Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

# *Informe de divulgación*

# *Predicciones sobre amenazas para 2016*

| | |
|---|---|
| Tipo de documento: | *Informe* |
| Autor del documento: | *AndalucíaCERT* |
| Código del Documento: | *CERT-IF-9776-160128* |
| Edición: | *0* |
| Categoría | *Uso Interno* |
| Fecha de elaboración: | *28/01/2016* |
| N° de Páginas | *1 de 13* |

# 1 TABLA DE CONTENIDOS

## 2 OBJETO

Es objeto de este documento es dar a conocer las predicciones de industrias referentes en el mundo de la seguridad, como los principales antivirus, de aquellos riesgos y amenazas que afectarán en este año 2016, basándose en la evolución de estos últimos años y las nuevas tecnologías que están apareciendo y que requerirán un apartado de seguridad para poder seguir evolucionando.

## 3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía. Debe contemplarse como una visión general de aquellos temas que puedan afectarnos a lo largo de este año 2016.

Por otro lado, aclarar que estos informes no tienen un acierto absoluto sobre sus predicciones pero sirven para estar al tanto de cómo van evolucionando los distintos riesgos y estar preparados para tomar medidas y acciones ante ellos.

## 4 SITUACIÓN

Hoy en día el mundo de la seguridad crece a un ritmo vertiginoso debido a la gran demanda, ya que aparecen nuevas tecnologías, ataques, malwares o fallas de seguridad que afectan a nivel global, hacen de la seguridad un desafío y una tarea cada vez más importante, desde el sector de los negocios hasta los gobiernos pasando por los usuarios particulares a nivel global.

Los éxitos y fracasos de incidentes de ciberseguridad nos enseñan lecciones importantes y nos proporcionan pistas de lo que podría suceder en el futuro. Si se repasan dichos incidentes y analizan la evolución de las nuevas tecnologías se puede obtener una perspectiva de futuro.

En este último año se ha vivido una intensa lucha contra aquellas botnets de cibercrimen y el incremento exponencial de malware para dispositivos móviles. Ya se ha hablado en estos años atrás del *Internet de las Cosas* (IoT) pero es ahora cuando está más presente que nunca, no solo en el ámbito particular con televisiones, relojes, automóviles y otros dispositivos inteligentes, sino en industrias, empresas y gobiernos.

A lo largo de este artículo se podrán ver una serie de puntos que intentarán abarcar aquellos temas más relevantes en el mundo de la Seguridad de la Información para este 2016. Se tocarán puntos que han estado muy presente en este año pasado como los Ransomware, seguridad en dispositivos de movilidad, peligros en la web para los menores e incluso los riesgos que están apareciendo con los aviones no tripulados.

## 5 INTERNET DE LAS COSAS

A día de hoy la interconexión de millones de dispositivos de toda índole intercambiando información supone grandes y novedosos desafíos para la comunidad de la seguridad. Cada vez hay más dispositivos conectados a internet y son más accesibles por lo que la superficie de ataque está creciendo. Según un informe de consultoras actualmente existen cerca de 5 mil millones de dispositivos conectados a Internet y se estima que serán sobre los 25 mil millones en 2020.

Las empresas y gobiernos invierten en este sector, para mejorar la vida de la población, pero aún existen barreras que impiden que se profundice en el cambio y aceptación de nuevos dispositivos para bienes y servicios dentro de esta nueva revolución industrial. Entre estas barreras las dos más importantes son la *financiación* y *poder garantizar la protección y seguridad de los datos intercambiados*. Por ejemplo, dos casos que puedan ayudar a entender cómo de importante es este problema, podrían ser:

- El control remoto desde internet de vehículos puede provocar ante fallos o ataques la manipulación de los mismos con los desastres que ello conllevaría.
- *Wearables* para que los padres localicen la posición de sus hijos puede provocar el rastreo de los mismos por parte de terceros.

Por ejemplo, este año apareció el Apple Watch que, durante un tiempo, tuvo una vulnerabilidad que permitía reiniciarlo usando una conexión remota y, posteriormente, conectarlo a otro iPhone saltándose de esta forma el PIN de seguridad y obteniendo toda la información del mismo.

En la actualidad el gobierno alemán está trabajando con la Agencia Europea de Seguridad de la Información y las Redes (ENISA) para ayudar a desarrollar buenas prácticas en las infraestructuras críticas inteligentes emergentes.

En resumen, en 2016 seguirán apareciendo desafíos de seguridad que permitan asegurar la privacidad, seguridad y confidencialidad de usuarios, empresas y gobiernos al usar estos nuevos dispositivos interconectados a través de internet.

## 6 RANSOMWARE

Hablar de ransomware es hablar del malware que más dolores de cabeza ha traído tanto a empresas como a usuarios desde equipos personales. El objetivo de este malware es cifrar todos aquellos archivos que pueda dentro de un equipo o servidor, y posteriormente, mostrar un mensaje en el que se propone el intercambio de la clave de descifrado de toda esa información a cambio de dinero, lo que viene a ser un secuestro (*ransom*).

En este último año este malware ha tomado mucha relevancia en el campo de la seguridad debido a la ganancia que los cibercriminales obtienen de estas campañas maliciosas. Se puede utilizar el *Ransomware as a Service* (*RaaS*) a través de una herramienta llamada *Tox* que permite la creación de distintas variantes de este malware sin necesidad de tener conocimientos avanzados sobre el mismo, e incluso se ha publicado

*Hidden Tear*, el primer ransomware de código abierto abriendo una nueva ventana al desarrollo de variantes creando malware más sofisticado y masivo.

CryptoLocker o CTB-Locker han sido este año dos de los ransomwares más explotados. También se lleva un tiempo combatiendo contra los ransomware de los dispositivos Android (Sistema Operativo más usado), actuando de la misma forma, cifrando los datos personales del usuario y pidiendo un rescate a cambio.

Para este 2016, en relación con el punto anterior del internet de las cosas, se prevee que será uno de los objetivos del ransomware. Poder crear malware para realizar "secuestros" de relojes, televisiones inteligentes, automóviles... no está muy lejos, incrementándose las posibilidades cuando dichos dispositivos utilizan Android como sistema operativo.

Podemos resumir en que se busca el mismo objetivo pero en más tipos de dispositivos. El desafío recae en garantizar la disponibilidad de la información, además de la detección y eliminación de este tipo de ataques. Buenas prácticas en la configuración de los dispositivos hacen que sea más complicado corromperlos con malware y así conseguir que los usuarios puedan disfrutar de la tecnología actual de forma segura.

# 7 ATAQUES DIRIGIDOS

Desde hace unos años se están reportando ataques con el término APT (*Advanced Persistent Threats*) que no se comportan como una campaña que intenta afectar al mayor número de usuarios posibles sino que se dirigen a algún objetivo más específico, llegando a convertirse en uno de los mayores desafíos a los que una organización se puede enfrentar en términos de Seguridad de la Información.

Durante este año pasado, ha habido ciertos ataques que generaron gran controversia en base a la información que se filtró. El más claro ejemplo fue el de *Hacking Team que filtraron desde sus servidores* 400GB de información, aproximadamente, generando gran revuelo respecto al listado de clientes y herramientas que la empresa comercializaba. De la misma forma el caso de la filtración de los clientes del servicio *Ashley Madison* ha causado un enorme impacto.

Campañas específicas contra servidores web u otros servicios que estén disponibles en la web son objetivos de cibercriminales para dar fuerza a sus ataques y pasar desapercibidos teniendo sus actividades en dichos equipos durante el mayor tiempo posible. Aunque en la mayoría de los casos no lleguen a salir a la luz, los mayores ataques dirigidos los mantienen los gobiernos buscando obtener información de otros.

¿Se consideran entonces las APT un arma del futuro o se verá decrementado su uso en estos próximos años?. No se puede predecir cuándo una empresa u organismo será objetivo de un ataque dirigido, por ello los correspondientes equipos de seguridad deben proteger la información que reside en sus organismo de todo tipo de ataques, sean dirigidos o no. No solo debe protegerse un organismo a nivel perimetral, ya que se detecta que la protección de los equipos finales y el cifrado de la información importante son medidas que no se suelen encontrar en la mayoría de las organizaciones.

En 2016 seguirán apareciendo reportes de APTs contra empresas, gobiernos o personas individuales, por lo que se deberá seguir invirtiendo en seguridad y formación intentando evitar en toda medida de lo posible el acceso a la información.

Llegados a este punto es necesario hablar de la *Haxposición*, que es el término usado para definir lo mencionado anteriormente con el caso de *Hacking Team*, en el que se combina el robo de datos mediante ataques informáticos y la divulgación pública de la misma. Publicar información corporativa en las redes sociales hace que esta se distribuya a nivel mundial en minutos provocando caídas en picado del valor corporativo (caso dieselgate o Volkswagen) con implicaciones legales sobre privacidad y protección de datos personales.

Es muy difícil saber cómo evolucionará este tema en 2016, pero si es verdad que si las empresas consiguen evitar este tipo de ataques y trabajan junto con la policía para llevar los responsables ante la justicia, podría ser un elemento de disuasión. Por otro lado, los secretos empresariales arriesgados o el afán de los cibercriminales de actuar cómo árbitros de la justicia pueden provocar un incremento de búsquedas de secretos y exponerlos públicamente.

## 8 DISPOSITIVOS MÓVILES

Los principales riesgos en este punto siguen siendo los mismos que hasta ahora, la pérdida de dichos dispositivos o la instalación de aplicaciones maliciosas. Pero existe una diferencia, cada vez se dispone de información más sensible en estos tipos de dispositivos como podría ser los datos bancarios para pagar con el móvil en los establecimientos, por ejemplo.

En estos años anteriores se descubrieron distintas vulnerabilidades que permitían, por ejemplo desbloquear un dispositivo que había sido bloqueado por pérdida o robo, o llegar a comprometer cuentas de redes sociales gracias a una vulnerabilidad de los navegadores. También apareció el tan conocido Virus de la Policía pero orientado a Android. Ransomwares y algunos troyanos bancarios han traído también dolores de cabeza a los usuarios.

Un factor muy importante en este último año vuelve a ser la ingeniería social, utilizando servicios de mensajería como Whatsapp o Facebook para aumentar el alcance de las campañas de malware multiplataforma. Se tiene que seguir teniendo en cuenta que para los códigos maliciosos, si se trata de un dispositivo que ha pasado por una fase de *Jailbreak* o *rooteado*, es más fácil llegar a adquirir los permisos de administrador necesarios para ejecutar comandos sin la autorización del usuario. También pierden el mecanismo de actualizaciones soportado nativamente por la plataforma, por lo que no podrán beneficiarse de actualizaciones o parches de seguridad que se vayan lanzando, dejando al equipo vulnerable.

Merece ser mencionada la falla que más se ha hecho notar, la plataforma *Stagefright* que podía permitir a un atacante robar información del dispositivo a través de un código ejecutado de manera remota con tan solo enviar un SMS preparado, dejando vulnerables a 950 millones de usuarios de Android. De la misma forma, se detectaron en las tiendas oficiales aplicaciones con malware en su interior que los usuarios se podían descargar y no habían sido detectadas.

Entonces, con todo lo que ya hemos andado sobre seguridad en estos años atrás, ¿Cuáles serán las tendencias en los próximos años?. Tal y como se había comentado en los primeros puntos de este documento, el internet de las cosas será uno de los principales objetivos, por lo que es muy importante corregir todo lo posible en sistemas móviles y crear buenas prácticas para no caer en los mismos errores con el otro punto.

Los nuevos métodos de pago suscitarán el interés de los ciberdelincuentes (ya sean en tarjetas de crédito con tecnología *EMV* o el monedero digital) y las plataformas de pago supuestamente "seguras" quedarán en entredicho.

No todo son malas noticias, en estos dos últimos años se ha conseguido un gran avance en el uso de tecnologías biométricas. Se espera que siga creciendo de forma significativa en los principales sectores de la industria de desarrollo con autenticaciones biométricas como FIDO y TouchID, ya disponibles en dispositivos móviles de gama alta. El consumidor obtiene una mejor seguridad no solo en el desbloqueo del terminal sino en las compras y pagos por ejemplo. Esta evolución se está trasladando a las empresas pudiendo comenzar a ver una reducción en la dependencia de las contraseñas.

Se prevé un crecimiento exponencial del malware móvil auspiciado por el comportamiento relajado de usuarios no concienciados. Este Malware será cada vez más sofisticado, ya que sus creadores para dispositivos móviles desarrollarán nuevas maneras de complicar el análisis de sus creaciones, haciendo cada vez más difícil analizar las muestras y saber si se trata de código malicioso o no. De esta forma se recupera un punto nombrado en párrafos anteriores en el que si las tiendas oficiales no son capaces de detectar dichos códigos maliciosos podrán llegar a publicarse en las mismas, estando disponibles para millones de usuarios.

## 9 INFRAESTRUCTURAS CRÍTICAS

¿Están a día de hoy todas las empresas e industrias preparadas para afrontar los desafíos venideros?. Desde hace ya unos años empresas e instituciones han empezado a darle importancia a la Seguridad de información en infraestructuras críticas, pero hoy día sigue habiendo evidencias que indican que falta seguir mejorando esta materia.

Aparece en este punto la dificultad, ya sea por presupuesto, personal, tiempo... que sufren instituciones en actualizar sistemas operativos ya obsoletos. Es decir, mucha empresas gestionan infraestructuras críticas con sistemas operativos antiguos, vulnerables y conectados a Internet, aumentando las posibilidades de un incidente. Recordar que tener estos equipos de cara a internet incrementa el riesgo ya que se encuentran disponibles a todas. La política de gestión debe contemplar que el acceso se otorgue solo cuando haya que realizar soporte o que las comunicaciones vayan sobre una VPN.

El uso de Firewalls y otros dispositivos ayudan con al seguridad perimetral, pero esto no nos exime de que se puedan recibir ataques a nuestro organismo de otra forma, como por ejemplo, desde un equipo infectado desde dentro de la propia red. La frase "si funciona, no lo toques" indica que los equipos de seguridad y sistemas no realizan las tareas de mantenimiento correspondientes. Esto presenta problemas de seguridad, ya que la falta de actualizaciones y revisiones de estos sistemas puede generar una falla de los mismos o incluso un acceso indebido por parte de un atacante.

Además del sector industrial, el sector de la salud es uno de los más expuestos. Durante este último año, según el *Reporte de Investigaciones de Fuga de Información de Verizon* se han identificado cerca de 80 mil incidentes de seguridad, 234 relacionados con la salud y 2.100 fugas de información, siendo 141 de este mismo sector. Se ha producido un aumento del 125% en los ataques cibercriminales con respecto a 5 años atrás, siendo los portátiles perdidos o robados la principal causa de fugas de datos.

El estudio de 2015 titulado "*Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*" concluye que la mayoría de las organizaciones no está preparada para responder a nuevas amenazas y no cuenta con los recursos adecuados para proteger la información de los pacientes. No solo hay que tener en cuenta los equipos informático, este año investigadores de seguridad demostraron a través de *Shodan* (rastreador de ordenadores en internet) pudieron encontrar hasta 68.000 sistemas y equipos médicos vulnerables de una misma entidad de salud en EEUU, entre los que se encontraban dispositivos quirúrgicos entre otros.

¿Cómo evolucionará estos problemas a lo largo del próximo año? Para responder a esta pregunta hace falta mirar los errores comentados en estos años pasados. Hace falta mucha concienciación y educación en materia de Seguridad de la Información en empresas y administraciones públicas. Los atacantes intentarán aprovechar cualquier brecha para acceder a esta información. Tal es la importancia de proteger las infraestructuras críticas que, por ejemplo, la Fundación Nacional para la Ciencia de los Estados Unidos ha entregado a la Universidad Cristiana de Texas cerca de 250 mil dólares para ayudar a crear medidas efectivas que protejan los dispositivos médicos de ciberataques. Por el mismo camino se encuentra *ENISA* (Agencia Europea de Seguridad de la Información y Redes) que afirmó que durante 2016 enfocará su atención al desarrollo de buenas prácticas en lo que refiere a "infraestructuras críticas inteligentes emergentes".

Si bien se han realizado algunos cambios en muchas de las industrias buscando mejorar la seguridad, aún falta mucho trabajo por realizar en los diferentes sectores. Para 2016 los ataques a este tipo de infraestructuras podrían incrementarse si no se sigue avanzando de forma rápida en su adecuada protección, por lo tanto todas las actividades vinculadas con la Seguridad Informática en este tipo de escenarios seguirá ganando terreno como un factor clave en la gestión.

## 10 SEGURIDAD EN LA NUBE

Anteriormente las empresas implementaban las redes de forma que los servidores se encontraran en centros de datos o DMZ. De esta forma ha sido más fácil el bloqueo de datos sensibles y controlar cuidadosamente el acceso a los servidores de centro de datos y herramientas de seguridad de la intranet. Hoy en día, muchas organizaciones están migrando los servidores a la nube pasando al Software como servicio (*SaaS* ) en aplicaciones como el CRM, email, compartición de ficheros... Incluso adoptando en la nube aplicaciones de productividad como Microsoft Office 365 y Google para trabajar.

Esta transición seguirá viéndose en gran cantidad de empresas a lo largo de 2016 ya que, además de ahorros en costes, permite un fácil acceso a las aplicaciones de negocio desde cualquier ubicación. Esto supone también nuevos retos en el ámbito de seguridad:

- Una mayor superficie de ataque. Antes era necesario que los atacantes accedieran a la red corporativa antes de que pudieran intentar atentar contra la información o aplicaciones de la misma.

- Es mucho más complicado controlar el acceso a aplicaciones de terceros (SaaS) que a aplicaciones internas ya que normalmente dicha comunicaciones viajan cifradas.
- Control limitado sobre la seguridad ya que la seguridad recae sobre los proveedores de dichas aplicaciones, aunque han sido sometidos a rigurosas auditorías SAS70, ISO27001...
- Aumento del tráfico en el perímetro de la red. El uso de servicios en la nube aumentará la carga sobre pasarelas seguras y servidores de seguridad perimetral. Dado que gran parte de ese tráfico se cifra, las empresas deben asegurarse de que sus dispositivos de seguridad pueden mantenerse al día con la demanda.

## 11 SEGURIDAD Y ATAQUES A DRONES

El crecimiento del sector de aviones no tripulados aumentará en este próximo año, con expectativas de generar más de mil millones en ingresos. Sin embargo, su creciente popularidad introducirá nueva seguridad cibernética y riesgos de seguridad física. Estos drones sirven para multitud de propósitos, desde militares, agricultura, vigilancia o entrega de paquetes por ejemplo. Un ejemplo de un buen uso de los mismos se produjo en unas inundaciones de Chennai, en las que se utilizaron estos drones para localizar y rescatar a 200 ciudadanos atrapados.

Sin embargo estos drones representan también una amplia gama de riesgos, desde la invasión de la privacidad con el espionaje industrial hasta el terrorismo. Por ejemplo, localizando las zonas donde empresas petroleras buscan u obtienen petroleo o para aproximarse a redes WiFi y tener una mejor cobertura para el acceso a dicha red.

Mientras que los drones no suponen una amenaza tan grave como otros ataques cibernéticos, como por ejemplo malware o APTs, los responsables de seguridad de determinados tipos de empresas deberán contemplar a lo largo de este año 2016 los riesgos de seguridad que puedan representar estos aviones no tripulados para la información de su organización.

## 12 LEYES Y REGULACIONES

Cuando nos referimos a la Seguridad de la Información, toda empresa y organismo debe cumplir de forma obligatoria unos requisitos como las legislaciones enfocadas en proteger los datos personales de los usuarios o clientes de la empresa. De la misma forma aquellas organizaciones comprometidas con la protección de la información propia o de terceros, deberían adoptar de forma voluntaria los estándares o normas de seguridad existentes.

Las organizaciones pueden adoptar normativas por iniciativa del propio personal interesado en la protección de la información, o bien por el cumplimiento con algún requisito contractual o regulatorio. Es aquí donde aparecen marcos de referencia o estándares que avalan y certifican las medidas de seguridad adoptadas y adaptadas en las empresas. La mayor referencia continúa siendo la *ISO/IEC 27001*, es un estándar internacionalmente usado para gestionar la seguridad de la información.

En estos últimos años se sigue viendo crecer el número de organizaciones que se alinean con las directrices y buenas prácticas de la ISO27001. En 2014 fueron 23.972 certificados emitidos en todo el mundo,

siendo un 7% más que 2013. Respecto a los países que más se involucran con esta certificación, encabeza la lista Japón seguido del Reino Unido e India. En el mapa representado en la *Ilustración I* puede verse una distribución de las certificaciones emitidas por países.

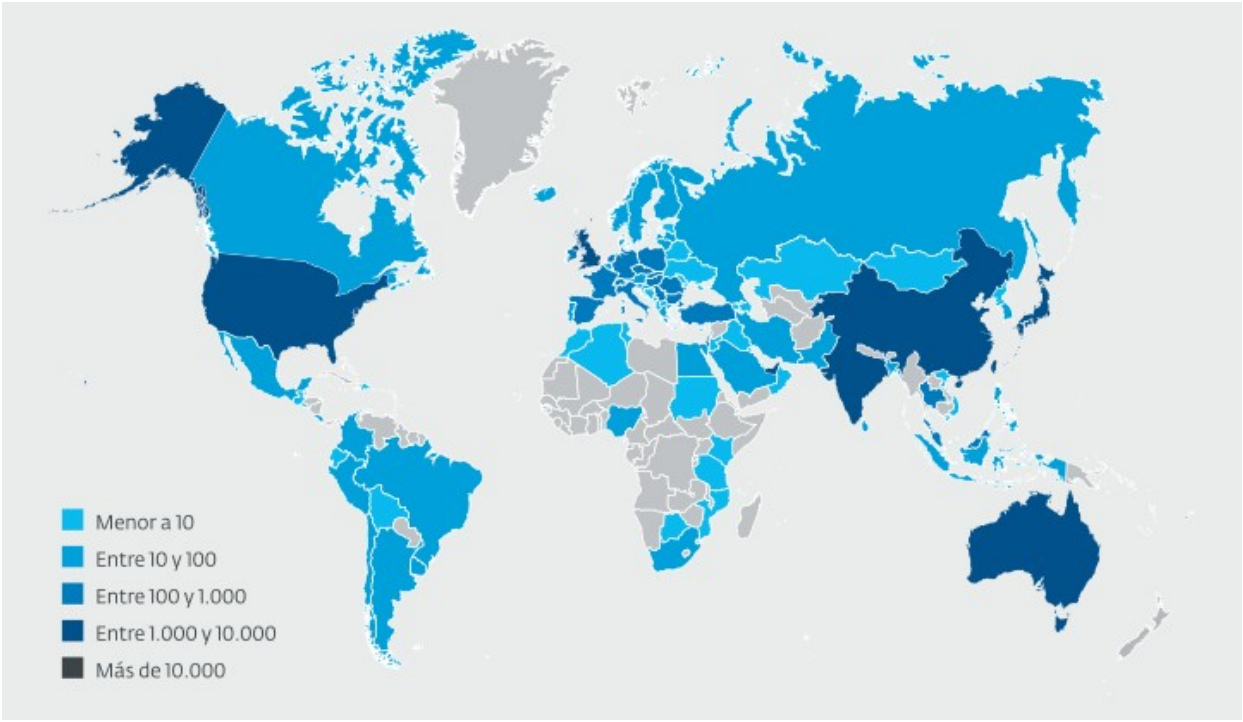


*Ilustración 1: Certificaciones ISO /IEC27001 a nivel mundial. Fuente: ISO*

Si nos centramos en la información de carácter personal, aquella asociada a una persona que permite identificarla, caracterizarla y determinar sus actividades, la legislación europea indica que cada individuo es dueño de su información personal y es quien decide si la comparte o no, así como la forma en la cual debe ser tratada por las entidades que acceden a ella. Entre los datos personales se pueden encontrar datos relacionados con el empleo, características físicas, médicos, bienes que posee, etc.

Es tal la importancia de esta información, que en estos dos últimos años más de 100 países han adoptado leyes de privacidad y protección de datos en posesión de gobiernos y empresas privadas. Otro impulsor de la leyes de protección de datos han sido los negocios. La privacidad se ha convertido en una condición necesaria para el comercio entre países, por lo que el incumplimiento de las normas de protección puede significar la pérdida de oportunidades de negocio.

Tanto para este año 2016 como para años venideros, la premisa seguirá siendo "*La Seguridad de la Información, asociada a la protección de datos y a la privacidad, requiere de los esfuerzos de los gobiernos, empresas y usuarios*".

## 13 AMENAZAS A LOS MENORES EN LA WEB

La interacción entre los menores de edad e internet ha pasado de tener unos horarios de conexión al día a que estos menores "vivan conectados". Cerca del 95% de los adolescentes tienen perfiles en redes sociales, interactuando, compartiendo fotografías e información sobre sus vidas y con mucha probabilidad no todos sus contactos son "amigos".

¿Y cómo afrontan los padres esta situación?. Encuestas revelan que aproximadamente el 50% de los padres no saben lo que hacen sus hijos en internet y uno de cada diez chicos indican que sus padres no conocen las tecnologías que utilizan. Este poco control provoca que los ataques a la privacidad de los menores en Internet emergen como riesgo basado en tres pilares:

- Datos personales
- Datos financieros
- Sexualidad

Es necesario hoy día que la población conozca los siguientes términos:

- *Sexting* - Es el término que se refiere al envío de contenidos eróticos de forma voluntaria por medio de canales digitales.

- *Grooming* – Uno de los delitos con más impacto. Se trata de la labor deliberada de un adulto hacia un menor a través de Internet para lograr que éste realice acciones de índole sexual.

- *Ciberbullyng* – Hostigamiento a través de medios informáticos como redes sociales, chat, correo electrónico o sitios web. Consiste en molestar, amenazar, humillar o acosar a una persona usando estos medios. Según ESET el 90% de estos actos se han visto a través de Redes Sociales.

A lo largo de este año 2016, se verá como la legislación sigue adaptándose a estos tipos de problemas. Los primeros que deberán detectarlo serán los padres, los cambios de conducta o humor en los menores puede ser una señal a tener en cuenta. También seguirán apareciendo *aplicaciones de control parental* (tanto para entornos de escritorio como para móviles), que están comenzando a ser una herramienta indispensable para los adultos ante el creciente uso de las tecnologías por parte de los niños.

En definitiva, la concienciación en conjunto hacia adultos y menores, será fundamental para disminuir la negligencia con la que se abordan en muchos casos estas situaciones que son tendencia hoy día.

## 14 CONCLUSIONES

A lo largo de las anteriores secciones se ha repasado los sucesos y desafíos que la seguridad deberá enfrentar tanto en el 2016 como en los años venideros. Será constante la mayor preparación que van a necesitar los equipos de seguridad de empresas y organismos para afrontar estos retos, de la misma forma que los usuarios particulares deberán aprender a tomar las medidas adecuadas para salvaguardar su información personal. La combinación tecnológica, gestión y educación son cada vez factores más importantes para que usuarios y empresas estén protegidos.

Tener en 5 años cerca de 25 mil millones de dispositivos conectados no debe provocar una paranoia acerca de su privacidad y la seguridad de la información pero si deben estar concienciados. De cara a las empresas y organismos, la implementación de diferentes capas de protección o distintas tecnologías que sean capaces de detectar un ataque en sus diferentes etapas, minimizan la exposición a ser víctimas de casos de fuga de información, exposición de datos, acortando la brecha de exposición y los tiempos de respuesta de cara al incidente.

De cara a las predicciones para el 2016, hay que remarcar que la seguridad de la información no es algo que depende de los avances que logren los cibercriminales en sus herramientas, sino de las medidas que usuarios, gobiernos y empresas adopten para proteger la información, los sistemas y la infraestructura. A pesar de la necesidad de responsables de la protección de datos, menos del 50% de las organizaciones contará con ellos a finales de 2016, siendo cerca del 23% de las empresas encuestadas las que han admitido no tener conocimiento de la legislación aplicable.

Se considera que este año el cifrado, el internet de las cosas, la movilidad y la nube traerán los nuevos retos en seguridad para los responsables de la misma. Para prepararse ante estos riesgos, la empresas deberán implementar una defensa por capas que proteja servidores y equipos finales, independientemente de que estos servidores se encuentren en un centro de datos localizado o en la nube, y que los equipos finales sean ordenadores tradicionales o dispositivos móviles.

2016 será un año más que desafiante, pero no hay que afrontarlo con miedo, sino con una actitud proactiva, ocupándose de todas las aristas de la seguridad recogidas a lo largo de este informe, y poniendo foco en todos los nuevos dispositivos que aparecerán en los próximos años.

## 15 GLOSARIO

*Wearables* : En el mundo de la tecnología, es aquel dispositivo electrónico que se lleva sobre, debajo o incluido en la ropa y que está siempre encendido, no necesita encenderse y apagarse. Por ejemplo los relojes inteligentes.

*FIDO* : De las siglas en inglés *"Fast IDentity Online"*, es un consorcio que apareció en febrero de 2013 para hacer frente a la interoperabilidad de los dispositivos de autenticación y la dificultad de recordar múltiples nombres de usuario y contraseñas. Su objetivo es apoyar una gama completa de tecnologías de autenticación, incluyendo datos biométricos tales como huellas digitales, escáneres de iris, voz y reconocimiento facial.

*TouchID* : Touch ID es una función de reconocimiento de huella digital diseñado y lanzado por Apple Inc, encontrándose actualmente en gran parte de sus dispositivos móviles.

## 16 DOCUMENTACION DE REFERENCIA

- http://www.trendmicro.es/informacion-seguridad/investigacion/previsiones-de-seguridad-para-2016/
- *http://www.fortinet.com/resource_center/whitepapers/2016-predictions-evolving-threat-landscape.html*
- *http://www.theborneopost.com/2015/12/08/symantec-predictions-for-2016-looking-ahead/*
- *https://blog.kaspersky.com/kaspersky-predictions-2016/10801/*
- *http://www.tecnogaming.com/2016/01/eset-lanza-reporte-de-tendencias-de-seguridad-informatica-2016/*
- *https://securelist.com/analysis/kaspersky-security-bulletin/72771/kaspersky-security-bulletin-2016-predictions/*
- *https://www.a10networks.com/sites/default/files/A10-WP-21127-EN.pdf*
- *http://efytimes.com/e1/179930/Press-Release/Sophos-Releases-Cybersecurity-Predictions-For*
- *http://www.slideshare.net/AlertLogic/top-5-cloud-security-predictions-for-2016*
- *http://www.networkworld.com/article/3015442/security/a-few-cybersecurity-predictions-for-2016.html*
- *http://www.ibmbigdatahub.com/presentation/top-12-predictions-2016-leading-cybersecurity-experts*
- *http://blog.imperva.com/2015/12/5-cyber-security-predictions-for-2016.html*
- *http://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-16-security-predictions-for-2016.html*
- *http://www.mynewmarkets.com/articles/182655/experts-predict-top-cyber-threats-for-2016-through-2020*