PANORAMA ACTUAL DE LA CIBERSEGURIDAD

ARTURO RIBAGORDA GARNACHO
Universidad Carlos III de Madrid

Desde hace poco más de 50 años asistimos a una revolución de resultados aún inciertos, pero equiparable a la revolución agrícola, hace más de 2000 años, o la industrial comenzada el siglo XVII. Eso sí, extendiéndose a una vertiginosa velocidad en comparación con aquellas. Esta nueva revolución, que nos ha introducido en la era de la información, o más aún en la era del conocimiento, está propiciada por las tecnologías de la información y las comunicaciones, TIC, y su rasgo distintivo respecto de las anteriores es la rapidez con la que se ha extendido y la profundidad de los cambios que está provocando en todos los sectores empresariales y sociales e incluso en la vida personal de los individuos. Así, resulta difícil encontrar un proceso administrativo, financiero, industrial, comercial, etc. que se siga realizando sin el concurso necesario de las TIC. Y las mismas relaciones humanas están siendo profundamente transformadas por ellas.

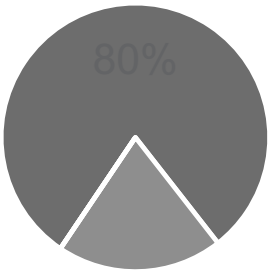
Por ello, dependemos críticamente de los sistemas construidos en base a estas tecnologías, de modo que su inoperatividad o malfuncionamiento, sea accidental o deliberado comporta graves consecuencias para los actores que los sufren. O incluso para la sociedad en general, como sucede con las infraestructuras críticas que soportan, sin posibles alternativas, servicios esenciales que son imprescindibles para el funcionamiento de la sociedad.

No puede extrañar, por consiguiente, que delincuentes de todo tipo traten de hallar vulnerabilidades en las mismas, que explotadas después les permitan obtener pingües beneficios económicos, políticos, propagandísticos o crear sensaciones de inseguridad y terror entre la ciudadanía.

Así, en Europa, según el Informe del Estado de la Unión 2017 (1), el 80% de las compañías europeas sufrieron al menos un incidente de seguridad en 2016 (Figura 1) y estos incidentes en el sector industrial crecieron un 38% respecto de 2015 (Figura 2). Además, en algunos Estados miembros el año 2016 el 50% de todos los delitos son ya Ciberdelitos (Figura 3), habiéndose multiplicado por cinco en los últimos cuatro años [1].

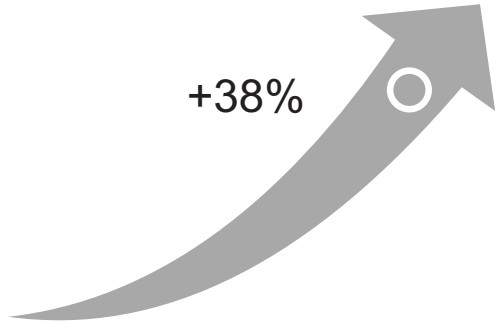
Este imparable incremento de los ciberdelitos trae causa no solo en los elevados beneficios que reportan con una escasa inversión, sino también por la confianza que da a los ciberdelincuentes el saber que las correspondientes infracciones penales son de enorme dificultad probatoria y por tanto gozan de una elevada probabilidad de impunidad.

FIGURA 1
EL 80% DE LAS COMPAÑÍAS EUROPEAS SUFRIERON UN ATAQUE EN 2016



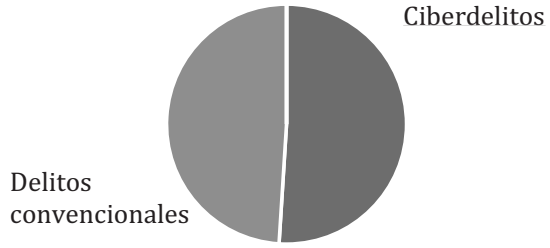
Fuente: (1)

FIGURA 2
INCREMENTO DE LOS ATAQUES AL SECTOR INDUSTRIAL RESPECTO DE 2015



Fuente: (1)

FIGURA 3
CIBERDELITOS VS. DELITOS CONVENCIONALES EN ALGUNOS PAÍSES EUROPEOS



Fuente: (1)

DEFINICIÓN DE LA CIBERSEGURIDAD

Antes de ahondar en el tema del artículo, parece lógico definir con precisión el término ciberseguridad y diferenciarlo de su pariente próximo, seguridad de la información.

Desde la década de los noventa del pasado siglo, se ha venido definiendo la seguridad de la información vinculándola a tres propiedades de la misma (también conocidas como dimensiones): la confidencialidad (que la información solo sea revelada a los usuarios autorizados); la integridad (que sea exacta y completa, lo que está relacionado con que solo sea modificada por los usuarios habilitados) y la disponibilidad (que esté disponible en tiempo y forma exclusivamente por los usuarios legitimados). Sin embargo, con posterioridad se empezaron a añadir otras propiedades, aunque no todas unánimemente aceptadas: la autenticidad (que provenga de la fuente alegada), el no repudio (que el autor no pueda rechazar su autoría), la trazabilidad (que pueda rastrearse su ciclo de vida), etc. Caso de admitir esta ampliación, a estas últimas incorporaciones es usual denominarlas dimensiones secundarias y a las tres primeras citadas dimensiones principales.

Un claro ejemplo de ello se tiene en la norma UNE-ISO/IEC 27000 (2), que establece que la seguridad de la información es: «La preservación de la confidencialidad; la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad».

Otra definición de seguridad de la información, equivalente en el fondo, pero no en la forma, se halla en (3) y (4): «Disciplina cuyo objetivo es el estudio de los métodos y medios de protección frente a revelaciones, modificaciones o destrucciones de la información o ante fallos en el proceso, almacenamiento o transmisión de dicha información».

Sin embargo, son escasas, hasta ahora, las definiciones unánimemente aceptadas del término ciberseguridad, destacando, por su carácter normativo la adoptada por la UIT-T (5): «La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad (que puede incluir la autenticidad y el no repudio) y confidencialidad».

De todo ello, resulta que la diferencia sustancial entre ambas definiciones, de la ciberseguridad y de la seguridad de la información, es que la primera pone el acento en las TIC («ciberentorno», «tecnologías que pueden utilizarse para proteger los activos», etc.), mientras que la segunda es omnicomprensiva, abarcando a la información sea cual sea su soporte (papel, electrónico, microfilm, etc.) o su medio de procesamiento (automatizado o manual).

CAUSAS DE LA INSEGURIDAD DE LOS SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Es cierto que la inseguridad de estas tecnologías y, sobre todo, de los sistemas de información construidos a partir de ellas, provoca una general perplejidad, pues aunque todo el mundo sabe que la seguridad absoluta en cualquier ámbito es una utopía, de ahí al elevado número de graves incidentes de ciberseguridad que registramos diariamente media un gran trecho que conviene cuanto menos explicar, ya que no justificar.

Unas de estas causas son intrínsecas a la propia naturaleza de estos sistemas y otras generales a la seguridad en cualquier ámbito, aunque acentuadas por diversas singularidades de los sistemas de información y redes de comunicaciones.

Respecto de las primeras, cabe destacar su complejidad pues, como es sabido, ésta es uno de los principales enemigos de la seguridad. Por ejemplo, un sistema operativo cualquiera tiene millones (usualmente decenas de millones) de líneas de código, ejecutándose sobre ellas el resto de los programas (ofimáticos, navegadores, localizadores, de ocio, sistemas de videoconferencia, de control de dispositivos ponibles [2], etc.), que usualmente están también conformados por otros millones de líneas de código y a menudo también interconectados entre sí.

Todo ello constituye una maraña de líneas de código de una complejidad inigualable (se considera la obra humana más compleja), lo cual comporta como penitencia la inseguridad del conjunto. Lamentablemente, para atenuar este problema deberíamos renunciar a dos logros muy valorados en nuestros equipos. Primero, la sencillez de su uso y, segundo, a integrar multitud de programas en un sólo equipo que los hace una especie de monumental navaja suiza, pero con todas sus herramientas conectadas entre sí.

Desde luego retroceder décadas para hacer los equipos solo accesibles a unos pocos iniciados (volviendo a las líneas de comando y omitiendo iconos, imágenes, menús desplegables, mandatos de voz, etc.) y además limitando sus funcionalidades a unos pocas (para desistir de tener todo en uno), haría a estas máquinas intrínsecamente mucho más simples, pero con un coste en usabilidad que nadie estaría dispuesto a tolerar.

Además, la absoluta conectividad de los equipos -todos conectados con todos-, los hace grandemente interdependientes. De este modo, un equipo en las antípodas infectado o en poder de un delincuente puede dañar grave e instantáneamente a sistemas situados en el otro extremo del mundo. Y a pesar de este riesgo, en un mundo tan globalizado como el actual, no podemos prescindir de esta interrelación entre equipos y sistemas.

Por lo anterior, no se vislumbra que los problemas de ciberseguridad puedan solventarse en un futuro razonable y deje de ser una importante preocupación en nuestras sociedades.

No obstante, ello no significa que solo quede resignarnos, pues hay tareas que acometidas cuanto antes, deben mejorar la situación expuesta.

La primera viene de un diseño más depurado de los programas informáticos, de modo que, aunque la complejidad ya citada de los mismos haga impensable la carencia de fallos, el empleo de técnicas de desarrollo seguro minimice al máximo estos errores. En este sentido, todos los expertos coinciden que el principal problema lo constituye el deficiente diseño. Así, un informe del prestigioso *Software Engineering Institute* (SEI) de la CMU (6) establece que nada menos que el 70% de los fallos de seguridad traen causa de errores de diseño. Por eso, un principio fundamental para aminorar los problemas de seguridad es el conocido como seguridad por diseño, que establece que los requisitos de seguridad se deben considerar desde la primera fase del desarrollo de software (la fase de diseño). De hecho, este principio, junto el de seguridad por defecto (por omisión, los programas deben incorporar los mecanismos de seguridad pertinentes) vienen recogidos en el artículo 25 del Reglamento General de Protección de Datos de reciente aplicación (7).

Pero, por si estos fallos de diseño no fuesen suficientes, también son numerosos los errores en el desarrollo. Según datos del mismo SEI arriba citado, un experimentado analista de aplicaciones comete en promedio un error cada nueve líneas de código que escribe y además cada millón de líneas de código contiene tras finalizar el desarrollo del programa entre 1.000 y 5.000 fallos (8). Datos que indican la importancia de aplicar técnicas de desarrollo seguro, lo que se ve dificultado por la escasez de técnicos experimentados en ello.

La segunda de las tareas no es tanto una medida técnica como de gestión y dentro de las de este tipo (todas de gran importancia y algunas expuestas más adelante) destaca sobremanera la concienciación de la sociedad, que evitaría el aprovechamiento por los ciberdelincuentes de los fallos expuestos. Ya en el lejano 2003, en EE UU, la National Strategy to Secure Cyberspace (9), establecía: «*Many cyber vulnerabilities exist because of a lack of cybersecurity awareness on the part of computer users, systems administrators, technology developers, auditors, chief information officers and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructures*».

No obstante, y a pesar del tiempo transcurrido, nos encontramos con profesionales cualificados y no, empresarios y personas en general, carentes no ya de una mínima formación en seguridad, sino aun de la más pequeña concienciación. Conscientes de ello, algunos países están introduciendo la formación en ciberseguridad en la Enseñanza Secundaria, lo que es el caso de EE UU, programa CyberPatriot (10) y Gran Bretaña, iniciativa CyberCenturion (11). En España cabe destacar la loable iniciativa del INCIBE, que bajo el nombre de Espacios de Ciberseguridad lleva la formación en ciberseguridad (en forma de talleres prácticos) a estudiantes de Bachillerato y FP en cualquier lugar de nuestra geo-

FIGURA 4
MEDIDAS DE SEGURIDAD AUTOMATIZADAS

Fuente: (11)

FIGURA 5
MEDIDAS DE SEGURIDAD

Fuente: (11)

grafía (12). En paralelo, también imparten formación a profesores de esos estudios (13) para capacitarles para impartir estos mismos talleres a sus alumnos.

Estas carencias explican la facilidad con que los ataques de *phising* tienen tanto éxito o que ante un incidente con pérdidas de datos sea imposible su recuperación, pues las copias de seguridad periódicas son casi una rareza en muchos ámbitos.

Pero quizás, esta falta de concienciación se acusa fundamentalmente en el desconocimiento de la importancia de mantener todo el software (sistemas operativos, antivirus, programas ofimáticos, etc.) permanentemente actualizado. Que la actualización del software sea extraña para muchos, explica que según el CERT Coordination Center (CERT/CC) del citado SEI, el 90% de los ataques son causados por ciberdelincuentes que explotan vulnerabilidades ya conocidas (14).

Una demostración de las consecuencias de ello se tuvo el 12 de mayo del pasado año, cuando el *ransomwere* WannaCry secuestro infinidad de ordenadores de empresas de todo tamaño (en España, entre otras, varias del Ibex 35) obligando a cerrar alguna de ellas. Lo penoso del caso, es que ese programa maligno se aprovecho de una vulnerabilidad (EternalBlue) del sistema operativo Microsoft Windows que esta compañía había parcheado dos meses antes. Es cierto que esta actualización no incluía a las versiones antiguas Windows, pero en muchos casos el ataque afecto también a versiones modernas que sin embargo no estaban actualizadas a pesar del tiempo transcurrido [3].

En España, centrándonos en los hogares, según un reciente informe del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) (15) en el segundo semestre de 2017 más de un cuarto de hogares españoles no tenían programas an-

TABLA 1
THE 2015 (ISC)2 GLOBAL INFORM. SEC. WORKFORCE STUDY

Thousands	2014	2015	2016	2017	2018	2019
Demand-Meeting Projection	3,568	3,972	4,416	4,908	5,424	5,963
Security Professionals' Hiring Projection	3,477	3,756	4,053	4,369	4,706	5,061
Supply-Constrained Projection	3,400	3,593	3,796	4,007	4,227	4,456
Shortfall	**168**	**378**	**621**	**901**	**1,172**	**1,536**

Fuente: Frost & Sullivan

tivirus y casi la mitad no actualizaban sus sistemas operativos (Figura 4). Por lo que respecta a las llamadas en el Informe medidas de seguridad activas, solo un 55,7% usan contraseñas y solo el 33,6%, obtiene copias de seguridad (Figura 5).

Finalmente, tres últimos factores influyen negativamente en la seguridad de cualquier ámbito y naturalmente en la ciberseguridad. El primero de ellos es el costo (elevado en el caso que nos ocupa) que a muchas empresas les es difícil de admitir, pues erróneamente lo ven como un gasto y no como una inversión. Y, sin embargo, las pérdidas económicas y de imagen a las que se pueden ver abocadas ante un incidente de ciberseguridad superan con gran holgura el desembolso que pueden suponer las medidas de seguridad. El rendimiento es otro inconveniente, pues la implantación de los numerosos controles que se precisan consume elevados recursos informáticos que hace que el rendimiento se resienta. Finalmente, la usabilidad se ve resentida por la ciberseguridad, ya que los controles exigidos por ésta hacen que el uso de los sistemas de información sea más incómodo y dificulten las tareas de los usuarios.

INVERSIÓN ANUAL Y MERCADO LABORAL

Según la ciberseguridad ha ido alcanzado una importancia singular, el presupuesto dedicado a ella en el mundo se ha incrementando notablemente, siendo en los últimos años en torno al 10% anual. Así, según un reciente informe de la consultora Gartner (16), la inversión mundial en ciberseguridad en el 2017 ascendió a 101.544 y en 2018 llegará a ser de 114.000 millones de dólares lo que supone un incremento global del gasto en ciberseguridad en 2018 respecto del 2017 será 12,4%.

Además, otro rasgo distintivo ya mencionado de estas tecnologías es su fulgurante difusión en muy escasos decenios, lo que comporta una grave y destacable consecuencia: la carencia de técnicos expertos en ciberseguridad en sus dos facetas principales: de detección de ataques o vulnerabilidades y de construcción de sistemas seguros). Y este déficit no se vislumbra que vaya a solucionarse próximamente, entre otros motivos porque no hay suficientes académicos ni profesionales especializados en ciberseguridad, para formar a nuevos «ciberexpertos».

Ratificando lo dicho, un estudio de 2015 de la consultora Frost & Sullivan cifra en casi seis millones de profesionales de la ciberseguridad los necesarios en el mundo en 2019, mientras que estima en casi cuatro millones y medio los profesionales efectivamente existentes en esa fecha. Es decir, un déficit de casi un millón y medio (Tabla 1) (17).

Igualmente, en un informe del presente año de la multinacional Manpower Group (18) y en el apartado «Los 10 perfiles más demandados en el mundo: 6. Tecnologías de la Información» los «Expertos en ciberseguridad» ocupan el primer lugar.

En el mismo sentido, la empresa estadounidense CiberSeek cifra en casi 770.000 los profesionales de la ciberseguridad trabajando en EE UU, y aun así, señala que son más de 300.000 los puestos sin cubrir en ese mismo mercado (19).

Finalmente, volviendo a nuestro país, en el estudio de Spring Professional (20) del Grupo Adecco de este año, la figura de «Experto en seguridad TI» aparece dentro del sector Telco como el perfil más cotizado.

EL DELITO INFORMÁTICO (CIBERDELITO) Y LOS CIBERDELINCUENTES

En ausencia de una definición legal española de ciberdelito (no está contemplado como un tipo penal diferenciado en la vigente Ley Orgánica 10/95 del Código Penal), se puede tomar la siguiente definición de la norma ISO/IEC 27032:2012 (21). «*Cybercrime: Criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime*».

Por lo que atañe a los ciberdelincuentes, posiblemente la más adecuada sea la contenida en el Documento de la Unión Europea COM (2007) 267 final, acerca de la ciberdelincuencia (22): «Actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas».

O de otro modo, y simplificando, son ilícitos para los cuales los sistemas de información y las redes de comunicación son el medio para perpetrar el delito (fraude, interceptación de comunicaciones, revelación de secretos, etc.) o el fin del propio hecho delictivo (borrado del disco duro, interrupción del servicio web, etc.). En el primer caso son delitos tradicionales y solo en el segundo nos encontraríamos ante delitos de nuevo cuño.

La misma Comunicación, establece seguidamente que, en la práctica, la ciberdelincuencia engloba tres tipos de actividades delictivas. En primer lugar, formas tradicionales de delincuencia (fraude, falsificación, suplantación de personalidad, etc.) cometidos mediante redes y sistemas de información. En segundo, publicación de contenidos ilegales por medio de redes comunicación (pedofilia, incitación al odio racial, etc.). Y, por último, delitos específicos de las redes electrónicas, por ejemplo, los ataques contra los sistemas informáticos, la denegación de servicio y la piratería informática. Como colofón, señala que estos ataques también se pueden dirigir contra infraestructuras críticas, enfatizando su gravedad en el contexto europeo.

En España, los delitos informáticos son un hecho sancionable por Código Penal (23) y caso de tener idénticos objetivos que los tradicionales, tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción penal para la interceptación del correo electrónico que para una intromisión en el correo postal.

Respecto de los ciberdelincuentes, en un principio jóvenes poco sociables y escasa autoestima, que buscaban en el acceso a ordenadores ajenos satisfacer su ego (a menudo sin ánimo de daño alguno), pasaron a principios de los noventa del pasado siglo, a mutar en favor de un tipo diferente cuyo propósito exclusivo era la obtención de un lucro económico. En este tipo de ciberdelincuente se encajó enseguida la delincuencia organizada, que vio en estas tecnologías bien un fin en sí mismas o bien un instrumento delincuencial. En ambos casos, con características impagables: altas dosis de anonimato; pingües beneficios con escasas inversiones; rastreo complejo y extraterritorialidad jurisdiccional, lo que comporta una elevada dificultad probatoria y, por consiguiente, con una alta probabilidad, impunidad [4]. Así, según el Estudio sobre Criminalidad en España 2017 (24), en este año se conocieron 81.307 hechos (con un incremento del 22,1% frente a 2016) de los que fueron esclarecidos 22.111 (el 27,2%), siendo 4.912 los detenidos e investigados.

No obstante, estas organizaciones delictivas han debido acomodarse a nuevos modelos organizativos, que exigen diversos agentes muy diferenciados, unos altamente cualificados, como desarrolladores de software (a menudo reclutados a través de foros de la Dark Web), otros expertos en psicología social, otros simples intermediarios de fondos (muleros), etc. Todos ellos estructurados mediante relaciones efímeras y mutuo desconocimiento. A esto se añade que son negocios de elevada internacionalización y con una débil jerarquización, lo que contrasta con los modelos organizativos de las mafias tradicionales, con estructuras muy rígidas y jerarquizadas y vínculos robustos entre los integrantes del sistema.

Un último punto para reseñar acerca de estas organizaciones es la incorporación a su modelo de negocio del denominado *crime as a service*, que les permite ofrecer herramientas de ataque bajo la modalidad de alquiler, a aquellos que no tengan la capacidad tecnológica para desarrollar sus ataques o sólo ocasionalmente tengan como objetivo personas, empresas u organismos concretos. Este puede ser el caso de empresas que deseen obtener informaciones confidenciales de sus competidores, atacar la disponibilidad de sus recursos, desacreditarlos ante su clientela, etc.

Un ejemplo de estas organizaciones que prestan servicios delictivos bajo demanda lo constituyen aquellas que construyen las denominadas *robot network*, más conocidas por su acrónimo *botnet* (redes de ordenadores que controlan sin conocimiento de sus legítimos propietarios), para alquilarlas a quien desee hacer campañas de *spam*, o ataques de denegación de servicio distribuida a servidores web, por ejemplo, de empresas de la competencia, o difundir programas malignos.

Pero, aunque parezca lo contrario, estos atacantes externos a la empresa no son los causantes exclusivos de ataques, ya que internamente, empleados o subcontratados de las empresas son potenciales atacantes y a menudo más peligrosos. En efecto, tanto unos como otros conocen mejor que los ajenos los sistemas, medidas y personal de seguridad, etc. de la empresa. Así mismo, son conscientes de los momentos oportunos para desencadenar un ataque, sea por operaciones de mantenimiento, por periodos vacacionales o ausencias puntuales del personal de seguridad más capacitado, etc. Y, finalmente, además de la misma motivación económica que el atacante externo, pueden hallarse resentidos, por sentirse estancados en el escalafón, relegados en la formación, desatendidos en sus demandas, postergados en sus trabajos, etc. O sea, pueden aunar los requisitos idóneos para delinquir: conocimiento, oportunidad y motivación, que raramente son reunidos por atacantes extraños.

Una reciente encuesta de Cibersecurity Insider and Crowds Reseaarch Partner (25) realizada a 472 profesionales de la ciberseguridad, arroja el dato de que un 56% de ellos considera que la mayor amenaza proviene de empleados sin especiales responsabilidades, seguida de usuarios con acceso a informaciones sensibles, como usuarios con especiales derechos de acceso y gerentes (55%), seguidos por personal subcontratado.

De este modo no puede extrañar que ya el Plan Estratégico 2013-2016 de nuestra Policía Nacional (26) estable-

FIGURA 6
RANSOMWERE

Fuente: Terabytezone.com

ciese que: «El tercer delito más lucrativo a nivel mundial es el cibercrimen, después de la prostitución y el tráfico de drogas, por ello se convierte por primera vez en una prioridad estratégica.»

Y, por si lo anterior fuese poco, recientemente han aparecido nuevos actores en este panorama. Se trata de ciberterroristas, ciberespías, ciberactivistas, etc. cuyos fines no suelen ser estrictamente económicos sino políticos, de desinformación, propagandísticos, terroristas, de influencia sobre líderes sociales o políticos, etc.

Algunos de estos grupos trabajan con elevada probabilidad en la órbita gubernamental de ciertos países (cada vez más numerosos), aunque otra cosa es la atribución indubitable de ello. Las víctimas de estos grupos son partidos políticos, instituciones democráticas, etc. y es que todos los países han aprendido que los sistemas y redes de comunicaciones (incluyendo naturalmente a las redes sociales) son una formidable herramienta de desestabilización de otros estados, de propaganda y de influencia como se ha comprobado hace poco con la más que probable injerencia de una potencia mundial en las elecciones de varios países democráticos europeos y, especialmente, EE UU.

Respecto del ciberterrorismo y ciberactivismo, ni los grupos *yihadistas* ni otros terroristas, ni los *hacktivistas* constituyen hoy en día una grave amenaza, pues no parece que tengan aún capacidades suficientes para realizar ataques de gran envergadura (27).

En cualquier caso, el dato relevante es que el número de ataques a los sistemas y redes de información está creciendo vertiginosamente en todo el mundo. Centrándonos en nuestro país, el número de incidentes gestionados por el Centro Criptológico Nacional en su ámbito competencial (Sector Público y empresas de interés estratégico) se elevó en 2017 a 26.472, cuando en el 2016 los incidentes fueron 20. 807, lo que supone un incremento del 27,22%. Aun más preocupante, este 2017 el CERT [5] Gubernamental (CERT gestionado por el CCN/CNI) afrontó un promedio de cuatro ataques cada día de peligrosidad muy alta o crítica, clasificación que atiende al tipo de amenaza, su origen, perfil del usuario afectado, número o tipología de sistemas afectados, impacto, etc. (28).

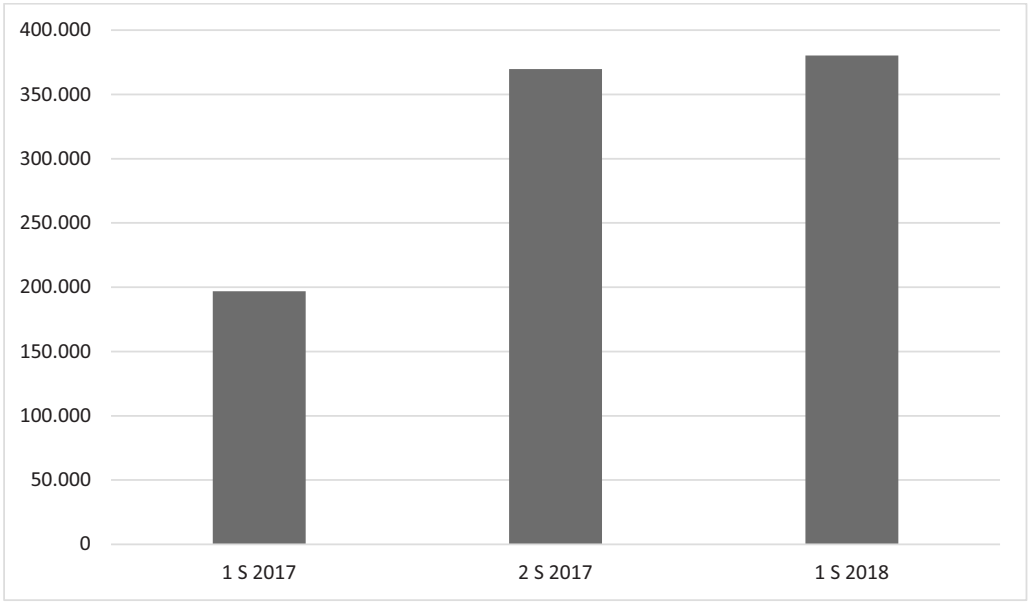
Y si nos referimos a los ataques padecidos por las empresas, la red IRIS (red académica constituida por centros universitarios y de investigación) y los ciudadanos ascendieron en 2017 a 123.064 frente a los 115.257 registrados en 2016. De aquellos, 885 los sufrieron infraestructuras críticas cuando en 2016 fueron «tan solo» 479 (29).

En cualquier caso, y dejando de lado los ataques deliberados, no pueden olvidarse los incidentes no intencionados cuyas consecuencias pueden ser de tan extrema gravedad como los intencionados y que deberían ser contrarrestados mediante medidas de seguridad, pero sobre todo con campañas periódicas de concienciación, o incluso formación, del personal usuario de ordenadores en la empresa. Además del establecimiento de medidas disciplinarias si los incidentes traen causa de negligencias.

HERRAMIENTAS DE ATAQUE

Las herramientas de ataque, son muy variadas y cambiantes con el tiempo. Por destacar algunas de las más importantes a día de hoy, se pueden citar:

FIGURA 7
RANSOMWERE DETECTADO EN EL MUNDO. ÚLTIMOS TRES SEMESTRES



Fuente: (31)

Ransomwere

El ransomwere (de *ransom*, rescate) es un programas dañino que impide de alguna manera el acceso al disco duro del ordenador de la víctima, que solo recupera el control tras pagar una cantidad económica (usualmente en *bitcoin*, aunque últimamente han comenzado a usarse otros medios anónimos de pago). Usualmente, una vez instalado en el disco duro, genera una clave secreta de cifrado (diferente para cada ordenador infectado) con la cual cifra dicho disco mediante un sistema simétrico. Tras ello, remite al atacante la clave secreta cifrada con un sistema asimétrico mediante la clave pública de dicho ciberdelincuente. A este le basta con descifrar el mensaje recibido para obtener la clave secreta que le será devuelta a la víctima tras pagar el rescate (Figura 6). Aunque hay otras formar de imposibilitar el uso del ordenador esta es la más empleada por los atacantes.

La prevalencia de este tipo de ataque en 2017 fue muy elevada, estimándose que el 60% del código maligno difundido era de este tipo. Sólo en Europa (1) se registraron más 4.000 ataques al día, siendo el más conocido de estos ataques el protagonizado por el famoso WannaCry que según el Departamento de Seguridad Nacional afectó a más de 360.000 ordenadores de 180 países en mayo de 2017 (30). El sector atacado preferido fue el financiero con una acusada tendencia a dirigirse también al sector sanitario.

No obstante, estos programas maliciosos han perdido fuelle en el primer semestre de este año en el que a nivel mundial se han detectado un total de 380.299 programas de este tipo, frente a los 369.698 del último semestre de 2017 (Figura 7), lo que supone un escaso 3% de incremento (31).

A menudo estos programas se denominan también criptovirus, haciendo referencia a las técnicas que suelen emplear.

Phishing

Bajo el término *phising* se comprenden ataques basados en técnicas de ingeniería social, que pretenden engañar al usuario para que revele una contraseña, acceda a una página web fraudulenta, descargue un fichero comprometido o cualquier otra acción contraria a sus intereses o los de la empresa. Habitualmente, el mensaje engañoso se transmitía mediante *spam* dirigido a una pluralidad de direcciones de correo. El costo del *spam* es insignificante, de modo que, aunque solo piquen el anzuelo un porcentaje ínfimo de receptores, las ganancias son muy importantes.

Empero, con el tiempo, el *phishing* indiscriminado ha ido dejado de ser una argucia eficaz, por lo cual los ciberdelincuentes investigan la vida profesional de usuarios específicos para personalizar el engaño. Es el caso de mandar a uno de estos usuarios un correo supuestamente de su jefe (con datos empresariales no comúnmente conocidos, para ganarse su confianza) y solicitarle que ejecute alguna actuación o descubra alguna información. Normalmente se dirigen a individuos de una empresa que, sin ocupar en el organigrama posiciones del más alto nivel, por su responsabilidad en cierta área puede tener un alto interés para el atacante. Es el denominado *spear phising* o *phising* dirigido.

Amenazas persistentes avanzadas (*Advanced Persistent Threat*).

Conocidas por su sigla en inglés APT, se hicieron mundialmente conocidas al descubrirse el gusano Stuxnet que atacó los sistemas SCADA de la planta iraní de Natanz de depuración de uranio, consiguiendo ralentizar la misma, posiblemente durante meses, antes de ser descubierto en el año 2010. Como vector de propagación para acceder a la red de la central, aislada de Internet (*air gapped*), se cree que se uso un dispositivo USB infectado por el gusano, que después se propagó por los sistemas operacionales de la planta.

El nombre hace honor a sus características: son programas muy sofisticados y complejos, al alcance de muy escasos grupos de atacantes del mundo, y se diseñan para pervivir durante largo tiempo en las máquinas sin ser descubiertos.

Este programa nocivo, así como otros que han ido apareciendo, solo pueden haber sido creados por grupos de expertos trabajando en la órbita de gobiernos con grandes recursos: EE UU; Rusia; Israel; China y Corea del Norte, por citar los principales.

Botnet

Una *botnet* (*Robot network*) es una red de ordenadores, denominados *bots* (en ocasiones también *zombies*), que han sido infectados y son controlados desde un ordenador central, denominado *bootmaster*. Las comunicaciones entre el *bootmaster* y los *bots* se realizan a través de un servidor de Comando y Control (C&C, *Command and Control*). El *botmaster* manda un comando, a través del C&C, y los *bots* se encargan de ejecutar la tarea programada correspondiente.

Estas redes se utilizan para múltiples propósitos, entre los que destaca el envío de publicidad (*spam*), los ataques de denegación de servicios basados en bloquear la disponibilidad de un servicio y la distribución de todo tipo de programas malignos.

Las *botnet* llegan a estar constituidas por decenas (e incluso centenas) de miles de *bots* gestionadas por organizaciones delictivas que las alquilan en la Dark Web (*Crime as a Service*) a quienes desean realizar un ataque de los citados que precisa de estas grandes redes.

Denegación de servicio (*Denial of Service*, DoS)

El objetivo de este ataque es atentar contra la disponibilidad de un servicio: correo electrónico o mensajería; servicio web, etc. Usualmente, esto se consigue generando un enorme número de peticiones al servidor que proporciona el servicio hasta que se desborda su capacidad y colapsa. De ahí el nombre de ataques de inundación que esporádicamente también reciben.

Como es imposible que el atacante con una sola máquina, o un número pequeño de ellas, pueda generar el ingente número de peticiones que se requieren para colapsar un servicio, en el año 1999 se comenzaron a usar *botnet*. Por motivos obvios, el ataque recibió el nombre de Denegación distribuida de servicio, que se abrevia por su sigla en inglés DDoS (*Denial Distributed of Service*).

Este ataque, aunque antiguo, no ha perdido actualidad y más de un tercio de las organizaciones analizadas por el CCN/CNI en su estudio anual «Ciberamenazas y Tendencias Edición 2018» (28) se enfrentaron a un ataque de DDoS, en comparación con el 17% de 2016. Es de destacar que este ataque es muy usado por *ciberhacktivistas* con afán de hacer daño y crearse una falsa reputación de audacia y competencia. Ejemplos los tenemos en nuestro país, y muy abundantes, durante el último año.

Internet of Things (IoT).

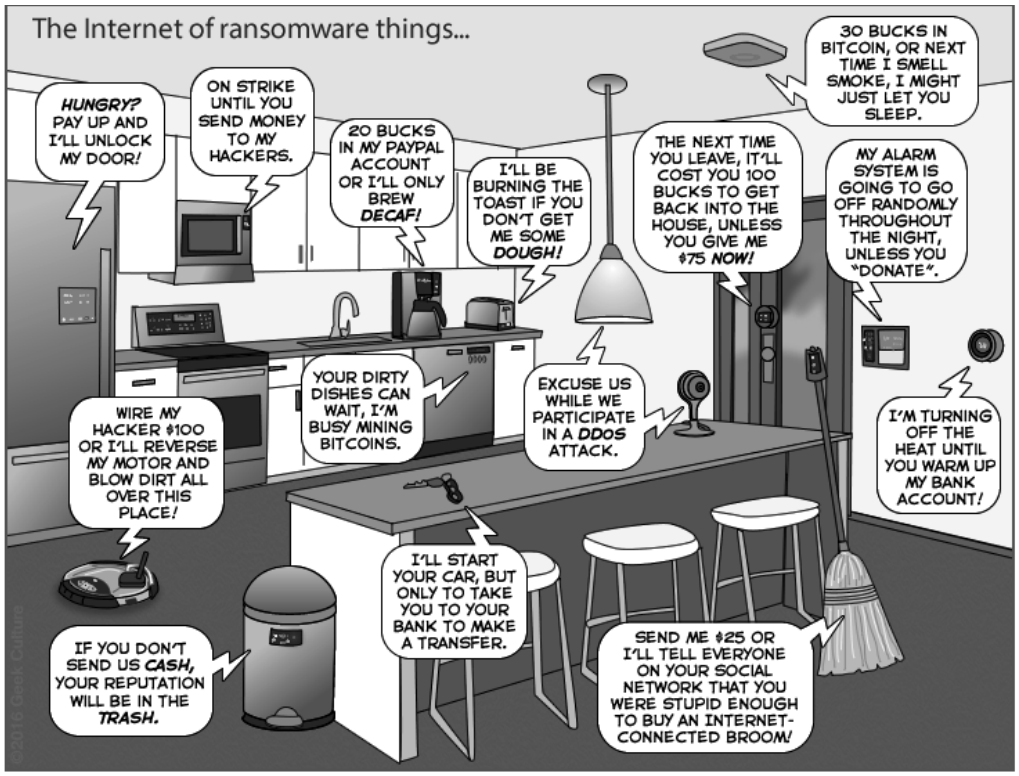
Hasta hace poco tiempo, Internet interconectaba a personas a través ordenadores de todo tipo: servidores, personales, tabletas, móviles, etc. Sin embargo, en poco tiempo los objetos de nuestro entorno (domóticos, dispositivos ponibles, *router*, cámaras de fotos, dispositivos médicos implantables, juguetes, etc.) directamente conectados a la red y sin intervención humana es más numeroso que el de ordenadores, estimándose que en el año 2020 superarán holgadamente los 20.000 millones y aun algunos analistas elevan esta cifra a 50.000 millones (32).

Estos dispositivos presentan grandes problemas de seguridad, pues disponen de muy poca potencia de cálculo (lo que imposibilita el uso de ciertas medidas de seguridad que requieren más potencia) y escasa capacidad de almacenamiento. Además, a menudo, es imposible cambiar la contraseña que traen de fabrica o si ello es posible, pero se adquieren en grandes cantidades para implantarse en multitud de productos de consumo (vehículos, electrodomésticos, etc.) este cambio resulta muy costoso.

Las características anteriores los hacen dispositivos ideales para construir *botnet* con las que lanzar ataques de DDoS (Figura 8) u otros y en poco tiempo se han registrado numerosos ejemplos de ellos. Es el caso de la *botnet* Mirai, cuyas *bots* (se afirma que más de 150.000 dispositivos IoT) constituidas por cámaras de fotos y *router*, se estrenó en 2016 colapsando mediante ataques de DDoS a importantes firmas mundiales.

Pero, además de ser elementos activos de ataque a otros equipos, también pueden ser objetos pasivos, fin en si mismos de ataques. Por ejemplo, ya se han descubierto vulnerabilidades en varios dispositivos médicos implantables (bombas de insulina y marcapasos) conectados a Internet para permitir una monitorización continua desde el correspondiente hospital.

FIGURA 8
BOTNET DE INTERNET OF THINGS



Fuente: http://www.geekculture.com/joyoftech/joyarchives/2340.html

Además, sobre estos dispositivos se sustenta la Industria 4.0 del futuro inmediato, por lo que están suscitado una gran preocupación en estos sectores empresariales.

Minado malicioso de criptomonedas

Como es sabido, la verificación de los pagos realizados con criptomonedas conlleva la ejecución de laboriosos algoritmos matemáticos, sobre bloques de transacciones, que consumen grandes recursos informáticos y de energía eléctrica. El proceso de verificación se denomina minería y aquellos que lo llevan a cabo mineros. La remuneración del primer minero que concluye la verificación consiste un cierto número de criptomonedas (actualmente, en el caso del *bitcoin*, 12,5$).

La minería es una actividad muy lucrativa, pero los procesos de verificación son tan complejos que caen fuera del alcance de cualquier usuario individual. Por eso, se han creado empresas que instalan «granjas» con multitud de ordenadores trabajando cooperativamente para minar las criptomonedas.

Naturalmente, el negocio no ha pasado inadvertido para los ciberdelincuentes, que tratan de introducir sigilosamente programas nocivos de minado en los ordenadores de usuarios individuales, empresas y organismos públicos para realizar estas tareas, naturalmente a costo cero para los ciberdelincuentes, pues el costo computacional y de energía lo abona el usuario del ordenador infectado. Este fraude es conocido como *cryptojacking*, de *cryptocurrency* (criptomoneda) y *hijacking* (secuestro).

Aunque este tipo de programa maligno tiene varios años, según todos los informes en el último se ha incrementado exponencialmente. Así, según un informe reciente de Trend Micro el número de detecciones de estos programas ha pasado de 326.326 en el último semestre de 2017 a 787.146 en el primero de 2018 (Figura 9) (33).

En el mismo sentido el informe de Check Point (34), señala que ha sobrepasado ya al *ransomwere* afectando el primer semestre del presente año al 42% de las organizaciones del mundo, cuando en el último semestre de 2017 solo estaban infectadas el 20,5%. Además, sigue este informe, en el primer semestre de 2018 las pérdidas sufridas por sus víctimas han sido de 2.500 millones de dólares.

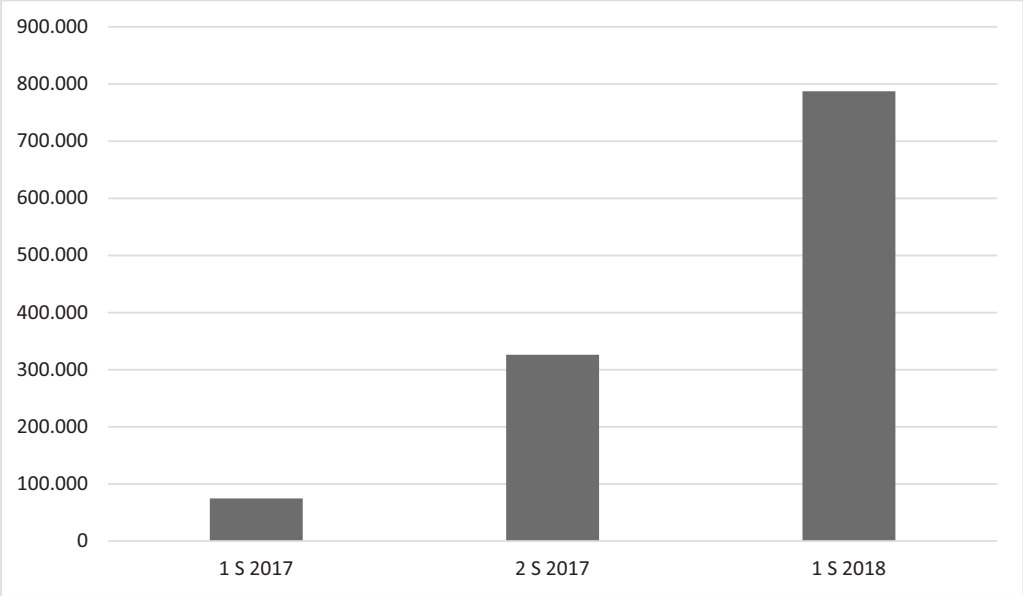
PLATAFORMAS Y DISPOSITIVOS

Entre las plataformas y dispositivos que más ataques concentran y preocupación concitan, se encuentran:

Redes sociales

Muy usadas por los ciberdelincuentes para extraer información muy valiosa de sus usuarios con la que des-

FIGURA 9
PROGRAMAS MALICIOSOS DE MINADO DETECTADOS EN EL MUNDO



Fuente: 33

encadenar un variado elenco de ataques: suplantación de personalidad; *phising* dirigido (*spear phising*); ...

Por otra parte, es creciente el empleo de estas redes por oscuros departamentos gubernamentales en campañas de desinformación para: sesgar a la opinión pública en las elecciones democráticas; tergiversar la realidad para acusar de totalitarios a regímenes democráticos; alterar la confianza de la opinión pública en empresas, difamar personajes públicos, etc.

Móviles inteligentes *(smart)*

Los cuales almacenan valiosas informaciones de sus usuarios: contraseñas de acceso a cuentas corrientes y aplicaciones empresariales, números de tarjetas bancarias y comerciales y otros. Cabe enfatizar, que estos riesgos se han visto notablemente incrementados por el auge en las empresas del conocido como BYOD (*Bring your own devices*), que frente a la ventaja de que los empleados manejan dispositivos (móviles, portátiles, tabletas) de su propiedad presentan riesgos asociados al menor control de los técnicos de seguridad sobre los mismos.

Infraestructuras industriales/estratégicas/críticas

Hasta hace poco, los sistemas de control industrial (SCADA) eran sistemas cerrados (caja negra), de propósito específico, incluso diseñados para un concreto sector y solo de valor en el mismo. Por ello, eran escasos los expertos en los mismos fuera del ámbito de sus empresas fabricantes.

Por otro lado, eran sistemas aislados (*air gapped*), de internet y de posibles redes administrativas, y utilizaban protocolos de comunicación de propietario, o sea no estándares y de conocimiento restringido.

Sin embargo, el éxito de los sistemas convencionales y de los protocolos TCP/IP condujo a una reconsideración de los anteriores supuestos, de modo que poco a poco estos sistemas industriales pasaron a ser predominantemente Windows y usuarios de los protocolos normalizados de Internet. En paralelo, el personal de estas industrias, expertos en sus tecnologías operacionales (OT) y su seguridad se han ido viendo enfrentados a las tecnologías de la información (IT) sus vulnerabilidades y amenazas sin estar suficientemente formados en las mismas.

Todo ello, supone para estas instalaciones unos riesgos sin precedentes, pues de ser atacadas con éxito, sea por ciberdelincuentes con ánimo de lucro o peor por ciberterroristas, podrían producir gravísimos incidentes como señala el Instituto británico Chatham House (35), uno de los más prestigiosos *Think Tank* mundial.

MEDIDAS DE SEGURIDAD (CONTROLES)

Para hacer frente a los riesgos que se han ido exponiendo anteriormente, las sociedades en su conjunto (organismos públicos y privados y ciudadanos) se han ido dotando de diversas medidas de seguridad (también denominadas controles) que se fueron desarrollando o aplicando según iban siendo necesarias. De este modo, hasta la década de los años sesenta eran las medidas de tipo físico, como se correspondía con el entorno de trabajo de aquellos años, las únicas que se consideraban. Los ordenadores estaban aislados de cualquier línea de transmisión, en salas cuyo acceso físico estaba muy restringido (solo accesibles por ope-

radores y técnicos de sistemas) y el acceso lógico de los usuarios solo posible mediante fichas perforadas que eran cargadas, exclusivamente por los operadores, al sistema mediante equipos lectores. Además, los procesos informáticos eran escasos, raramente críticos y excepcionales las personas con conocimientos para perpetrar ataques.

Por tanto, las únicas medidas de seguridad aplicadas eran de prevención y extinción de incendios, de control de inundaciones, de compensación de anomalías en el suministro eléctrico, monitorización de acceso de personas y objetos y poco más.

No obstante, todo cambió en el decenio de 1970, en la que se generaliza la tendencia, ya incipiente a finales de los sesenta, de conectar los ordenadores mediante módem a líneas de transmisión para permitir el teleproceso. Con ello, se hace imprescindible el uso de sistemas de autenticación mediante contraseñas, de control de acceso lógico, de registros de auditoría y se empieza a utilizar el cifrado de datos en la transmisión de información. Medidas todas ellas que se pueden englobar entre las de tipo técnico.

Además, ya se empieza a teorizar sobre los programas malignos y se desarrollan los primeros especímenes, bien que aún en entornos controlados como laboratorios. Pero es en la década siguiente, años 80, cuando la difusión en 1986 del primer virus desarrollado para el sistema operativo MS-DOS de IBM (el virus Brain) y el primer gusano (de Morris) en 1988, abre una nueva dimensión en los ataques hasta entonces muy limitados.

Finalmente, en el decenio de los 90, con la aparición de la web y los navegadores, Internet se hace omnipresente y se inicia una carrera en la que ataques de todo tipo y plataformas de cualquier naturaleza se hacen cada vez más sofisticados y graves, desarrollándose en paralelo nuevos sistemas de técnicos protección, cortafuegos, sistemas de detección de intrusiones, plataformas SIEM. Estos sistemas se han ido incorporando bajo el principio de defensa en profundidad que, a diferencia de los primeros sistemas, de defensa perimetral, no se quedan solo en la frontera de los sistemas con internet, frontera que ha desaparecido, sino que profundizan hasta proteger a todos los equipos del sistema e incluso a programas dentro de estos.

Además, muy recientemente, empiezan a usarse técnicas basadas en la inteligencia artificial que prometen no solo desplegar una defensa reactiva, como ocurre con los sistemas actuales, sino también, y sobre todo, proactiva, el sueño de toda defensa.

Por otro lado, a partir del presente siglo, y según los sistemas de información y las redes van alcanzando todos los rincones de las empresas, la ciberseguridad deja de ser una cuestión que solo involucra a los técnicos para concernir a todos los sectores y llegar también a los más elevados niveles del organigrama, que hacen suya la frase de uno de los más reputados expertos mundiales, Bruce Schneier: «*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology*» (36). O, en otras palabras del mismo experto: «*Security is a not a product, but a process*».

Comienzan así a aparecer marcos de gestión de la seguridad de la información, de entre los cuales sobresalen COBIT y la familia de normas de la serie 27000 de ISO/IEC (las tres primeras, 27000, 27001, 27002, también nomas europeas, EN, y españolas, UNE), que constantemente va integrando nuevos estándares en un esfuerzo normalizador de gran transcendencia para contar con sistemas cada vez más seguros.

En paralelo con esta progresiva incorporación de medidas de seguridad de distinta naturaleza: físicas primero; técnicas después y finalmente de gestión, los países van añadiendo a su marco legal nuevas disposiciones que regulan esta materia.

En definitiva, la ciberseguridad se ha repensado como una ingeniería similar a cualquier otra, con sus objetivos, recursos y límites legales y normativos, es decir como aquella que tiene como objetivo el diseño, construcción y mantenimiento de sistemas seguros frente a errores y amenazas deliberadas o accidentales, atendiendo a los recursos disponibles y respetando las obligaciones legales y normas técnicas pertinentes.

CONCLUSIONES

Ante los problemas expuestos, solo existen dos soluciones. La primera es incrementar la inversión en ciberseguridad (incluyendo la I+D+i) para tener mejores y eficientes medidas de seguridad, potenciar la cooperación entre todos los agentes involucrados y, muy importante, incrementar la concienciación, y si cabe formación, por parte de toda la sociedad, de las amenazas que nos acechan, los actores de las mismas, las cambiantes y crecientes vulnerabilidades de las TIC y las medidas de seguridad que tenemos a nuestro alcance para aminorar, ya que cancelar es imposible, los ataques o, si ello no resulta, sus consecuencias.

La segunda solución, seguir las denominadas tres reglas de oro de Robert Morris, relevante informático norteamericano, que trabajó en la Agencia Nacional de Seguridad (y padre del creador del gusano de Morris):

Do not own a computer;
Do not power it on;
and do not use one

NOTAS

[1] Como atinadamente afirmó John Chambers, exCEO de CISCO: Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que han sido hackeadas.

[2] Según la FUNDEU es preferible a vestible como traducción de *wearable*.

[3] Las empresas no pueden instalar los parches nada más liberarse, pues en ocasiones programas específicamente desarrollados para las mismas fallan al apli-

car dichos parches. En todo caso, dos meses para estudiar el impacto de los parches en los sistemas, y caso de problema corregirlos, se antoja mucho tiempo.

[4] Según la vigente Estrategia de Ciberseguridad Nacional 2013, son características de los ciberataques: su bajo coste; su ubicuidad y fácil ejecución; su efectividad e impacto y su reducido riesgo para el atacante.

[5] *Computer Emergency Response Team.* El primero fue creado por el gobierno de EE UU en 1988 a raíz de la difusión del gusano de Morris, primer gusano liberado en Internet. Se ubicó en la Carnegie Mellon University y desde entonces estos centros han proliferado en todo el mundo, en ocasiones con funciones ligeramente distintas y nombres también diversos como SOC *(Security Operation Center)*, CSIRT *(Computer Security Incident Response Team)*, etc.

BIBLIOGRAFÍA

1. Informe Estado de la Unión 2017. Cybersecurity. Resilience, Deterrence and Defence. Building strong cybersecurity in Europe. http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity.en.pdf (consultado en agosto de 2018). [En línea] [Citado el: 25 de agosto de 2018.] http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity.en.pdf.

2. *UNE-ISO/IEC 27000:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.* s.l. : UNE-ISO/IEC 27000, 2014.

3. Ribagorda., A. *Glosario de Términos de Seguridad de las T.I.* s.l. : Ediciones CODA, 1997.

4. GUÍA DE SEGURIDAD (CCN-STIC-401). Centro Criptológico Nacional del Centro Nacional de Inteligencia: GLOSARIO Y ABREVIATURAS. *CCN/CNI.* [En línea] 2015. https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html.

5. ciberseguridad., Recomendación UIT-T X.1205. Aspectos generales de la. [En línea] https://www.itu.int/rec/T-REC-X.1205-200804-I/es.

6. Mellon, Software Engineering Institute (SEI). Universidad de Carnegie. [En línea] 25 de Agosto de 2018. https://resources.sei.cmu.edu/asset_files/Presentation/2002_017_001_24393.pdf.

7. D, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la.

8. [En línea] [Citado el: 29 de Agosto de 2018.] https://www.csm.ornl.gov/~sheldon/csiirw06/McGregorTalk6.ppt.

9. EE UU. THE WHITE HOUSE. *The National Strategy to Secure Cyberspace.* February 2003.

10. https://www.uscyberpatriot.org/. [En línea] [Citado el: 3 de septiembre de 2018.]

11. https://www.cybersecuritychallenge.org.uk/. [En línea] [Citado el: 3 de septiembre de 2018 de 2018.]

12. INCIBE. [En línea] https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes.

13. —. [En línea] https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/profesores.

14. *A Portal for Software Security.* MEAD, NANCY R. y MCGRAW, GARY. 4, s.l. : Security & Privacy Magazine. IEEE, 2005, Vol. 3.

15. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI). *Estudio sobre la Ciberseguridad y Confianza en los hogares españoles.* Red.es. 2018.

16. Gartner Forecasts Worldwide Information Security. Sydney, Australia. [En línea] 2018. [Citado el: 30 de Agosto de 2018.] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

17. Study., The 2015 (ISC)2 Global Inform. Sec. Workforce. [En línea] [Citado el: 25 de agosto de 2018.] https://www.cybercompex.org/fileSendAction/fcType/0/fcOid/445471828686010375/filePointer/445471828686010530/fodoid/445471828686010527/frostsullivan-ISC2-global-information-security-workforce-2015.pdf.

18. talento., 2018 Estudio sobre escasez de. [En línea] 2018. [Citado el: 3 de septiembre de 2018.] http://ssn.manpower.es/ManpowerGroup/Escasez_Talento/Escasez_de_Talento.pdf?__hssc=114700248.1.1537298289940&__hstc=114700248.0506b1b06deeb34460c398626cb5a3f9.1537298289939.1537298289939.1537298289939.1&__hsfp=2913731818&hsCtaTracking=461ed61e-328b-41dd-8.

19. Map., Cybersecurity Supply/Demand Heat. [En línea] https://www.cyberseek.org/heatmap.html.

20. Spring Professional. Grupo Adecco. XIII INFORME LOS + BUSCADOS 2018. 2018.

21. SO/IEC 27032:2012. Information technology-Security techniques-Guidelines for cybersecurity. s.l. : ISO/IEC, 2012.

22. COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM(2007) 267 final. Bruselas : s.n., 2007.

23. Ley Orgánica 10/1995 de 23 de noviembre (BOE número 281). Madrid : B.O.E.

24. Ministerio del Interior. . Estudio sobre la Criminalidad en España 2017. 2017.

25. Cibersecurity Insiders and Crowds Research Partner. INSIDER THREAT 2018 Report. . 2018.

26. Policía Nacional. Plan Estratégico 2013-2016. 2013.

27. CCN-CERT. IA 07/18 Informe Anual 2017. Hacktivismo y Ciberyihadismo. 2018.

28. CCN/CERT. IA-09/18. Ciberamenazas y tendencias. Edición 2018. 2018.

29. 2017., INCIBE. BALANCE seguridad. [En línea] 2018. [Citado el: 23 de Agosto de 2018.] https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_2017_final_esp.pdf.

30. DEPARTAMENTO DE SEGURIDAD NACIONAL. Iinforme Anual de Seguridad Nacional 2017. 2018.

31. Trend Micro. Unseen Threats, Imminent Losses, 2018 Midyear Security Roundup. 2018.

32. The Internet of Everything. Connections Counter. CISCO. [En línea] [Citado el: 3 de Septiembre 2018 de 2018.] https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342 .

33. TrendMicro. 2018 Midyear Security Roundup. Unseen Threats, Imminent Losses . [En línea] https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf .

34. Check Point . Cyber Attack Trends: Mid-Year Report 2018. 2018.

35. Chatham House Report. . Cyber Security at Civil Nuclear Facilities. Understanding the Risks. [En línea] https://www.cha-

thamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks.

36. Schneier, Bruce. Secrets and Lies. Digital Security in a Networked World. s.l. : John Wiley and Sons, 2000.

3f9.1537298289939.1537298289939.1537298289939.1&__hsfp=2913731818&hsCtaTracking=461ed61e-328b-41dd-8.

19. Map., Cybersecurity Supply/Demand Heat. [En línea] https://www.cyberseek.org/heatmap.html.

20. Spring Professional. Grupo Adecco. *XIII INFORME LOS + BUSCADOS 2018.* 2018.

21. *SO/IEC 27032:2012. Information technology-Security techniques-Guidelines for cybersecurity.* s.l. : ISO/IEC, 2012.

22. COMISIÓN DE LAS COMUNIDADES EUROPEAS. *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM(2007) 267 final.* Bruselas : s.n., 2007.

23. *Ley Orgánica 10/1995 de 23 de noviembre (BOE número 281).* Madrid : B.O.E.

24. Ministerio del Interior. *Estudio sobre la Criminalidad en España 2017.* 2017.

25. Cibersecurity Insiders and Crowds Research Partner. *INSIDER THREAT 2018 Report.* 2018.

26. Policía Nacional. *Plan Estratégico 2013-2016.* 2013.

27. CCN-CERT. *IA 07/18 Informe Anual 2017. Hacktivismo y Ciberyihadismo.* 2018.

28. CCN/CERT. *IA-09/18. Ciberamenazas y tendencias. Edición 2018.* 2018.

29. 2017., INCIBE. BALANCE seguridad. [En línea] 2018. [Citado el: 23 de Agosto de 2018.] https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_2017_final_esp.pdf.

30. DEPARTAMENTO DE SEGURIDAD NACIONAL. *Iinforme Anual de Seguridad Nacional 2017.* 2018.

31. Trend Micro. *Unseen Threats, Imminent Losses, 2018 Midyear Security Roundup.* 2018.

32. The Internet of Everything. Connections Counter. CISCO. [En línea] [Citado el: 3 de Septiembre 2018 de 2018.] https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342.

33. TrendMicro. 2018 Midyear Security Roundup. Unseen Threats, Imminent Losses. [En línea] https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf.

34. Check Point. *Cyber Attack Trends: Mid-Year Report 2018.* 2018.

35. Chatham House Report. . Cyber Security at Civil Nuclear Facilities. Understanding the Risks. [En línea] https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks.

36. Schneier, Bruce. *Secrets and Lies. Digital Security in a Networked World.* s.l. : John Wiley and Sons, 2000.