andalucíasmart
PLAN DE IMPULSO AL DESARROLLO INTELIGENTE DEL TERRITORIO

Vectores de Ataque

Smart Cities

26/12/2016

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

Índice

1. INTRODUCCIÓN

El concepto actual de ciudades y municipios se encuentra en continuo proceso de transformación hacia las Smart Cities, con la finalidad de conseguir un entorno en el cual se cumplan los criterios de eficiencia, sostenibilidad, gestión de recursos (infraestructuras, tecnologías, comunicaciones, plataformas, etc.) que requiere la ciudadanía, así como salvaguardar los datos generados, almacenados y transmitidos por los diferentes servicios, sistemas y actores que componen las Smart Cities.

El concepto de Smart City se basa en una ciudad en la que existe una gestión eficiente, realizada de forma inteligente sobre los servicios que se ofrecen, principalmente al ciudadano -dentro de los actores que integran el ecosistema-, los cuales están soportados por las tecnologías de la información y las comunicaciones.

Es en la vertiente de seguridad y su constante evolución, donde reside la mayor preocupación de la industria tecnológica. Principalmente, debido a la transformación de los procedimientos, herramientas y métodos utilizados, tanto por los atacantes cibernéticos, como por aquellos involucrados en la defensa de los activos de información.

Por todo ello, es importante conocer la evolución seguida desde que se empezaron a realizar los primeros ataques -aprovechando las vulnerabilidades de los dispositivos tecnológicos y los sistemas de información-, hasta la formación de los complejos y sofisticados vectores de ataque utilizados hoy en día. De esta forma, es posible observar las tendencias que se van a producir en un periodo de tiempo determinado, permitiendo analizar posibles salvaguardas con la finalidad de proteger el principal motor de las Smart Cities (las infraestructuras TIC), y así conseguir los objetivos marcados para la configuración del ecosistema.

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

2. ANÁLISIS DE LOS VECTORES DE ATAQUE

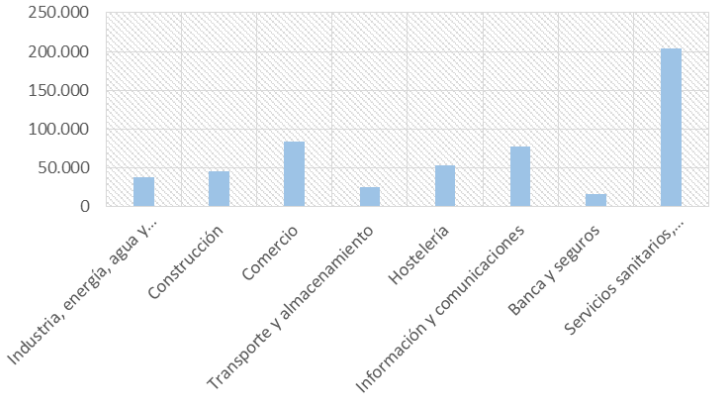
Con el objetivo de conocer la evolución seguida por los ciberataques, así como para poder realizar una primera aproximación al impacto que pudiera ocasionar la materialización de cualquier amenaza en el ecosistema SmartCity, se han llevado a cabo varios análisis:

- Principales sectores empresariales en Andalucía, para estimar el número potencial de empresas que podrían verse involucradas en un ataque a un sector específico
- Vulnerabilidades más importantes asociadas a Internet Of Things (IoT), ya que constituyen la base fundamental sobre la que se asienta una Smart City
- Vectores de ataque utilizados, con objeto de analizar la evolución de los métodos y procedimientos utilizados en los ciberataques

Principales sectores empresariales en Andalucía

A continuación se muestran algunas estadísticas del *Instituto de Estadísticas y Cartografía de Andalucía*, con el objetivo de conocer los sectores con mayor tasa de crecimiento en Andalucía en 2015. Ello, en conjunción con el análisis de los servicios que prestan y de la infraestructura TIC que utilizan, servirá para intentar anticipar cuáles podrían ser los principales vectores de ciberataque en Andalucía.

	Provincias								
SECTOR ACTIVIDAD	Almería	Cádiz	Córdoba	Granada	Huelva	Jaén	Málaga	Sevilla	**Total General**
Industria, energía, agua y gestión de residuos	2.998	3.984	5.784	4.670	1.952	4.035	5.663	8.763	37.849
Construcción	4.702	5.065	4.461	5.685	2.307	3.089	11.680	9.419	46.408
Comercio	14.246	22.329	17.908	18.694	9.645	12.961	35.287	38.788	84.257
Transporte y almacenamiento	2.611	3.205	2.288	2.865	1.151	1.818	5.107	5.812	24.857
Hostelería	4.438	7.804	4.543	6.164	3.164	3.289	13.208	10.607	53.217
Información y comunicaciones	495	714	587	889	286	322	2.094	2.258	78.074
Banca y seguros	1.412	1.956	1.606	1.786	938	1.378	3.330	3.851	16.257
Servicios sanitarios, educativos y resto de servicios	15.649	25.174	17.511	23.014	10.007	12.699	50.497	48.891	203.442
Total General	46.551	70.231	54.688	63.767	29.450	39.591	126.866	128.389	559.533



Fuente: Instituto de Estadísticas y Cartografía de Andalucía

Analizando los datos recopilados durante el año 2015, se ha observado que la presencia de actividad empresarial en **Andalucía** es mayor en los sectores *"Servicios sanitarios, educativos y resto de servicios"*, *"Comercio"* e *"Información y comunicaciones"*. Teniendo en cuenta que dichos sectores centran su actividad empresarial en torno a dispositivos tecnológicos y sistemas de información, el impacto que podría ocasionar la materialización de un ciberataque, podría llegar a detener el funcionamiento de algunas organizaciones que prestan un servicio fundamental a la ciudadanía, siendo el ejemplo más claro un ciberataque basado en la denegación de servicios de los sistemas de información de un hospital, utilizando dispositivos tecnológicos que conforman el entorno **IoT**.

Internet of Things (IoT)

La sociedad, desde hace unos años, se encuentra sumergida en un proceso de transformación drástica, donde los métodos utilizados para la generación de información se han ido modificando debido a la implantación de los Sistemas de Información en la sociedad. Como consecuencia de este proceso, el papel que el ser humano tenía anteriormente, pierde importancia en la generación de información, incrementándose de forma exponencial por parte de los dispositivos tecnológicos.

Esto se debe a que los dispositivos inteligentes -móviles, tabletas, frigoríficos, video vigilancia, etc.- utilizados hoy en día (para uso personal, empresarial o industrial), independientemente su autonomía o interacción con el usuario, están dotados de múltiples sensores y de capacidades que hacen posible que el propio dispositivo pueda recopilar, analizar, generar y transferir grandes cantidades de información.

Como ejemplo, desde 2014 se han reportado varios ataques contra contadores inteligentes. Los ciberataques pueden ser dirigidos contra el contador, contra los concentradores (utilizados para recopilar datos, enviarlos a los servidores y transmitir órdenes a los contadores), o bien manipular físicamente los mismos.

El impacto de la implantación de los sistemas de información y de los dispositivos tecnológicos en la sociedad, ha generado cambios drásticos en los estilos de vida de sus usuarios, generando nuevas incertidumbres y objetivos en materia de seguridad.

Los ámbitos competenciales según el Plan de Acción AndalucíaSmart 2020 (http://bit.ly/AndaluciaSmart), son los siguientes:

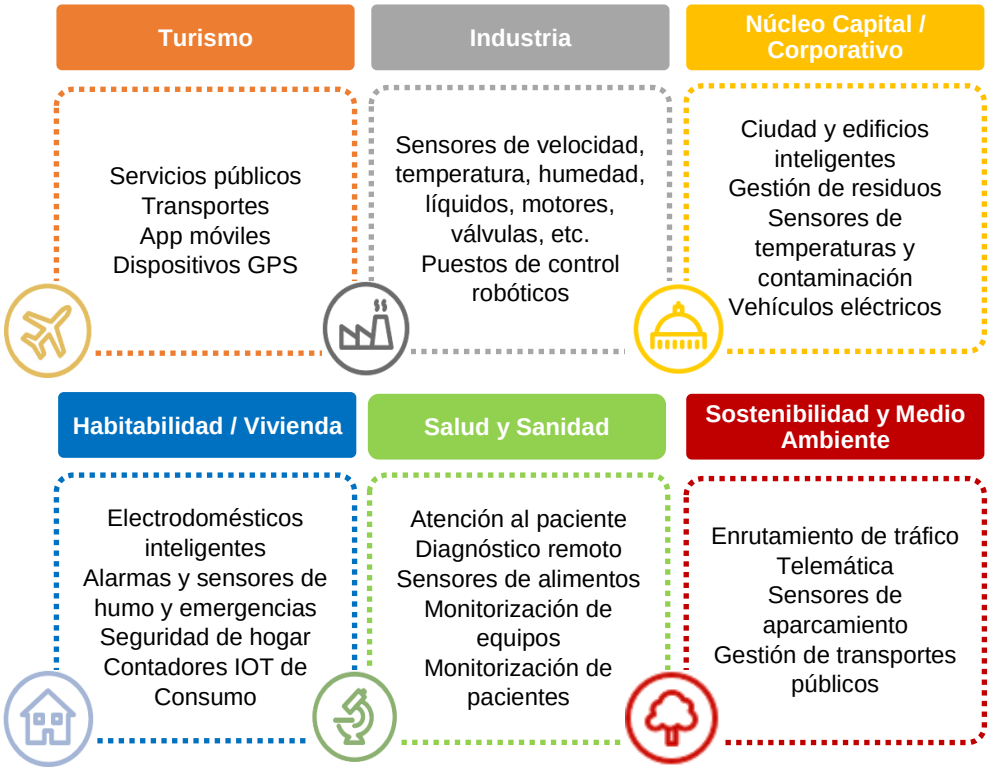
ÁMBITOS COMPETENCIALES

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA

Las líneas estratégicas definidas en el mismo plan, son las siguientes:

LÍNEAS ESTRATÉGICAS

A continuación, se muestran algunos Sistemas y Servicios de Información que se pueden observar en los diferentes sectores que conforman el ámbito de las Smart Cities.

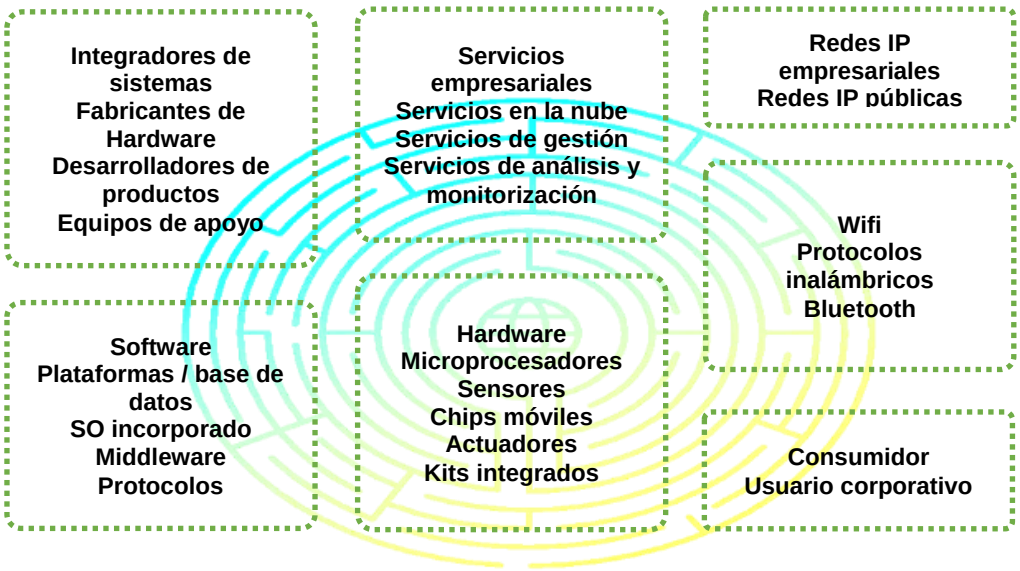


Todos estos sistemas y servicios identificados anteriormente, son susceptibles de presentar vulnerabilidades que pueden ser explotadas por ciberatacantes, pudiendo

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

utilizar diferentes vectores de ataques para conseguir su explotación, en función de los objetivos perseguidos.

Profundizando en el ecosistema IoT, debido a su importancia en la Smart City, una clasificación de los sistemas y servicios podría ser la siguiente:



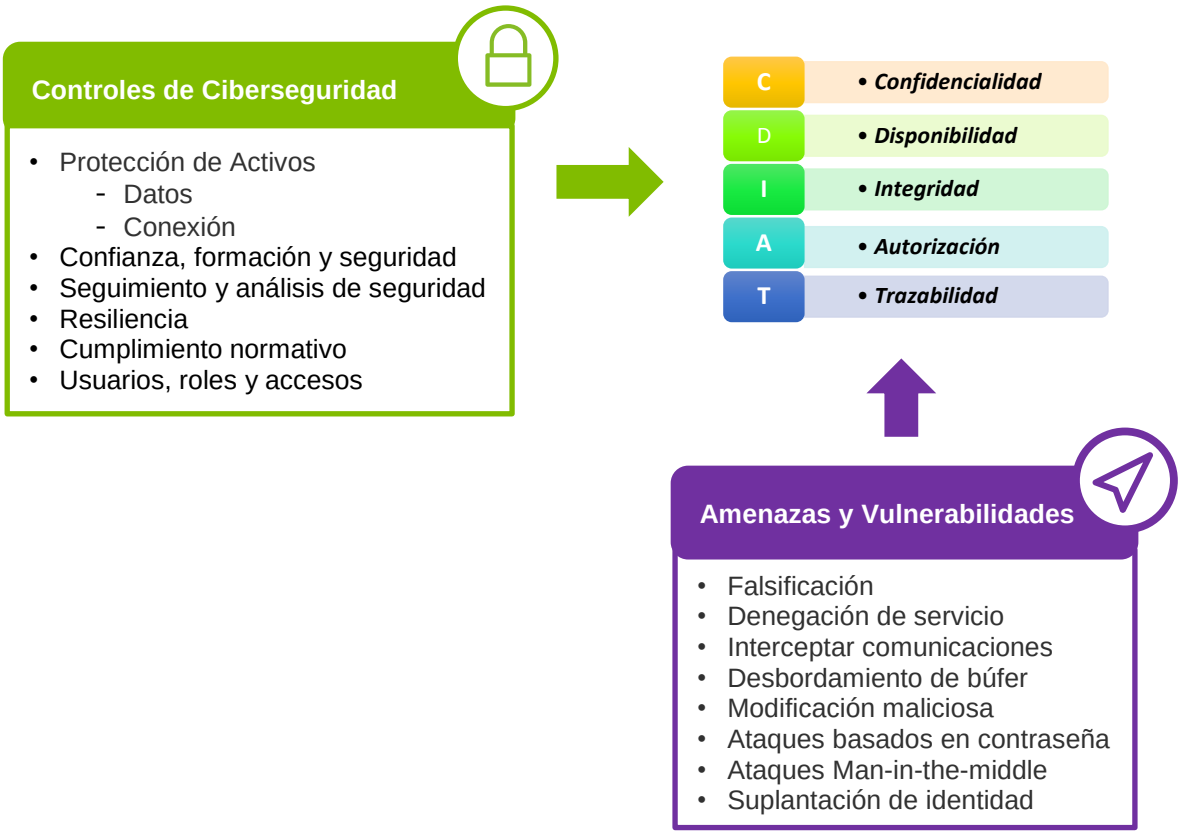
La principal causa de que los dispositivos inteligentes sean objeto de cada vez más ataques, se debe a la conjunción de varios factores. Entre ellos, podríamos destacar que la inmensa mayoría de los mismos están continuamente conectados a internet, así como que las medidas de control aplicadas para proteger del abanico de amenazas posibles, tanto a la conexión como al propio dispositivo, suelen ser mínimas. Ello, unido a la falta de concienciación y sensibilización, ha creado el caldo de cultivo idóneo para que los dispositivos inteligentes se constituyan en el método más utilizado para el ciberdelito, hoy en día la mayor "industria" a nivel mundial, por delante del narcotráfico.

Sin tener que indagar mucho, es de público conocimiento que se han producido casos significativos y evidentes de explotación de vulnerabilidades a través de los dispositivos inteligentes; en algunos casos, generando incluso conflictos diplomáticos entre países, a cuenta de la utilización de los mismos por los servicios de inteligencia.

Las principales motivaciones para realizar estos ciberataques, son:

- Obtención de información confidencial que genere ventaja competitiva, bien por la utilidad intrínseca de la información, bien para la utilización de la misma para generar un deterioro de la imagen o marca de la entidad atacada
- Imposibilitar el suministro de los servicios por parte de una organización
- Sustracción de datos de carácter confidencial, recopilación de información para elaborar perfiles y comportamientos de personas o entidades para, posteriormente, ser vendida a terceros o utilizada para realizar un ciberataque
- Creación de nuevas vías de intercambio de información, de nuevos métodos de pago, que imposibilitan la detección y trazabilidad (por ejemplo, Bitcoin)

Debido a que en este entorno la característica principal es la interoperabilidad de todos los sistemas y servicios, se han analizado e identificado las mínimas áreas de ciberseguridad que deben ser cubiertas por toda organización, entidad o usuario, con el fin de salvaguardar los pilares fundamentales en los que se basa la seguridad:



Vectores de Ataque

Dentro del entorno Smart City, los sistemas que interactúan están sometidos a una serie de amenazas, las cuales pueden conseguir materializarse a través de diferentes vectores de ataque, impactando sobre el activo o sistema objetivo. Habitualmente, se aprovechan fallos de seguridad, ya sea en aplicaciones (por ejemplo, en Adobe Flash), protocolos (por ejemplo, en SSL), dispositivos (por ejemplo, fallos de diseño en Smart TV), etc. o en cualquier otro tipo de método que permita atacar un sistema.

Para intentar medir un nivel de ***RIESGO*** determinado, se tendrá en cuenta el **valor** del sistema o conjunto de sistemas para calcular el **impacto** que la materialización de una **amenaza** ocasionaría, en función de la **probabilidad** de que sucediera.

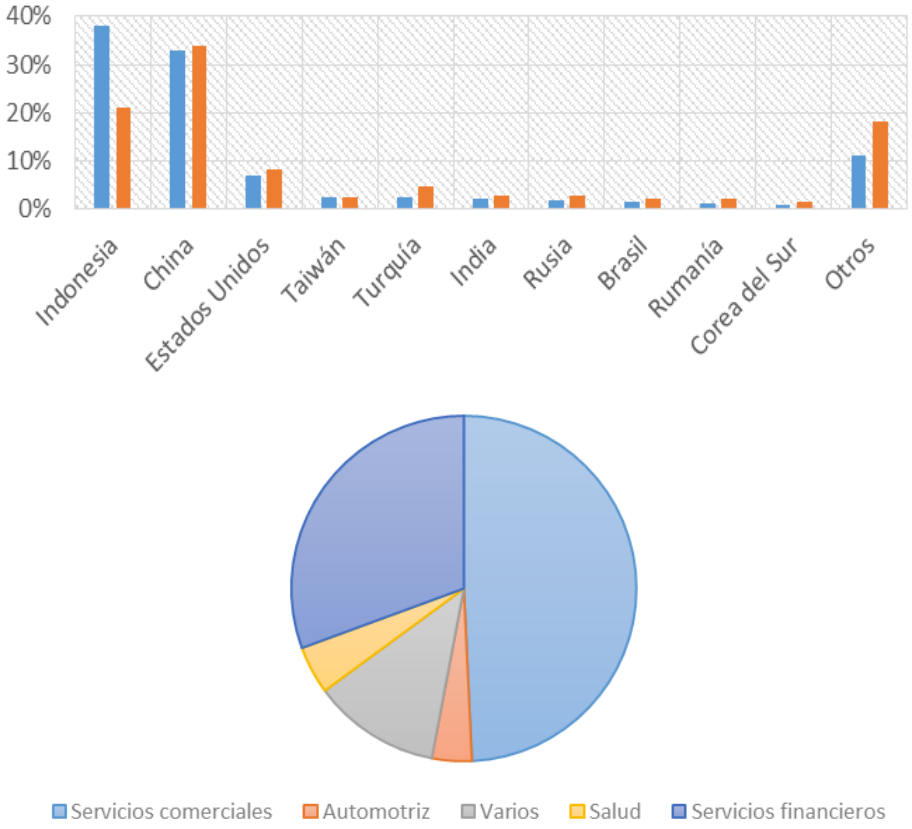
Un ciberataque puede utilizar múltiples vectores de ataque para intentar conseguir sus metas, lo que incrementa su complejidad. Tomando como base la finalidad última de los ciberataques, surge el ciberdelito, el ciberespionaje, el cibervandalismo, etc.

Como ejemplo reciente, un ciberataque en Gran Bretaña consiguió tomar el control de los sistemas SCADA de una potabilizadora de agua, modificando la concentración

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA

de los productos químicos que se añaden al agua en su proceso de potabilización, lo que provocó concentraciones letales. Afortunadamente, fue detectado a tiempo.

Como se observa en la siguiente gráfica del CCN (Centro Criptológico Nacional), que muestra el origen de los ciberataques producidos durante el primer y segundo trimestre del año 2016 en diferentes países, se aprecia como en el segundo trimestre, *los ciberataques se han incrementado en todos los países* (excepto en Indonesia). Ello refuerza la hipótesis de que el número de incidentes se irá incrementando de forma significativa con el transcurso del tiempo, debiendo adoptar las organizaciones las medidas necesarias para reforzar su ciberseguridad, dotándose de los medios necesarios para hacer frente a escenarios cada vez más complejos.



Fuente: Centro Criptológico Nacional

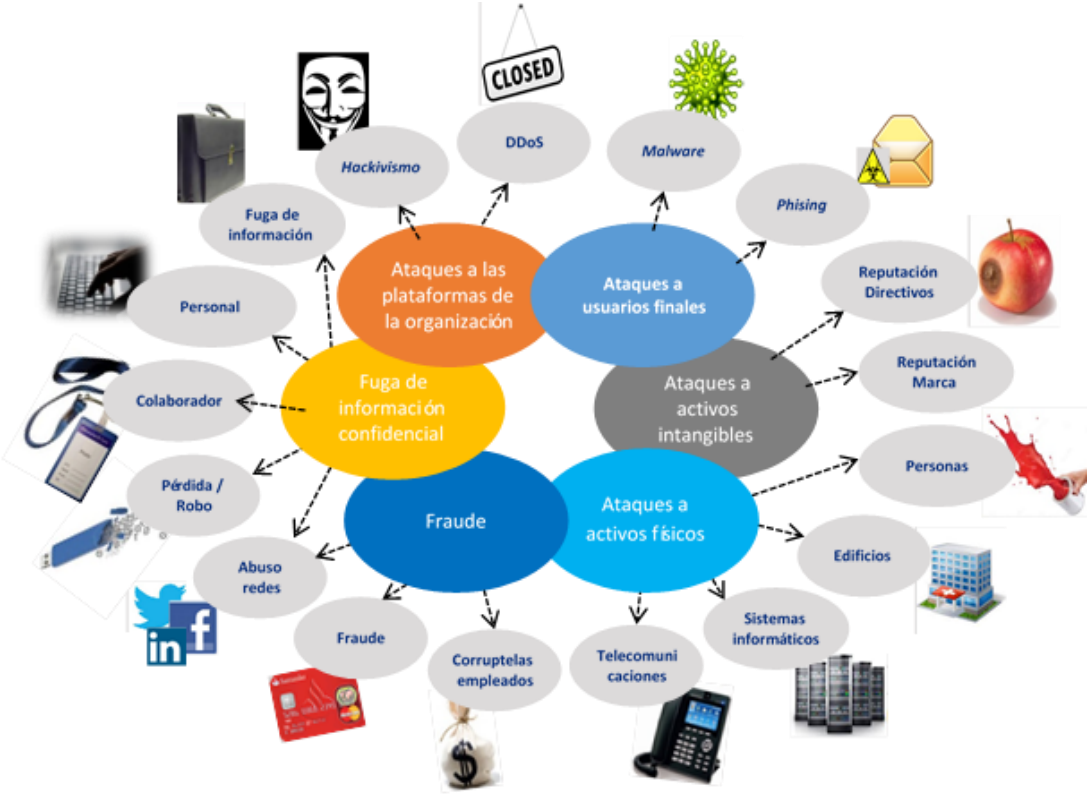
Las organizaciones que sufrieron mayor número de ciberataques fueron aquellas que prestan servicios comerciales, seguidas de las de servicios financieros. En Andalucía, conforman un pilar fundamental dentro del tejido empresarial, por lo que ciberataques dirigidos contra estos sectores podrían impactar sobre un gran número de empresas.

A continuación, se muestran los principales tipos de ataque identificados por el CCN (Centro Criptológico Nacional), apareciendo en primer lugar los más importantes.

Siendo Ramsonware un tipo de malware, lo mencionan de forma independiente debido a la prevalencia y generalización de ese tipo de ataque.

Año 2013	Año 2014	Año 2015
Malware Ransomware DDoS Exploits APT Watering Hole Descentralización Ataques DNS Autenticación de factores Ataques M2M Botnets	Malware Ransomware DDoS Exploits Botnets APT Desconfiguraciones de páginas web Ejecución remota Spam Phishing Servicios Cloud	Malware Ransomware DDoS Botnets Exploits APT Spam Phishing Watering Hole Inyecciones SQL Inyecciones de ficheros Ejecución remota

Basándonos en diferentes fuentes, la mayoría de los incidentes registrados en España han sido originados por código dañino, ransomware, troyanos o Exploits Kits. Cómo vemos en la imagen que se muestra a continuación, los objetivos, los medios utilizados y la magnitud de las consecuencias de los diferentes ciberataques, aumentan cada año de forma exponencial; a medida que la tecnología evoluciona, a medida que se incrementa el número y tipología de dispositivos, usuarios y canales disponibles, el abanico de posibilidades de ataque se va ampliando, apareciendo nuevos actores cada vez más profesionalizados y peligrosos.



Es necesario resaltar la **necesidad de estar preparado ante nuevas amenazas, ante nuevos escenarios** que hace poco eran ciencia-ficción, debido a la aceleración en la incorporación de avances tecnológicos, tanto en el ámbito empresarial como en el personal. Ello implica que la gestión de riesgos debería ser un proceso periódico, revisable.

Un claro ejemplo de lo expuesto, lo tenemos en la imparable utilización de los drones para diferentes tareas. Como botón de muestra, gigantes como Amazon están valorando utilizarlos en el reparto de mercancías, encontrándonos ante un escenario impensable hasta hace muy poco, como es la posible toma de control de dichos dispositivos por parte de usuarios no autorizados. Valga como ejemplo el incidente ocurrido en abril del 2016 por un avión de British Airways que, en su aproximación al aeropuerto de Heathrow, chocó contra un dron. Mientras que el daño producido por el impacto de aves es un fenómeno ampliamente estudiado, no hay muchos datos acerca de las consecuencias de un choque contra un elemento de éste tipo. Y es una amenaza real que está siendo incorporada por los gestores aeroportuarios.

A continuación, en los siguientes apartados, se detallan los **PRINCIPALES VECTORES DE ATAQUE** que afectan en diferente medida a las Smart Cities, clasificados de acuerdo a su importancia y prevalencia.

1.1. MALWARE

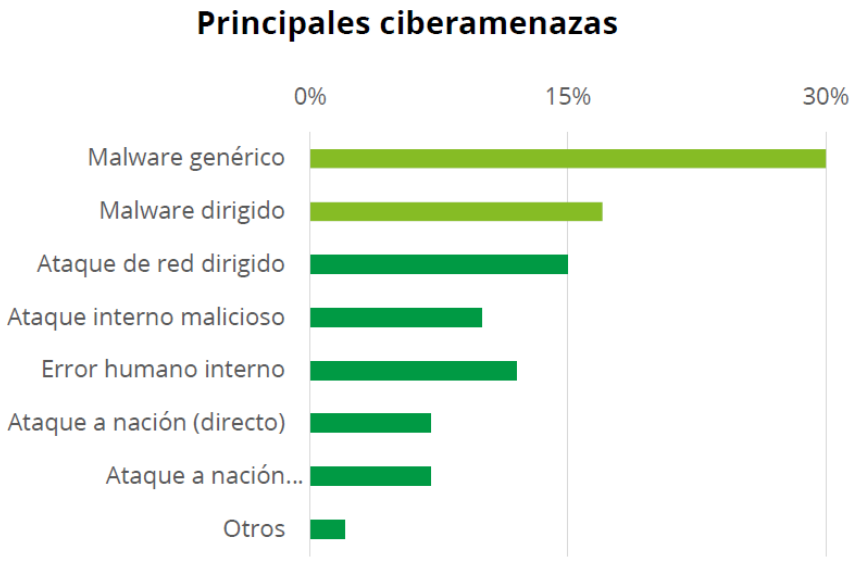
Software malicioso instalado sin autorización. Suele ser el vector más utilizado en la actualidad -junto con los Exploit Kits-, según la mayor parte de las fuentes especializadas, *sirviendo en muchos casos como mecanismo de entrada de otros tipos de ataques*, ya que una vez instalado normalmente se convierte en la puerta trasera para intentar tomar el control de sistemas y entornos de forma silenciosa. Cómo veremos más adelante -en el apartado correspondiente-, el malware suele ser la base sobre la que se construyen las Amenazas Persistentes Avanzadas (APT, Advanced Persistent Thread)

Puede infectar sistemas y aplicaciones, realizar modificaciones ilegítimas, extraer o destruir información, etc. Aunque, en consonancia con el apartado anterior, cada vez en mayor medida se destina a infectar ordenadores y dispositivos para crear Botnets.

Baste decir que, a principios del 2015, se descubrió que un ataque que llevaba dos años funcionando sin ser detectado, había conseguido sustraer en torno a mil millones de euros de diferentes bancos. A través de correos maliciosos, se implantaba malware que permitía que diferentes cajeros repartidos por Europa, dispensaran billetes de manera automática.

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

A continuación se muestran las principales ciberamenazas de 2016 según Intel Security, observándose la prevalencia del malware como vector de ataque.



Fuente: Intel Security

Como ejemplo más cercano, la infección de routers con código malicioso no es algo nuevo. Según análisis de ESET (reconocida compañía de seguridad, fabricante del antivirus NOD32), al menos el 15% de los routers domésticos no están protegidos. Es fácil extrapolar y calcular cuales serían los riesgos y el daño que podría causar un ataque masivo DDoS utilizando esta infraestructura, ya que el parque total estimado es de cientos de millones.

La gran *AMENAZA PARA LAS SMART CITIES* en este ámbito, se basa en la capacidad de los *dispositivos IoT* de ser utilizados como ***vía de infiltración*** *para alterar la ciudad y su gestión, al sector empresarial y a la ciudadanía* en general. En entornos críticos, el daño potencial se multiplica de forma exponencial.

Como muestra llamativa de las capacidades de los ciberatacantes para conseguir sus fines, se ha demostrado la posibilidad de *interferir en los sistemas electrónicos de varios automóviles*, consiguiendo en algunos casos operar de forma remota diferentes elementos de los mismos, incluyendo el motor. Algunas demostraciones son públicas, pudiendo visualizarse en plataformas de video por streaming.

A día de hoy, los atacantes suelen utilizar diferentes vías para realizar la infección o inserción de malware:

- Campañas de spam, principalmente mediante correo electrónico. Aunque se utilizan también otros medios, en la forma de SMS, aplicaciones de mensajería instantánea, etc.
- Sistemas ya infectados con otro malware, utilizado como caballo de Troya para instalar malware adicional

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

- Exploit Kits: una vez detectada una vulnerabilidad, alguna de las herramientas del paquete de software malicioso, instala malware
- Sitios web maliciosos, normalmente con publicidad engañosa
- Dispositivos externos

A continuación, se muestran los tipos de malware más utilizados actualmente:

Hay que resaltar que, en la mayor parte de los informes de ***INFECCIONES POR MALWARE, ESPAÑA SUELE ESTAR SITUADA ENTRE LOS DIEZ PRIMEROS A NIVEL MUNDIAL.***

Debido a su importancia, a continuación se detalla un tipo de malware que ha tenido una prevalencia significativa en los últimos años: **RAMSOMWARE**

1.1.1. RANSOMWARE

Software cuyo fin es comprometer la disponibilidad de la información y los sistemas. En la mayor parte de las ocasiones, se requiere un desembolso económico por parte del afectado para la recuperación de los datos, ya que la operativa de la organización afectada puede verse comprometida por completo, en función de la gravedad de la infección.

A efectos didácticos, podría simplificarse considerando el ramsomware como un malware que infecta todos los sistemas de información que tenga a su alcance, con la finalidad de cifrar la información y extorsionar económicamente a las víctimas si quieren recuperar dicha información. Aunque, dependiendo de la fuente utilizada, el número de empresas de paga el rescate pero que nunca recupera sus datos, suele rondar entre el 15% y el 25%.

Se trata de una amenaza en constante crecimiento, debido a:

- La cantidad de software de tipo ransomware disponible. Se estima que existen más de 60.000 variantes en la actualidad, siendo las más conocidas CryptoWall y TorrentLocker.

- La relativa facilidad de infectar un equipo con este tipo de software malicioso, sin tener que robar los datos y revenderlos luego. En gran parte de los casos detectados, los ciberatacantes utilizan la ingeniería social para engañar a la víctima, haciendo pasar el ransomware por otro tipo de software. En muchos casos, suele tratarse de software de pago ofrecido gratuitamente en páginas de descarga, páginas legítimas que han sido comprometidas, a través de anuncios fraudulentos (malvertisement) o mediante campañas de email con enlaces al malware. Las campañas de propagación suelen ser de tres tipos:
    - *Generalistas*: campañas de temática variada
    - *Dirigidas*: su destino es un objetivo concreto -o un conjunto de ellos-, modificando y personalizando el ransomware, con la finalidad de evadir las defensas
    - *Indirectas*: los equipos infectados, posteriormente son utilizados en Botnets de ransomware. Como parte de la estrategia para esconder el origen de las conexiones, se utilizan equipos zombis
- El rendimiento económico obtenido suele ser muy alto. Hay intermediarios que ofrecen campañas de ramsomware, en el que los ciberdelincuentes pagan, bien por el software, bien por la infraestructura en modo servicio que se pone a su disposición
- El medio de pago en moneda virtual o criptomoneda (p.e. Bitcoin) hace difícil rastrear al "beneficiario" de la transacción

Como aproximación al **posible impacto que el ramsomware podría provocar en la Smart City**, podríamos mencionar que *durante el año 2016 el sector sanitario se convirtió en un objetivo preferente* para los ciberdelincuentes, debido al éxito de sus campañas de ramsomware. De la misma forma, investigadores han demostrado la capacidad de ataque del ransomware sobre dispositivos IOT. Por ejemplo, sobre un termostato, incrementando la temperatura al máximo y bloqueándolo a continuación.

1.2. EXPLOIT KITS

Se trata de **paquetes de software, que incluyen un conjunto de programas y utilidades ya desarrolladas, destinados a explotar diferentes vulnerabilidades de programas y sistemas**, afectando a la disponibilidad, integridad y/o confidencialidad del objetivo. Este tipo de paquetes incluyen módulos para la explotación de vulnerabilidades, distribución de malware, control del sistema objetivo, etc.; en definitiva, constituyen un esquema completo de herramientas que permiten automatizar en gran medida los ciberataques.

Normalmente se utilizan para inyectar malware, en muchos casos a través del navegador de internet, aunque existen otros medios que redirigen a los usuarios hacia los servidores que albergan los Exploit Kits. Los ataques se van sofisticando hasta el punto de que son capaces de operar sin necesidad de instalar nada, girando progresivamente su atención sobre dispositivos IoT.

Actualmente se trata de uno de los vectores de ataque más utilizados para comprometer los sistemas, no solo por el número de Exploit Kits y sus capacidades, sino por la facilidad de uso, lo que los convierte en muchos casos en un arma al alcance de gran número de posibles atacantes.

Esta forma de ataque se ha profesionalizado hasta tal punto, que hay ciberdelincuentes dedicados, no al uso de este tipo de herramientas para realizar ciberataques como medio de conseguir un beneficio económico, sino a venderlas a un tercero que será el que finalmente haga uso de las mismas. O, incluso, a ofrecer los Exploit Kit como un servicio.

A día de hoy, es posible encontrar modificaciones de Exploit Kits que incorporan las desde las últimas vulnerabilidades detectadas en diferentes productos de software, hasta vulnerabilidades de tipo Zero-Day (sin descubrir), llegando incluso a ofrecer servicios de actualización de los mismos.

Los ciberdelincuentes no solo están invirtiendo en el desarrollo de este tipo de herramientas, sino en la búsqueda de vulnerabilidades en los productos de software, sobre todo en los más utilizados (Internet Explorer, Firefox, Adobe Flash, Windows, Android, etc.), lo que les permitiría ofrecer Malware como Servicio a un amplio espectro de posibles ciberdelincuentes interesados.

Algunos de los Exploit Kit más utilizados, son:

- Neutrino
- Rig
- Sundown
- Magnitude
- DarkComet
- Zeus
- Blackshades
- Citadel
- Blackhole

Fuente: Avgthreatlabs, McAfee, KASPERSKY, Esset, Symantec

1.3. PHISHING

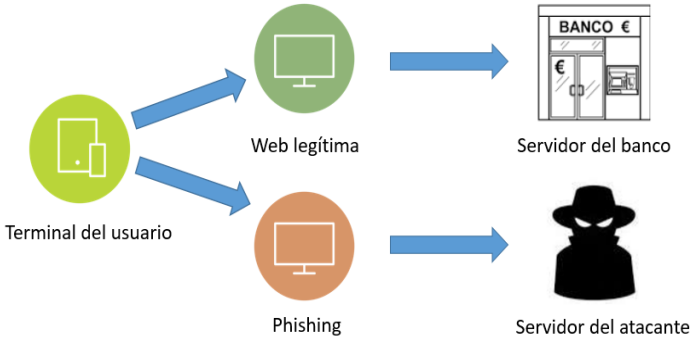
Ataque que utiliza la suplantación de servicios y webs, engañando al usuario para -entre otros fines- robar información confidencial, así como inyectar software malicioso.

Desde hace unos años, se ha detectado un notable incremento de los ciberataques mediante Phishing, como consecuencia de la escasa complejidad y de la poca preparación que necesitan, unido a la falta de concienciación por parte de los usuarios. En el caso de ataques dirigidos a objetivos concretos (Spear Phising) -que suelen ser más efectivos al personalizar el engaño-, la publicación en redes sociales de datos de toda índole permite a los atacantes disponer de la información necesaria mediante técnicas de inteligencia de fuentes abiertas (Open Source Intelligence - OSINT). Un ejemplo podría ser el caso Anthem (empresa de seguros de salud), en que el uso de Linkedin permitió identificar objetivos para iniciar el ataque, lo que permitió robar datos de 79 millones de personas.

Este vector no sólo se puede optimizar para centrar el ataque en objetivos concretos, sino que hay técnicas que tienen como finalidad minimizar y retrasar la posibilidad de su detección, aumentando la probabilidad de impacto y de materialización del ciberataque. Por ejemplo, utilizando el filtrado por geolocalización para restringir el acceso a las web falsas utilizadas por los ciberdelincuentes, para que sólo los usuarios de un determinado país accedan a ellas, evitando su detección por parte de aquellos a quienes no va dirigido el ataque.

Las cifras del alcance, de la magnitud que pueden tener este tipo de ataques, lo encontramos en el robo de los datos de 1.000 millones de cuentas de correo de Yahoo; estimándose en torno a 3.500 millones el número total de usuarios de internet. De la misma forma, ataques a Myspace, Linkedin, Adobe, etc., han permitido sustraer datos de cientos de millones de usuarios adicionales.

Un gran número de ataques tienen como finalidad sustraer información de tarjetas de crédito y datos personales, observándose una tendencia a dirigir este tipo de ataques hacia sistemas Cloud debido al incremento en su utilización. En esa línea, el robo de credenciales de Office 365 ha sido el objetivo de recientes campañas de Phishing.



Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA

Los **PRINCIPALES MEDIOS** para llevar a cabo este tipo de ataques, son:

Por otro lado, la **TIPOLOGÍA DE INFORMACIÓN** confidencial que los atacantes buscan robar cuando realizan estos ciberataques, suele ser la siguiente:

Las **PRINCIPALES CONSECUENCIAS** de estos ciberataques son:

- Robo de dinero (cuentas bancarias, Paypal, Bitcoins, etc.)
- Utilización fraudulenta de tarjetas de crédito
- Compra/venta de datos personales e información confidencial
- Estafas
- Suplantación de identidad
- Como vector para llevar a cabo otro tipo de ataque

La gran amenaza para las **SMART CITIES** se centra en el *robo de credenciales*, que servirán de **pasarela para acceder a dispositivos IoT** a los que los usuarios cuyos datos se han obtenido de forma fraudulenta, tengan permiso. En el caso de infraestructuras críticas, la amenaza es aún mayor.

1.4. DENEGACIÓN DISTRIBUIDA DE SERVICIOS (DDOS)

Un **Ataque de Denegación de Servicio** (*Distributed Denial of Service*) se basa en provocar la saturación del objetivo, en la red y/o en los sistemas (servidor, sitio web, etc.), impidiendo el acceso a los usuarios; normalmente, de forma temporal, hasta que se consigue restablecer el servicio.

Existen *diferentes tipos de ataques DDoS*, clasificados en función de los métodos o procedimientos utilizados para explotar las vulnerabilidades. Algunos ejemplos son:

- Syn Flood
- Zombi Flood
- ICMP Flood
- Non-service Port Flood
- Service Port Flood
- Fragment Flood
- HTTP GET Flood
- Blended Food
- Anomalous Packet Flood
- Inundación de una Región Foránea

Estos ataques son explotados en diferentes capas del modelo OSI. A continuación, se muestran las dos tipos más utilizados en la actualidad:

- **Explotación en capa de Red** (capa 3/4): normalmente, ataques con grandes cantidades de paquetes que consumen los recursos disponibles, o provocan una sobrecarga de tráfico en el servidor.

- **Explotación en la capa de Aplicación** (capa 7): aprovechan una brecha o vulnerabilidad con objeto de saturan el servidor o la BB.DD., siendo más difíciles de detectar

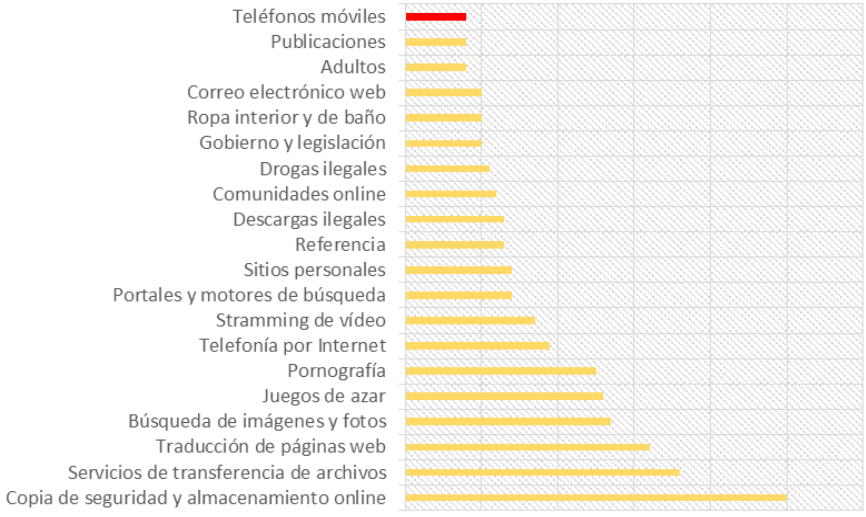
Las *motivaciones* más frecuentes para realizar este tipo de ataque, son:

- Económicas: habitualmente, mediante extorsión, solicitando una cantidad de dinero para que un ataque inminente no se produzca; o, con posterioridad al mismo, para que no vuelva a repetirse. O mostrando, frente a terceros, la capacidad para realizar este tipo de ataques y/o la infraestructura de la Botnet.

- Socio-Políticas: la finalidad suele ser, bien provocar un impacto lo suficientemente grande para que tenga repercusión social -y, por tanto, llamar la atención sobre algún tipo de reivindicación-, bien realizar un ataque a un organismo con fines políticos

- Diversión/Ego: intenta, mediante este tipo de ataques, probar su valía como atacante, poner a prueba su capacidad para la realización de este tipo de acciones

Las estadísticas de CISCO (solicitudes de cambios en el protocolo HTTPS durante el periodo comprendido entre enero y septiembre de 2015), muestran *nuevas tendencias* de los ciberdelincuentes, basadas en ataques DDoS *utilizando terminales o dispositivos móviles para conformar una Botnet*.



Ejemplos recientes indican una ***tendencia mucho más peligrosa*** para el entorno de las *Smart Cities*, que ha llegado para quedarse: los **ATAQUES DDoS MÁS IMPORTANTES SE REALIZAN MEDIANTE DISPOSITIVOS IoT**.

En octubre de 2016, empresas como New York Times, Twitter, eBay, Netflix, PayPal y Spotify -entre otras-, tuvieron serias dificultades para prestar su servicio, o fueron inaccesibles. El motivo fue un **ataque DDoS masivo** contra Dyn, proveedor de DNS. Se sirvieron, en su mayor parte, de **elementos IoT** (principalmente cámaras IP de vigilancia, grabadoras digitales de video y routers domésticos), consiguiendo generar un tráfico récord en este tipo de ataques (método primario de clasificación de la potencia del mismo).

Como botón de muestra, los dos mayores ataques DDoS -en función del tráfico generado-, fueron de *662 Gbps* (contra la web KrebsOnSecurity.com) y *1.1 Gbps* (contra OVH, empresa francesa de hosting); en ambos casos a través de dispositivos IoT. Observamos como los dispositivos IoT no securizados se están convirtiendo en el arma preferida de los ataques DDoS; normalmente, mediante malware, consiguen controlar remotamente los dispositivos infectados, y dirigir tráfico sin parar hacia un mismo objetivo (DynDNS).

Para aprovechar vulnerabilidades en este tipo de infraestructuras, los atacantes disponen ya de varias herramientas. Una de ellas, **Mirai** (cuyo código fuente se ha publicado), permite buscar en Internet dispositivos con las claves del fabricante por defecto, infectándolos a continuación para controlarlos a distancia y utilizarlos a conveniencia en ataques DDoS.

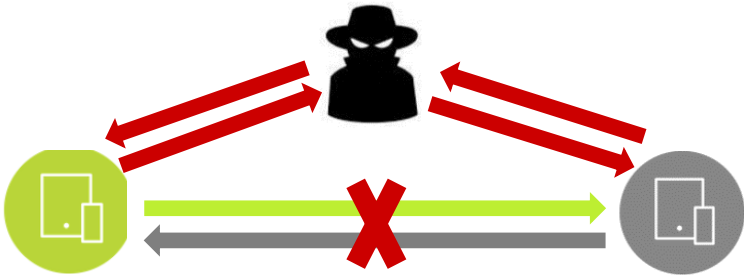
Los dispositivos IoT se han convertido en objetivos muy atractivos, principalmente por su **falta de seguridad**. Las causas más comunes son:

- Usuarios y contraseñas embebidas por defecto; en muchos casos, con permisos de administración
- Contraseñas débiles, fáciles de atacar por fuerza bruta. A ello se une que no suelen implementar -o funcionalmente es imposible- el bloqueo por intentos fallidos de acceso, por lo que en la mayor parte de los casos es únicamente cuestión de tiempo y recursos dedicados
- Configuraciones erróneas por defecto
- Vulnerabilidades conocidas –antiguas en bastantes ocasiones-. Las amenazas provienen de que en muchos casos los fabricantes no tienen en cuenta la seguridad a la hora del diseño, en otros no se corrigen los fallos, y que muchos dispositivos no se actualizan nunca
- Actualmente hay una gran cantidad de dispositivos conectados a internet, previéndose un aumento ingente en los próximos años. Según el "Mobility Report" de Ericsson, en 2018 el número de elementos IoT será superior al de móviles, experimentando un incremento compuesto anual del 23% entre 2015 y 2021; y, en 2021, existirán 28.000 millones de dispositivos conectados, de los que 16.000 millones formarán parte de IoT.

1.5. INTERCEPTACIÓN, ROBO O SABOTAJE DE DATOS

En este vector de ataque, los ciberdelincuentes explotan las **vulnerabilidades de protocolos inseguros de comunicación y de transmisión de información entre dos dispositivos o sistemas de información**; o, en otros casos, errores en la configuración de protocolos.

Para la interceptación, el ataque denominado "Man in the Middle" suele ser el más habitual. En él, los ciberdelincuentes aprovechan las vulnerabilidades de los diferentes protocolos utilizados durante el proceso de comunicación, consiguiendo posicionarse en medio de los intercambios de información, obligando a que todo el flujo, ya sea unidireccional o bidireccional, pase por el ciberdelincuente. A través de estos ataques se puede comprometer tanto la integridad, como la confidencialidad de los datos.



Ataque "Man in the Middle"

El impacto de esta tipología de ciberataques dependerá de la información que pueda verse afectada. Es por ello, que normalmente estos ciberataques se producen tras un periodo de investigación por parte del atacante, permitiéndolo estudiar e identificar aquellos objetivos que transmitan información con mayor relevancia.

Actualmente, existe una gran diversidad de herramientas destinadas a la detección de esta tipología de ciberataques; aunque al mismo ritmo que evolucionan éstas, también lo hacen las diferentes metodologías que los ciberatacantes utilizan para sortear las barreras, así como para dificultar su detección por dichas herramientas. Debido a la facilidad de la utilización de herramientas automáticas con guías para llevar a cabo un ataque "Man in the Middle", muchos de los atacantes no requieren de experiencia previa para utilizar este vector.

Debido a la evolución de la tecnología, que camina a pasos agigantados hacia la autorregulación inteligente de servicios (Autómatas, Bots, Inteligencia Artificial, etc.), así como a la creciente necesidad de acceder a información crítica bajo demanda y en tiempo real (en muchos casos para la toma de decisiones), este tipo de ataques se convierte en crítico. No tanto por la posibilidad de interceptación, sino por el robo y -por encima de todo- el sabotaje o alteración de datos.

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

En el **ECOSISTEMA SMART**, la *toma de decisiones* se convierte en crítica para gobiernos, corporaciones, investigadores, ciudadanos, etc., ya la interacción entre ellos y los elementos que componen la Smart City, será inviable si no se confía en la ***autenticidad e integridad de la información***. Lo que lo convierte en más peligroso aún, en el caso de infraestructuras críticas.

Un ejemplo de ello podría ser el de ZigBee, protocolo que sectores críticos como la Salud y el Transporte utilizan cada vez más. Ello es debido al bajo consumo de energía, a la robustez de las comunicaciones y a su escalabilidad, característica que permite que sea un protocolo adecuado también para su utilización en entornos industriales (CERTSI). Es por ello que cualquier vulnerabilidad en su diseño o implementación, hace que el riesgo global sea muy alto, afectando de lleno a las *Smart Cities*. Baste decir que muchos dispositivos electrónicos de seguridad doméstica lo utilizan también, para darse cuenta de las repercusiones que podrían acarrear la manipulación o alteración de los datos transmitidos por los mismos.

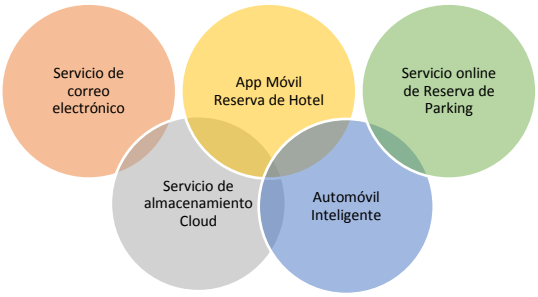
Hay estudios, uno de ellos de *INCIBE*, que ponen de manifiesto que La principal debilidad que existe en la implementación de mecanismos de seguridad en ZigBee, deriva directamente de la limitación de recursos en los dispositivos, debido a que la mayoría de ellos se alimenta mediante baterías, tienen poco poder de cálculo y poca memoria. Las claves utilizadas en los dispositivos ZigBee se guardan en memoria, por lo que un intruso puede simplemente leer la clave directamente de la memoria si tiene acceso físico al mismo (mediante software) y no existen mecanismos de seguridad, así como acceso al software de seguridad. Resumiendo, en este caso la seguridad depende directamente de una correcta configuración de los dispositivos, debiendo prestar atención a la integración y la configuración de los dispositivos conforme a las necesidades del sistema.

Otro botón de muestra fue el ataque que se llevó a cabo en Vietnam en julio de 2016, contra dos de los aeropuertos más importantes y un operador aéreo de vital importancia (Vietnam Airlines). Los atacantes consiguieron tomar el control de las pantallas de información de vuelos y de los sistemas de megafonía, transmitiendo mensajes políticos cuya autoría fue atribuida por las autoridades vietnamitas a un grupo chino. Igualmente, consiguieron redirigir la página web del operador aéreo hacia una web maliciosa, publicando asimismo datos de un número indeterminado de pasajeros.

En el caso de sabotaje de datos, la indisponibilidad, degradación, modificación o eliminación de datos, se convierte en crítica en sistemas o elementos en los que dichos datos constituyen la base de la toma de decisiones, ya sean automáticas o manuales. Tomando como ejemplo un hospital, podríamos encontrarnos desde no disponer temporalmente de los datos clínicos, pasando por la alteración de los resultados de maquinaria de análisis, hasta la pérdida de vidas humanas por la modificación de elementos de radioterapia o… marcapasos. Baste decir que en los años 80 murieron varios pacientes de radioterapia, y en 2008 ya se comprobó que era posible alterar la configuración de algunos marcapasos, con riesgo para la vida.

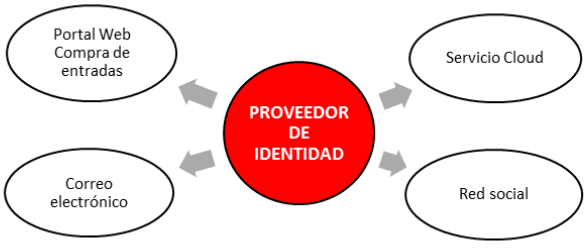
1.6. PÉRDIDA DE CONTROL EN EL ACCESO A DATOS CLOUD

Tanto el uso de servicios Cloud por parte de dispositivos inteligentes, como por parte de los usuarios tradicionales, para uso privado o empresarial, implica que se intercambien, almacenen y centralicen datos en unos pocos proveedores, de manera que se va perdiendo el control sobre quién/es o qué podrá tener acceso a los datos compartidos, cómo se aseguran y utilizan, suponiendo una amenaza contra la confidencialidad de la información. La información de múltiples organizaciones tiende a concentrarse, convirtiéndose en objetivos muy apetecibles para los ciberatacantes.



Ejemplo de compartición de datos entre servicios y dispositivos

Una ***FEDERACIÓN DE IDENTIDADES*** es un grupo o conjunto de entidades que comparten la tecnología y estándares, permitiendo transmitir entre ellas de manera segura la información de la identidad de un usuario, facilitando la autenticación y autorización entre diferentes servicios. La identificación se realiza en los Proveedores de Identidad, interconectando a los terceros con nuestros sistemas. En los servicios Cloud está muy extendido, por lo que si se consigue el robo de la identidad utilizada (por ejemplo, robando el token de federación de identidad) se podría perder el control sobre los servicios interconectados por medio de esta identidad y los datos que gestiona, elemento de vital importancia para el funcionamiento de las SMART CITIES.



Ejemplo de compartición de datos entre servicios y aplicaciones

El número de ataques destinados a proveedores de este tipo de servicios se incrementa a medida que su uso se extiende, siendo el malware y las botnets las mayores amenazas. Si tomamos en consideración el aumento del acceso a los datos desde dispositivos inteligentes, escritorios virtualizados, etc., el escenario se complica. Mediante ataques "Man in the Cloud", en el caso de repositorios compartidos por múltiples usuarios, cualquier infección se propagará con mayor rapidez, comprometiendo mayor número de recursos.

1.7. OTROS VECTORES DE ATAQUE SOBRE LA INFRAESTRUCTURA TIC

A continuación, se describen brevemente una serie de vulnerabilidades relacionadas con las infraestructuras TIC, que afectan en mayor o menor medida a la SMART CITY.

1.7.1. CREDENCIALES O CONFIGURACIONES POR DEFECTO

Este fallo o vulnerabilidad puede afectar a múltiples elementos, ya sean aplicaciones, sistemas operativos, dispositivos de campo (como PLC, "Programmable Logic Controller"), dispositivos de red, etc.

La configuración por defecto puede ir desde credenciales de acceso, hasta puertos y servicios innecesarios activados. Este tipo de vulnerabilidades pueden permitir a un atacante tanto el acceso al sistema y manipular el mismo en función del perfil y los permisos en función de las credenciales, o bien explotar vulnerabilidades asociadas a algunas de las aplicaciones instaladas.

Cómo vimos en apartados anteriores, este vector fue utilizado para crear Botnets en dispositivos IoT, con la finalidad de realizar ataques DDoS.

1.7.2. INSUFICIENTE SEGREGACIÓN Y SEGMENTACIÓN DE REDES

Falta de aislamiento con respecto a accesos externos a las redes internas, ya sean corporativas como industriales (redes de gestión de semáforos, PLC de medición de la calidad del aire, etc.). Este fallo puede ser aprovechado por un eventual atacante para acceder a redes internas y a los dispositivos conectados a las mismas.

1.7.3. FALTA DE REDUNDANCIA Y TOLERANCIA ANTE FALLOS

La falta de redundancia en los componentes considerados críticos, ya sean servidores, elementos de red, concentradores de comunicaciones industriales, puede ocasionar que ante una incidencia o falta de disponibilidad de los mismos, se detenga todo el servicio que soportan.

1.7.4. ACCESO FÍSICO NO RESTRINGIDO

El hecho de no disponer de los mecanismos suficientes para proteger el acceso físico indebido a dispositivos de campo, servidores, salas de control, etc., puede facilitar a un atacante la manipulación de los mismos.

1.7.5. Fallos en los procesos de Backup

La falta de respaldo o los fallos en el proceso de Backup y almacenamiento de los mismos tanto para equipos, servidores, como sobre las configuraciones de los dispositivos de red y dispositivos de campo como los PLC y otros dispositivos, puede ocasionar desde la pérdida de información, hasta la falta de disponibilidad continuada al no poder restaurar el sistema en caso de ser necesario.

1.7.6. Errores en la gestión del cambio y mantenimiento

La falta de una política de gestión de cambios en sistemas y dispositivos, o las deficiencias en su diseño e/o implementación, causan diferentes problemas: errores al aplicar actualizaciones, la incompatibilidad en la integración de nuevos sistemas, la imposibilidad de restaurar el sistema a una versión anterior, o la falta de control en cuanto al mantenimiento de los mismos.

Esto podría conllevar desde errores en los sistemas hasta modificaciones no autorizadas, con la dificultad que supondría su detección a tiempo.

1.7.7. Datos no eliminados en soportes y servicios Cloud

La remanencia de los datos se denomina a los datos residuales que aún permanecen en un medio de almacenamiento una vez se ha procedido a eliminar el dato.

Cuando se trate de fallos en el proceso de borrado o eliminación de los datos guardados en soportes físicos de almacenamiento, una persona que tuviese acceso al soporte podría llegar a reconstruir parcialmente o todos los datos almacenados en el mismo que no hayan sido adecuadamente eliminados.

En el caso de datos almacenados en proveedores de servicios Cloud, el hecho de que puedan seguir almacenados aún después de que el cliente haya enviado la orden de borrado, permitiría a un atacante que consiguiera acceder o recuperar datos supuestamente eliminados.

3. CATÁLOGO DE AMENAZAS ACTUALES

El análisis que se muestra a continuación, toma como punto de partida los servicios que conforman el modelo de Smart City planteado por el **Libro Blanco de AndalucíaSmart para las Ciudades y Municipios de Andalucía** (http://bit.ly/AndaluciaSmart).

En primer lugar, se resaltan las dimensiones de la seguridad (integridad, confidencialidad y disponibilidad) más afectadas, más importantes, si cada uno de los diferentes servicios se viera afectado por un ataque. Es decir, en el cuadro adjunto, se muestran los aspectos más importantes de la seguridad que habría que proteger, aquellos en los que sería aconsejable minimizar -en la medida de lo posible- los riesgos asociados.

SERVICIOS	Integridad	Confidencialidad	Disponibilidad
Gestión del riego			x
Medición medioambiental calidad del aire, ruido, etc.)	x		
Gestión de la red de puntos limpios	x		x
Gestión de la red y consumo de gas en edificios municipales	x		x
Gestión y monitorización de la red eléctrica y consumo	x		x
Gestión de la red de saneamiento y depuradores	x		x
Control del tráfico, semáforos y paneles de señalización	x		
Gestión de transportes	x		x
Gestión de peajes	x		x
Gestión de red de bicicletas públicas	x		x
Gestión de estacionamiento limitado y aparcamientos	x		x
Portal de transparencia	x		
Redes sociales		x	x
Espacios digitales de participación			x
Sede electrónica y trámites on-line		x	x
Páginas web	x	x	x
Aplicaciones móviles de información y servicios al ciudadano		x	x
Inventario electrónico de activos	x		
Aplicaciones móviles para turismo y comercio		x	x
Servicios electrónicos turismo y comercio			x
Video vigilancia		x	
Seguimiento y actividad de efectivos y brigadas		x	
Centros de control de seguridad y emergencias		x	x
Servicios de tele consulta, tele diagnóstico y tele asistencia	x	x	x

A continuación se analiza, para cada servicio, cuáles son los vectores de ataque con mayor incidencia en la actualidad. La matriz resultante nos servirá de guía a la hora de centrar esfuerzos encaminados a reforzar la seguridad de los servicios, tomando en consideración que hay dimensiones de la seguridad (las que se muestran en el cuadro anterior) donde será más importante minimizar riesgos.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
GESTIÓN DEL RIEGO	x	x			x	x		x	x		x	x	x	
MEDICIÓN MEDIOAMBIENTAL (CALIDAD DEL AIRE, RUIDO, ETC.)	x	x			x	x		x	x	x	x	x	x	
GESTIÓN DE LA RED DE PUNTOS LIMPIOS	x	x			x	x		x	x		x	x	x	
GESTIÓN DE LA RED Y CONSUMO DE GAS EN EDIFICIOS MUNICIPALES	x	x			x	x	x	x	x	x	x	x	x	
GESTIÓN Y MONITORIZACIÓN DE LA RED ELÉCTRICA Y CONSUMO	x	x			x	x	x	x	x	x	x	x	x	x
GESTIÓN DE LA RED DE SANEAMIENTO Y DEPURADORES	x	x			x	x	x	x	x	x	x	x	x	
CONTROL DEL TRÁFICO, SEMÁFOROS Y PANELES DE SEÑALIZACIÓN	x	x				x	x	x	x	x	x	x	x	
GESTIÓN DE TRANSPORTES	x	x			x	x	x	x	x	x	x	x	x	
GESTIÓN DE PEAJES	x	x			x	x	x	x	x	x	x	x	x	
GESTIÓN DE RED DE BICICLETAS PÚBLICAS	x	x			x	x	x	x	x	x	x	x	x	
GESTIÓN DE ESTACIONAMIENTO LIMITADO Y APARCAMIENTOS	x	x			x	x	x	x	x	x	x	x	x	
PORTAL DE TRANSPARENCIA	x	x	x	x	x			x		x			x	
REDES SOCIALES	x	x		x	x	x	x			x			x	x
ESPACIOS DIGITALES DE PARTICIPACIÓN	x	x	x	x	x	x	x	x		x			x	x
SEDE ELECTRÓNICA Y TRÁMITES ON-LINE	x	x	x	x	x	x	x	x	x	x		x	x	x
PÁGINAS WEB	x	x	x	x	x	x	x	x	x	x			x	x
APLICACIONES MÓVILES DE INFORMACIÓN Y SERVICIOS AL CIUDADANO	x	x	x		x	x	x						x	x
INVENTARIO ELECTRÓNICO DE ACTIVOS	x	x	x				x	x				x	x	x
APLICACIONES MÓVILES PARA TURISMO Y COMERCIO	x	x	x		x	x	x						x	x
SERVICIOS ELECTRÓNICOS TURISMO Y COMERCIO	x	x	x	x	x	x	x	x	x	x		x	x	x
VIDEO VIGILANCIA	x	x	x			x	x	x	x	x	x	x	x	x
SEGUIMIENTO Y ACTIVIDAD DE EFECTIVOS Y BRIGADAS	x	x	x			x			x			x	x	
CENTROS DE CONTROL DE SEGURIDAD Y EMERGENCIAS	x	x	x	x		x			x	x	x	x	x	
SERVICIOS DE TELE CONSULTA, TELE DIAGNÓSTICO Y TELE ASISTENCIA	x	x	x	x	x	x	x	x	x	x		x	x	x

1 Malware	**2** Ransomware	**3** Exploit Kits	**4** Phishing	**5** DDOS
6 Interceptación, robo o sabotaje de datos	**7** Pérdida de control en el acceso a datos Cloud	**8** Credenciales o configuraciones por defecto	**9** Insuficiente segregación y segmentación de redes	**10** Falta de redundancia y tolerancia ante fallos
11 Acceso físico no restringido	**12** Fallos en los procesos de Backup	**13** Errores en la gestión del cambio y mantenimiento	**14** Datos no eliminados en soportes y servicios Cloud	

4. TENDENCIAS DE LOS VECTORES DE ATAQUE

Intentando anticipar la evolución de los vectores de ataque, en primer lugar se analizarán las tendencias Socio-Económicas a alto nivel, con la finalidad de aproximarnos a la infraestructura TIC que daría respuesta a futuras necesidades. Una vez que dibujemos dicho escenario TIC, podremos estudiar las amenazas emergentes y las posibles soluciones para mitigar los riesgos. En cualquier caso, veremos cómo las Smart Cities se convertirán el eje central de la mayor parte de los vectores de ataque del futuro.

La fuente que utilizaremos a continuación será la de INCIBE (Instituto Nacional de Ciberseguridad), que realizó un estudio a mediados del año 2016.

1.8. NUEVOS MODELOS SOCIALES Y ECONÓMICOS

La masiva presencia de la tecnología ha provocado una revolución respecto a los modelos históricos. Ello, unido al ritmo acelerado en el que se van produciendo los cambios, sugiere que las líneas evolutivas sociales y económicas se dirigen hacia un modelo en el que lo físico y lo digital convivirán y se mezclarán de forma que será difícil, por no decir imposible, separarlos. Independientemente de la velocidad de los cambios, las tendencias parecen dibujar el siguiente escenario, cuyo eje es la **Smart City**:

Auge de las megaciudades

Proliferarán la grandes ciudades autosuficientes y **sedes del talento, inversión, creación de riqueza y crecimiento económico**

Desequilibrio en la conectividad

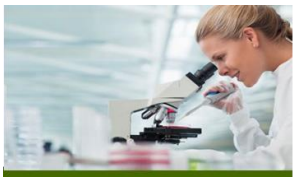
La mayoría de la **población** estará **hiperconectada** a la red, mientras que una **parte significativa apenas** tendrá **conexión**

Mejora del nivel de vida por medio de tecnología

Avances sin precedentes en la **asistencia sanitaria**, la **neurociencia**, la **tecnología**, la **informática**, la **nanotecnología** y el **aprendizaje**

Economía sustentada por multinacionales y pequeñas empresas

Las pequeñas empresas encuentran **mayores áreas de desarrollo y crecimiento intactas** por las grandes multinacionales

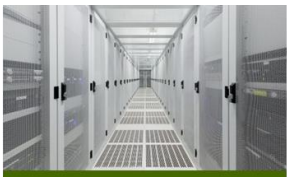


Necesidad de talento

Fomentar, desarrollar y mantener **generaciones de empleados cualificados** se ha convertido en una prioridad global

Innovación disruptiva

El centro de la innovación exponencial se fomenta en la **continua mejora tecnológica** por todo tipo de industrias, funciones y disciplinas



Generación masiva datos

Los consumidores recopilarán y venderán sus datos, que se convertirán en **moneda de transformación** para soluciones, aplicaciones y estrategias de negocio

Nuevos modelos de pago

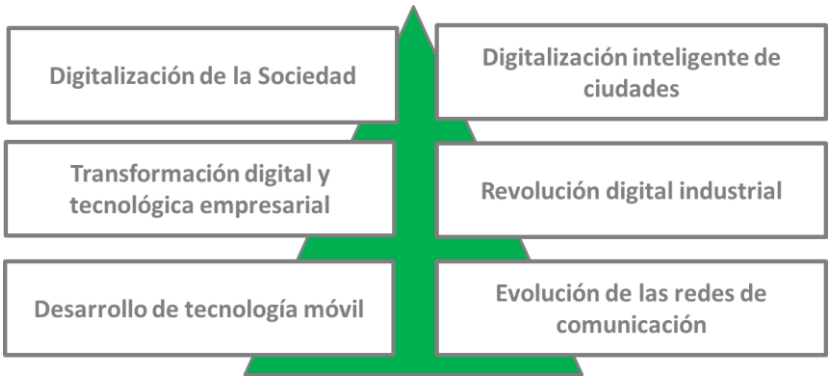
Las **alternativas al dinero en efectivo y los sistemas financieros tradicionales** ganarán un importante impulso en la economía digital

Fuente: INCIBE

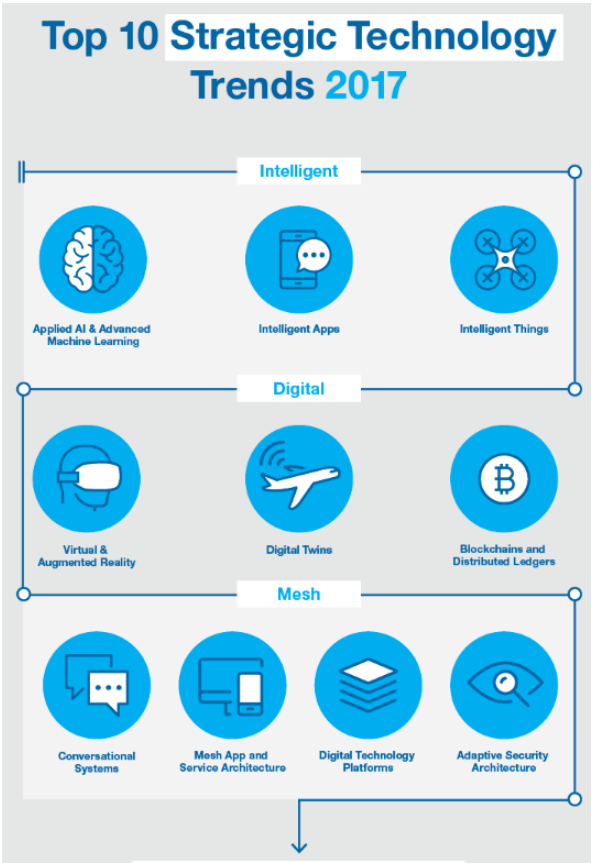
1.9. EVOLUCIÓN TECNOLÓGICA

La tecnología evoluciona a pasos agigantados, en gran medida debido a la revolución que ha supuesto la sociedad digital, provocando un cambio radical del modelo tradicional, mediante una ingente inversión en TIC, que ha permitido alcanzar el grado de madurez suficiente en servicios que permitirán transformar cualquier aspecto de nuestra vida diaria en una interacción entre mundos físicos y digitales.

La base del cambio social, se sustenta en una serie de pilares tecnológicos.



A corto plazo, según Gartner, el año 2017 estará marcado por las siguientes tendencias:



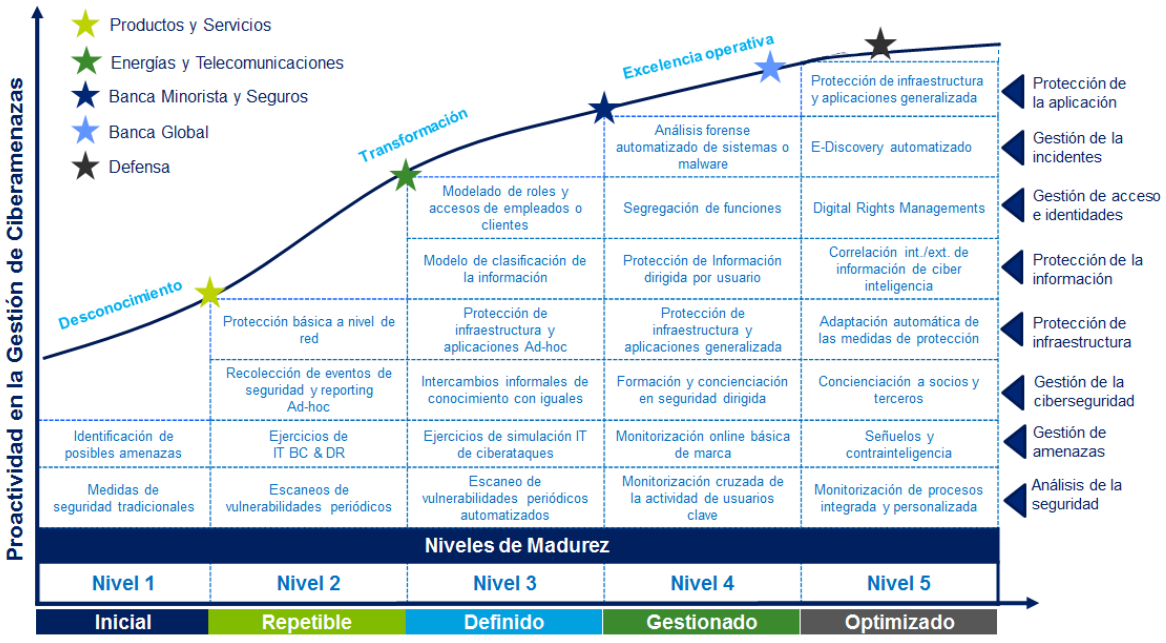
Fuente: Gartner

Tomando como referencia las predicciones del Instituto Nacional de Ciberseguridad, la evolución de la tecnología se centraría, principalmente, en las siguientes materias:

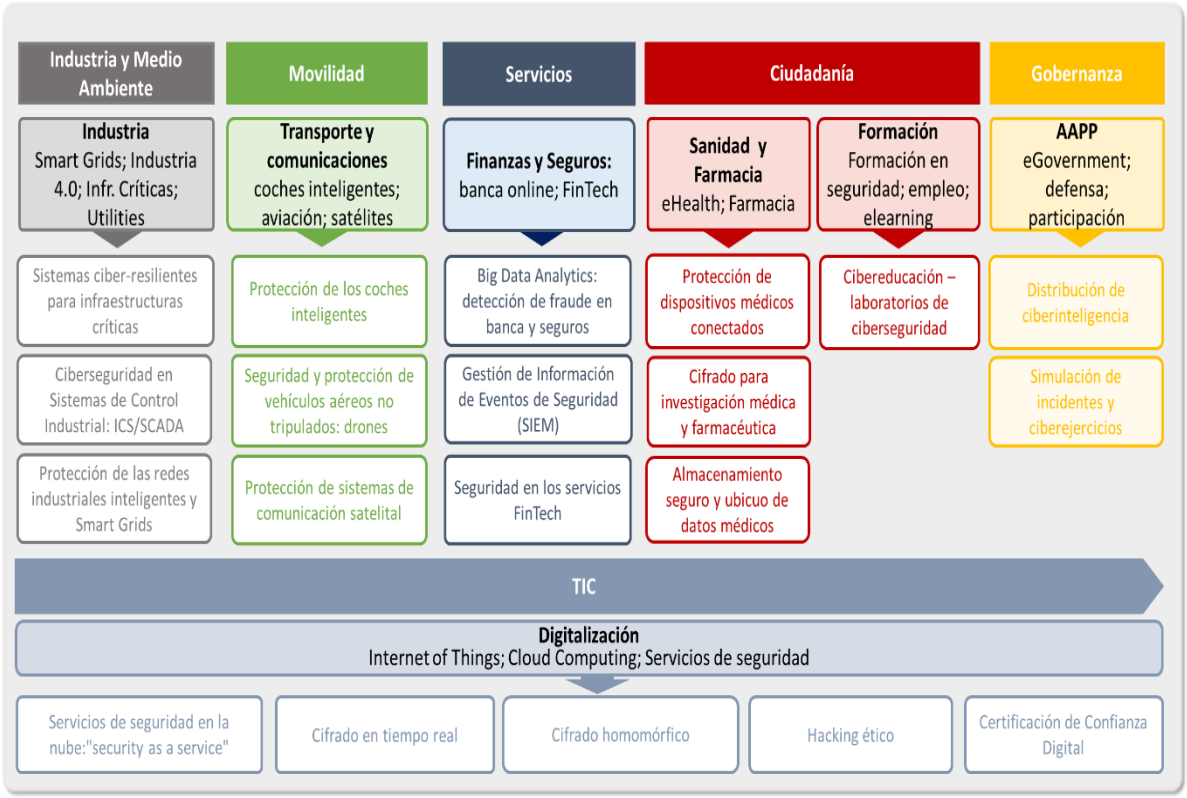
1.10. CIBERSEGURIDAD

Una vez analizadas las principales tendencias tecnológicas a corto/medio plazo, podríamos anticipar cuál será la evolución esperada de los servicios de ciberseguridad, que se deberán adaptan a una realidad cambiante, en continua evolución.

En el siguiente cuadro se muestra el nivel de madurez esperado en ciberseguridad de varios sectores, lo cual nos permite anticipar la existencia de necesidades que deberán ser cubiertas, en línea con las demandas sociales y empresariales.



A continuación, vemos cuales serían las principales tendencias en ciberseguridad, agrupadas en función de las necesidades de distintos sectores.



Fuente: INCIBE

1.11. ANÁLISIS DE TENDENCIAS

Como resultado del análisis global de vectores de ataque y tendencias evolutivas, vemos como la **SMART CITY** SE CONVIERTE EN EL EJE donde pivotarán la mayor parte de los elementos tecnológicos. La utilización de diferentes dispositivos del entorno IoT será un factor importantísimo, ya que los requerimientos de conectividad, integración y software ligero con pocas posibilidades de añadir capas de seguridad, asociado a la economía de costes, conformarán un escenario preocupante a corto/medio plazo.

Para reforzar esa premisa, baste decir que ENISA (European Union Agency for Network and Information Security) ha girado su atención sobre los elementos que componen la Smart City, publicando guías para securizar algunos sectores; como botón de muestra uno de los últimos, de diciembre de 2016, titulado "Securing Smart Airports".

En cuanto al **OBJETIVO** buscado, la tendencia en Europa y Norteamérica sugiere que se incrementarán los daños en infraestructuras, mientras que en otras regiones, el robo de fondos, de propiedad intelectual e información, junto con el chantaje y extorsión, seguirá copando las primeras posiciones. Los esfuerzos del CCN (Centro Criptológico Nacional) de cara a 2017, se centrarán en el ciberespionaje, los ataques DDoS y los sistemas de control industrial del sector público (puertos, hospitales, compañías hidrográficas, etc.), en vista de la evolución de las amenazas en España.

Es por ello, que dada la **EVOLUCIÓN DE LOS VECTORES DE ATAQUE**, el comportamiento de los sistemas y los avances tecnológicos que dan respuesta a las necesidades sociales y económicas, se pueden identificar las siguientes **TENDENCIAS**:

- Mayor complejidad y preparación a la hora de diseñar y realizar los ataques, los ciberdelincuentes están cada vez mejor formados y bajo las órdenes de organizaciones mafiosas, gubernamentales o de agencias de espionaje. Ello les permitirá lanzar ataques contra las infraestructuras inteligentes de las ciudades

- Aumento exponencial de ataques sobre dispositivos IoT, y utilización de los mismos para desarrollar botnets y realizar ataques de DDoS (denegación de servicio). Se estima que en 2020, en torno al 20-30% de los ataques involucrarán elementos IoT. Dichos dispositivos pueden ser empresariales y personales, observándose un gran incremento en aquellos dirigidos a dispositivos móviles

- Vectores de ataque APT más potentes, debido a la detección de nuevos malware que se enmascaran simulando la actividad normal de un usuario. Ello, unido a la utilización de ingeniería social mucho más elaborada como vector de entrada, dibujan un escenario potencialmente muy peligroso

- Ransomware en crecimiento exponencial, aumenta rápidamente su capacidad para afectar a elementos IoT

- Los servicios e infraestructuras estarán dentro de los objetivos en caso de que se produzcan ciberguerras entre países, o ataques de ciberterrorismo. Debido a la alta capacidad, formación y financiación, los ataques son cada vez más complejos, pudiendo atacar y causar graves daños sobre infraestructuras críticas de países o ciudades

- Aumento de ataques y herramientas especializadas, dirigidos específicamente contra infraestructura Cloud. Su grado de evolución es tal, que en algunos casos pueden aprovechar fallos de hardware/firmware

- Incremento del robo de información estática de usuarios (que no puede cambiarse o anularse, como el número de la Seguridad Social), que permitiría identificarlos de forma inequívoca y permanente

- Evolución de los Exploit Kits para integrar herramientas automatizadas, más potentes, que permiten evadir las contramedidas de las soluciones de seguridad

- Ataques recientes muestran como los ataques pueden ir dirigidos a desinformar y crear opiniones falsas o interesadas, en una línea que va desde daños reputacionales, hasta llegar a influir en asuntos de estado (ejemplo reciente de las elecciones presidenciales USA)

Como marco de trabajo a la hora de diseñar e implantar medidas de ciberseguridad, el siguiente ciclo se va abriendo paso, en empresas y organismos públicos, como modelo de gobierno:

SECURIZACIÓN / **VIGILANCIA** / **RESILIENCIA**

PARA PREVENIR, ES IMPRESCINDIBLE IMPLANTAR CONTROLES, QUE EN SU VERTIENTE HUMANA DEBEN IR ACOMPAÑADOS DE ACCIONES DE SENSIBILIZACIÓN, CONCIENCIACIÓN Y FORMACIÓN. MONITORIZAR, CORRELACIONAR, Y DOTAR DE INTELIGENCIA LA DETECCIÓN SERÍA EL SIGUIENTE PASO NATURAL. LA FINALIDAD ÚLTIMA, LIMITAR EL DAÑO, RECUPERAR Y RESTABLECER LA OPERATIVA NORMAL, NEUTRALIZANDO LAS AMENAZAS Y EXTRAYENDO LECCIONES DE LO SUCEDIDO.

Como propuesta de mínimos, se deberían abordar las siguientes actuaciones, como una forma de aproximación, ya que existen múltiples **SOLUCIONES**:

- Establecer un Marco de Seguridad con políticas, normas y procedimientos de seguridad, aplicables tanto de forma individual a los elementos de la infraestructura, como al conjunto de procesos que soportan los servicios ofrecidos por la **Smart City**, considerando la seguridad como una parte fundamental en el ciclo de vida de diseño, implantación, gestión, mantenimiento y baja de la misma. Este Marco de Seguridad deberá ser implantado y actualizado, realizando auditorías periódicas de seguridad y del grado de adecuación al mismo, para acometer las medidas correctoras y realizar su seguimiento
- Establecer procedimientos, así como medir, analizar y definir los umbrales normales de respuesta y operación de los elementos involucrados, para detectar anomalías que puedan incidir en la seguridad
- Exigir a fabricantes e integradores que incorporen la ciberseguridad como uno de los pilares básicos de actuación. La industria de la ciberseguridad deberá enfrentarse al reto que supone asumir el coste de unos recursos que deben ser proporcionales a la infraestructura del atacante
- Dotarse de pólizas de Ciberseguros, ya que a diferencia de los países más avanzados en este sentido, la mayoría de organizaciones españolas no disponen de ciberseguros que cubran los daños reputacionales y económicos asociados a un ciberataque

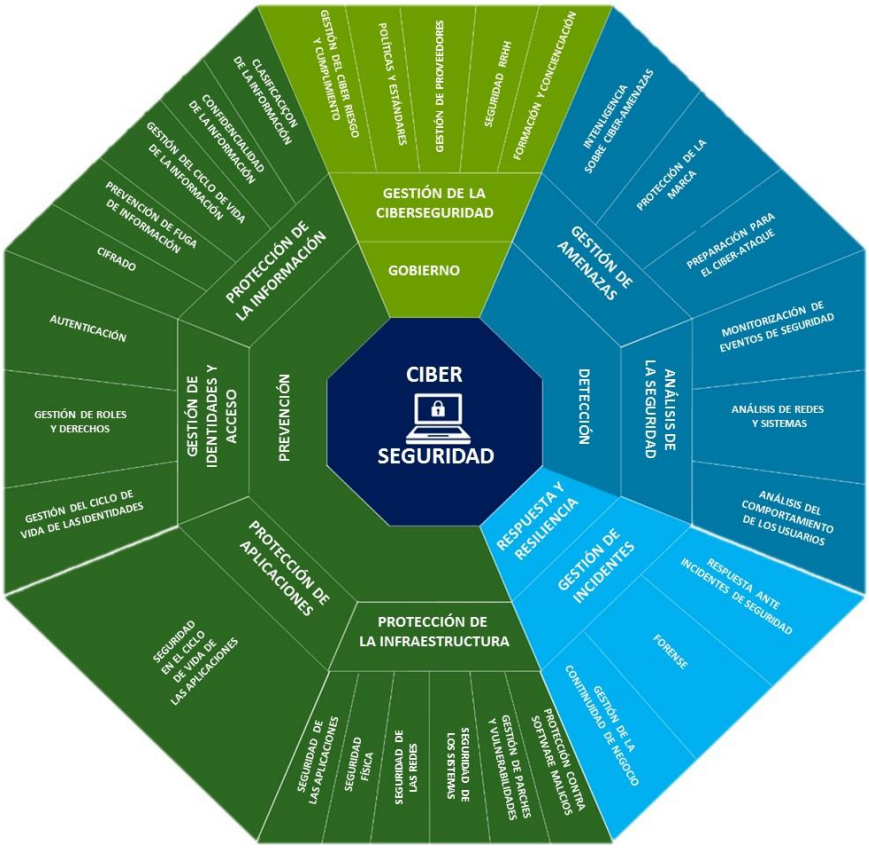
Como conclusión, los vectores de ataques se incrementan rápidamente, así como su complejidad. Y, en el caso concreto de aquellos dirigidos a la Smart City, irán ganando en importancia y repercusión, pudiendo llegar a convertirse en el talón de Aquiles de su desarrollo.

En el siguiente capítulo, ofrecemos una aproximación a un modelo de cibercapacidades, que pensamos que debería ser analizado en profundidad, que debería estudiarse de forma exhaustiva para su adaptación a las necesidades específicas de las Smart Cities.

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

5. MODELO DE CIBERCAPACIDADES Smart City

El **MODELO DE PROVISIÓN Y PRESTACIÓN DE SERVICIOS DE SEGURIDAD TIC** asociado a la **SMART CITY** podría estructurarse en 29 capacidades agrupadas por dominios. Además de las áreas clásicas de la seguridad IT, estas capacidades reflejan dominios más modernos y asociados con los conceptos de ciberseguridad y ciberresiliencia.



G **Gobierno** de la organización para gestionar los riesgos implantando estructuras de gobierno que permitan mantener y evolucionar sus capacidades de ciberseguridad

D **Detección** de las amenazas mediante el uso de las múltiples fuentes de ciberinteligencia con el fin de poder gestionarlas proactivamente

P **Prevención** frente a ciberataques manteniendo las inversiones y mejorando las medidas para proteger sus activos de información digitales

R **Respuesta y Recuperación** adecuadas ante un ciberataque exitoso, con el fin de poder limitar su impacto sobre la organización

Unión Europea
Fondo Europeo de Desarrollo Regional
JUNTA DE ANDALUCIA

6. GLOSARIO DE TÉRMINOS

- ***Trazabilidad:*** *principio de seguridad que determina el nivel de registro sobre las operaciones realizadas en un sistema de información*
- ***Confidencialidad:*** *principio de seguridad que determina que solo usuarios, sistemas o procesos autorizados que tengan acceso a la información*
- ***Integridad****: principio de seguridad que determina que la información es procesada correctamente y no ha sido modificada sin autorización*
- ***Disponibilidad****: principio de seguridad que determina que la información estará disponible cuando los usuarios, sistemas o procesos lo precisen*
- ***Autorización****: principio de seguridad que determina los recursos a los cuales un usuario está autorizado a acceder, así como determinar el tipo de acceso que tendría*
- ***Protocolo SSL:*** *un conjunto de reglas que definen cómo se transmiten e interpretan datos a través de un medio*
- ***SSL*** *(Secure Socket Layer)*
- ***Vulnerabilidades:*** *eventos que afectan a los sistemas de información, tales como equipos informáticos, servidores, máquinas virtuales, programas o aplicaciones, sistemas operativos, etc.*
- ***Botnets:*** *conjunto de redes de sistemas, equipos y dispositivos que son utilizados con el objetivo de ejecutar actividades maliciosas*
- ***Spyware y Adware:*** *herramientas que exceden su cometido legítimo, de forma que realizan acciones intrusivas de cara al usuario y su actividad*
- **Exploit:** software cuyo fin es explotar aquellos errores de desarrollo de programas, *aplicaciones, así como los errores de configuración de los sistemas*
- ***Ingeniería social:*** *ataques basados en convencer a un ciudadano para realizar una actividad determinada que afecte a la seguridad de los sistemas, sin que conozca el posible impacto de la acción que está realizando*
- ***Ransomware:*** *software malicioso cuyo fin es comprometer el principio de disponibilidad de la información y los sistemas*
- ***Bankers:*** *software especializado en comprometer la disponibilidad de la información y los sistemas bancarios*
- ***Keyloggers:*** *software cuyo fin es registrar las pulsaciones que se realizan sobre un teclado, con objeto de conseguir información relevante, por ejemplo, credenciales de accesos*
- ***BackDoor:*** *punto de acceso a los sistemas comprometidos por esta vulnerabilidad, que permite a un atacante acceder a los mismos y transferir información hacia el exterior*
- ***Zero-Day:*** *vulnerabilidad software para la cual el fabricante o desarrollador del mismo aún desconoce la vulnerabilidad o no ha conseguido resolverla*

- ***SSL:*** *(Secure Socket Layer) protocolo utilizado en las comunicaciones de red*
- ***INCIBE:*** Instituto Nacional de Ciberseguridad de España, sociedad dependiente del Ministerio de Energía, Turismo y Agenda Digital (MINETAD) a través de la Secretaría de Estado y para la Sociedad de la Información y Agenda Digital (SESIAD). Es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos