Temas candentes de la Ciberseguridad

Un nuevo espacio lleno de incógnitas

Crecimiento Inteligente

Un programa para apoyar a las empresas y a las Administraciones Públicas en el tránsito hacia un nuevo modelo productivo sostenible basado en la innovación, la calidad, el talento y el valor añadido.

pwc

www.pwc.es

Índice

Un nuevo espacio lleno de incógnitas

Gonzalo Sánchez
Presidente de PwC España

Si hay un mundo que ha evolucionado drásticamente en los últimos años ha sido el tecnológico. La llegada de Internet a nuestros hogares, a nuestras empresas y a nuestro día a día ha revolucionado la manera de comunicarnos y de hacer negocios, poniendo un innumerable abanico de opciones a nuestra disposición en tan solo un instante.

Al mismo tiempo, crecen los riesgos relacionados con las nuevas tecnologías y podríamos afirmar que un buen número de organizaciones y de usuarios no son plenamente conscientes de las amenazas a las que todos estamos expuestos en este campo.

Todos somos actores y partes en el ciberespacio y tenemos que saber que nos ofrece una miríada de alternativas, pero también hay riesgos que es preciso gestionar.

Teniendo en cuenta que estamos ante un riesgo global, con algunos condicionantes novedosos y que puede tener consecuencias graves para la economía o la seguridad de los ciudadanos, cabe preguntarse si estamos preparados para asumir los desafíos a los que nos enfrentamos y de las respuestas necesarias para afrontarlos.

¿Estamos gestionando adecuadamente nuestra Ciberseguridad? ¿Somos realmente conscientes de las amenazas que existen en este ciberespacio? ¿Tenemos las herramientas necesarias para hacer frente a estas amenazas? ¿Estamos perdiendo un tiempo precioso para gestionar unos riesgos que pueden afectarnos en mayor medida de lo que pensamos?

En PwC estamos convencidos de que es preciso hacer una reflexión conjunta por parte del sector público, de las empresas y de todos aquellos que tengan algo que aportar, porque nos jugamos mucho como país, como ciudadanos e incluso como entidades públicas y privadas. Solo desde la colaboración, la coordinación y el intercambio de información es posible avanzar en un campo en el que es muy complicado hacerlo en solitario.

Al mismo tiempo, es fundamental tener claro que avanzar en materia de Ciberseguridad se consigue con soluciones que trasciendan lo puramente tecnológico. Se necesita un nuevo marco legal, se necesita reforzar la colaboración entre los poderes públicos y las empresas, se necesita concienciar a la población y, también, se necesitan nuevas herramientas tecnológicas capaces de neutralizar ataques cada vez más sofisticados.

Lo que está claro es que se trata de un asunto que no puede obviarse ni dejar de abordar con solidez y atención. Algunos de los foros más prestigiosos lo han incluido dentro de sus agendas, como el World Economic Forum de Davos, del mismo modo que los consejos de administración de la mayoría de empresas y los órganos de dirección de las grandes organizaciones. Los escándalos de incidentes de

Ciberseguridad a gran escala se han abierto hueco en los informativos de todo el mundo. Wikileaks, Anonymous, Edward Snowden u otros más recientes como Sony, han avivado el debate y han puesto de manifiesto que estamos en un entorno en donde no todo es tan seguro como parece.

Con el fin de identificar la dirección que es necesario tomar y los campos en los que es preciso focalizarse, en PwC hemos puesto en marcha la publicación ***Temas Candentes de la Ciberseguridad en España, un nuevo espacio lleno de incógnitas***. El proyecto se inscribe en el marco de *Crecimiento Inteligente*, una iniciativa de PwC, cuyo objetivo es abordar los asuntos clave que marcan el presente y el futuro de nuestro país desde una perspectiva plural.

A partir de un debate donde han participado responsables del mundo académico, empresarial e institucional, hemos recogido las ideas y opiniones sobre un tema tan relevante, tanto para el sector público como para las empresas. El mundo globalizado es cada día más complejo y la velocidad a la que se suceden los cambios aumenta por momentos. Por ello, es especialmente importante abordar esta cuestión lo antes posible y de manera conjunta con los principales agentes involucrados para definir una solución que garantice la seguridad de instituciones, empresas y ciudadanos.

La Ciberseguridad es un asunto clave plagado de incógnitas que tienen que ser abordadas por los líderes públicos y empresariales de nuestro país. Por eso creemos que es un tema candente que merece la pena analizar en un marco plural en el que representantes de diferentes ámbitos aporten sus conocimientos y experiencia en aras de avanzar de manera conjunta. Esperamos que nuestra iniciativa sirva como punto de encuentro, pero también como punto de partida para impulsar un debate especialmente relevante.

Participantes

Este documento tiene su origen en las aportaciones de un grupo de trabajo formado por profesionales y expertos relacionados con los riesgos tecnológicos. Aunque ha sido elaborado por PwC, el informe recoge las valiosas indicaciones y contenidos planteados y contrastados en una reunión de trabajo celebrada el pasado año.

Un borrador previo al documento definitivo fue remitido antes de su publicación a los expertos que participaron en el debate. No obstante, esto no significa que los miembros del grupo tengan que identificarse con la literalidad del documento final, ni siquiera con la selección de temas identificados como candentes.

Desde PwC queremos agradecer las aportaciones de los participantes en la sesión de trabajo, su tiempo y su interés a la hora de participar en esta iniciativa.

Responsable de la iniciativa

Jordi Sevilla, *senior counselor* de PwC. Exministro de Administraciones Públicas.

Relación de participantes externos a PwC

- Javier Candau, Centro Criptográfico Nacional.
- Juan Cobo, Ferrovial.
- Javier García Carmona, Iberdrola.
- Fernando Hervada, ENEL.
- Guillermo Llorente, MAPFRE.
- José Mañas, Universidad Politécnica de Madrid.
- Javier Nozal CNMV.
- Miguel Rego, Instituto Nacional de Ciberseguridad, INCIBE.
- Elvira Tejada, Fiscalía General del Estado.
- Marta Villén, Telefónica.

Responsables por parte de PwC

- Elena Maestre, socio responsable de Seguridad y Riesgos Tecnológicos de PwC.
- Javier Urtiaga, socio de Seguridad y Riesgos Tecnológicos de PwC.
- César Tascón, director de PwC.
- Ignacio García López, *senior manager* de PwC.

Resumen ejecutivo

Se podría decir que la palabra "Ciberseguridad" está de moda. En el mejor de los casos, se puede afirmar que es una inquietud; en muchos otros, simplemente una incógnita. En ocasiones, sí somos conscientes del impacto que podría causar, pero desconocemos en qué medida estamos expuestos. En otros casos, lamentablemente, ni tan siquiera eso.

Es innegable que la sociedad se ha lanzado a explorar un apasionante mundo global, donde las telecomunicaciones y la tecnología han puesto al alcance de un "click" y de nuestros bolsillos infinitas posibilidades. Sin embargo, persiste una sensación de estar ante algo desconocido. No importa quién sea el explorador: usuario, negocio, ciudadano, Administración, fuerzas de seguridad, etc. Todos nosotros hemos avanzado sin tener muy claro el destino final o el camino a seguir. Obviamente, hay quien se aprovecha fraudulentamente de estas incertidumbres.

¿A qué nos referimos cuando hablamos de Ciberseguridad?

Aunque se trata de un concepto de actualidad que está presente en la agenda de administraciones y empresas, el término Ciberseguridad sigue siendo difuso y no siempre se entiende de la misma manera en todas partes. En lo que todo el mundo se pone de acuerdo es en el carácter global de las amenazas y, por ende, en la necesidad de encontrar soluciones igualmente globales para hacer frente a estos nuevos desafíos.
A la hora de utilizar o entender este concepto, es preciso tener en cuenta que se trata de algo que va más allá de la tecnología y, por tanto, debe ser abordado desde una óptica multidisciplinar que tenga en cuenta la variable legal, organizacional o de seguridad, entre otras. No se trata de una cuestión de ordenadores y redes, sino de un fenómeno más complejo que incluye múltiples aspectos y que afecta a instituciones, empresas y ciudadanos.

Hoy día, al hablar de Ciberseguridad se tiene muy en cuenta el concepto de "**amenaza**". Si hasta ahora el objetivo era "proteger" el perímetro; hoy prima la anticipación y la observación de los riesgos con el fin de prevenir los ataques. Ya no es posible vivir de espaldas a los riesgos confiando en un escudo más o menos seguro; ahora es preciso prevenir y prepararse antes de que el asalto tenga lugar.

Aunque no cabe duda de la importancia de la **tecnología** en el campo de la Ciberseguridad, es preciso entender que se trata de una materia que no se acaba en lo que sucede en un ordenador. Es precisamente el efecto multiplicador de las redes y la capacidad de estas para amplificar un ataque lo que hace de la Ciberseguridad un concepto más complicado que requiere soluciones más complejas.

En todo caso, a la hora de abordar esta materia es necesario articular una **respuesta multidisciplinar**. La multiplicidad de factores y la necesidad de aunar fuerzas desde distintos ámbitos (legislación, sensibilización social, colaboración público-privada, etc.) exige avanzar desde la colaboración con una óptica integral que vaya más allá de la tecnología.

Cuando la red me amenaza

En los albores de Internet, cuando se restringía su alcance casi exclusivamente a redes académicas o militares, los primeros ataques eran más parecidos a un juego que a una amenaza real, aunque pudieran generar impactos que hoy serían catastróficos. Pero actualmente se trata de algo profesional y que mueve miles de millones. Organizaciones criminales y entidades gubernamentales se han apoyado en el ciberespacio para sus operaciones. Es aquí donde aparecen las amenazas, tanto a nuestros intereses como a nuestros derechos.

El ciberespacio tiene una característica general nunca vista hasta ahora, que es la exposición. Esa inmensa capacidad de comunicación y de acceso, de intercambio de información con otros, es una espada de doble filo.

Los mismos procesos y las mismas tecnologías pueden dar lugar de igual modo a un nuevo negocio o a una nueva amenaza, alcanzando miles de millones de potenciales clientes o de potenciales víctimas.

Para hacer frente a estas amenazas, el elemento fundamental es la información, que se ha convertido en el activo principal de muchas organizaciones y es el objeto de muchas de estas amenazas. Pero también es la evidencia de la realidad, el registro indudable de lo que está pasando. La respuesta a dos preguntas: ¿qué está pasando? y ¿cómo ha pasado?

Esta información es cerrada, compleja e ininteligible para casi todos. Pero la clave está en procesarla y traducirla al lenguaje adecuado. Que sea accesible y fácil de entender por todos, víctimas y actores de estas amenazas. Porque con esa información es como iremos adquiriendo consciencia y estaremos facultados para ir tomando las decisiones que nos incumban de la manera más adecuada posible.

Cabe recordar que la capacidad de protección empieza en cada uno de nosotros, pero necesita apoyo. Para ello, todos en nuestro papel debemos ser conscientes de lo que podemos aportar, pero hay un actor clave, la Administración.

No estoy solo. El papel de la Administración

La Administración Pública es un entorno complejo. Por eso, cuando se trata de ser ágiles y de adaptarse a un escenario cambiante, es difícil que genere una respuesta rápida y puede llegar a lastrar a otros agentes. En realidad, de la Administración dependen muchos de los factores claves de éxito en el mundo de la Ciberseguridad. Las grandes empresas de este país disponen, en muchos casos, de los conocimientos y las herramientas tecnológicas adecuadas para hacer frente a los perfiles de atacante más frecuentes y sencillos. Pero quién, si no es la Administración, va a poder colaborar en casos más drásticos donde el atacante está organizado y profesionalizado e incluso apoyado por toda la maquinaria nacional de una potencia extranjera. Quién les va a decir que colaboren y se coordinen porque se están enfrentando a lo mismo, a dos organizaciones, compañeros y competidores en un sector, que temen que su debilidad les reste negocio en beneficio del otro. Quién puede proveerles de marcos administrativos y jurídicos para protegerse y perseguir a los atacantes que obran con una sensación de impunidad absoluta amparados en el supuesto anonimato de la red. Quién va a proteger a aquellos que no pueden hacerlo por sí mismos, como las pequeñas y medianas empresas o los ciudadanos, actores también de este escenario global de Ciberseguridad.

La respuesta, tan sencilla y compleja al mismo tiempo, está en manos de la Administración. Cuerpos de seguridad, reguladores, jueces, fiscales u otros poderes, deben estar alineados para defender con los mismos criterios del mundo tradicional el nuevo escenario cibernético. Para ello, todos deben ser conscientes de cuáles son las diferencias y las nuevas reglas del juego. Ese conocimiento está ya presente en muchos puntos, tanto de la infraestructura empresarial privada, como de las instituciones académicas y la propia Administración. El siguiente paso es saber escucharles, entenderles y darles respuesta en tiempo y forma. Puede sonar sencillo, pero no lo es.

¿Estamos desarmados frente a las ciberamenazas?

Nos centramos en la tecnología cuando estamos hablando del mundo "ciber", y cierto es que no podemos dejarla de lado, pero no es lo único. Cuando nos referimos a las soluciones y armas que tenemos frente a las ciberamenazas, es preciso destacar que no solo nos estamos refiriendo a soluciones tecnológicas.

Es cierto que se trata del aspecto más desarrollado y, a priori, más útil para hacer frente a este tipo de riesgos. Nos bombardean con soluciones mágicas a nuestros problemas en materia de Ciberseguridad en forma de tecnología. En muchos casos la herramienta que necesita la víctima es simplemente una ley clara que persiga el delito, que sea robusta y que permita a los Cuerpos de Seguridad, a la Fiscalía y a la Judicatura la persecución eficaz de los delincuentes. Tan centrados estamos en las medidas de defensa que si éstas nos fallan nos sentimos abandonados.

En cierto modo no nos sentimos cómodos con lo que tenemos a nuestra disposición. Por muy robusta que sea la protección y la confianza que genere, ver cómo te están atacando sin éxito no es agradable. Un ataque siempre provoca inquietud porque hoy se ha podido con ello, pero se sabe que volverá otro día y lo hará de manera más fuerte, más sofisticada y más veloz, lo que genera cuestionamientos razonables sobre la preparación de la organización.

No obstante, esta inquietud no es negativa, al contrario. Lo que sería negativo sería acomodarse debajo del escudo.

Debemos ser capaces de trasladar la línea de actuación hacia los pasos previos a los ataques. Pasar de reaccionar ante lo que nos viene a anticiparnos y estar prevenidos. Las soluciones nos tienen que acompañar en ese camino. La regulación para perseguir al atacante es un buen ejemplo. La ley no puede quedarse simplemente en una tipología de delito con el que procesar, debe dar soporte a una investigación, a una actuación incluso antes de que lancen sus actividades.

Si esto se hace en el mundo real para prevenir el terrorismo o el crimen organizado, por qué no vamos a poder disponer de ello en el ámbito de la Ciberseguridad.

Este tipo de soluciones existen, pero menos desarrolladas que las tecnológicas de detección y defensa. Tenemos que aspirar a tener un entorno de desarrollo más dinámico y homogéneo, colaborando entre todos, para elaborar estas soluciones, donde ninguna de las áreas se quede atrás para poder estar a la altura del reto que suponen las ciberamenazas.

1

¿A qué nos referimos cuando hablamos de Ciberseguridad?

Ciberseguridad es un término que ha irrumpido con fuerza en nuestro día a día y es, seguramente, uno de los más difusos. Incluso entre los que pudieran considerarse los expertos del área podríamos encontrar grandes discrepancias si les pidiéramos definir los grandes conceptos que se engloban dentro del término "Ciberseguridad". Tanto es así que hasta los gobiernos que han decidido legislar al respecto, han encontrado dificultades para identificar los conceptos, los límites y los perímetros de los asuntos a abordar.

A efectos prácticos uno de los pocos puntos que parecen estar claros es la relevancia y globalidad que se le debe otorgar a la Ciberseguridad. No se trata de un tema informático, ni siquiera es solo un tema tecnológico, sino algo más complejo que va mucho más allá y que incluye otra serie de variables que es preciso tener en cuenta.

Estamos hablando de que la Ciberseguridad debe protegernos de un nuevo espectro de amenaza que nos afecta a todos. Instituciones, organizaciones, empresas y ciudadanos estamos expuestos a los riesgos del ciberespacio y a unas amenazas que, dado su carácter global, exigen una respuesta igualmente global.

Normalmente se incluyen dentro de Ciberseguridad aquellas actividades orientadas a responder a determinadas amenazas, que usando la tecnología e Internet como medio, puedan verse tremendamente amplificadas.

Podemos afirmar que cuando hablamos de Ciberseguridad estamos hablando de amenazas, de entender lo que está sucediendo, quién está detrás y por qué. Estamos hablando también de tecnología, inherente ya en todos los procesos, pero en éstos en particular en mayor medida. En este documento nos centraremos fundamentalmente en la tecnología como medio en la amenaza, pero aportaremos otras perspectivas a la hora de ofrecer respuestas.

Amenazas

Posiblemente uno de los puntos más relevantes en esta tendencia a darle relevancia a la Ciberseguridad es la importancia creciente del concepto amenaza. Anteriormente, cuando se hablaba de seguridad de la información, el punto central era la defensa del entorno, del perímetro, de los controles preventivos y detección, etc. Incluso en algún momento parecía que la seguridad era en sí misma un indicador que si alcanzaba un determinado nivel ya era suficiente. Hoy en día, la Ciberseguridad ha desplazado ese foco a la amenaza, a la observación del entorno en el que nos desenvolvemos.

Porque por mucho que nos empeñemos en pensar de otro modo, la evidencia está ahí. Argumentos del tipo "*quién va a querer atacarme a mí", "eso es muy poco probable que me pase*", etc. chocan con la cruda realidad de ver que, a nuestro lado, a alguno de nuestros competidores le están sucediendo.

Otra cuestión es el complejo equilibrio entre las ventajas para la concienciación global y los intereses particulares de los afectados a la hora de publicar la información relativa a un incidente. Hay países que incluso han legislado al respecto, pero al tratarse de normativa específica de un país puede parecer que estos episodios solo suceden en otros lugares, como es el caso de EEUU. Compartir información se revela como una pieza clave en los procesos relacionados con la Ciberseguridad, ya sea entre pares, o bien entre la Administración y las empresas o los ciudadanos, pues solo conociendo a qué nos enfrentamos podremos poner todas las soluciones a funcionar adecuadamente.

Tecnología

Al fin y al cabo, cuando estamos incluyendo el término "ciber" en un concepto, es porque tiene una componente tecnológica importante, se realiza a través de Internet, el medio es telemático, aprovecha una nueva tecnología, etc. Pero es fundamental tener claro que no solo se centra en aquello que se puede hacer desde un ordenador o desde la Red, sino que incluye también aquello que aprovechando esos elementos, adquiere una nueva dimensión. Un ejemplo podría ser el tradicional virus informático del que todos hemos oído hablar y que, evidentemente, es una amenaza de seguridad. Se convierte en una amenaza de Ciberseguridad cuando se les dota de toda la complejidad que poseen ahora. Hoy es posible "contaminar" millones de ordenadores en todo el mundo, infectados con un virus y comunicándose con un centro de control en una red de "ordenadores zombie" o "botnet" para ponerlos a disposición de un atacante. El ataque puede resultarle rentable al delincuente simplemente por el daño realizado al ponerlos a la vez a conectarse a una página web en el mismo instante, o buscar quienes de ellos son clientes o empleados con acceso a una determinada organización, para utilizarlos como puerta de entrada.

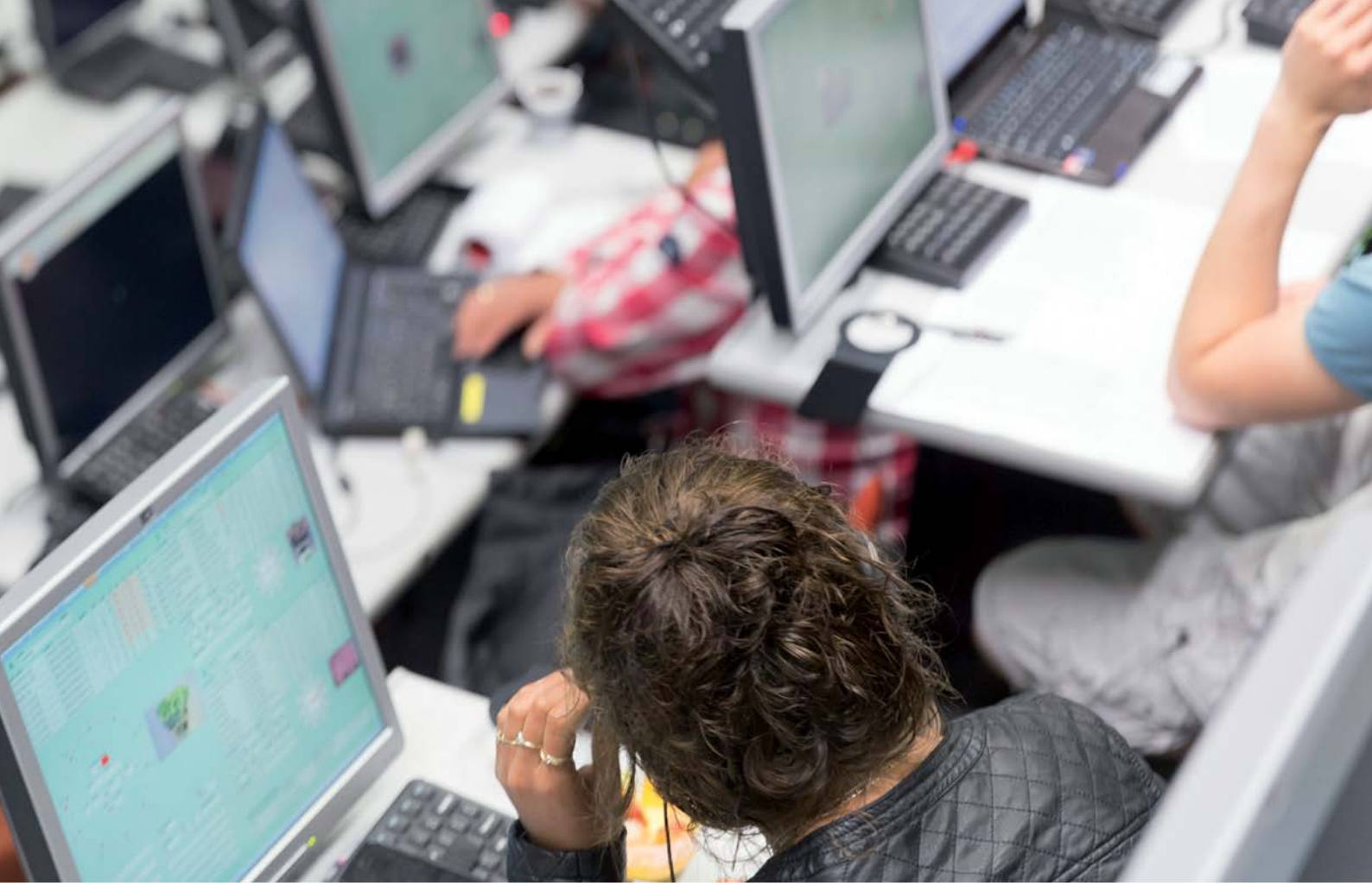
Otro ejemplo puede ser el robo y fraude con tarjetas de crédito, algo que ha existido desde su invención se convierte en un asunto relacionado con la Ciberseguridad cuando se fabrican dispositivos específicos a medida de un modelo concreto de cajero automático para que encaje a la perfección y se coordina una operación para utilizarlos a la vez en todo el mundo, aprovechando al máximo los días desde su aparición hasta que se empiezan a desplegar medidas para contrarrestarlo.

El entendimiento de esa componente tecnológica es crucial para poder hacer frente a estas amenazas y más aún considerando a la velocidad a la que puede cambiar, porque se convierte en *driver* del éxito del escenario y es lo que va a provocar un cambio de tendencia, de que algo no pase, porque no funciona lo suficientemente bien para el atacante, a que de repente nos vaya a pasar a todos.

Respuesta multidisciplinar

Aunque el entendimiento tecnológico sea una pieza fundamental para la Ciberseguridad, no quiere decir que el mejor enfoque para hacer frente a este problema sea desde una perspectiva puramente centrada en las tecnologías de la información.

Para entender que la Ciberseguridad va más allá de la tecnología, se puede hacer un paralelismo con el fenómeno de las redes sociales. En el plano tecnológico, los *social media* no son más que un nuevo mecanismo de comunicación que ha desplazado a otros anteriores, como los de mensajería o los *chats*.



Una movilización, coordinada y distribuida con la inmediatez de estos medios, puede tener un impacto incalculable y las herramientas tecnológicas habituales no solo no funcionan, sino que, en muchos casos, pueden ser contraproducentes.

A modo de ejemplo, cabe citar el caso de Sony, uno de los episodios de ataque más famosos de los últimos meses. Hace ya algunos años la multinacional japonesa se enfrentó a un ataque coordinado que desembocó en el robo de datos de millones de usuarios, el cierre temporal de su red de juego online y pérdidas multimillonarias. El desencadenante fue un decidido movimiento legal que lanzaron contra el primer usuario que logró saltarse la protección de la PlayStation 3. Lo que pretendía ser una acción de disuasión, tuvo un efecto llamada demoledor con los datos personales y de pago de más de 70 millones de usuarios comprometidos.

En los últimos meses han vuelto a aparecer noticias preocupantes relacionadas con la Ciberseguridad. La filtración a la red de sus últimas producciones se produjo, supuestamente, como respuesta de Corea Norte al contenido de una de sus películas. Muchas incógnitas existen todavía en este caso, pero el mismo presidente Obama tuvo que comparecer ante los medios al hilo de este escándalo.

¿Propaganda? ¿Maniobras de distracción? Probablemente nunca lo sabremos, pero, desde luego, se trata de un caso que tiene bastante más transcendencia que un mero problema tecnológico.

Debido a la multiplicidad de variables resulta especialmente complicado gestionar los ciberataques. No solo son mundos muy diversos los que deben coordinarse para dar respuesta a una amenaza de Ciberseguridad, sino que, probablemente, para cada una de ellas, el equipo y el planteamiento deberían ser distintos.

2

Cuando la red me amenaza

Desde los albores de lo que ahora conocemos por Internet, abrir las puertas de un entorno propio a la "red de redes" ha supuesto innumerables ventajas, pero algún que otro inconvenientae. Al principio era un juego, un mensaje al administrador, una página modificada, etc. Generalmente inofensivo en un principio, ha ido profesionalizándose hasta límites sorprendentes.

Un poco de historia

Recientemente se han cumplido 25 años del "Gusano de Morris". Conocido popularmente con ese nombre, aunque no fue el pionero en demostrar la posibilidad de que un programa se replicara a sí mismo, sí que fue el que obtuvo notoriedad de manera general. Lo que para el autor iba a ser una broma, acabó en el caos y el colapso de la red de entonces.

En aquel tiempo (1988), la red se denominaba ARPANET y era un experimento entre los mundos académicos y militares de Estados Unidos, concentrado en facilitar el acceso y el intercambio de información. Por ello, los mecanismos y protocolos que nacieron en aquella época adolecen de mecanismos de seguridad que hoy ya no son, pero que se mantienen. Por ejemplo, el correo electrónico: aunque ha habido multitud de esfuerzos por cambiarlo, su envío se realiza de tal manera que prevenir que te inunden de mensajes no deseados o donde el origen está falsificado es una misión casi imposible.

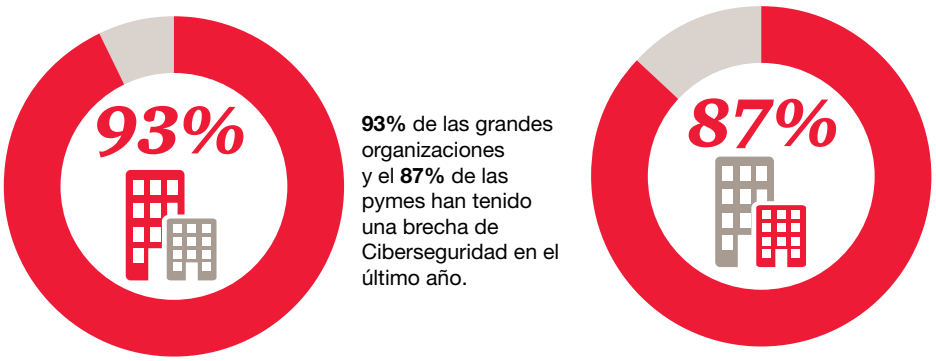
Aquel gran incidente del "Gusano de Morris" fue el desencadenante de la creación del primer CERT (Computer Emergency Response Team) ante el escenario obvio de que en la red podía haber acontecimientos que requerían una actuación inmediata para evitar que se produjera un daño relevante. Desde entonces esta importancia no ha hecho más que crecer existiendo cientos de CERT entre públicos y privados.

Detrás de ellos se escondía habitualmente un profundo conocimiento técnico y un afán por demostrar que "se podía" realizar un programa así, de obtener notoriedad por la complejidad y grado de difusión de su creación.

Este mismo afán de ser reconocido por sus hazañas, fue el que marcó las siguientes etapas. Metidos ya dentro del mundo más extenso de una Internet más genérica y global, los distintos organismos quieren tener presencia y las empresas se están lanzando a intentar desarrollar sus negocios.

Ese fue el entorno en el que fueron creciendo grupos autodenominados *hackers*, deseosos de explorar ese mundo, sin tener a menudo claros los límites de sus actividades. Curiosos por naturaleza, fueron encontrando un ciberespacio inmaduro en medidas de seguridad, que les permitía avanzar a su antojo.

Figura 1.



Fuente: PwC, 2013, Information Security Breaches Survey.

Los incidentes más típicos eran los "*defaces*", modificaciones de las páginas web a gusto del atacante como demostración del acceso, a menudo con su propio mensaje y pseudónimo. Otras veces el acceso permanecía más tiempo oculto, sin actividad ni daño alguno.

Situación actual

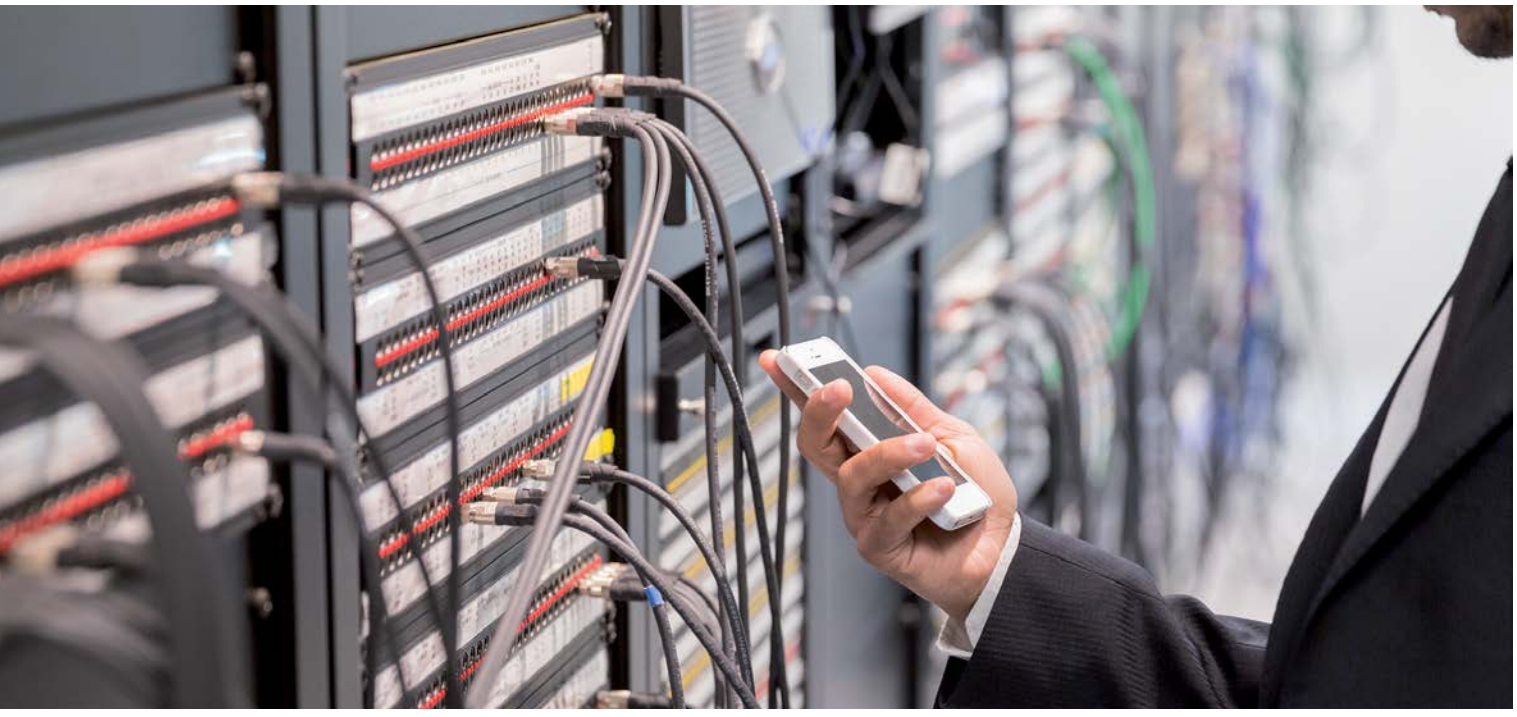
No ha sido hasta los últimos años cuando se ha percibido un cambio de tendencia. Lento pero definitivo: la profesionalización. Organizaciones de todo el mundo han sabido ver en la red un campo de actuación para sus operaciones. De esto modo, mafias organizadas o entidades a la sombra de algún gobierno han seguido un método similar. Ellos tienen claros sus objetivos: fraude, información estratégica o propiedad intelectual, entre otros. Ellos saben perfectamente lo que tienen que hacer una vez logren el objetivo y simplemente se han apoyado en aquellos que pudieran tener el conocimiento suficiente para obtenerlo.

Esta maquinaria puesta en marcha como si fuera una gran empresa nos ha llevado a la situación que tenemos en la actualidad. La amenaza es mayor que nunca porque la motivación dejó de ser intelectual o de notoriedad para ser, como mínimo, económica.

Escenarios actuales: la empresa

Las empresas han sido las que han visto en primer lugar este cambio de perfil en la amenaza externa y fundamentalmente las del entorno financiero. Sus activos económicos han sido siempre objeto de deseo de los amigos de lo ajeno, tanto en el mundo físico como en el digital.

Ya hace unos cuantos años descubrieron que iban a ser el foco de amenazas ciber que no tenían contempladas: clonación de tarjetas, modificaciones de cajeros automáticos, *phising*, *pharming*, troyanos, etc. Todo ello desarrollado específicamente para cada empresa.



También descubrieron que no era un tema puntual, sino continuo, y que tenía un impacto real y tangible para sus intereses como empresa.

En su caso, la amenaza se ha profesionalizado tanto que hasta tiene su propio modelo de negocio como proveedor de servicios orientados al fraude. En el mercado negro puedes comprar por unos pocos miles de euros todo un "kit" preparado para que cualquiera organice un ataque o puedes comerciar con datos robados, como números de tarjeta o datos de acceso a la banca por Internet.

Otros sectores han descubierto más tarde la relevancia que podía tener para ellos el panorama de ciberamenazas y han visto el mismo escenario global, donde, aunque no conocen el riesgo real al que se enfrentan, entienden que el impacto podría ser demoledor. En todas las industrias se ha registrado algún gran incidente que les ha hecho reflexionar sobre su vulnerabilidad.

Esta inquietud desde las más altas instancias es, sin duda, uno de los aspectos que ha cambiado el concepto de Ciberseguridad en la actualidad.

Escenarios actuales: los usuarios

Los usuarios somos otro de los grandes cambios de este escenario "ciber". Hemos pasado todos de la retaguardia al frente de batalla en un abrir y cerrar de ojos debido a nuestros hábitos de consumo. Suele decirse que la seguridad de una cadena es la de su eslabón más débil. Hoy por hoy, ese eslabón parece estar en el factor humano.

El riesgo aparece simplemente por ser clientes de cientos de servicios digitales y formar parte del entramado digital del ciberespacio con nuestras conexiones a Internet, nuestros *smarphones*, etc.

Por ello, hemos pasado a ser víctimas y objetivos de los ataques y, en muchos casos, incluso miembros involuntarios de un ejército en manos desconocidas.

Es muy fácil, una vez se tiene la maquinaria suficiente, operar a gran escala. Ese ordenador de casa, que va un poco lento puede ser parte, junto con algunos millones más, de una red de equipos zombies o *botnet* en manos de un atacante mínimamente organizado. Incluso puedes alquilarlas por horas por unos pocos euros.

Es importante tener en cuenta que cada sistema puede ser más o menos peligroso en función de las manos que lo manejen. En los casos más básicos, simplemente por la capacidad del propio equipo dentro de Internet o por la actividad que tiene el usuario (desde robo de sus claves, hasta espionaje y extorsión con sus correos o imágenes de la webcam).

En otros, más elaborados, es la estructura de lanzamiento ideal. Quizá alguno de esos usuarios de la *botnet* es empleado de la organización que busca el atacante o incluso se mandó al correo personal ese documento confidencial para trabajar el fin de semana.

Escenarios actuales: la defensa nacional

Con este escenario sobre los usuarios y las empresas, es lógico pensar que hay que ir más allá. La visión global de estas amenazas y la capacidad para reaccionar ante ellas simplemente transciende hasta un asunto de Estado.

Porque al Estado es a quien le corresponde la defensa de sus ciudadanos y de los intereses económicos de sus empresas. Si algo nos queda claro con estas amenazas es que el impacto puede ser muy alto. En este punto hay que tener en cuenta que, al fin y al cabo, la infraestructura crítica nacional (electricidad, agua, transporte, banca, etc.) también está compuesta de sistemas informáticos y puede ser objetivo de un ciberataque de consecuencias catastróficas.

Desde ese punto de vista, el espectro de las amenazas es muy superior, así como el potencial número de víctimas, atacantes y obligaciones dentro del escenario internacional.

También es mayor la complejidad de las acciones a realizar y dudosos los límites de éstas. Las medidas de seguridad suelen tener un coste en la funcionalidad o usabilidad del entorno y lograr un balance adecuado es complejo. Por ejemplo, la monitorización de ciertas comunicaciones puede ser un medida de seguridad efectiva; pero, ¿hasta dónde se puede invadir la privacidad de los ciudadanos aunque el objetivo sea protegerles?

Principales conclusiones

- **Los atacantes se han profesionalizado** enormemente en los últimos años y cuentan con grandes infraestructuras y organizaciones para lograr sus objetivos.
- **La motivación** de las grandes ciberamenazas no es técnica ni intelectual, sino económica o política.
- **Todos los usuarios de Internet somos víctimas potenciales** y estamos sujetos a amenazas constantes por el propio uso de la tecnología.

3

No estoy solo. El papel de la Administración

Tenemos que reconocerlo: el panorama actual es poco alentador. Es muy fácil sentirse perdido y desorientado en lo que respecta a Ciberseguridad y, lo que es peor, solo. El mismo ruido que nos llena las noticias de exóticas historias de *hackers* o el buzón de correo de *spam* hace que veamos más lejos una solución realista al problema o un camino claro al que dirigirnos.

No cabe duda de que sigue habiendo aspectos sin resolver, dudas básicas que cualquiera puede plantear y que no pueden quedar sin respuesta. Porque el derrotismo en Ciberseguridad es sinónimo de una condena segura.

Cuando estamos sufriendo un ataque, digital o físico, necesitamos saber que estamos protegidos o que podemos estarlo; que se puede evitar; que el delincuente no quedará impune o que otros ya han pasado por eso y lo han superado. Pero en el campo de la Ciberseguridad no siempre se percibe así por parte de los usuarios.

No hay nada más desalentador que una respuesta negativa y absoluta. Si tenemos que asumir que no podemos hacer nada ante un ataque (más que esperar a que acabe) y además creemos que poco podemos hacer legalmente en el caso improbable de que llegáramos a identificarlo, estamos perdiendo la batalla. La consecuencia inmediata es que el usuario se sentirá solo, abandonado y, seguramente, derrotado.

La llave de muchas de estas respuestas está en la Administración. Ella es la responsable de instrumentalizar las iniciativas y poner en marcha su maquinaria. Esta actividad podría estructurarse en cuatro roles principales que debe asumir la Administración: impulsor, regulador, protector y coordinador. Se trata de cuatro papeles imprescindibles que el sector público debe desempeñar con el fin de asegurar una variable clave en materia de Ciberseguridad: la necesaria colaboración entre los distintos agentes públicos y privados.

El papel como impulsor

La crisis económica que hemos atravesado en los últimos años se ha traducido en ajustes presupuestarios, desde la Administración a los ciudadanos, pasando por todo tipo de empresas y organizaciones.

Partiendo de esa coyuntura, impulsar cualquier iniciativa nueva que no redunde directamente en una reducción de costes o aumento de los ingresos resulta especialmente complicado en cualquier organización. Por ello, uno de los principales roles de la Administración es el de impulsar el crecimiento y la protección en materia de Ciberseguridad.

Para ello, dispone de múltiples organismos, unos para definir y estructurar ese crecimiento y otros para desplegarlo. De este rol han salido, entre otras, iniciativas muy diversas, como la creación del Instituto Nacional de Ciberseguridad-INCIBE (anterior INTECO), el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el Centro Criptológico Nacional (CCN), la aprobación del Esquema Nacional de Seguridad (ENS) y, a nivel militar, el Mando Conjunto de Ciberdefensa o la formulación de la Estrategia Nacional de Ciberseguridad.

Parece claro que el rol de impulsor está bastante patente en nuestra Administración. Sin embargo, con la amenaza creciente del mundo “ciber”, la duda que surge es si somos capaces de ser lo suficientemente ágiles como para estar a la altura.

Solo una apuesta decidida y el compromiso de los distintos actores pueden llevar a buen puerto a este barco sin temer el temporal, sorteando los escollos que se lo puedan impedir.

Ese esfuerzo impulsor tiene un largo camino, y ser lo suficientemente intenso como para atravesar las distintas capas de la Administración y llegar a la ciudadanía, esto es, ser palpable en nuestras casas y nuestras empresas.

Hasta que a nuestros hijos no les eduquen en las escuelas y universidades sobre los peligros de la red, cómo intentarán engañarles o el riesgo que entrañan las redes sociales, no habremos conseguido que el impulso sea adecuado.

No se verá, mientras los ciudadanos y las empresas no seamos conscientes de que el Estado nos protege, que las fuerzas del orden son capaces de responder a estas amenazas, pero que nosotros tenemos que hacer nuestra parte. Entonces podremos hablar de que el impulso ha sido el correcto. Hasta entonces, simplemente tendremos que ver lo mucho que nos queda por avanzar.

El papel como coordinador

Cuando nos enfrentamos de manera común a una amenaza externa cada dato y cada detalle pueden ser relevantes.

Ya no estamos tratando con iniciativas individuales, sino con un modelo de atacante sistemático y bien organizado, con lo que es de esperar que habitualmente, las técnicas y herramientas tecnológicas utilizadas se vayan repitiendo a la vez que mejorando en cada iteración.

Si nuestra respuesta a esa amenaza es inicial en cada uno de los puntos, estaremos en una situación de absoluta desventaja. La única manera de poder hacer frente a estas amenazas es capitalizando la información existente y obtenida en un proceso de ataque, y utilizarla como punto de partida en el siguiente.

La dificultad estriba en encontrar el mecanismo adecuado para compartir este tipo de información de una manera neutral y buscando el beneficio común a largo plazo. Los diversos foros industriales que existen son un mecanismo, pero tienen el mismo hándicap: esa información puede ser de una importancia estratégica, puede ser una diferencia competitiva entre empresas en el mismo sector.

Ese es uno de los principales motivos para que la Administración, como responsable del interés general, deba hacerse cargo de este rol de coordinación.

Otra de las razones es debida al resto de papeles que juega dentro del mundo “ciber”. Los mecanismos de coordinación que establezca servirán también para tomar el pulso para identificar si las medidas de protección o

regulación están siendo adecuadas para hacer frente a las amenazas o hay que potenciar y darles más impulso.

Adicionalmente, también será el canal habitual de interrelación entre el mundo público, privado y la ciudadanía, así como la entrada natural de información internacional relativa a iniciativas globales o incidentes de gran escala. Por ello, es especialmente importante reforzar la coordinación internacional para colaborar con otros países u organizaciones que puedan aportar conocimientos, experiencias o recursos.

Varias iniciativas se han puesto en marcha ya con el objetivo de facilitar la coordinación entre partes, algunas amparadas en los CERT*, centros de respuesta ante incidentes del INCIBE, y del Centro Criptológico Nacional (CCN). Pero hay que seguir apostando por compartir información y hacerlo de manera proactiva y bidireccional.

Es preciso reforzar una estrategia proactiva, porque tenemos que desplazar nuestras líneas de actuación del "después" al "antes" de un incidente. Es importante saber reaccionar adecuadamente, pero nuestro objetivo tiene que ser que no se materialice o, en cualquier caso, lo haga con el mínimo impacto.

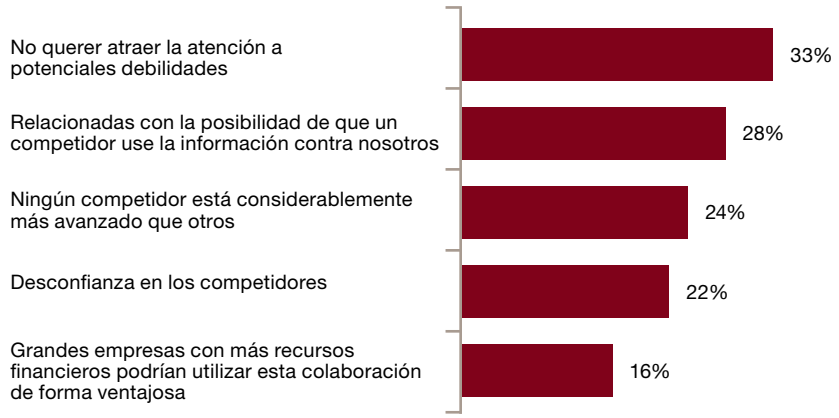
También tiene que ser una estrategia bidireccional porque no solo deben aprender los distintos colectivos de la información que les provee la Administración. También ésta debe escuchar atentamente. Lo que la industria y los expertos demandan es eso, sentirse escuchados en un ambiente de confianza mutua. Ellos también tienen mucho que aportar para construir entre todos un escenario donde las ciberamenazas sean menores.

El papel como regulador

La sensación de impunidad del atacante en el mundo de la Ciberseguridad es especialmente preocupante. Seguramente no haya ninguna otra actividad delictiva en la actualidad que comparta esa sensación.

* Este CERT es cooperado conjuntamente por INCIBE y por CNPIC, y su denominación es CERTSI o CERT de Seguridad e Industria.

Figura 2.
Razones para no colaborar en material de seguridad de la información



Fuente: PwC, Global Information Security Survey, 2013.

De hecho, dificulta las actuaciones porque las víctimas son reticentes a iniciar el proceso de una denuncia, desmotivadas en cuanto a su utilidad. Y eso nos ocurre porque a nivel legal, a pesar del esfuerzo de la Fiscalía, estamos por detrás de las amenazas. Aspectos como la suplantación y el robo de identidad en Internet no son claramente constitutivos de delito según nuestras leyes actuales.

Sin el marco legislativo adecuado, perseguir estas actividades se torna excesivamente dificultoso, principalmente porque buscar la semejanza con el delito tradicional dota de cierta inestabilidad a todo el proceso y no se puede perseguir la actividad en sí misma.

Otro aspecto fundamental del regulador es crear el marco donde encuadrar el resto de actividades que tiene que acometer la Administración (coordinación, medios, seguridad jurídica, etc.), así como el impulso definitivo para que se den los pasos necesarios.

Si queremos que nuestra infraestructura crítica esté protegida, lo primero es ayudarles a alcanzar el nivel necesario de conocimientos y protección. A continuación, la Administración tiene la obligación de regular los pasos, las medidas o los procesos necesarios, puesto que, teniendo en cuenta la disparidad de intereses de los diferentes actores, solo con el papel regulador de lo público será posible avanzar de manera coordinada.

En este sentido la Ley para la protección de infraestructuras críticas, fundamentalmente con el impulso del CNPIC, establece diversos instrumentos de planificación tendentes a homogeneizar los niveles de seguridad de los operadores críticos de los distintos sectores estratégicos para la sociedad.

La mayor dificultad vuelve a ser la velocidad y puesto que cada resquicio va a ser aprovechado para ganar tiempo por aquellos que se aprovechan de la situación, ya sea porque son parte de la amenaza o porque son reticentes a formar parte de la solución.

Otros problemas surgen como consecuencia del propio espacio de actuación de las amenazas “ciber”. Las regulaciones y legislaciones tienen, por definición, un ámbito de actuación delimitado. Pero “ciber” es un nuevo ámbito. ¿Cómo regular y perseguir un delito puramente digital? Las ubicaciones de atacantes, sistemas utilizados como medio, sistemas objetivos y propietarios de estos pueden ser totalmente dispares. ¿Qué jurisdicción debe aplicar?, ¿qué límites de actuación? Si ni tan siquiera en países afines la respuesta es uniforme a estas preguntas, poca esperanza podemos tener en el proceso. Y eso sin entrar a valorar que en algunos casos ciertas amenazas pueden estar soportadas gubernamentalmente.

Algunos pasos se han dado ya para formalizar un marco común, como el "Convenio sobre la Ciberdelincuencia". Firmado en 2001 en Budapest. Este documento era inicialmente de ámbito europeo y pretendía dar cabida a una estructura uniforme de actividades que debían considerarse delictivas, sobre las que sería preciso establecer una legislación uniforme.

De este modo se facilitaría la persecución internacional del ciberdelito. En la actualidad lo han firmado unos 50 países, incluidos, entre otros, EEUU, Japón y buena parte de América Latina. España firmó el convenio en sus orígenes, pero su contenido no ha entrado en vigor formalmente.

El papel como protector

Pero sin duda el aspecto más complejo en el que debe tener la Administración un rol crítico es en la protección.
Los cuerpos y fuerzas de seguridad del Estado y los servicios de Inteligencia, son los únicos capaces de ir más allá de la simple defensa pasiva ante las ciberamenazas.

Habrá áreas, organismos y principalmente empresas privadas que puedan encargarse de manera bastante solvente de la protección de sus activos y sus usuarios, pero otras estarán mucho más desamparadas. Además, incluso en el caso de que cada una pudiera tener un nivel de protección adecuado, la globalidad de todos los actores no puede suplirse con la de cada una de las partes.

Como mínimo, la Administración debería ayudar a definir las prioridades y los objetivos de protección, y ejercer el liderazgo en su consecución. Además, es preciso que el sector público colabore con

la puesta en marcha de "Planes de Apoyo Operativo" que permitan impulsar y mejorar la colaboración público-privada en materia de Ciberseguridad.

Es una gran oportunidad para que, siguiendo la estrategia de protección que se defina, la Administración se dirija a las empresas y a los ciudadanos, así como para que se interese por su situación, por sus problemas y por el alineamiento de estos con la estrategia global. También es importante que en las instituciones, este contacto se haga al máximo nivel para ayudar a concienciar a los mayores responsables que son los que toman las decisiones.

La Estrategia de Ciberseguridad Nacional

A finales de 2013 se publicó oficialmente la "Estrategia de Ciberseguridad Nacional", documento firmado por el presidente del Gobierno. La expectativa que suscitó fue muy relevante y su lectura y análisis siguen centrando el debate del sector, junto con el borrador de la futurible Directiva Europea sobre Ciberseguridad (Network and Information Security, NIS).

La estructura que se ha establecido, gira alrededor de seis objetivos que persiguen, una meta final que ellos describen como:

"Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques".

En la estrategia se recoge de manera clara la intención de tomar el liderazgo en cuanto a la coordinación público-privada e internacional, adquiriendo las capacidades necesarias e impulsando la protección de la Administración Pública, el tejido empresarial y los propios ciudadanos.

Sin embargo, a la hora de ponerse manos a la obra en el lanzamiento de estas iniciativas, únicamente se establece la formación de dos comités bajo la estructura del Consejo de Seguridad Nacional. Esta estructura, sin duda necesaria, queda todavía muy lejana de algunos de los objetivos de la estrategia y de las propias necesidades de los usuarios.

En varias ocasiones se incide en que la responsabilidad para crear un ciberespacio más seguro para los intereses nacionales es compartida entre los distintos actores y que, aunque la propia Administración ejerza de líder y de coordinador, cada uno de los roles tiene su función y encomienda. Es por ello que algunos reclaman haber tenido más participación desde su propia concepción y que esta estrategia ya tenía que haber sido fruto de la colaboración entre el Estado y el sector privado. En cualquier caso, este documento sí que representa el compromiso por parte de la Administración en adquirir la mayor parte de los papeles que se necesitan para el desempeño eficiente de sus funciones en materia de Ciberseguridad, tal y como hemos venido enumerando: impulsor, protector y coordinador. Habrá que esperar todavía para ver su marcha y velocidad de despliegue, lo que se realiza a través del otro papel requerido, el de regulador en la materia.

La propia estrategia nacional de Ciberseguridad lo hace notar justamente en su último párrafo:

"La puesta en marcha [...] y la armonización de su funcionamiento con los órganos existentes, se realizará paulatinamente mediante la aprobación de las disposiciones normativas necesarias y el reajuste de las vigentes".

Esperemos que pueda ser lo suficientemente ágil como para responder al reto que tiene por delante.

Figura 3.
Objetivos de la Estrategia de Ciberseguridad Nacional

Principales conclusiones

- **La Administración juega un papel primordial** en el escenario "ciber", asumiendo retos principalmente como **impulsor, coordinador, regulador y protector.**
- Ante un desafío tan relevante, es necesario establecer canales de **comunicación y cooperación entre lo público y lo privado** o, de lo contrario, aumentarán las amenazas, disminuyendo la capacidad de ciudadanos y empresas para hacer frente al cibercrimen.
- **El mayor reto** que asume en general la Administración en todas estas actividades **es la agilidad** a la hora de adaptarse y responder a unas amenazas que cambian a una velocidad vertiginosa.
- **La comunicación y coordinación debe ser en proactiva** para que sirva a la hora de prevenir, no solo reactiva tras un incidente.
- **La Administración debe saber escuchar** las demandas de los distintos actores del escenario "ciber" y responder adecuadamente.

4

¿Estamos desarmados frente a las ciberamenazas?

Son tiempos inciertos en los que exploramos este ciberespacio con poca cautela y le confiamos nuestros negocios y nuestra intimidad a desconocidos. Ya hemos visto que las amenazas que nos acechan en ese mundo son muy relevantes y cuentan con grandes infraestructuras, métodos y tecnología para sus fines. Nosotros, por nuestra parte, disponemos de múltiples opciones; pero, ¿son suficientes?, ¿son adecuadas?

Para poder valorarlo tenemos que reflexionar acerca de las alternativas y las capacidades que nos aportan.

Recursos a nuestra disposición

Tenemos a disposición una miríada de herramientas para luchar contra las ciberamenazas. Existen múltiples *frameworks* y estándares que definen medidas de seguridad a adoptar, foros de discusión y debate, herramientas tecnológicas y, en definitiva, un interesante abanico en el que escoger.

Su adopción, como en todos los aspectos, tiene sus ventajas e inconvenientes. Pero tradicionalmente hemos venido dedicando demasiado esfuerzo a la parte tecnológica y hemos descuidado otras. Tendemos a pensar que se trata de un problema y de una amenaza tecnológica y que su solución también reside en la tecnología; pero lo cierto es que no es así. El ciberespacio es el nuevo ámbito de actuación propiciado por la tecnología. Las amenazas se generan y materializan en ese campo y no se puede ignorar la tecnología para combatirlas, pero tampoco podemos caer en el error de pensar que es la solución por sí misma.

El problema está localizado en la orientación de la mayor parte de estas herramientas tecnológicas. Uno de los principales problemas es afrontar estos

retos desde una óptica puramente tecnológica, pero también desde una actitud exclusivamente “defensiva”.

Esa parte del puzle está exhaustivamente desarrollada y se convierte en relativamente simple. Dependiendo de la capacidad de inversión, se van implementado medidas de protección (técnicas, organizativas, servicios, formación, etc.) que, aunque puedan ser difíciles de priorizar, van mejorando la situación.

Las otras áreas son las que tienen mayor dificultad porque están infinitamente menos desarrolladas. Principalmente por el hecho de que fuera de la actuación en tu propio entorno el terreno es más resbaladizo e incomprensible.

Herramientas más o menos pasivas ya tienen su complejidad. Llevamos unos meses donde las noticias se han poblado de escándalos relacionados con Ciberseguridad por espionaje y monitorización externa, principalmente con el caso Snowden, donde un exempleado de la Agencia Estatal de Seguridad de Estados Unidos desveló detalles de los programas masivos de vigilancia, tanto de sus propios ciudadanos como a otras naciones, incluidos sus aliados.

Tenemos una información muy valiosa en el exterior, que debemos ser capaces de analizar y dotar de criterio, así como de relacionarla y enriquecerla, pero no es algo sencillo ni siempre se sabe cómo proceder de manera adecuada.

Los límites son muy delicados y normas como la Ley Orgánica de Protección de Datos no están preparadas para marcar el camino en un mundo donde la entrada de las redes sociales en el panorama y la publicación voluntaria de datos en ellas es inmensa.

Legítima defensa

En el mundo físico existe el concepto de legítima defensa como causa que permite ciertas conductas que de otro modo serían sancionadas. Muchos reclaman su trasposición al mundo “ciber” y algunos países, como por ejemplo Holanda, lo han aprobado. Otros ni siquiera se plantean que puedan existir límites a las actuaciones en defensa de sus intereses.

España debe contar con capacidad de actuación, sobre todo a nivel empresarial, dado que se considera que no hay equilibrio de fuerzas. Los que están detrás de las amenazas, navegan sin bandera ni respeto alguno por legislación, norma o frontera. Por el contrario, el que se defiende de ellos e intenta hacerlo de manera activa, aparte de proteger sus intereses tiene que estar pendiente de las normas que le aplican, cosa que a menudo desconoce.

Por ahora los ámbitos de actuación no parecen ir por este camino, pero la indefinición no beneficia a nadie más que a los atacantes.

Soluciones de grupo

Extrapolando más allá de la tecnología, hay algunos elementos cuyo único sentido está en una acción colectiva. Principalmente aquellas orientadas a la continuidad de los procesos.

Mucho se ha hablado de la "Ciberresiliencia" en distintos foros, que podríamos entender como la capacidad de asumir y sobreponerse a un ataque, e incluso, de salir reforzado.

El riesgo de ver interrumpirse un servicio crítico, vital incluso, como la electricidad o el agua potable o la capacidad de transporte o de realizar operaciones financieras, sea seguramente el mayor de los miedos cuando estamos hablando de la amenaza "ciber" en su concepción más amplia.

Incluso foros globales como el World Economic Forum de Davos (que valoran las ciberamenazas como uno de los riesgos más relevantes a nivel global), entienden que las soluciones para garantizar la disponibilidad de los procesos críticos son soluciones de grupo. Ellos mismos incluso han lanzado una, el "Partnering for Cyber Resilience". Esta iniciativa pretende identificar el rol que cada organización juega en los procesos globales y trata de organizar una respuesta conjunta a un escenario de ataque al proceso y sus componentes.

Figura 4.
Prácticas en ciberseguridad por grandes regiones

	Sudamérica	Asia Pacífico	Europa	Norteamérica
Los gastos en seguridad aumentarán en los próximos 12 meses	66%	60%	46%	38%
Cuentan con una estrategia global de seguridad	75%	79%	77%	81%
Cuenta con un CISO o director de seguridad de la información	75%	74%	68%	65%
La alta dirección conciencia en materia de seguridad	68%	69%	51%	55%
Mide o revisa la eficacia de las políticas de seguridad y de los procedimientos del pasado año	70%	69%	53%	49%
Tiene una política de *backup* y recuperación/continuidad de negocio	58%	55%	45%	47%
Requiere a los terceros y proveedores en el cumplimiento de las normas de privacidad	55%	58%	55%	62%
Cuenta con formación y concienciación a los empleados en materia de Ciberseguridad	54%	63%	55%	64%
Tiene procedimientos para la protección de la propiedad intelectual	20%	24%	17%	21%
Cuenta con tecnología de detección de intrusiones	64%	67%	63%	67%
Tiene inventario de los datos personales que se recopilan, transmiten y almacenan	53%	60%	52%	64%
Colabora con otros para mejorar la seguridad y reducir los riesgos	66%	59%	45%	42%

Fuente: PwC, Global State of Information Security Survey, 2014.

Para acabar de andar este camino de colaboración y aprender realmente el funcionamiento de estas herramientas, la solución por la que se está optando es la simulación. Se trata de ejercicios de Ciberseguridad, donde se pone a prueba, no solo la capacidad tecnológica de las herramientas, sino la reacción de los recursos humanos en los procesos y actividades en caso de crisis. Se trata de ejercitarse en escenarios globales de emergencia para conocer de primera mano qué sucedería y las decisiones complejas a las que habría que hacer frente en caso de ataque.

En los entornos más maduros en cuanto a seguridad ya se han realizado las primeras iteraciones. En algunos casos, de adhesión voluntaria. En el Reino Unido, el propio Gobierno ha obligado a sus entidades financieras a participar en un ejercicio para verificar su capacidad, dado que se trata de una preocupación de Estado. Un ataque global a la cotización del mercado de valores y a las entidades que lo operan y participan sería un problema para el conjunto del país y por ello es preciso abordarlo al más alto nivel.

Las conclusiones que se obtuvieron de ese estudio van completamente en línea con lo demandado por las organizaciones, una coordinación única por parte del Gobierno, un marco legal más claro para estas amenazas y unos mecanismos de intercambio de información más ágiles y que aporten valor real.

Principales conclusiones

- **Las herramientas no son exclusivamente tecnológicas** cuando hablamos de hacer frente a las ciberamenazas.
- La mayor parte la actividad se centra en la **defensa y protección**, pero se tendría que ampliar el espectro de actuación, fundamentalmente mediante la anticipación y la prevención del impacto de las ciberamenazas.
- **Se requiere un mayor ámbito de actuación y adoptar un enfoque global** en vez de protegerse solo localmente.
- **Es conveniente probar la coordinación** de los distintos actores a la hora de reaccionar adecuadamente a una ciberamenaza como base para el aprendizaje y la confianza mutua.

Contactos

Elena Maestre
Socio responsable de Seguridad y Riesgos Tecnológicos de PwC España
+34 915 685 019
elena.maestre@es.pwc.com

Javier Urtiaga
Socio de Seguridad y Riesgos Tecnológicos de PwC España
+34 915 684 456
javier.urtiaga@es.pwc.com

César Tascón
Director de Ciber de PwC España
+34 915 685 362
cesar.tascon.alvarez@es.pwc.com

PwC ayuda a organizaciones y personas a crear el valor que están buscando. Somos una red de firmas presente en 157 países con más de 195.000 profesionales comprometidos en ofrecer servicios de calidad en auditoría, asesoramiento fiscal y legal y consultoría. Cuéntanos qué te preocupa y descubre cómo podemos ayudarte en www.pwc.es