiva y con tantas posibilidades y riesgos como es el IoT.

8. Referencias bibliográficas

ARC Advisory Group & Kaspersky. (2020). Obtenido de https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf

Bloomberg. (Julio de 2021). Obtenido de https://www.bloomberg.com/press-releases/2021-07-12/retail-logistics-market-size-worth-498-34-billion-by-2028-cagr-11-8-grand-view-research-inc

Deloitte Insights (2020 - 2022). Varias fuentes.

ENISA. (Noviembre de 2019). *ENISA good practices for security of Smart Cars.* Obtenido de https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

Ernst, R. (Octubre de 2019). *Creating IoT ecosystems in transportation.* Obtenido de https://www2.deloitte.com/global/en/insights/focus/internet-of-things/transportation-iot-internet-of-things-ecosystem.html

Gregersen, G. (Diciembre de 2018). Obtenido de hhttps://www.nabto.com/guide-iot-protocols-standards/

IAT. (Junio de 2020). Obtenido de https://iat.es/tecnologias/internet-de-las-cosas-iot/agricultura/

Incibe. (Noviembre de 2020). Obtenido de Incibe: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/advantech-victima-incidente-tipo-ransomware-conti

Incident Hub. (Julio de 2022). Obtenido de https://hub.tisafe.com/

Livingston, L. - Deloitte. (Septiembre de 2018). *Deloitte Insights.* Obtenido de https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf

Statista. (2022). *Internet of Things (IoT) in Europe.* Statista.

Anexos

Normativa y estándares de referencia

TÍTULO			
Norma ISO/IEC 30141 sobre Internet de las Cosas (IoT) – Arquitectura de Referencia, publicada en noviembre de 2018			
ORGANISMO EMISOR O RESPONSABLE	Comité Técnico ISO/IEC, subcomité SC 41	ÁMBITO DE APLICACIÓN	Internacional
RESUMEN DEL CONTENIDO			
Este documento proporciona una arquitectura de referencia de IoT estandarizada que utiliza un vocabulario común, diseños reutilizables y las mejores prácticas de la industria. Utiliza un enfoque de arriba hacia abajo, comenzando con la recopilación de las características más importantes de IoT, abstrayéndolas en un modelo conceptual genérico de IoT, derivando una referencia basada en el sistema de alto nivel con la posterior disección de ese modelo en cinco vistas de arquitectura desde diferentes perspectivas.			
ENLACES AL CONTENIDO			
https://www.iso.org/standard/65695.html			

TÍTULO			
Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación			
ORGANISMO EMISOR O RESPONSABLE	Gobierno de España	ÁMBITO DE APLICACIÓN	Nacional
RESUMEN DEL CONTENIDO			
La complejidad técnica y el nuevo paradigma de la tecnología 5G hacen que los retos de seguridad que plantea no puedan abordarse en su totalidad con las normas sobre seguridad e integridad de las redes de comunicaciones electrónicas existentes. Por otro lado, el importante cometido de los suministradores en la arquitectura y en la gestión de la red, así como su apertura a múltiples usos y aplicaciones que aumentan los posibles puntos de ataque, aconsejan tomar precauciones para evitar incidentes que sean atribuibles a dichos suministradores. Por este motivo, el Real Decreto-Ley 7/2022 somete a los suministradores 5G a estrictos controles de seguridad para garantizar su fiabilidad técnica y su independencia de injerencias externas.			
ENLACES AL CONTENIDO			
https://www.boe.es/eli/es/rdl/2022/03/29/7/con			

TÍTULO			
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos			
ORGANISMO EMISOR O RESPONSABLE	Parlamento Europeo y Consejo de la Unión Europea	ÁMBITO DE APLICACIÓN	Europeo
RESUMEN DEL CONTENIDO			
Normativa europea que define las directrices a seguir relativas para garantizar la de protección de datos de las personas físicas. Establece un marco de referencia con el que armonizar las prácticas realizadas por los distintos Estados Miembro en materia de protección de datos.			
ENLACES AL CONTENIDO			
https://eur-lex.europa.eu/eli/reg/2016/679/oj			

TÍTULO			
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales			
ORGANISMO EMISOR O RESPONSABLE	Agencia Española de Protección de Datos	ÁMBITO DE APLICACIÓN	Nacional
RESUMEN DEL CONTENIDO			
Normativa española aprobada en 2018 que deroga la LOPD 15/1999 que define, al igual que el RGPD, las directrices a seguir para garantizar la de protección de datos de las personas físicas. Tanto la normativa en sí como las diferentes guías publicadas por la Agencia Española de Protección de Datos establecen las directrices necesarias para el correcto tratamiento de los datos tanto en formato físico como en digital.			
ENLACES AL CONTENIDO			
https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf			

TÍTULO			
Industrial Automation and Control Systems Security Standards (ISA/IEC 62443)			
ORGANISMO EMISOR O RESPONSABLE	International Society of Automation & International Electrotechnical Comission	ÁMBITO DE APLICACIÓN	Internacional
RESUMEN DEL CONTENIDO			
Familia de estándares que define los requisitos y procesos para la implementación y mantenimiento de la seguridad en sistemas automatizados de control industrial. Estos estándares establecen las mejores prácticas para la seguridad y proporcionan una forma de evaluar el nivel de rendimiento de seguridad.			
ENLACES AL CONTENIDO			
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards			

TÍTULO			
Ley 8/2011, de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas.			
ORGANISMO EMISOR O RESPONSABLE	Secretaría de Estado de Seguridad	ÁMBITO DE APLICACIÓN	Nacional
RESUMEN DEL CONTENIDO			
Normativa española que tiene por objetivo establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, así como las obligaciones que deben asumir las Administraciones Públicas y operadores de aquellas infraestructuras que se determinen como infraestructuras críticas.			
ENLACES AL CONTENIDO			
https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf			

Deloitte.

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS