

Privacidad y seguridad en Internet

A la hora de hablar de privacidad y seguridad en Internet, debemos conocer las tendencias a corto, medio y largo plazo, para saber cómo van producirse ciertos cambios. Actualmente existe un mapa de tendencias tecnológicas centrado en tres ejes significativos: *Bigdata*, *Cloud Computing* y el llamado Internet de las Cosas (IoT). La irrupción de estas nuevas tendencias tecnológicas en la vida digital de usuarios, empresas o administraciones deben ser aprovechadas por ciudadanos, organizaciones y gobiernos para hacer más confiable y segura una Red en la que estamos llamados a confluir.

¿En cuántos servicios y plataformas de la Red o Internet estamos registrados conscientemente? ¿En cuántos otros servicios tenemos una cuenta de usuario



Marcos Gómez Hidalgo

Subdirector de Servicios de Ciberseguridad
Dirección de Operaciones. INCIBE

o están depositados nuestros datos inconscientemente? ¿Cuántas veces hemos aceptado cláusulas legales y de privacidad de aplicaciones (gratuitas o no) sin leernos los términos de uso? ¿Cuántas veces cedemos parte de nuestra identidad digital a un tercero o a varios en cadena? ¿En cuántas plataformas de alojamiento en la nube tenemos depositados nuestros datos e información? ¿Sabemos que cuando hacemos una foto podemos estar publicándola automáticamente casi por defecto? ¿Nos suenan las palabras *opt in* y *opt out*? ¿Y entendemos que son? ¿Y conocemos otras aún más enigmáticas como *double opt in* o por ejemplo *soft opt in*? Todas estas y muchas otras cuestiones son preguntas que afortunadamente nos estamos empezando a hacer y ya nos estamos parando a pensar, porque ya reflexionamos en esa parte de nuestra vida que se ha transformado en ceros y unos, que forma parte del Ciberespacio, de un ámbito en el que no tenemos el control que teníamos antes sobre nuestra información.

Pero hay otra gran pregunta que nos hemos hecho y nos haremos los seres humanos a lo largo de nuestra historia: ¿Por qué estamos aquí? ¿Qué nos ha



Figura 1. Tendencias macro económicas y sociales (1/2)



Figura 2. Tendencias macro económicas y sociales (2/2)

traído o nos ha llevado a esta situación? Y siempre tendremos una buena respuesta para estas cuestiones, que es -básicamente- la constante evolución y el ánimo de innovación de nuestra raza, de la humanidad, de mejorar nuestra situación actual, y dejar un mundo mejor para nuestros hijos. Podemos, en muchas ocasiones, echar un vistazo al pasado y sacar rápidas y potentes conclusiones de cómo y por qué hemos llegado a este momento, a un momento crucial en lo social, lo económico, lo tecnológico, que muchos llaman la transformación digital, pero que quizás nadie sabe definir de una

manera sencilla, sobre todo porque estamos desgastando ya un concepto que está recientemente acuñado, abusando del mismo o aplicándolo en todo a discreción. Y otro “pero” más, que es la transformación de la propia cuestión o pregunta, el saber con más certeza qué va a ocurrir, cuál es la tendencia o tendencias futuras en el corto, medio y largo plazo que van a determinar los siguientes pasos en todos los ámbitos mencionados. Concretamente desde INCIBE hemos realizado en el ámbito tecnológico o de las TIC un potente estudio de tendencias en el mercado de la ciberseguridad, en el

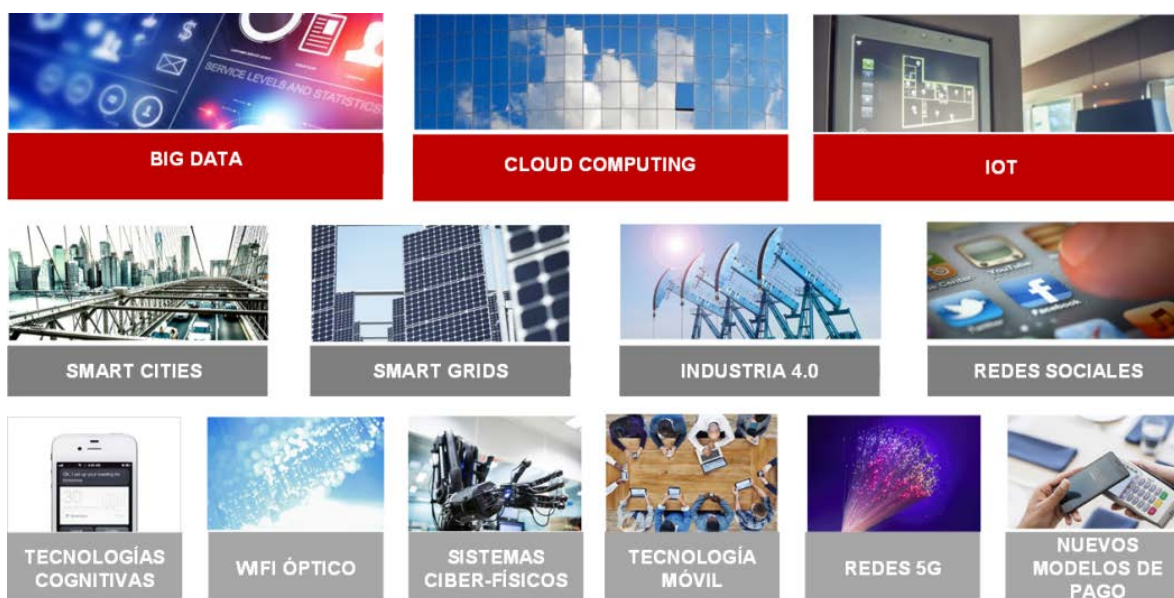


Figura 3. Tendencias TIC

que hemos tenido en cuenta una serie de macro tendencias sociales y económicas (80 tendencias), más de 10 tendencias TIC, y más de 30 tendencias en necesidades de ciberseguridad estudiadas, que han dado lugar a un mapa de tendencias en ciberseguridad que nos marcarán los próximos años.

Un estudio en profundidad de la situación económica y social actual y su dependencia de las TIC ha configurado un mapa de tendencias tecnológicas que se centran en tres ejes muy significativos de lo que está aconteciendo:

- ▶ **Big Data:** Cada día se generan más de 2.5 quintillones de bytes. Transformarlos en conocimiento es la principal vía de innovación. El gasto TIC mundial en Big Data alcanzará los 55.000 M\$.
- ▶ **Cloud Computing:** como componente esencial para incrementar las capacidades de las tecnologías móvil, y la analítica y procesamiento de datos. Esta tecnología es ya utilizada por un 41% del tejido empresarial e institucional español.
- ▶ **Internet de las Cosas (IoT):** hoy en día tenemos ya más de 28.000 dispositivos conectados a Internet, y en cinco años, habrá más de 50.000 millones. La aplicación de esta tendencia TIC es en todos los sectores y ámbitos de actividad, es lo que se conoce también como Smart Anything.

En un nivel secundario, pero altamente dependiente de estas tres tendencias, tenemos temas tan importantes como las *Smart cities*, *Smart grids*, Industria 4.0, redes sociales, tecnologías cognitivas, redes 5G, tecnologías móviles, nuevos modelos de pago, etc.

Finalmente, el ejercicio de esta investigación ha dado lugar a la configuración de un mapa de tendencias en el mercado de ciberseguridad que marcará con alta probabilidad los siguientes pasos en este ámbito.

En todas las tendencias analizadas podemos encontrar (para ciudadanos, empresas e instituciones o gobiernos) que la información es el principal activo, el activo más crítico o esencial, desde datos alojados en servicios de la Administración Electrónica, pasando por los transaccionales, o los más sensibles relativos a ámbitos médicos o sanitarios pero también en los relativos a la I+D+i.

Y si ahora cambiamos el plano de estudio de las tendencias, y nos movemos hacia el de los riesgos y amenazas solo tenemos que mirar brevemente que está pasando hoy en día en cuanto a ciberataques. Para ello, como referencia, os invito a que sigáis periódicamente la Bitácora de Ciberseguridad de INCIBE que recoge en cada momento los hechos más destacados relativos a la actividad de ciber-

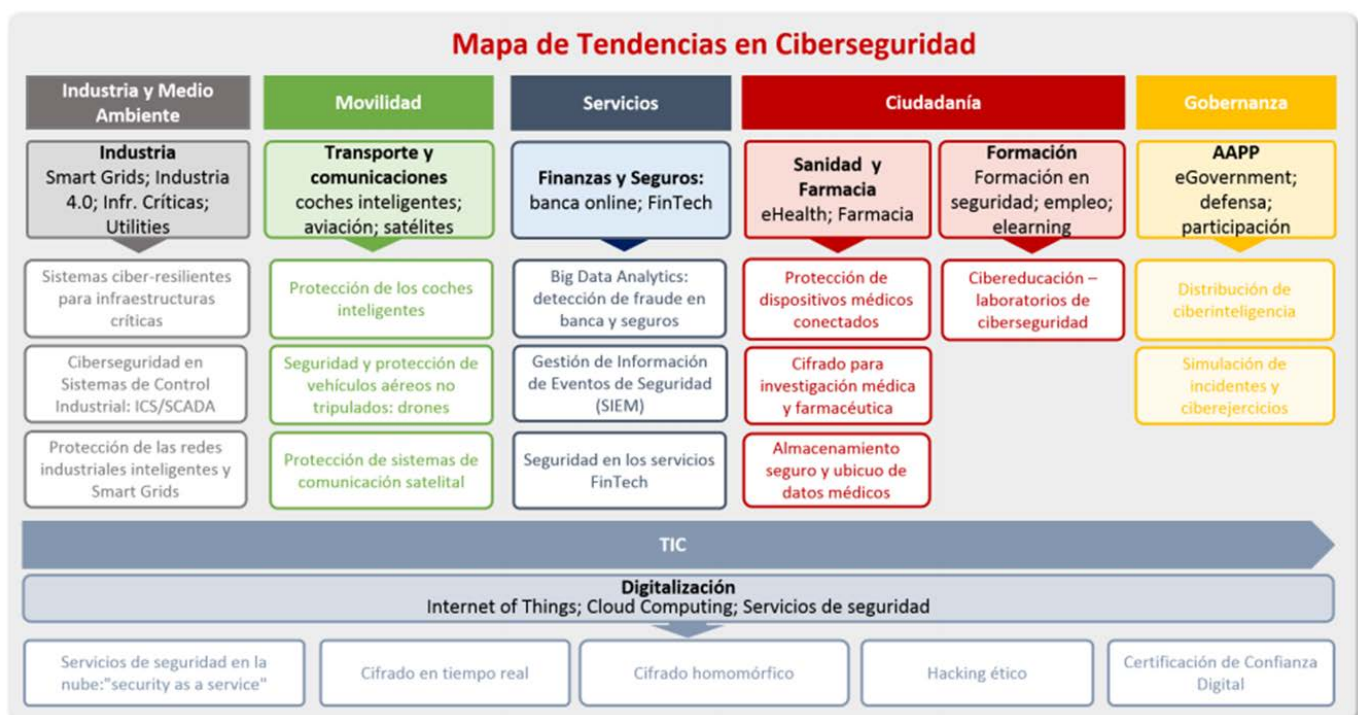


Figura 4. Mapa de Tendencias en Ciberseguridad

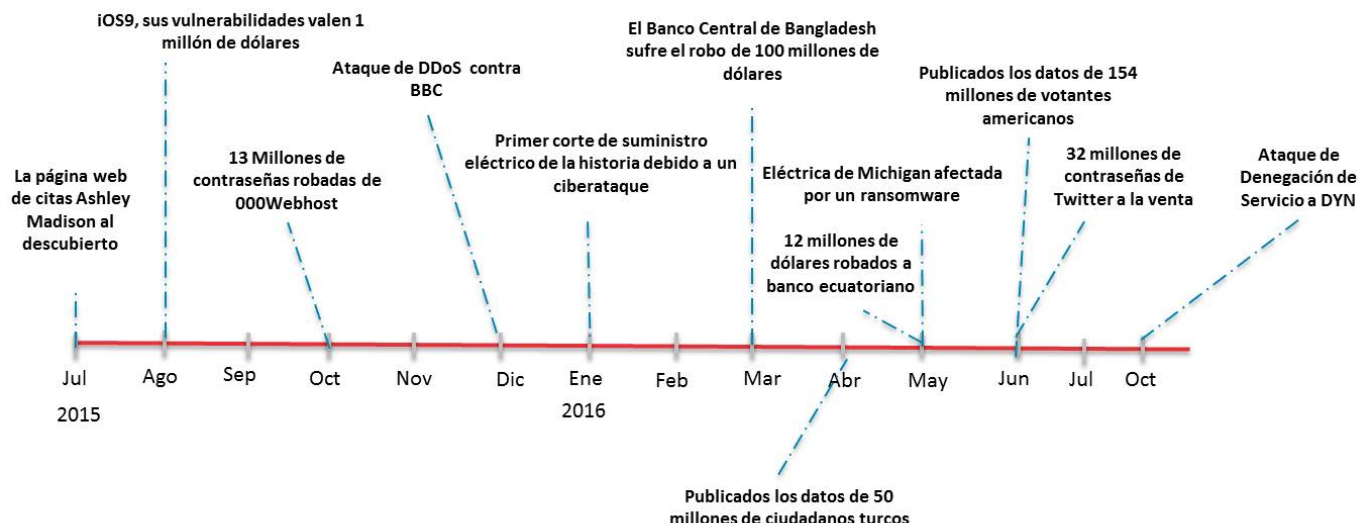


Figura 5. Bitácora de Ciberseguridad de INCIBE 2015-2016.

criminales, ciberterroristas, y ataques a empresas, gobiernos, instituciones, ciudadanía. Sin ir más lejos, en los dos últimos años analizando más de 200 hechos relevantes las principales ciberamenazas se centran en:

- ▶ Los ataques a la privacidad, con robos y fugas de información, incluyendo los intentos de exfiltración y robo de patrimonios, también el tecnológico y la I+D.
- ▶ Las extorsiones a grandes corporaciones o ataques de denegación de servicio a importantes infraestructuras de la Red, incluyendo también otros sectores críticos como la energía y subsectores, el transporte o el ámbito económico y financiero.
- ▶ El robo de importantes sumas de dinero, a través de clásicas estafas o campañas de fraude electrónico o la intrusión en sistemas y redes de grandes entidades bancarias o financieras.

Estas tendencias de ataques, amenazas cibernéticas y riesgos no hacen de la Red o del Ciberespacio un lugar inseguro o en el que desconfiar, pero sí un síntoma de otra actividad tradicional del ser humano: aprovecharse de una situación para buscar una oportunidad de lucro o de causar un impacto o perjuicio en otros, y por lo tanto es otra tendencia que sin duda alguna hay que tener en cuenta para establecer nuevas políticas, normativas, procedimientos, buenas prácticas, desarrollar una cultura de seguridad y ciberseguridad dinámica, impulsar la colaboración público privada a nivel nacional y a nivel internacional, etc.

Si nos centramos en la privacidad, y en la ciberseguridad en el entorno de Internet, y lo hacemos además en los

dos sectores más afectados por estos riesgos y amenazas, (la ciudadanía y el sector empresarial), estamos ante un panorama muy prometedor, que se inició ya en 2012 y 2013 con:

- ▶ La Agenda Digital para Europa, su homónima en España con la Agenda Digital para España y el Plan de Confianza en el ámbito Digital.
- ▶ La aprobación de la Estrategia Nacional de Seguridad y su importante capítulo de Estrategia Nacional de Ciberseguridad.
- ▶ El acuerdo de la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (recientemente renombrada Secretaría de Estado de Sociedad de la Información y Agenda Digital, SESIAD) del Ministerio de Industria, Energía y Turismo (recientemente también renombrado Ministerio de Energía, Turismo y Agenda Digital), que ha dado lugar al CERT de Seguridad e Industria, operado y coordinado conjuntamente por INCIBE y la OCC y CNPIC.
- ▶ La aprobación de la Directiva Europea NIS, aprobada en 2016 y en proceso de transposición, con la incorporación de la obligación, entre otros temas, de comunicación de incidentes de ciberseguridad por parte de los prestadores de servicios digitales.
- ▶ La Directiva de Privacidad y Comunicaciones Electrónicas aprobada en 2016 y en proceso de transposición, con un nuevo Reglamento Europeo de Protección de Datos.

Sobre las “primeras necesidades” se identifica en todas estas acciones estratégicas y políticas, aunque



Figura 6. Guía de Privacidad y Seguridad en Internet. INCIBE y AEPD.

también organizativas y procedimentales, dos con un carácter crítico y transversal, que son -por un lado- la protección de las infraestructuras críticas, por su alta dependencia de las TIC, y asegurar así la prestación de los servicios esenciales, expuestos hoy en día a los ciberataques y más con la llegada de la Industria 4.0. Y -por otro lado- seguir impulsando y fortaleciendo la cultura de ciberseguridad en todos los estamentos, haciéndola más ciberresiliente a los ciberataques, que se siguen perpetrando hoy en día a través de la ingeniería social. Es decir: según esto último, el eslabón más débil sigue siendo el ser humano, la persona, tanto una que opera un sistema de control industrial, como el que accede a su cuenta en una red social, lee una noticia en un foro de Internet o se conecta a Internet usando su dispositivo móvil. Atención importante hemos de tener con nuestros jóvenes y menores, en los que algo que “está empezando” (aunque ya lleva tiempo entre nosotros), ciberacoso, sexting y sextorsión, pornografía en la Red y pederastas digitales, etc., no puede, ni debemos

permitirlo, en una lacra para que esta parte de la humanidad que ha nacido con la tecnología ya incorporada a sus vidas, no le tenga miedo a las tecnologías, o por lo menos que hagan un uso seguro y responsable de las mismas, porque ellos son al fin y al cabo nuestro futuro inmediato.

Volviendo al principio o al final recientemente comentado, la irrupción de nuevas tendencias tecnológicas en la vida digital de empresas, usuarios y administraciones, y llamémosle lo que queramos: movilidad, wifi óptico, wereables, o los drones, o las redes de contactos de adultos, o los coches inteligentes, smart grids... o en el ámbito de los ciberataques, los ransomwares y ciberextorsiones, el hacktivismo, exposición de bases de datos de usuarios y contraseñas, denegaciones de servicio..., estamos ante un reto, un desafío, y una gran oportunidad, que debemos aprovechar, los ciudadanos, las empresas, y los gobiernos, para hacer más confiable y segura una Red o un Ciberespacio en el que vamos a convivir sí o sí, y como en muchas ocasiones la educación es lo primero. Por ello, cualquier acción es positiva y suma, como la publicación reciente de la Guía de Seguridad y Privacidad de INCIBE y la AEPD¹, donde se recogen todos estos temas de actualidad, y en definitiva un kit de primeros auxilios para enfrentarnos a situaciones en la Red, y poder resolverlas con unas pautas mínimas de seguridad y cuidado de nuestra privacidad.

Si disponen de dos horas, y no hace falta que sean seguidas, les animo a que si todavía no disponen de parte de esa cultura de ciberseguridad, se pongan al día con esta información, y nos sigan en www.incibe.es y www.osi.es (y nuestras redes sociales) para estar al corriente y disfrutar de la Red y el Ciberespacio con todas sus ventajas y, al menos, con pocos inconvenientes.

¹ <https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet>

Internet Privacy and Security

We must know the technological trends on matters of internet privacy and security, in order to face the challenges of digital transformation, always respecting

fundamental rights and striving to make Cyberspace a trustworthy and safe place. Information is a fundamental asset for citizens, companies and institutions, which

is why protecting these rights poses a great challenge for professionals within our sector, who without a doubt will be capable of tackling it.