d+i desarrollando ideas
LLORENTE & CUENCA

» Ciberriesgos y el nuevo paradigma reputacional

Madrid » 05 » 2017

"España es el quinto país del mundo con más sistemas que controlan todo tipo de instalaciones y procesos industriales conectados a Internet, la mayoría sin protección alguna[1]" . Son palabras de la periodista especializada en ciberamenazas, Mercè Molist. Según los datos de Molist, en España se multiplicaron el año pasado los ciberataques un 357 %. Aunque la cifra parezca una exageración, la del Instituto Nacional de Ciberseguridad (INCIBE) muestra que los ataques pasaron de 50.000 a más de 120.000 el último año. ¿Están las empresas preparadas para afrontar el reto que supone proteger su reputación? Algunas dirán que sí, pero el cambio regulatorio que supone la Directiva NIS y el nuevo Reglamento Europeo de Protección de Datos (GDPR), puede poner contra las cuerdas a más de uno. Vamos a tratar de aclarar todo a partir de este punto.

No desvelamos nada nuevo si afirmamos que la vulnerabilidad digital es muy alta para todas las empresas, solo cabe mencionar tres ejemplos. El ataque ocurrido hace unos días con el gusano WannaCry a más de 150 países. El ataque de denegación de servicio que

se produjo el año pasado a los servidores de Dym en Estados Unidos. Este incidente afectó a 1.000 millones de usuarios de empresas como Twitter, Amazon, Whatsapp o el New York Times. También resulta interesante recordar el ataque de unos ciberdelincuentes que consiguieron vaciar a distancia los cajeros automáticos de doce entidades financieras distintas en la UE. Y esto solo acaba de comenzar.

Para intentar limitar el daño, promover una cultura de la gestión de riesgos y asegurar que los incidentes sean reportados, se ha aprobado la Directiva para la Seguridad de la Información y de las Redes (NIS) y el nuevo Reglamento Europeo de Protección de Datos que estará vigente a partir de mediados de 2018. Ambas normativas están ahora en fase de ser transpuestas al ordenamiento jurídico en España y representan un cambio significativo en la cultura empresarial respecto a la privacidad, los derechos y las obligaciones en la seguridad del tratamiento digital de los datos personales y prestación de servicios.

El reglamento señala y obliga que, para mayo de 2018, cualquier tipo de brecha de seguridad, sea por ataque informático o por incidencia propia, deberá ser notificado al CERN (u organismo que finalmente se decida) en menos de 72 horas, así como a los propios afectados. Si la organización desconoce qué clientes están viendo sus datos personales comprometidos, deberá, además, comunicarlo de manera pública.

> – ¿Cómo? Pero si hago eso obviamente estaré gritando al mundo que los datos de mis clientes han sido comprometidos y poco después tendré a decenas de periodistas pidiéndome explicaciones.

[1] La ciberseguridad de la industria española es un sainete, y los ataques se están disparando Mercè Molist 2017 http://www.elconfidencial.com/tecnologia/2017-03-20/ciberseguridad-industria-espanola-infraestructuras-criticas_1350398/

– Efectivamente. Ese es el panorama.

Pongamos un ejemplo. Una entidad bancaria a la que le secuestren los datos de sus clientes, si no es capaz de determinar a cuántos de ellos les está afectando el ataque, deberá informar a todos. Da lo mismo que no haya trascendido. A partir de ahí las redes sociales harán el resto. Unos minutos más y la información no solo estará en Internet, sino en los medios de comunicación. Indiscutiblemente, la reputación y el valor de su acción (si su empresa es cotizada) se verán afectados.

"Las sanciones económicas pueden llegar, según lo previsto en el nuevo Reglamento Europeo de Protección de Datos, hasta millones de euros o el 4 % de la facturación general anual"

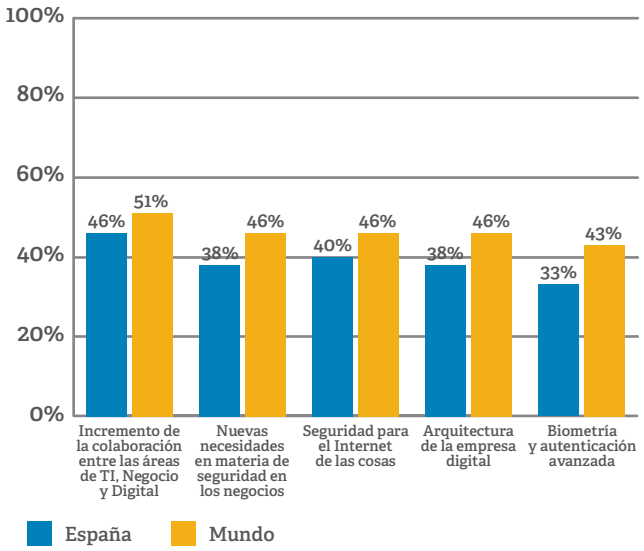
SANCIONES ECONÓMICAS

– ¡Ah! ¿Pero que hay más?

– No lo dude. Una norma sin su capítulo sancionador no es digna de tal nombre. Además de que le hayan hackeado, las sanciones económicas pueden llegar, según lo previsto en el nuevo Reglamento Europeo de Protección de Datos, hasta millones de euros o el 4 % de la facturación general anual.

Algunos Chief Information Security Officer (CISO) ya han llegado a calificar públicamente la ley como un auténtico chantaje normativo, que puede borrar del mapa a muchas empresas y que favorecerá aún más la formación de oligopolios.

Figura 1. ¿Dónde van a intervenir en ciberseguridad las empresas en los próximos doce meses?



Fuente: PwC, *The Global State of Information Security Survey 2017.*

– Pero, espere, que aún le va a tocar gastar un poco más, ¿o es que no ha oído aún hablar de la figura del Delegado de Protección de Datos? Todas las empresas deberán tener a alguien que les represente en esta función, bien dentro o fuera de la organización. Esta persona será el interlocutor único para todas estas cuestiones, se encargará de comunicar ante organismos y autoridades competentes asignadas todos los ataques sufridos o la exposición de cualquier clase de datos que se produzcan –una IP ya está considerado como un dato personal–. Es decir, será necesario dotarse de nuevos y específicos procedimientos de prevención, protección y gestión ante ciberataques, que implicarán una documentación, notificación y comunicación específica. Algunas grandes compañías que sufren decenas de ataques diarios tendrán que crear unidades específicas cuya misión será reportar los ataques sufridos a la administración y comunicar, en ocasiones, a los clientes.

EL NUEVO PARADIGMA DE LA SEGURIDAD

A estas alturas es importante ser consciente de que vivimos en un nuevo paradigma de la comunicación caracterizado por la información digital sincrónica, en red, líquida e inserta en un marco de hípertransparencia.

Pero hoy en día, cada uno de nosotros no somos solo un medio de comunicación en potencia, gracias a nuestras extensiones móviles, sino que también nos hemos convertido, por el mismo motivo, en un punto potencial de riesgo para toda organización en la que nos insertamos. Para la nuestra, eso sí, y para la de los demás. Somos un auténtico vector de riesgo. Y no es precisamente nuestro PC el punto más crítico. Seguramente nuestro puesto de trabajo está bajo la fuerte vigilancia del equipo informático. Pero, ¿qué pasa con nuestro teléfono móvil o nuestra *tablet*?

El paradigma de la seguridad no se ha adaptado a las nuevas dinámicas: comportamiento social digital, movilidad, *cloud* e información (*Big Data*). Nos hemos pasado los últimos años hablando de la transformación digital de las organizaciones sin preocuparnos, al tiempo, de los riesgos que tal cambio conlleva. La alta complejidad de los cuatro elementos señalados cambiará todo el planteamiento preventivo puesto que el perímetro a proteger es más extenso. De hecho, es un perímetro global. Nuestras conexiones son globales y, de igual manera que viralizamos la información globalmente en *real time*, y en cuestión de segundos, la amenaza se reproduce a la misma velocidad.

Es pues lógico que ante una vulnerabilidad de semejante envergadura, los Estados tomen cartas en el asunto para proteger el sistema, las organizaciones y las empresas buscando tener la trazabilidad completa de los datos. Pero ejercer el control en esta situación va a suponer una fuerte limitación de derechos y libertades. Solo es cuestión de tiempo que comencemos a sufrir un mayor control. Lo hemos visto recientemente tras el atentado de Berlín. Las autoridades alemanas clamaban por poder acceder a los datos de WhatsApp para luchar contra los terroristas. Los ciberataques no serán una excepción sino, más bien, una nueva motivación. Nos jugamos la seguridad de infraestructuras críticas, el sistema económico y la seguridad, como no, de los ciudadanos.

Siendo así, no falta mucho tiempo para que veamos diferentes niveles de acceso a los datos que van a suponer la definición de nuevas Cibercastas sociales. Diferentes perfiles de acceso, servicios y tarifas según la interacción de datos. Y éstos, a su vez, generarán castas sociales en función de nuestro nivel de vulnerabilidad.

LA NUEVA LICENCIA SOCIAL PARA OPERAR

Mantener la licencia social para operar ya no estará condicionada únicamente por mantener nuestra reputación a salvo. Al estar constantemente bajo la vigilancia del regulador, las empresas se van a ver obligadas a demostrar, de forma constante, que protegen de manera eficiente los datos de sus clientes, y que son capaces de sostener la operatividad de sus sistemas. Implica un cambio de cultura empresarial a favor de una responsabilidad proactiva. Sometidos al escrutinio constante del regulador, y a la información continua a sus clientes, las compañías se verán obligadas a modificar su ADN haciéndolo especialmente transparente y colaborativo. De hecho, solo aquellas empresas que se adapten al nuevo escenario podrán seguir operando en el mercado.

> **"Según publicó *PR Newswire*, en 2016 el 90 % de los ciberataques tuvieron su origen en información robada a los empleados una vez hackeados sus sistemas"**

EL EMPLEADO. EL ELEMENTO MÁS VULNERABLE

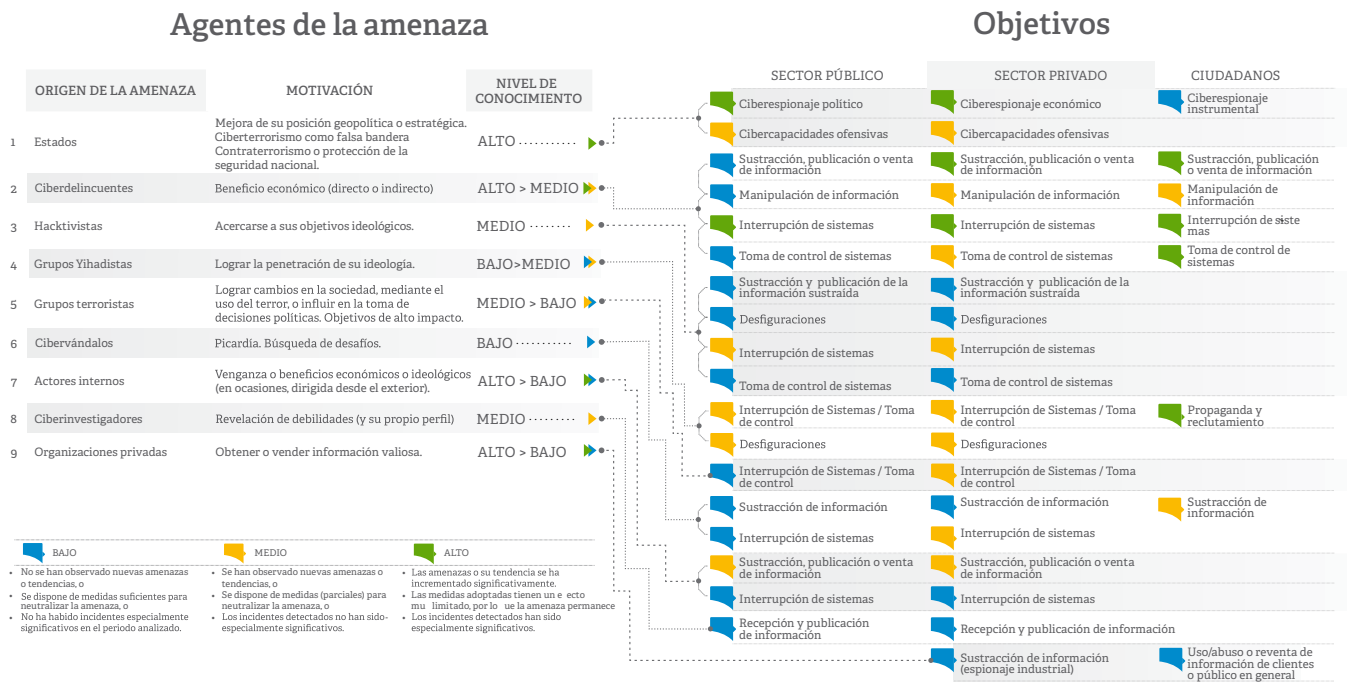
Según datos recogidos por IBM en 2016, dos tercios de los ataques en las compañías fueron llevados por agentes internos[2] . Según publicó *PR Newswire*, en 2016 el 90 % de los ciberataques tuvieron su origen en información robada a los empleados una vez hackeados sus sistemas. No sorprende, por lo tanto, que, según el barómetro Allianz de Riesgos de 2017[3], el daño reputacional, sea para el 69 % de las empresas la principal causa de pérdidas tras un ciberataque.

Por lo tanto, en nuestra opinión, el nuevo paradigma del riesgo reputacional lleva a que quien tiene acceso

[2] Según IBM, los datos comprometidos por ciberataques aumentaron un 566 % en 2016 Telam 2017 http://www.telam.com.ar/notas/201704/185558-ciberataques-seguridad-crecimiento-2016-informe-ibm-sector-financiero.html

[3] Allianz Risk Barometer 2017, Allianz 2017 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

Figura 2. Agentes de la Amenaza.



Fuente: CN-Cert, Centro criptológico nacional.

a los datos de la compañía puede reescribirlos, lo que supone reescribir al tiempo la reputación de la misma. Siendo así las cosas, una correcta protección de los datos de la empresa será condición indispensable para preservar su reputación.

Conocido el riesgo, al CEO y a la compañía no les queda más remedio que liderar la seguridad digital, aspecto transversal de toda la organización, porque, no es algo que compete solo al departamento de sistemas (IT), para cumplir con la normativa y proteger la reputación. De hecho, la confiabilidad corporativa dividirá a las empresas entre las que están preparadas para hacer frente a las ciber amenazas y las que no.

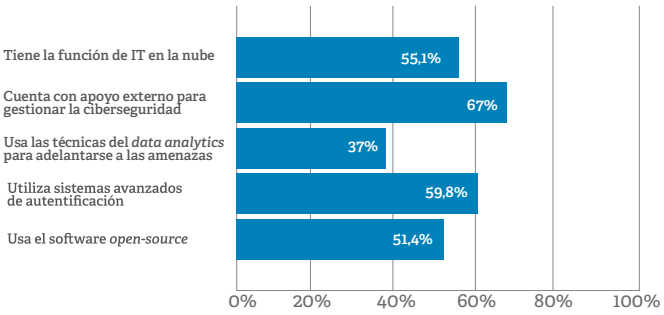
> **"La confiabilidad corporativa dividirá a las empresas entre las que están preparadas para hacer frente a las ciber amenazasy las que no"**

SÍNTOMAS DEL CIBERESTRÉS REPUTACIONAL

El nuevo paradigma del riesgo ciber va a generar un mayor estrés en la organización motivado por:

- El incremento de la presión normativa y regulatoria y adaptación técnica y organizativa de estas nuevas medidas jurídicas.
- El incremento del estrés organizativo en la compañía. La necesidad de proteger el *endpoint* que supone como riesgo cada empleado: su puesto de trabajo y sus extensiones móviles.
- El incremento de la presión societaria sobre la dirección de la compañía por la hípervulnerabilidad en el detrimento del valor de las organizaciones.
- La falta de un sólido escudo protector reputacional que garantice la identificación de los posibles riesgos y los procedimientos operativos preventivos y de gestión *ad hoc* para cada ciberamenaza tanto desde su gestión como de su manejo de la comunicación.

Figura 3. Cinco tendencias en materia de seguridad entre las empresas españolas.



Fuente: PwC, *The Global State of Information Security Survey 2017.*

RIESGO REPUTACIONAL EN EL NUEVO PARADIGMA DEL CIBERRIESGO

Consecuencia de esta nueva situación, el riesgo reputacional que tradicionalmente afectaba a la empresa se verá a partir de este momento, sustancialmente incrementado en dos grandes direcciones:

- La constante comunicación e información de las compañías sobre los ataques sufridos y sus dificultades para proteger los datos, va a suponer un incremento exponencial en la desconfianza ante la vulnerabilidad de la empresa. Los usuarios exigirán mayores garantías en la protección de sus datos y acudirán a las grandes empresas que sean capaces de darles más garantías.
- Las empresas van a verse obligadas a desarrollar nuevos procedimientos de comunicación con sus clientes, a través de todos los canales, con el fin de mantenerlos informados en tiempo real y de manera segura, con el objetivo de evitar que los medios de comunicación pongan el foco en su vulnerabilidad. Esto va a llevar a reforzar equipos de comunicación y a plantearse el continuo informativo. Las críticas online se producirán a cualquier hora y deberán ser neutralizadas lo antes posible. La exposición pública es cada vez mayor y, por lo tanto, será necesario de estar preparado en cualquier momento y a cualquier hora.

¿CÓMO ENFRENTAR EL NUEVO ESCENARIO DEL CIBERRIESGO REPUTACIONAL?

Realizado el análisis sobre la nueva situación de riesgo reputacional, al que en breve se enfrentarán las compañías, es evidente que no queda más remedio que una preparación multidisciplinar que reduzca el riesgo. En ese sentido se presentan algunas medidas para abordar los temas tratados anteriormente:

- **Protección de datos:** invertir en expertos de IT. Será necesario incrementar la inversión en tecnología de protección y, fundamentalmente, en la mejora de la cultura de prevención en las compañías.
- **Proteger las pruebas en caso de ataque:** contar con un equipo multidisciplinar conformado por IT, Legal y Financiero y mejorar así los procesos de formación interna para promover una cultura de protección de las pruebas entre los empleados. Para ello será imprescindible disponer de herramientas de protección de pruebas para el posterior análisis forense.

- **Big data e inteligencia artificial:** aplicarlo al análisis de elevados volúmenes de datos implementando la mejor tecnología para realizar informes de riesgo y de daños sufridos.

- **Presión Normativa y Regulatoria:** contar con expertos en *compliance* y protección de datos. Será preciso mejorar el relacionamiento con instituciones reguladoras y supervisoras.

- ***Stress* organizativo:** apostar por la modificación de los procesos internos de gestión en la organización involucrando a Recursos Humanos, crear un Comité de Crisis entrenado en ciberamenazas y mejorar la formación preventiva interna entre los empleados con la máxima exigencia.

- **Presión societaria:** incrementar los canales de información que permitan neutralizar la percepción de riesgo en su inversión mediante la entrega de informes que justifiquen cómo se incrementa y garantiza la seguridad de datos, pruebas y reputación.

- **Riesgo reputacional y escudo protector:** crear equipos de comunicación preparados en procedimientos de prevención específicos para gestionar ciberriesgos con cobertura y disponibilidad total. Será imprescindible utilizar herramientas digitales de monitorización y gestión capaces de reducir de forma sustancial la distancia entre el tiempo humano y el tiempo máquina a la hora de manejar alertas, fijar estrategia y ejecutar la táctica de gestión de crisis.

- **Reducción de Tiempos:** para la gestión de ciberriesgos será de vital importancia sumar la unión de nuevas herramientas digitales específicas con la perspectiva de expertos analistas de datos, del ámbito legal, financiero y reputacional de la comunicación.

En definitiva, el reto al que se enfrentan las grandes compañías en materia de ciberseguridad es mayúsculo. Las empresas deben hacer un esfuerzo notable para adaptar sus materiales, procedimientos y metodologías a las exigencias de la nueva normativa y regulación, sin olvidarse de que la gestión de la comunicación de los ataques cibernéticos será un elemento clave en el manejo de la reputación de la organización para no quebrar la confianza de los clientes, accionistas y grupos de interés. Así pues, el paradigma de la seguridad estará vinculado a la transformación digital holística de la empresa, a la adaptabilidad de las organizaciones a las nuevas dinámicas de comunicación y comportamiento social digital.

Luis Serrano es director del área de Comunicación de Crisis de LLORENTE & CUENCA. Licenciado en Periodismo, es uno de los mayores expertos de España en la gestión de la comunicación en situaciones de emergencias y catástrofes, así como en el desarrollo de protocolos de actuación de crisis en redes sociales. Durante 17 años ha sido jefe de prensa del Centro de Emergencias 112 de la Comunidad de Madrid, donde ha participado activamente en el manejo de situaciones tan relevantes como el atentado del 11M de Madrid. Ha intervenido en más de 100 siniestros industriales, accidentes con múltiples víctimas, accidentes en centros de ocio, crisis sanitarias, etc. Fruto de sus experiencias es el libro *11 M y otras catástrofes. La gestión de la comunicación en emergencias*, del que es autor. Posee, asimismo, una dilatada experiencia docente en el campo de la emergencia y la gestión de crisis. Es profesor del Máster de Urgencias y Emergencias del CEU-TASSICA, así como del Máster de Fuego de la Universidad de Lleida. Máster de Comunicación Política de la Universidad Camilo José Cela, Máster en Seguridad y Emergencias de la Fundación Ortega y Gasset y Universidad Rey Juan Carlos, Máster de Emergencias de la Universidad de Murcial-Alebat. Además, es profesor-colaborador desde hace 12 años de la Escuela Nacional de Protección Civil del Estado. Como periodista, trabajó durante siete años en los servicios informativos de Onda Cero.

lserrano@llorenteycuenca.com

Natalia Sara es gerente del área de Crisis de LLORENTE & CUENCA. Licenciada en Ciencias de la Información por la Universidad de Navarra, postgrado en Comunicación para el Liderazgo y Dirección de Personas y master en Marketing, Internet y Nuevas Tecnologías por ESIC Business & Marketing School. Cuenta con 25 años de experiencia en el sector de la comunicación, los últimos 15 como consultora corporativa, *public affairs* y crisis, e inicialmente como periodista, donde ejerció en medios nacionales líderes como Expansión o Actualidad Económica. Especializada en comunicación de crisis y reputación con amplia experiencia en la elaboración de protocolos, manuales de crisis y ejecución estratégica para prevenir potenciales riesgos y gestionar situaciones adversas en marcas, personas y organizaciones. Imparte a directivos y profesionales formación en comunicación y manejo de la reputación digital y es docente en la Escuela de Periodismo y Comunicación Unidad Editorial en Comunicación Corporativa Digital y Gestión de Crisis Online y en el Foro Europeo Escuela de Negocios. Autora del apartado sobre gestión de crisis en el libro *Consultoría Política*, del Centro Internacional de Gobierno y Marketing Político (CIGMAP) de la Universidad Camilo José Cela (UCJC).

nsara@llorenteycuenca.com

d+i desarrollando ideas
LLORENTE & CUENCA

Desarrollando Ideas es el Centro de Liderazgo a través del Conocimiento de LLORENTE & CUENCA.

Porque asistimos a un nuevo guión macroeconómico y social. Y la comunicación no queda atrás. Avanza.

Desarrollando Ideas es una combinación global de relación e intercambio de conocimiento que identifica, enfoca y transmite los nuevos paradigmas de la sociedad y tendencias de comunicación, desde un posicionamiento independiente.

Porque la realidad no es blanca o negra existe **Desarrollando Ideas.**

www.desarrollando-ideas.com
www.revista-uno.com