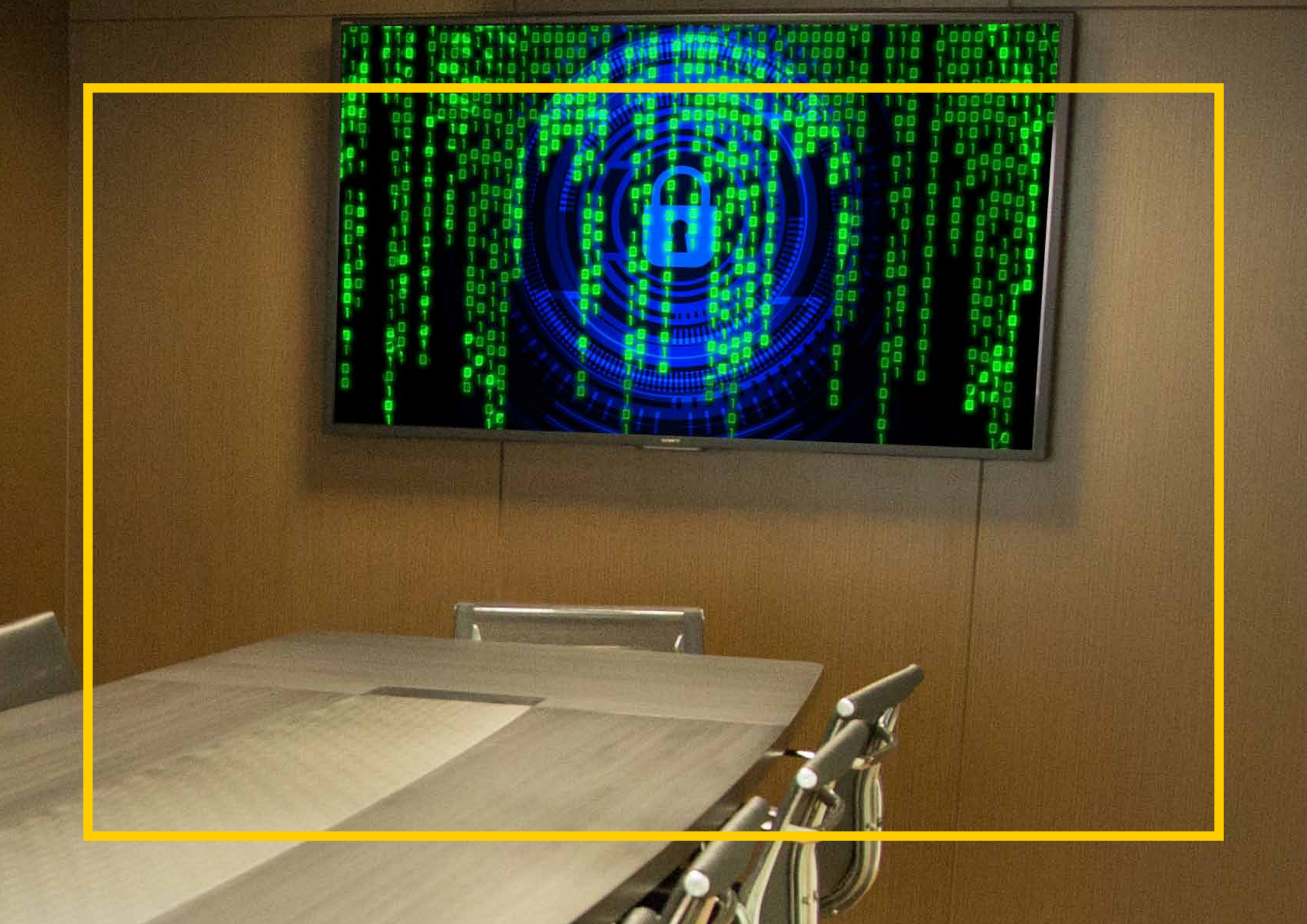
La responsabilidad del Consejo de Administración en la Ciberseguridad

Working Paper N° 7 / 16 de junio del 2018



La responsabilidad del Consejo de Administración en la Ciberseguridad

Encuentro Privado[1].

Working Paper. 7

16 de junio del 2018

1 Los Encuentros Privados, forman parte de la cartera de actividades que lleva a cabo del Global Corporation Center. Este Centro ha sido fundado por EY Fundación España y el IE Business School. Los Encuentros Privados son:
- Eventos cerrados dirigidos a colectivos homogéneos.
- El objetivo es desarrollar Networking y profundizar en temas relevantes.
- Cada encuentro genera un "paper" de reflexión y resumen.

Este Working Paper ha sido redactado en base a las intervenciones que, miembros de consejos de administración y expertos en materia de ciberseguridad, llevaron a cabo en la reunión, habida el pasado día 25 de abril del 2018, en el Global Corporation Center en el marco de un encuentro privado.

Giuseppe Tringali	Presidente del Global Corporation Center Vicepresidente International Advisory Board IE Business School
Miguel Ferré	Vicepresidente del Global Corporation Center Senior Advisor de EY
Elena Maestre	Socia de Ciberseguridad de EY
Alberto Hernández	Director General de INCIBE (dependiente del Ministerio de Energía, Turismo y Agenda Digital)
Ángel Durández	Consejero Externo Independiente de Repsol. • Vocal de la Comisión de Auditoría y Control • Vocal de la Comisión Nombramientos • Vocal de la Comisión de Retribuciones Consejero Independiente de Prosegur Vicepresidente Fundación Euroamerica
Fernando Fernández	Profesor de Economía y Finanzas del IE Business School Vocal de la Comisión de Auditoria de Red Eléctrica de España Consejero Independiente de Bankia Consultor internacional en temas macroeconómicos, regulatorios y financieros Miembro del comité científico de Bruegel y del Consejo Asesor de la Fundación de Estudios Financieros
José Massa	Ex Presidente Ejecutivo de Iberclear Senior advisor de BME
Gianluca D'Antonio	Master In Cybersecurity del IE School of Human Science & Technology. Director Chief Information Officer (CIO) de FCC. Cofundador y Presidente de la Asociación Española para el Fomento de la Seguridad de la Información ISMS Fórum Spain

Índice

Introducción

Las nuevas tecnologías IT ofrecen muchísimas oportunidades, pero también son un elemento de riesgo relevante.

Los ataques cibernéticos crecen y son difíciles de prever. Pueden tener una influencia importante en la utilización de datos sensibles, pueden determinar fraudes, pueden determinar sabotajes también y, por lo tanto, presentan problemas que las empresas y sus Consejos de Administración tienen que tener en cuenta, en mucha mayor medida de lo que se ha tenido hasta ahora, considerando las responsabilidades de los consejos de administración, a la luz de la ley 31/2014 por la que se modificó la ley de Sociedades de Capital para la mejora del gobierno corporativo donde la responsabilidad es jurídica y, por lo tanto, afecta de forma personal a todos los consejeros.

La CNMV esta evidentemente muy interesada en el tema, que formará parte de un análisis que harán para dar recomendaciones en este sentido.

2 "Se debe intensificar el seguimiento de los aspectos relacionados con los desarrollos tecnológicos en los mercados, trabajando para que la tecnología utilizada por los intervinientes en los mercados sea cada vez más resistente a los riesgos cibernéticos, reduciendo las contingencias y aumentando la confianza del público. La CNMV deberá, por tanto, trabajar para impulsar la utilización de las nuevas tecnologías en los mercados de capitales sin descuidar la supervisión de los riesgos que lleva asociada". Líneas estratégicas de la CNMV 2017-2018

1. Ciberataques y Ciberdelincuencia

El Resumen Ejecutivo del Global Information Security Survey 2017-2018 del Centro de Estudios EY, introduce el tema de los ciberataques y de la ciberdelincuencia que es pertinente enmarcar en la valoración de la gestión de riesgos[3] que se dan en las cotizadas españolas como tendencia internacional[4], porque, es evidente que, en este mundo globalizado, este es un fenómeno que afecta a todas las compañías. En materia de gobernanza corporativa, no se puede dejar de lado el peso significativo de todo lo que viene del mundo anglosajón y, en particular, Estados Unidos y de la SEC.

En materia de política de control y gestión de riesgos, la Ley de Sociedades de Capital marca, como facultad indelegable de los miembros del Consejo, decidir la política de supervisión de riesgos[5]. Por otra parte, la vía soft law y, concretamente de forma reciente, la guía técnica 3/2017 sobre Comisiones de Auditoría de Entidades de Interés Público[6], ya utilizó la palabra ciberseguridad al citar los riesgos emergentes. También, en la citada guía técnica se alude a que, en todas las reuniones de la comisión de auditoría se incluya con carácter general en el orden del día la supervisión, a lo largo del año, de todos los riesgos significativos, tanto financieros como no financieros, relacionados estos últimos, con aspectos tales como la fiscalidad, el cambio climático, la ciberseguridad y el cumplimiento normativo,[7]

3 El estudio pone de manifiesto que la mayoría de las empresas considera que el riesgo de sufrir un ciberataque es hoy mayor que hace un año, ya que las técnicas de los ciberdelincuentes son más sofisticadas y las empresas están más hiperconectadas que nunca. Las oportunidades que ofrece la digitalización son muy grandes a lo largo de la cadena de valor, pero también lo son los riesgos. Global Information Security Survey 2017-2018. Centro de Estudios EY Resumen Ejecutivo.

4 Las empresas deben asumir que lo peor puede suceder, y hay suficientes ejemplos de ciberataques a escala mundial (los virus Petya, WannaCry o Mirai, por ejemplo) como para evitar la complacencia. http://www.ey.com/es/es/home/ey-global-information-security-survey-2018.

5 El consejo de administración de las sociedades cotizadas no podrá delegar las facultades de decisión a que se refiere el artículo 249 bis ni específicamente las siguientes: b) La determinación de la política de control y gestión de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control. «Artículo 529 ter. Facultades indelegables. Ley 31/2014, de 3 de diciembre.

6 En lo que se refiere a diversidad de perfiles profesionales y conocimientos, debido al incremento de la digitalización y la importancia de los procesos virtuales en las entidades, sería deseable, en función de la complejidad, tamaño y, en particular, el sector de actividad de la entidad, que al menos uno de los miembros de la comisión de auditoría tenga experiencia en tecnologías de la información (IT). Entre otras razones, al objeto de propiciar una supervisión eficiente de los sistemas internos de control y gestión de los riesgos, los cuales utilizan, generalmente, aplicaciones informáticas complejas, y de poder evaluar adecuadamente nuevos riesgos emergentes, como el de ciberseguridad. GUÍA TÉCNICA 3/2017 sobre Comisiones de Auditoría de Entidades de Interés Público. 27 de junio de 2017. CNMV.

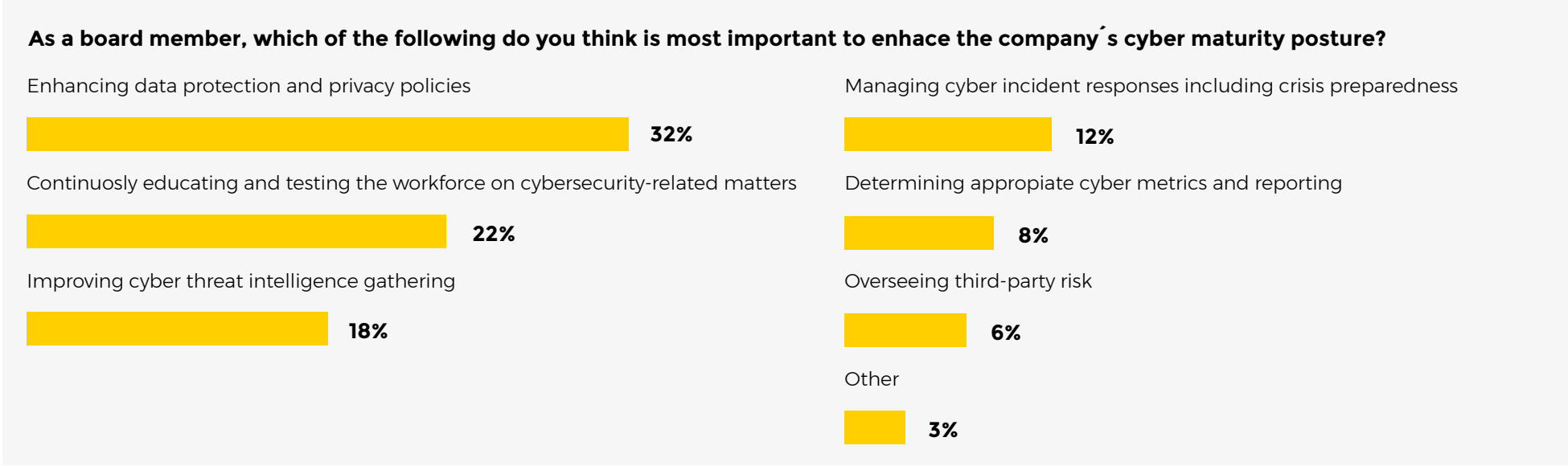
7 Incluir, con carácter general, la supervisión del riesgo en el orden del día de las reuniones de la comisión de forma que puedan analizarse a lo largo del año todos los riesgos significativos, tanto financieros como no financieros, relacionados estos últimos con aspectos tales como la fiscalidad, el cambio climático, la ciberseguridad y el cumplimiento normativo. GUÍA TÉCNICA 3/2017 sobre Comisiones de Auditoría de Entidades de Interés Público. 27 de junio de 2017. CNMV.

En el EY Center for Board *Matters* se establece que:

> *"For survival and success, Cybersecurity has become a priority for boards, who want to be better informed and know the right questions to ask"*[8]

Por otra parte, según el Global Information Security Survey de EY[9]:

> *"In our conversations with organizations of all shapes and sizes, it is clear cybersecurity is a priority issue from board level down"*



Fuente: Cyber — the director's perspective. EY Center for Board Matters

8 Cybersecurity was once relegated to a company's IT department. Today, we know that investing in a comprehensive, cross-department response program is essential — for survival and success. Cybersecurity has become a priority for boards, who want to be better informed and know the right questions to ask. We invited Kostas Georgakopoulos, Procter & Gamble's Chief Information Security Officer, to discuss his experience working with boards and what he's learned from building and leading security programs for global institutions. Listen to an insightful talk on how boards should be thinking about strategy and cybersecurity. Cyber — the director's perspective. EY Center for Board Matters

9 Two decades after EY first began publishing annual surveys detailing organizations' concerns about cybersecurity — and their efforts to confront these concerns — the imperative for a collaborative and coherent response to the changed threats could hardly be more pressing. In our conversations with organizations of all shapes and sizes, it is clear cybersecurity is a priority issue from board level down. But in a complex and evolving landscape, it can be difficult to see the wood for the trees: the cybersecurity threat is often well-camouflaged, hidden in plain sight. 20th Global Information Security Survey 2017–18.

Se observa pues que, en los consejos de las cotizadas de Estados Unidos, uno de los asuntos prioritarios, en este año 2018, es la ciberseguridad. Por tanto, se confirma que, la ciberseguridad es una materia que, al otro lado del Atlántico, donde están localizando muchos de los inversores institucionales y muchos asesores de voto, tiene que tratarse y, sobre la cual, van a preguntar en los consejos.

Este mismo año 2018, la SEC, la CNMV estadounidense, ha emitido una guía en materia de ciberseguridad que es de especial interés.

En el documento de EY Center for Board Matters "*SEC guidance on cybersecurity: board considerations*" se hace referencia a lo siguiente:

> *"On February 21, 2018, the Securities and Exchange Commission (SEC) unanimously approved the issuance of interpretive guidance regarding public companies' disclosure obligations under existing law regarding cybersecurity risk and incidents. The release updates and reinforces guidance provided in 2011 by the SEC's Division of Corporation Finance (2011 Guidance), which provided an overview of specific SEC disclosure obligations that may require companies to discuss cybersecurity risks and cyber incidents. SEC action on cybersecurity matters has been anticipated and, in a statement announcing the guidance, SEC Chair Jay Clayton noted that the SEC "will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed."*

2. Board considerations

"Cybersecurity risks pose grave threats to our investors, our capital markets, and our country," states the SEC in the release. It continues: "[a]s companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased. . . . Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack." We observed in our Top Priorities for Boards in 2018 that cybersecurity, along with other technology matters, is a top priority for board focus. Boards need to be aware of the SEC's new guidance as they continue to manage and enhance their oversight of cybersecurity risks and incidents, as well as company policies and procedures that should specifically address these matters.

3. Codes of ethics and insider trading policies

La "*SEC guidance on cybersecurity*" recomienda a las cotizadas que no puede darse detalles concretos que desvelen o desprotejan a las empresas ante posibles ataques cibernéticos:

"The release reminds companies that information about cybersecurity risks and incidents may be material nonpublic information. As such, the SEC encourages companies to consider how their codes of ethics and insider trading policies take into account and look to prevent trading on the basis of material nonpublic information regarding cybersecurity risks and incidents".

"Significantly, the SEC states that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure".

"Boards, or the appropriate board committee, should discuss with management whether the company's insider trading policy and code of ethics adequately explain that cybersecurity matters may be material and thus required to be disclosed, and that, prior to disclosure of material information about an existing cybersecurity matter, prohibitions will be imposed on trading in the company's securities. Revisions to insider trading policies and codes of ethics may be appropriate. In particular, in view of the SEC's statement regarding avoiding the appearance of improper trading, careful consideration should be given to policies and procedures regarding trading windows and blackout periods and possibly on Rule 10b5-1 trading programs and plans".

4. Vulneración del Riesgo Cibernético

Para la SEC la vulneración del riesgo cibernético afecta no sólo a los ejecutivos, sino que afecta también a los inversores y a los mercados de capitales.

De acuerdo con la "*SEC guidance on cybersecurity*":

"The release updates and reinforces the 2011 Guidance by reminding companies that the SEC's disclosure requirements apply to cybersecurity risks and incidents that could have a material impact on the company, including:

- *Risk factors*
- *Management's discussion and analysis of financial condition and results of operations*
- *Business description*
- *Legal proceedings*
- *Financial statement disclosures*

The SEC expects companies to disclose material cybersecurity risks and incidents that are material to investors, including the financial, legal or reputational consequences. In this regard, the SEC also reiterates that companies are not expected to "publicly disclose specific, technical information about their cybersecurity systems, the related networks or devices, the potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity".

Por tanto, la divulgación o la transparencia en cuanto a los planes de supervisión y de prevención, de la ciberseguridad es vital y en el documento de la SEC, recogido por el informe de EY[10] citado anteriormente, se da una buena referencia.

10 https://www.ey.com/Publication/vwLUAssets/ey-sec-guidance-on-cybersecurity-board-considerations/$File/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

5. El Ciberespacio y La Ciberseguridad

El INCIBE (Instituto Nacional de Ciberseguridad de España) es una entidad pública, que depende de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Es una entidad civil que trabaja en la ciberseguridad que, como problema o como reto, requiere una visión y aproximación holística.

El INCIBE, es uno de los organismos públicos que, en España, trabajan en ciberseguridad y, fundamentalmente, en el ámbito de la ciberseguridad del ciudadano y de todo el sector privado, desde la pequeña y la mediana empresa a la gran empresa, especialmente, aquellas empresas que son de carácter estratégico o que operan infraestructuras críticas en nuestro país.

Hay otros organismos que aportan diferentes aproximaciones, porque el problema es diferente en función del ámbito de aplicación.

El Mando Conjunto de Ciberdefensa[11] tiene la capacidad en las Fuerzas Armadas de responder ante un conflicto militar porque, en el ciberespacio[12], se pueden desarrollar operaciones militares y, de hecho, ya han ocurrido en el pasado[13].

11 El Mando Conjunto de Ciberdefensa (MCCD) es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. http://www.emad.mde.es/CIBERDEFENSA/

12 Technologies, such as wireless networks and voice-over-IP (VoIP), extend the reach and scale of the Internet. In this regard, the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, the latter with public and private incarnations. Thus, with VoIP technology, a desk telephone is part of the cyber environment. However, even isolated devices can also be part of cyber environment if they can share information with connected computing devices through removable media. The cyber environment include the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment. ITU, ITU-T Recommendation Rec. ITU-T X.1205 (X.cso), 2008. https://blogs.cisco.com/security/cyberspace-what-is-it

13 La OTAN señala que los incidentes informáticos que gestionaron en 2016 supusieron un aumento del 60% respecto al año 2015 (NATO, 2017c: 24). La tendencia de este tipo de incidentes es vista por muchos analistas como una situación de vulnerabilidad que podría llegar a afectar a suministros que consideramos básicos, como el agua, la telefonía o la electricidad, como ya ocurrió en Ucrania en 2015 (CERTSI, 2016). A pesar de que estas tecnologías se han incorporado al terreno militar, supone todavía un desafío la conceptualización de determinados aspectos relacionados con la seguridad, la defensa y el ciberespacio. El ámbito cibernético está compuesto por la Internet, su arquitectura organizadora, los dispositivos conectados a la Internet y las redes convencionales inalámbricas (Chang y Granger, 2012: 84). La Internet que todos conocemos hoy día, que es tan sólo una parte del espacio cibernético, tiene su origen en los años sesenta del siglo XX, en pleno contexto de guerra fría y el desarrollo de un sistema de comunicaciones en el ámbito militar. En los años noventa, se extiende el uso de los navegadores (los programas que permiten el acceso a la Web) y de la World Wide Web[1] (Internet Society, 1997). La posibilidad de intercambiar información, principalmente en el ámbito de los negocios, su rápida incorporación a todos los ámbitos de la sociedad así como un desarrollo tecnológico incuestionable, ha supuesto que hoy día el ciberespacio sea un ámbito fundamental en nuestras sociedades. http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar

En estos momentos estamos, en una fase de amenaza híbrida[14].

El Centro Criptológico Nacional (CCN)[15] y el Centro Nacional de Inteligencia (CNI)[16] tienen como objetivo proteger a la Administración Pública porque, en general, las amenazas que afectan a dicha Administración suelen ser amenazas que provienen de organismos de inteligencia o de Estados. En el sector privado, la amenaza es diferente y afectan, al Ministerio de Interior (Policía Nacional y Guardia Civil) y a la Fiscalía (Ministerio de Justicia) para combatir el ciberdelito o al Ministerio de Asuntos Exteriores en el ámbito de las relaciones internacionales.

La ciberseguridad es un asunto de interés y de reto internacional. Si bien la seguridad tradicional es más un asunto de país o de Estado, aunque requiere colaboración internacional, la ciberseguridad claramente es un reto de nivel internacional. La amenaza es internacional, el origen de lo que pueda suceder en España se puede causar a miles de kilómetros de distancia que es lo que en realidad está ocurriendo. Gran parte de lo que ocurre en nuestro país se produce en otros países y llega al nuestro por lo que, la colaboración internacional, es fundamental.

14 There are state and non-state actors that are challenging countries and institutions they see as a threat, opponent or competitor to their interests and goals. The range of methods and activities is wide, including influencing information; logistical weaknesses like energy supply pipelines; economic and trade-related blackmail; undermining international institutions by rendering rules ineffective; terrorism or increasing insecurity. Hybrid threats are methods and activities that are targeted towards vulnerabilities of the opponent. Many things, including historical memory, legislation, old practices, geostrategic factors, strong polarization of society, technological disadvantages or ideological differences, can create vulnerabilities. If the interests and goals of the user of hybrid methods and activity are not achieved, the situation can escalate into hybrid warfare where the role of military and violence will increase significantly. https://www.hybridcoe.fi/hybrid-threats/

15 El Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material Criptológico y formar al personal de la Administración especialista en este campo. El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). De hecho, en la Ley 11/2002, de 6 de mayo, reguladora del CNI, se encomienda a dicho Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada, a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos. https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es

16 Ante los nuevos retos del escenario nacional e internacional, era necesario disponer en España de un Servicio de Inteligencia especializado y moderno con capacidad para afrontarlos con eficacia. La respuesta a tal necesidad es el Centro Nacional de Inteligencia (CNI), Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. (Art. 1 Ley 11/2002). https://www.cni.es/es/queescni/quees/

La ciberseguridad no solo es un reto a la seguridad nacional, sino que, es también un componente empresarial o industrial importantísimo.

Por un lado, porque los ciberataques producen pérdidas económicas, pero, por otro lado, porque la ciberseguridad presenta una oportunidad para desarrollar nuevos negocios. El sector de la ciberseguridad es un mercado que crece al 11-13% a nivel mundial. En España estamos en ese marco, entre el 11-13%, que genera una demanda de profesionales y de creación de puestos de trabajo muy importante y, por lo tanto, es una oportunidad también para que nuestro país y nuestras empresas desarrollen sus negocios en este nuevo sector.

Cada país ve de forma diferente la ciberseguridad y esto se debe a diferentes condicionantes. Los aspectos históricos de cada país influyen, también los aspectos culturales, la situación política, la situación social. La ciberseguridad, presenta una oportunidad para que, ciertos países tengan, a nivel internacional, superioridad geoestratégica y geopolítica.

En España, la ciberseguridad se trata como un problema, como un reto a la seguridad nacional, pero, también, como una oportunidad de desarrollo y de creación de puestos de trabajo, de desarrollo de nuevas empresas y de internacionalización de empresas. Hay otros países que ven también una oportunidad para que, mediante el desarrollo de empresas y su forma de ser percibidas lleguen a tener una posición geoestratégica en ciertas áreas del mundo. Otras naciones consideran la ciberseguridad como una herramienta para obtener información, para influir en la sociedad y, por lo tanto, en la opinión pública y cambiar tendencias o cambiar opiniones.

Por tanto, este es un entorno complejo que deriva de las especiales características que tiene el ciberespacio. La ciberseguridad (Internet, el ciberespacio y las tecnologías) es importante también a nivel de consejos de Administración. Ya tiene un nivel de penetración enorme en todas las organizaciones y, es indudable, que la va a seguir teniendo pues, no solo es una tecnología del presente, sino también del futuro. Proporciona muchas mejoras y ventajas en el desarrollo de nuestras empresas y de nuestra sociedad. El ciberespacio es global, como ocurre con la tierra, el mar, el espacio y el espacio profundo. El ciberespacio llega a todos los rincones del mundo, a día de hoy más de 4000 millones de internautas. En nuestro país hay más dispositivos móviles que ciudadanos[17].

17 El número de líneas móviles supera por primera vez a la población mundial. Los usuarios alcanzaron los 5.000 millones en 2017, pero las tarjetas SIM se elevaron a 7.800 millones. https://elpais.com/tecnologia/2018/02/27/actualidad/1519725291_071783.html

En los próximos años la penetración a Internet será masiva. Se debe tener en cuenta que, en el ciberespacio, los tiempos se miden en milisegundos, y ese es un aspecto muy importante a considerar. Es decir, la transición de la amenaza a la agresión o al ataque se produce en milisegundos y, sus efectos, se producen, también, en milisegundos. Este entorno proporciona anonimato, por diferentes razones, por razones técnicas, pero también, por razones culturales e históricas.

En España existe la Ley 25/2007 de Conservación de Datos[18], por la cual los operadores de telecomunicaciones deben conservar los datos de navegación, es decir, la IP y quién está detrás cuando se conectan a Internet. Bajo ciertas situaciones, y si lo autoriza el juez, esos datos se pasan a la Policía y la Guardia Civil para investigar pero, en otros países, por razones históricas, culturales y políticas existen leyes de Protección de datos que consideran, a la citada **Ley 25/2007**[19], como una agresión directa a un principio fundamental que es el de la privacidad y, por tanto, no existe esa ley.

El ciberespacio es un **espacio asimétrico**[20], lo que constituye también un aspecto fundamental que lo hace diferente de otros ámbitos. Cuando un país recibe ciberataques[21], aunque no se hayan originado allí, se encuentra con el problema de que se llega a una situación en la que ya no es posible proseguir. Este es una situación muy interesante para las organizaciones criminales que, antes operaban en el espacio físico y, ahora, operan en el ciberespacio[22].

18 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

19 La nueva Ley orgánica de protección de datos (LOPD), cuando entre en vigor (todas las previsiones han saltado por los aires después del cambio de gobierno del pasado 3 de junio), está llamada a desarrollar el Reglamento General de Protección de Datos (RGPD), cuyo norte es proteger los datos personales. La Ley 25/2007 pretende todo lo contrario, hacer posible que las fuerzas de seguridad accedan a datos de tráfico y de localización que, en la medida en que puedan permitir identificar a una persona, serían también datos personales, con el fin de perseguir delitos graves. Aunque una importante sentencia europea anuló la directiva de que traía causa, en España esta ley no se vio afectada, pues según nuestros tribunales, las garantías que faltaban en la norma europea están en la española.

20 En el Glosario de Términos Informáticos, Whatis (https://whatis.techtarget.com/) se dice: «El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física». la Estrategia Española de Seguridad (EES), es más explícita y lo define como «El espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos Es mucho más que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite».

21 La confrontación en el ciberespacio presenta frecuentemente las ca¬racterísticas de un conflicto asimétrico (13). El atacante puede ser muy inferior al atacado en medios técnicos y con relativamente pocos me¬dios y baratos puede causar tremendos perjuicios. Además, es fre¬cuentemente anónimo y clandestino. Así pues, atrae, no sólo a los gobiernos sino también a otros diferentes actores que incluyen los te¬rroristas (14) y las mafias del crimen organizado. El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

22 La estructura del ciberespacio. Tradicionalmente, siguiendo a Martin C. Libicki (3), se viene dividiendo el ciberespacio en tres capas, cada una de las cuales presenta sus vulnerabilidades y es objeto de un tipo concreto de ataques: la capa sintáctica, la capa semántica y la capa física. El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

Si hablamos de energía nuclear o de capacidad nuclear, normalmente hay un estado detrás, con miles de millones de dólares o euros de inversión y años de investigación[23]. Si hablamos de ciberarmas o de herramientas que permitan a las organizaciones criminales robar grandes cantidades de dinero hablamos de pequeños grupos bien organizados pero que lo que tienen es: conocimiento, una escasa inversión y, una rentabilidad enorme[24].

Respecto del sector privado, en España el año 2017 se gestionaron más de 123.000 incidentes de ciberseguridad que afectaron a nuestros ciudadanos en nuestras empresas. Gran parte de ello se deben a organizaciones criminales que operan en el ciberespacio y consiguen grandes cantidades de dinero. Evidentemente el impacto económico que tiene un fraude, una extorsión, un robo, es importante, pero, cuando hablamos de cantidades exponenciales, el impacto que tienen en la confianza de los clientes y en las entidades puede ser enorme. Cuando el modelo de negocio de una organización se basa fundamentalmente en la confianza que proporciona a sus clientes, un ciberataque lo pone en serio riesgo.

Por ejemplo, en algunos sectores, como el de los despachos de abogados o el sector financiero, se ve muy claro que, el impacto de sufrir ciberataques, no es la pérdida económica que pueda producirse, sino el cierre del negocio, porque se ha minado la confianza en el mismo y, por lo tanto, los clientes no van a ir a trabajar con ellos[25].

Por lo tanto, se está ante un problema complejo, con unas características que hacen que crezca continuamente y en el que, evidentemente, los ciudadanos y las empresas están inmersas, porque todos utilizan tecnología.

23 En la Paz de Westfalia (1648), las naciones firmantes se comprometieron a que los conflictos armados, llamados ya formalmente guerras, sólo deberían tener lugar entre Estados o fac¬ciones de un Estado con estructura de tales y mediando normalmente la oportuna declaración de guerra. Otro hito podría ser la firma de los Convenios de Ginebra y La Haya (1899-1907), fuente y principio del De¬recho Internacional Público moderno que tratan de reglamentar en cierto modo los usos y costumbres de la guerra, de proteger a la población civil y personal no combatiente así como a los prisioneros de guerra, a los heridos y a los enfermos, lo que se conoce como Derecho Internacional Humanitario y Derecho Internacional del Conflicto Armado. El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

24 El ciberespacio es el último dominio común en el que el hombre se ha aventurado. Se diferencia de los demás en su creador; en él sus leyes naturales son un conjunto de protocolos lógicos –sustentados por una capa física– creados y acordados por el hombre. Sin embargo, su creador no ha sabido, o no ha querido, imponer una ley positiva sobre su creación. Quizás no lo creyó necesario; posiblemente porque «entonces» no lo fuera. «Entonces» era un tiempo de certidumbres; la tercera guerra mundial en forma de apocalipsis nuclear aniquilaría los principales núcleos de población y las infraestructuras críticas de las potencias enfrentadas. El éxito pasaba por asegurar la detección, seguimiento e interceptación a tiempo de los bombarderos nucleares enemigos y la supervivencia de las comunicaciones entre centros de poder. Sus usuarios y administradores constituían una pequeña comunidad de interés que no requería vigilancia. Así nació ARPANET (1) y (2) y así evolucionó hacia lo que hoy conocemos como Internet: la Red, una tela de araña que supera los esquemas del viejo mundo westfaliano, que no conoce fronteras, Estados ni naciones y sobre la que no existen ni cuerpo legal ni «gendarmería» universales que garanticen el «buen» funcionamiento de la ingente cantidad de plataformas, equipos, aplicaciones, servicios, contenidos, comunidades de interés y un largo etcétera de mundos convergentes (3). El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

25 El alcance del ciberespacio dentro del mundo de las transacciones finan¬cieras no parece tener límite. Donde hay una oportunidad de negocio, allí están los delincuentes cibernéticos para aprovecharla. Estos ata¬ques ponen de relieve la vulnerabilidad de nuestros mercados financie¬ros y, por ende, del conjunto de nuestro sistema económico. Las redes en las que se llevan a cabo los negocios bursátiles, financieros o ban¬carios son infraestructuras críticas que necesitan ser convenientemente protegidas (40). La responsabilidad directa de su gestión y de su defensa está, desde luego, en manos privadas en la mayor parte de los casos, pero los efec¬tos de las intrusiones en las mismas son materia, sin lugar a dudas, de Seguridad Nacional al mismo nivel que los sistemas de generación y distribución energética y los de control del tráfico aéreo. El sistema infor¬mático del "The National Association of Securities Dealers Automated Quotation System (Nasdaq)", el índice bursátil tecnológico estadounidense, ya ha sido penetrado en ocasiones sin que se haya determinado el alcance de la intrusión aunque el potencial desestabilizador de la mera sospecha puede resultar alta¬mente significativo (41). El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

6. Reglamento General de Protección de Datos (RGPD)[26]

Reglamento General de Protección de Datos (RGPD), plenamente vigente desde el pasado 25 de mayo, ha introducido la obligatoriedad de notificar a la **Agencia Española de Protección de Datos (AEPD)**[27], en un plazo máximo de 72 horas, todas aquellas brechas de seguridad que puedan producirse en el seno de las organizaciones, siempre que exista "riesgo para los derechos y libertades de las personas físicas"[28].

La Agencia Española de Protección de Datos (AEPD) presentó el 19/06/2018[29] la **"Guía para la gestión y notificación de brechas de seguridad"**[30] junto a ISMS Forum[31] y en colaboración con el Centro Criptológico Nacional (CCN) e INCIBE. El objetivo de este documento es ofrecer a las organizaciones tanto recomendaciones preventivas como un plan de actuación, de forma que conozcan cómo evitarlas y cómo proceder en caso de que se produzcan.

El Reglamento General de Protección de Datos (RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Con anterioridad a la aplicación del RGPD, la obligación de notificar a la Agencia las brechas de seguridad que pudiesen afectar a datos personales se ceñía exclusivamente a operadores de servicios de comunicaciones electrónicas y prestadores de servicios de confianza. Desde el pasado 25 de mayo, esta obligación pasa a ser aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

26 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 Directiva 95/46/CE (Reglamento general de protección de datos)

27 https://www.aepd.es/

28 https://cincodias.elpais.com/cincodias/2018/06/19/legal/1529414872_553101.html

29 https://www.aepd.es/comunicacion/prensa/2018-06-19.html

30 https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

31 (Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector). https://www.ismsforum.es/

De acuerdo con el Reglamento, cuando el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe notificarlo sin dilación a la autoridad de control competente, y a más tardar en las **72 horas siguientes** a haber tenido constancia de ella. Esta notificación a la Agencia debe realizarse a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la brecha de seguridad entraña un alto riesgo para los derechos y libertades de las personas (como, por ejemplo, el acceso ilícito a usuarios y contraseñas de un servicio), además de la comunicación a la autoridad de control, el responsable del tratamiento debe, adicionalmente, comunicar a los afectados la brecha de seguridad con lenguaje claro y sencillo y de forma concisa y transparente.

La **"Guía para la gestión y notificación de brechas de seguridad"** va dirigida a responsables de tratamientos de datos personales con el objetivo de **facilitar la aplicación del RGPD** en lo relativo a la obligación de notificar a la autoridad competente y, en su caso, a los afectados, de modo que la notificación a la autoridad competente se haga por el canal adecuado, contenga información útil y precisa, y se adecúe a las nuevas exigencias del RGPD. Para elaborar el documento también se ha contado con la participación de numerosos profesionales y expertos del sector, recogiendo la experiencia y conocimiento de empresas que tienen implantados procedimientos de gestión de incidentes de seguridad.

Esta guía pretende cubrir el amplio abanico del tejido empresarial español, tanto pymes como grandes empresas y, del mismo modo, puede ser de ayuda a los responsables y encargados de tratamientos de las Administraciones Públicas involucrados en las tareas de gestión de las brechas de seguridad.

El documento está estructurado en cinco grandes bloques:

1. El primero está dedicado a la **detección e identificación** de brechas de seguridad, incluyendo: detalles sobre cómo debe estar preparada la organización;
2. El segundo trata de la **clasificación** de los Incidentes de seguridad
3. el tercero incluye un apartado dedicado a la **Gestión de las brechas de seguridad: plan de actuación**, en el que se presentan los aspectos básicos sobre cómo proceder ante un incidente;
4. El cuarto recoge las **Respuestas a las brechas de seguridad**
5. Por último, el quinto se refiere a la **Notificación de las brechas de seguridad**.

Por último, la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

El lanzamiento de la **"Guía para la gestión y notificación de brechas de seguridad"** completa los manuales de ayuda que la Agencia Española de Protección de Datos ha presentado para facilitar la adaptación de las organizaciones al RGPD, entre los que se encuentran el:

1. **Listado de cumplimiento normativo**
2. **Guías para Responsables de tratamientos de datos personales**[32]
3. **Cumplimiento del deber de informar**[33]
4. **Elaboración de contratos entre responsables y encargados**[34]
5. **Análisis de riesgos y Evaluaciones de impacto**[35]

32 https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

33 https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

34 https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

35 https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

7. Consejo de Administración y Riesgo Cibernético

¿Qué están haciendo las empresas para intentar reducir, al mínimo, este tipo de riesgo tan complejo? ¿Qué se puede hacer para minimizarlo? porque es un riesgo que afecta a las empresas, al negocio, a los Consejos de Administración y, por supuesto, a los inversores.

La CNMV, y, todas las instituciones que gobiernan el mundo corporativo, han dictado una serie de procedimientos o de requisitos que hay que tener con respecto a la ciberseguridad. La responsabilidad, en las empresas, está en su Consejo de Administración y por ende en sus consejeros. Ser consejero en una empresa conlleva una serie de responsabilidades enormes. El control de riesgos en general y de ciberataque en particular, es responsabilidad del Consejo, y este tiene que asegurarse de que, efectivamente, existen los mecanismos para que esos riesgos cibernéticos estén debidamente controlados o prevenidos.

Esta prevención y control se hace, en la mayoría de los Consejos, a través de la Comisión de Auditoría, que no deja de ser una Comisión representativa de lo que es el Consejo, lo que no quiere decir que el Consejo delegue su responsabilidad en la citada comisión sino que, simplemente, usa ese vehículo para depurar previamente los riesgos[36] que puedan existir.

En la mayoría de las grandes empresas, existe además una Dirección de Riesgos que, permanentemente, está vigilando la distinta variedad de riesgos que se puede dar en distintos ámbitos, dependiendo del tipo de empresa.

Desde luego, el ciber riesgo es enorme y difícil de prever. Se debe intentar paliarlo, desde luego. Los ciberataques son cada vez más importantes para los intereses de los distintos países e instituciones. También son muy importantes y siguen estando vigentes los intereses de los piratas, o espías, que quieren penetrar en las intimidades de las empresas[37].

36 Si bien se suele emplear el término amenaza como sinónimo de riesgo (4) no deben confundirse ambos, puesto que riesgo debería entenderse como estimación del grado de exposición a que una amenaza se materialice a través de vulnerabilidades, sobre uno o más activos propios causando daños o perjuicios en los mismos (5). El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

37 El espionaje es la actividad más frecuente en la guerra que tiene lugar en el ciberespacio. De todos los datos que se extraen, la propiedad intelectual es sólo una parte. Casos de tanta relevancia como la operación Shady Rat (5) que desvela el espionaje continuado a 70 empresas y organismos oficiales durante cinco años son sólo la punta del iceberg que sobresale al mar de secretismo que se guarda en torno a estos asuntos. El Ciberespacio. Nuevo Escenario de Confrontación. Centro Superior de Estudios de la Defensa Nacional Febrero, 2012

Los hackers[38] son capaces de alterar el diseño de los sistemas operativos y, de esta manera, instalar programas o rutinas que les habilitan para controlar subrepticiamente los sistemas operativos de las empresas.

Para combatir estos ataques, las grandes empresas están contratando a antiguos hackers como "jefe de datos". Este es, por ejemplo, el caso de Telefónica, que fichó a **Chema Alonso**, antiguo hacker, como experto en ciberseguridad del grupo y que, actualmente, desempeña el cargo de "*Chief Data Officer*" (CDO)[39].

38 Los protocolos, los sistemas operativos y demás lenguajes que sirven para hacer funcionar los programas y legibles los datos constituyen, a su vez, la capa sintáctica del ciberespacio. Contiene las instrucciones que los diseñadores y usuarios introducen en los sistemas y es básica para permitir que los terminales se comuniquen entre ellos. Los sistemas operativos son uno de sus elementos críticos. Su diseño constituye una de las vías de acceso más frecuentes para hackers e intrusos. La imperfec¬ción de su programación o la intencionada apertura de puertas traseras que permitan un acceso fácil y rápido para efectuar retoques y modifica¬ciones se utiliza por los expertos para instalar programas o rutinas que les habilitan para controlar subrepticiamente los sistemas.

39 http://www.elmundo.es/economia/2016/05/26/5746920e268e3efe4d8b4646.html

8. La prevención de riesgos

En el mundo empresarial, hay un factor primario y fundamental que es la prevención, que va unido a la educación, es decir, hay que formar a todos los responsables de la empresa para que sepan que, sobre ellos, pende una responsabilidad enorme, que es la posibilidad de que, parte de los asuntos de la empresa, los asuntos internos, se filtren a terceros, con los objetivos que quieran estos terceros, porque nunca se sabe cuáles son los objetivos finales. Pueden ser espionaje industrial, destrucción del competidor mediante ataques, etc.

En todas estas amenazas y riesgos deben estar pensando, a todos los niveles, los responsables de las empresas. Es vital que exista una gran concienciación sobre lo que implica la ciberseguridad y cómo afectará este nuevo mundo del siglo XXI. Por ejemplo, en los pendrives, hay una gran cantidad de información almacenada. Estos son una puerta de acceso a la información sensible que hay que cuidar para que no caiga en manos de terceros por los perjuicios que puede causar, tanto a la seguridad de la empresa como a la de su personal.

Hay empresas que han tomado la decisión, de que los temas que son verdaderamente estratégicos, no se digitalicen y, en consecuencia, no haya que usar el ordenador. Se vuelven a hacer escritos a máquina, en papel, y nada de copias a todo el mundo. Por ejemplo, las copias de los emails es una actividad muy extendida en las empresas donde todos envían copias a todos ¿Dónde acaba eso? ¿Cómo acaba? ¿Quién termina por tener acceso a eso? Todo eso son asuntos que hay que tener muy en cuenta.

Hay empresas que pueden conocer, en todo momento, qué tipo de ataques se está produciendo en el mundo. Por ejemplo, son empresas que son capaces de monitorizar cómo China o Rusia está intentando ir sobre Estados Unidos y viceversa.

> *"Estados Unidos presiona con más fuerza –mucha más fuerza– contra el robo cibernético de información de empresas y secretos comerciales". "Es mucho más firme y esa es la línea que Estados Unidos está tratando de marcar... 'Está bien espiar a los gobiernos, todo el mundo lo hace. No es correcto espiar los secretos de una compañía'"*, dijo Simon Denyer, el jefe de la oficina del *Washington Post* en Beijing, en el último episodio de *"On China"* de CNN.
>
> *"La economía es tan fundamental para la legitimidad del Partido Comunista que espiar en aras de beneficiar a las empresas de propiedad estatal, por ejemplo, es parte de la estrategia nacional del gobierno",* dijo Denyer".[40]
>
> De acuerdo con U-GOB (https://u-gob.com/), en el documento *"Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document"*[41] el organismo internacional indica que los gobiernos deben tratar a la ciberseguridad como un asunto económico, más que tecnológico, y con base en esta perspectiva coordinar políticas que abarquen todo el gobierno.
>
> > *La ciberseguridad no es un asunto de tecnólogos e ingenieros; los líderes del sector público, desde los más altos niveles, deben tener su atención en el tema y participar en los planes y tomas de decisiones. Los países necesitan una estrategia de ciberseguridad que sea conocida y apoyada por las cabezas del gobierno y esta debe considerar un enfoque global del gobierno, así como ser coherente con las políticas económicas y sociales.*
> >
> > *"Los riesgos en el mundo digital no se pueden eliminar, y un ambiente digital totalmente seguro es imposible si se quiere obtener el potencial que brinda el mismo"* afirma el Director de Ciencia, Tecnología e Innovación de la OCDE, Andrew Wyckoff. *"Sin embargo los riesgos pueden ser manejados efectivamente. Los líderes de las organizaciones son los que mejor conocen y pueden conducir los cambios culturales y organizacionales necesarios para reducir los riesgos a un nivel aceptable".*

40 http://cnnespanol.cnn.com/2015/08/26/ciberseguridad-el-problema-tecnico-en-la-relacion-entre-estados-unidos-y-china/

41 http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

La innovación tecnológica y en políticas públicas es clave para reducir los riesgos. La innovación debe fomentarse tanto en el diseño como en la operación de las actividades sociales y económicas que son apoyadas por el ambiente digital, así como en el diseño y desarrollo de las medidas de seguridad.

El riesgo de un ataque cibernético con implicaciones importantes es muy más alto porque, los ataques cibernéticos, se han convertido en un negocio muy rentable. De acuerdo con la información publicada por Expansión[42]:

1. *El impacto económico del 'cibersecuestro' de datos y archivos podría situarse entre los 3.000 y los 6.000 millones dólares a nivel mundial en 2017, según Sophos.*
2. *Estas cifras demuestran el rápido crecimiento de estas ciberamenazas ya que, en 2016, su impacto fue de mil millones de dólares.*
3. *Según el último Informe SophosLabs 2018 Malware Forecast, el malware ha trascendido los sistemas operativos, y hoy en día el ransomware tiene como objetivo a usuarios tanto de Android, como de Mac, como de Windows o Linux por igual.*
4. *Actualmente se está viviendo una oleada de ransomware alimentada por el RaaS (Ransomware-as-a-Service), negocio que consiste en comercializar dentro de la web oscura ciberataques de ransomware, vendiéndolos como paquetes al mejor postor. Esta avalancha de ataques se ha amplificado además por el resurgimiento de gusanos informáticos, que son aquellos malware que tiene la capacidad de duplicarse y hacen que la infección de los equipos sea rápida y fulminante.*

42 http://www.expansion.com/economia-digital/innovacion/2017/11/21/5a12f943468aebae078b4577.html

9. Prioridades y niveles de seguridad

Como sucede con todas las áreas de control de riesgo, hacerlo bien en seguridad quiere decir que no se nota que lo que se ha hecho. Esto tiene un problema añadido desde el punto de vista de gestión porque, hacerlo bien en seguridad, supone generar incomodidad para todos los empleados de la compañía y, si se quiere estar en niveles de muy alta seguridad, los niveles de incomodidad son muy altos y, si se quiere llevar al extremo se tendría que prohibir, por ejemplo, el uso del smartphone.

Otro aspecto muy importante a tener en cuenta, es que la ciberseguridad tiene una componente de costes muy importante, de manera que, la gerencia de la compañía, tiene que tomar decisiones sobre sus recursos, por definición escasos. Por ejemplo, ¿asigna los recursos de manera que permitan aumentar las ventas al 10%, o los asigna para reducir un 10 % los riesgos en seguridad? La tentación por dejarse llevar por la parte brillante del aumento de ventas es continua y está en la esencia de las empresas hacerlo así.

Forma parte de las tareas del Consejo de Administración ayudar a la gerencia a que tome las decisiones sobre prioridades en este tema de forma correcta. No necesariamente lo correcto es siempre invertir en seguridad, como tampoco es necesariamente correcto invertir siempre en crecimiento. Uno de los papeles del Consejo en esta materia, en lo que pueden de verdad ayudar a la compañía, es llamar la atención sobre si la gestión de prioridades en esta cuestión se está haciendo de forma correcta, sin prejuzgar cuál vaya a ser el resultado, porque cada compañía es un mundo, y cada situación concreta requiere respuestas distintas.

Por otra parte, el mundo del ciberespacio, es un arcano ignoto y, desde luego, absolutamente desconocido. Lo cual quiere decir que la gran mayoría de los miembros de la empresa y sus consejos de administración tienen un nivel de desconocimiento muy importante en este tema. Es decir, en general las empresas no tienen la capacidad de saber si las medidas de seguridad que se están implantando son las correctas y, por lo tanto, deben apoyarse en los criterios de otras personas que ayuden a determinar si lo que se está haciendo es correcto o no.

Pensando en términos del Consejo de Administración, es responsabilidad de los consejeros asegurarse de que las personas que les están asesorando sobre esta materia, son las personas correctas. Pues no se puede esperar de un consejero que sepa de todo. Por ejemplo, no se puede esperar de un consejero que sepa cómo se diseña una fábrica, cómo se diseña la seguridad, o cómo se hace una operación de cobertura con un swap. Por consiguiente, es responsabilidad de los consejeros tener la mejor asesoría.

10. El responsable de la ciberseguridad

Otro tema, también muy importante es el "organizativo". Con mucha frecuencia, la ciberseguridad se hace descansar en el responsable de informática. Esto es un error porque, es como hacer descansar la responsabilidad de control sobre el controlado. Precisamente el responsable de seguridad lo que tiene que hacer es monitorizar los sistemas de la compañía y contribuir a que no se comentan errores. Esto genera tensiones, pero son las mismas tensiones que generan todas las funciones de control. Es muy importante separar la función de seguridad de la función de informática.

11. Formación en las cuestiones de seguridad

Hay que destacar en el tema de seguridad la importancia que reviste la formación de todos los empleados de la compañía de forma continua en las cuestiones de seguridad. La experiencia refleja constantemente que, gran parte de los fallos de seguridad, han sido producidos por personal con baja formación en esta cuestión y un importantísimo porcentaje de las incidencias están allí. Es muy importante enseñar y concienciar a los empleados en lo que deben hacer y en lo que no deben hacer, dado que no hay forma de hacer un seguimiento ni personalizado ni continuo en el tiempo sobre las personas de la empresa.

Un riesgo muy serio cuando se diseña un Plan de Seguridad, es que se acabe convirtiendo en un trabajo burocrático, que hace que sea más importante rellenar la ficha que mirar las cosas. Vuelve a ser responsabilidad del Consejo ser conscientes de que el Plan de Seguridad hay que hacerlo porque ayuda a pensar de forma sistemática, pero su objetivo es entender de verdad lo que está pasando.

Las empresas no solo necesitan hackers blancos[43]. No se puede proteger una empresa protegiendo solo su infraestructura, por el simple hecho de que vivimos en un mundo totalmente digital. Hoy mismo cualquier empleado de la compañía es una pieza fundamental de esta infraestructura. No existe un perímetro de seguridad como, por ejemplo, los cortafuegos. Hoy mismo, estos cortafuegos, son inservibles dado que, las empresas, están totalmente conectadas con muchísimas otras empresas, proveedores, clientes, órganos regulatorios, mercados, etc.

Por tanto, todos los empleados de la empresa forman parte de la infraestructura de protección. Las empresas se protegen mediante la educación y la concienciación de que, cada empleado, puede poner en riesgo la red de protección.

43 Ethical hackers—which are more popularly known as white hats, white hat hackers, sneakers, or even white knights—are information and cyber security specialists who are well-versed in system examination, penetration testing, and many other network analysis approaches that guarantee the safety and integrity of many a company's information system. The sneakers appellation in particular refers to white hats who are actually employed by companies or organizations as network security professionals of sorts. In fact, the National Security Agency (NSA) offers certifications to these hackers such as the CNS 4011, which covers professional and principled hacking techniques and team management. On that note, an entire group of these experts are referred to by the CNS 4011 as red teams or tiger teams if they're acting as aggressors or invaders, and as blue teams if they're acting as defenders or patch makers. https://www.secpoint.com/what-is-a-white-hat.html

Por ejemplo Mondelez[44], dueña de marcas como Oreo, Tang, Milka o Toblerone, tuvo en junio de 2017, un ataque de un virus de tipo ransomware que desde la empresa de ciberseguridad Kaspersky señalaron que se trataba de un nuevo ransomware, que nunca antes se había visto al que bautizaron como NotPetya y que llegó a parar la producción de las empresas de Mondelez suponiendo una perdidas del 3% de las ventas.

La compañía de solvencia crediticia Equifax[45], perdió un 27% del valor de su cotización bursátil.

Un ciberataque puede llegar a comprometer entre un 25% y un 35% de la capitalización bursátil de una empresa lo que podría tener como consecuencia que, aprovechando estas caídas en la capitalización bursátil, las empresas fuesen sometidas a una OPA. Este hecho podría dar lugar a que una empresa contratase a alguien para llevar a cabo un ciberataque y hacer posteriormente una OPA. Por tanto, estamos ante un cambio total de paradigma.

Es cierto que los consejeros no tienen que saber de todo, pero, no deja de ser menos cierto que, los consejeros, conocen mejor el mundo de las finanzas que el de la ciberseguridad. Hay que cambiar entonces también este paradigma. La tendencia irreversible es que, las empresas y sus entornos, sean cada vez más digitales por lo que, los miembros del consejo de administración, no solo deben tener conocimiento de los mercados, sino que, además, deben tener conocimiento de los riesgos a los que pueden ser sometidas las compañías y, uno de ellos incuestionablemente, son los ciberataques. Esto no significa que se deban convertir en hackers blancos, pero si tener el conocimiento debido para poder formular juicios prudentes sobre lo que significan los ciberataques y por ende, la ciberseguridad.

El riesgo es inherente a cualquier actividad económica y, dicho riesgo, no se puede llevar a cero pues, un riesgo cero supondría un coste infinito. Por ello las empresas tienen que admitir la existencia de los riesgos y, por tanto, tener una estructura organizativa adecuada. Las empresas, de forma creciente, tienen que ser conscientes de que el riesgo digital está aumentando porque todos los sistemas de generación de valor de las empresas dependen cada vez más de la tecnología y de esta situación hay que ser absolutamente conscientes.

44 Mes y medio después del ciberataque WannaCry que puso en jaque a cientos de empresas y multinacionales en todo el mundo, los piratas informáticos han vuelto a actuar a nivel global contra organismos públicos y privados. Se trata de un virus sobre el que no existe unanimidad entre los expertos en seguridad informática. Mientras que según el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia (CNI),se trata de un virus de tipo ransomware -que secuestra la información de los equipos y sólo la devuelve a cambio de un rescate- variante de Petya (el diminutivo en ruso de Pedro) que ya habría atacado varios sistemas informáticos en todo el mundo en 2016, desde la empresa de ciberseguridad Kaspersky señalan que "se trata de un nuevo ransomware, que nunca antes se había visto" al que han bautizado como NotPetya. Por el momento, la lista de afectados la componen al menos 80 empresas de diversos sectores localizadas en países como Reino Unido, Estados Unidos, Francia, Rusia, España, India y Ucrania. En ella se encuentran algunas como la multinacional alimentaria Mondelez, que es dueña de marcas como Oreo, Tang, Milka o Toblerone.
http://www.elmundo.es/tecnologia/2017/06/27/595269e0ca4741fb3f8b4668.html

45 La compañía de solvencia crediticia Equifax con sede en Atlanta, maneja información de cerca de 820 millones de personas en todo el mundo, y el pasado 7 de septiembre de 2017 reconoció que, entre mayo y julio, había sufrido un ataque informático que pudo exponer datos de 143 millones de personas. Entre los datos a los que accedieron los piratas figuran números de tarjetas de crédito de 209.000 consumidores y documentos con información personal de 182.000 individuos.
https://elpais.com/economia/2017/09/26/actualidad/1506447652_267329.html

El 23 de marzo de 2018, el sistema informático del gobierno de la ciudad de Atlanta, en el sur de Estados Unidos, fue objeto de un ciberataque de ransomware[46] que dejó al Ayuntamiento de Atlanta sin 16 años de registros, dado que estaban digitalizados.

Las empresas tienen que concienciarse de que la tecnología les ayuda, pero también les puede perjudicar. Por ejemplo, como se ha citado anteriormente, las empresas prefieren gastarse un 10% más para aumentar las ventas sin ser conscientes de que, al ser todo digital, este aumento de las ventas se puede perder en una tarde como consecuencia de un ciberataque.

Por ejemplo, la compañía de solvencia crediticia Equifax ni construye casas, ni vende coches, lo qué maneja es información de cerca de 820 millones de personas en todo el mundo, y el pasado 7 de septiembre de 2017 reconoció que, entre mayo y julio, había sufrido un ataque informático que pudo exponer datos de 143 millones de personas.

12. El caso Facebook

Respecto del caso "Facebook", Enrique Dans, profesor del IE, comentaba lo siguiente[47]:

"¿Se trata acaso de algún tipo de ataque sofisticadísimo, de una filtración de datos sin precedentes o de la explotación de alguna vulnerabilidad desconocida que permitió a esa compañía robar los datos personales y trazar complejos perfiles psicológicos de cincuenta millones de norteamericanos, con entre tres mil y cinco mil datos sobre cada uno de ellos? (sí, existen tantos datos sobre ti... y puedes comprobarlo bajándote e inspeccionando lo que Facebook ha recolectado en el tiempo que llevas usándolo). Pues no, me temo que no. Hablamos de algo completamente normal, que lleva pudiéndose hacer en Facebook sin demasiados problemas ni limitaciones desde prácticamente los inicios de su actividad publicitaria. Utilizar un aparentemente trivial quiz, de esos pasatiempos que millones de ignorantes contestan todos los días en la red social para supuestamente saber algo más de sí mismos y compartirlos con sus amigos, para conseguir acceso a tantos perfiles como amigos tienen esos incautos. En realidad, lleva haciéndose desde la época de las aplicaciones de juegos, desde los FarmVille, los MafiaWars o los PetSociety, si no antes. Algo que Facebook, por mucho que ahora pretenda redefinirlo como "platform abuse", ha permitido de manera perfectamente consciente, como parte de una estrategia destinada a convertirse en el mejor francotirador del mundo, en el más acertado, en el que más sabe de sus usuarios. El problema no está en que Cambridge Analytica, Robert Mercer o Alexander Nix sean perversos genios del mal, sino en que la mismísima API de Facebook permite a terceras partes no solo acceder a tus datos con el simple permiso que otorgas para hacer un estúpido quiz, sino que, además, permite el acceso a los perfiles de todos tus amigos. Con simplemente 270,000 personas que rellenaron el quiz, muchos de ellos trabajadores pagados del Mechanical Turk de Amazon que ofrecieron acceso a sus perfiles personales incumpliendo las condiciones del servicio, la compañía obtuvo acceso, suponiendo una media muy conservadora de 185 amigos por usuario, a los perfiles de casi cincuenta millones de usuarios. Genial".

47 https://www.enriquedans.com/2018/03/facebook-de-la-ingenuidad-a-la-estupidez.html

13. Nivel de inversión en ciberseguridad

En la RSA Conference[48], se ha puesto de manifiesto que la mayoría de las empresas tienen un bajo nivel de inversión en ciberseguridad[49] lo cual es absolutamente contradictorio en un mundo con creciente uso de información digitalizada.

Este año 2018, en el World Economic Forum de Davos, donde uno de los 3 puntos de la agenda era ciberseguridad, se ha creado el "Global Centre for Cybersecurity"[50].

> *"The aim of the centre is to establish the first global platform for governments, businesses, experts and law enforcement agencies to collaborate on cybersecurity challenges. As a truly borderless problem, cyber-attacks are surpassing the capacities and institutions that are currently dealing with this threat in an isolated manner. Only through collaboration, information exchange and common standards can the global community successfully counter organized digital crime".*

Hace falta todavía una toma de conciencia en los niveles directivos de que la empresa de hoy es digital y, en cuanto tal, la gestión de los riesgos tecnológicos es más relevante que los otros riesgos tradicionales, como los riesgos de mercado y de la competencia. Los Consejos de Administración están todavía muy lejos de esta profundización en la toma de conciencia. No se exige que los consejeros deban ser expertos, pero tienen que tener muy presente que las empresas que asesoran tienen un nivel de digitalización cada vez más importante por lo que, los riesgos digitales, están alcanzando un importante nivel de relevancia.

48 RSA Conference conducts information security events around the globe that connect you to industry leaders and highly relevant information. We also deliver, on a regular basis, insights via blogs, webcasts, newsletters and more so you can stay ahead of cyber threats. https://www.rsaconference.com/

49 With so many technological advancements in the last decade, the business world has transitioned into a ground where customers' most sensitive information is stored, shared and accessed through the cloud. It is important for companies to safeguard this data, which is why cybersecurity should be of utmost importance in your organization. https://www.michaelpage.com/our-expertise/information-technology-recruitment/why-companies-need-invest-cybersecurity

50 "If we want to prevent a digital dark age, we need to work harder to make sure the benefits and potential of the Fourth Industrial Revolution are secure and safe for society. The new Global Centre for Cybersecurity is designed as the first platform to tackle today's cyber-risks in a truly global manner," said Alois Zwinggi, Managing Director at the World Economic Forum and Head of the Global Centre for Cybersecurity. New technologies like artificial intelligence, the internet of things and robotics and their application in sensitive areas such as finance, healthcare, telecommunications and mobility make it all the more important to keep up with the increasing speed and sophistication of cyber-attacks. The cost of cybercrime to the global economy could go up to $500 billion annually, according to experts. In comparison, the annual GDP of Switzerland in 2017 is estimated at $659 billion. The World Economic Forum has recognized cybersecurity as one of the world's most critical risks (https://www.weforum.org/reports/the-global-risks-report-2018). In response, the new Global Centre for Cybersecurity will draw on the Forum's government and industry support to work towards a more secure cyberspace through its established multistakeholder approach. https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

14. Riesgo de seguridad y de ciberseguridad. Plan de Actuación

Los consejos de las empresas grandes, son perfectamente conscientes del riesgo de seguridad y de ciberseguridad. Un ataque a la ciberseguridad de una empresa como Red Eléctrica o Bankia es muy importante porque, en el caso de Red Eléctrica, puede afectar a la seguridad nacional y, en el caso de Bankia, hay un importantísimo riesgo en su reputación pues, en este último caso, Bankia es una empresa que vende confianza, y es muy grave cuando se pierde la confianza en este tipo de instituciones como ya se citó en Equifax.

Por otra parte, alcanzar un nivel total de ciberseguridad es una batalla que nunca se va a ganar. Por consiguiente, la ciberseguridad y sus riesgos, se han convertido en un problema con el hay que aprender a convivir. Por ello los Consejos de Administración tienen que hacer los tradeoffs necesarios, no solo en términos de cuánto se gastan en ciberseguridad sino también en cómo se diseña la compañía, sus procesos, el personal que contrata, las inversiones que realiza, y de cómo interviene en todo esto el componente de la ciberseguridad.

Los consejos de administración no necesariamente deben contar con expertos en ciberseguridad, pero sí tienen que tener un plan de actuación que conste de:

1. **Un diseño específico de los riesgos** que su empresa contrae en esta área. Estos riegos, evidentemente, dependen de la naturaleza del negocio y son, por tanto, muy diferentes.

2. **Un protocolo de actuación específico** dado que aquí, el tiempo de reacción es crucial y, por lo tanto, es vital que las respuestas estén mecanizadas. Todo tiene que estar pensado de antemano y, en consecuencia, es muy importante que el Consejo se asegure de que los **protocolos de actuación** sean específicos y de respuesta inmediata.

Todas las empresas grandes utilizan estos hackers blancos para hacerse ataques a sí mismos. Esto es parte del proceso de ciberseguridad, que cualquier consultor recomienda, y que es obligatorio. Una de las primeras cosas que enseñan estos Hackers Blancos es que las empresas deben ser capaces de contactar con las personas cruciales, las personas críticas, para tomar decisiones oportunas, en tiempo real. Las empresas deben poseer los números de los teléfonos personales de sus empleados, tienen que tener acceso a sus páginas de Facebook y a los WhatsApp de los individuos que son críticos en una compañía para responder ante un ataque de ciberseguridad.

Las compañías son conscientes del problema y están en la fase de saber responder. Eso requiere, sin duda, cambios de cultura, de formas de pensar y de formas de actuar, es decir es un autentico proceso de aprendizaje transformacional de las personas pues, de lo contrario, no es posible la transformación digital.

Por otra parte, hay un problema serio de dar información al mercado, pero también es importante **qué tipo de información se da al mercado**, para evitar pánicos o efectos innecesarios.

De acuerdo con una información de Kaspersky del 2 de octubre del 2017[51]

1. El 43% de los ciberataques se dirigen contra las pymes.
2. Los costes directos en los que incurren las pequeñas y medianas empresas tras un ciberataque ascienden a unos 35.000 euros.
3. El 60% de las pequeñas compañías desaparecen dentro de los 6 meses siguientes a sufrir un ciberataque.

Es importante que las empresas se comparen con sus pares para determinar cómo están en temas de ciberseguridad en relación con las demás y cuáles son los riesgos que está asumiendo en relación a su mercado. Aquí es donde el papel de los consultores es muy importante pues pueden dar una orientación a la empresa diciéndole donde está en términos relativos. En la carrera de protección contra los ciberataques la empresa, ante un problema de riesgo penal en la persona de los consejeros, lo único que puede hacer es demostrar que ha hecho todo lo posible en temas de protección ante los riesgos cibernéticos y la prueba es que la empresa está por encima de la media.

51 https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals.
Las pequeñas empresas subestiman la posibilidad de ser objetivo de un ciberataque y no piensan en el impacto que a largo plazo puede tener en su negocio. La mitad de las empresas europeas entrevistadas (51%) no creía que pudiese llegar a ser víctimas de un ciberataque y el 68% de las que nunca habían sido víctimas de un ciberataque, pensaban que era poco probable o imposible sufrir uno. Pero no es sólo la reputación lo que está en peligro. Del estudio de Kaspersky Lab 2016 sobre los riesgos TI, se desprende que los costes directos en los que incurren las pequeñas y medianas empresas ascienden a una media de 35.000 euros y el 60% de las pequeñas compañías desaparecen en los 6 meses siguientes a sufrir un ciberataque. No hay víctima pequeña para los cibercriminales. Todo tipo de información sobre los clientes tiene valor, desde la información de suscripción, los datos personales, financieros, etc, ya que puede ser utilizada y aprovechada de muchas maneras, sobre todo para su reventa y luego utilizarla para cometer fraude.

Un aspecto muy importante es la colaboración dentro del sector porque, todas las empresas que están en el mismo grupo, por ejemplo, todos los bancos, están sujetos a los mismos tipos de ataques y todas las empresas de energía están sujetas a los mismos tipos de ataques. Por consiguiente, no solo es importante la colaboración con las instituciones públicas, como el Instituto Nacional de Ciberseguridad (INCIBE) o con el Centro Nacional de Protección de Infraestructuras Críticas CNPIC, sino también con el sector.

Aquí se presenta otro *tradeoff*. Cuánta información dan las empresas es un buen indicador de cuánta información van a recibir. En esta cuestión se presenta un límite a la información que se intercambia pues las empresas no pueden revelar todos los aspectos que afectan a la información sensible.

El proceso de aprender a colaborar entre empresas del sector es muy importante, porque al final, lo que se trata es de que, entre todas las compañías, sean capaces de hacerles la vida más difícil a los hackers.

Aunque generalizar es un absurdo, pues cada empresa tiene sus condicionantes específicos, estas deben bloquear el acceso, desde todos sus equipos, a cualquier página de internet a la que no den, expresamente, su permiso. Pero, si desde un dispositivo (ordenador, smartphone, etc.) en el que la empresa puede acceder a información de sus clientes, puede, a su vez, poderse conectar con diferentes páginas web que tienen publicidad, se le presenta un gran problema a la empresa porque, la publicidad, es uno de los caminos por el que se puedan hacer ciberataques.

Dada esta situación, la posición de las compañías ante los ciberataques debe ser absolutamente radical. Los gusanos informáticos[52] pueden entrar por un vídeo que se ve desde una página web, por ejemplo desde un periódico porque, un periódico pone un anuncio de alguien que conoce pero, ese anuncio, puede redirigir a otro sitio por donde penetra el gusano informático.

La seguridad tiene que acompañar a los procesos de transformación digital. En este sentido las empresas no se pueden situar en posiciones absolutamente rígidas pues, en ese caso, irían en contra de algo que es una ventaja empresarial también. Por lo tanto, cada caso, tienes sus características específicas, que hay que saber tratar, para evitar los ciberataques.

52 Malware que tiene la capacidad de duplicarse y hacen que la infección de los equipos sea rápida y fulminante.

Por ejemplo, hay muchísimas empresas que, de forma natural, tienen automatizado todo el proceso de pago de las facturas, incluida la aprobación del pago, a la confirmación de la recepción. Si algún malware entra en ese proceso, el problema que se le crearía a la empresa sería crítico.

En este caso, si una compañía incorpora una nueva plataforma de facturación electrónica, debe analizar de forma muy importante los riesgos que conlleva. Eso es lo que hay que evitar. La empresa debe ser absolutamente consciente del tipo de información que va a manejar y, si esa información, afecta a otras empresas o es una información que afecta a datos de carácter personal, pues hay una regulación que se debe cumplir.

Las empresas deben conocer: ¿Qué tipo de información y qué tipo de sensibilidad tiene la información? ¿Si la información es interna o está externalizada en un tercero?". Por tanto, la empresa debe tener unos niveles de gestión de sus accesos y, realizar unas pruebas periódicas que garanticen que, esa plataforma, si está expuesta en internet, tiene los adecuados niveles de protección. En cualquier caso, la empresa nunca tendrá la completa seguridad de no verse sometida a ciberataques.

Por ello, los procesos de transformación digital, deben estar acompañados con una gestión de riesgos y por una política de admisión de riesgos que cada empresa situará en los niveles que considere adecuados.

En consecuencia, es muy importante que, desde el Consejo de Administración, se defina el nivel de riesgo asumible. Porque una de las labores fundamentales del consejo, en un mundo en el que actualmente no es posible tener un nivel de seguridad total, es definir el nivel de riesgo asumible.

15. Conceptos afectados por la Ciberseguridad

Un tema muy importante es la imagen que, las grandes empresas y su entorno, tienen en materia de ciberseguridad porque, en definitiva, estas grandes empresas son un referente para el resto.

La ciberseguridad parece una cuestión solo relativa a los grandes detalles cuando también está en los pequeños detalles. Hay que tener presente que, los problemas que tienen las organizaciones pueden ser de gran calado, pero también existen otros que pueden ser más pequeños pero que, asimismo, pueden causar grandes complicaciones.

Fundamentalmente en ciberseguridad hay 3 grandes conceptos que pueden verse afectados:

- La **confidencialidad de la información** que es el activo estratégico que, hoy en día, tiene cualquier organización.
- La **integridad de la información**.
- La **disponibilidad de la información**, en el momento que la empresa la necesite.

Estos tres conceptos han cobrado una relevancia lógica porque, verdaderamente, las empresas están en un momento de transformación digital. Esta transformación, es una pieza clave para poder incorporar la revolución digital que está evolucionando radicalmente, (Blockchain, Cloud, Big Data, etc.) Esto es bueno para las compañías, siempre que los riesgos que conllevan sean gestionados lo mejor posible. Pero, no solo cambia la tecnología, sino que también cambian los sistemas de generación valor (procesos y plataformas), que están en una profunda fase de transformación, como por ejemplo la utilización de la robótica para hacer más eficientes a los sistemas de generación valor.

Además de transformar los sistemas de generación valor, toda la empresa está en un proceso de transformación estratégica, que le permite abordar nuevos negocios.

Las empresas ahora tienen un área de innovación para poder hacer cosas de forma diferente a como se venían haciendo, incluso diversificar los ámbitos de negocio.

La transformación digital hay que acompañarla de una nueva gestión de los riesgos que están surgiendo, lo que conlleva que toda organización tenga que hacer ese proceso de cambio.

Para poder llevar a cabo la transformación digital los temas organizacionales son importantes, pues la ciberseguridad y la gestión de los riesgos en una organización, son claramente una responsabilidad del Consejo de Administración. Aquí hay que aplicar 3 líneas de defensa.

Primera línea de defensa: **Implantación de las medidas de seguridad**. Esta primera línea está en el ámbito técnico, que solo personas técnicas pueden llevar a cabo porque son las que establecen las soluciones tecnológicas.

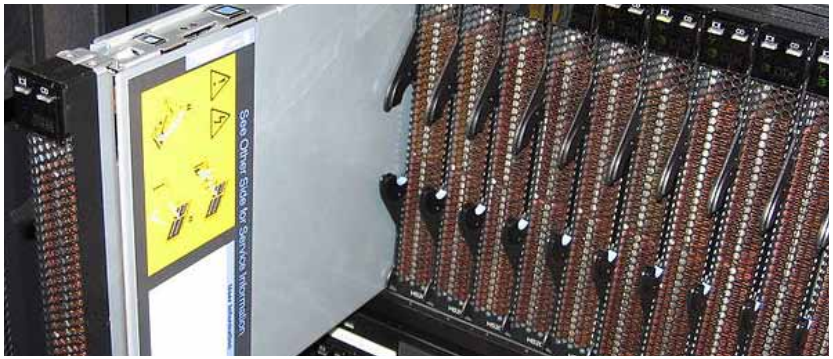
Segunda línea de defensa: **Establecer un marco de riesgos que, en materia de ciberseguridad, se están contemplando**. Aquí, las Direcciones de Riesgos tienen que trabajar con estos nuevos conflictos que el mundo de la ciberseguridad impone a las empresas, no solamente por las nuevas tecnologías, sino porque se cambia la forma en que se hacen las cosas.

Antes, los desarrollos tecnológicos eran proyectos de 2-3 años. Hoy en día se imponen temas que son resultados de 2-3 semanas.

Tercera línea de defensa: **Auditoría periódica y permanente**. En muchas grandes organizaciones, sus equipos de auditoría, no están dotados de, o no están suficientemente asesorados por especialistas que les puedan apoyar en los aspectos tecnológicos.

El Consejo de Administración tiene que ser absolutamente co-participe de todos los aspectos organizativos que están involucrados en la gestión del cambio tecnológico.

En Estados Unidos, se está viendo como buena práctica el asesoramiento tecnológico que, no necesariamente implica que se tenga que incorporar a alguien, pero sí que haya un asesoramiento en esta materia como para que el consejo de administración, tenga suficiente conocimiento que le permita analizar al nivel oportuno. Por tanto, de la misma manera que el consejo de administración no tiene especialistas en todos los ámbitos si debe tener, al menos, un asesoramiento en la transformación digital y sus consecuencias, en la que hay que dar un salto cualitativo.



Hay una pieza fundamental en la gestión de los riesgos, y es que el consejo tiene que conocer, de alguna forma, cómo se están gestionando los riesgos de ciberseguridad que están asociados a los procesos de transformación digital.

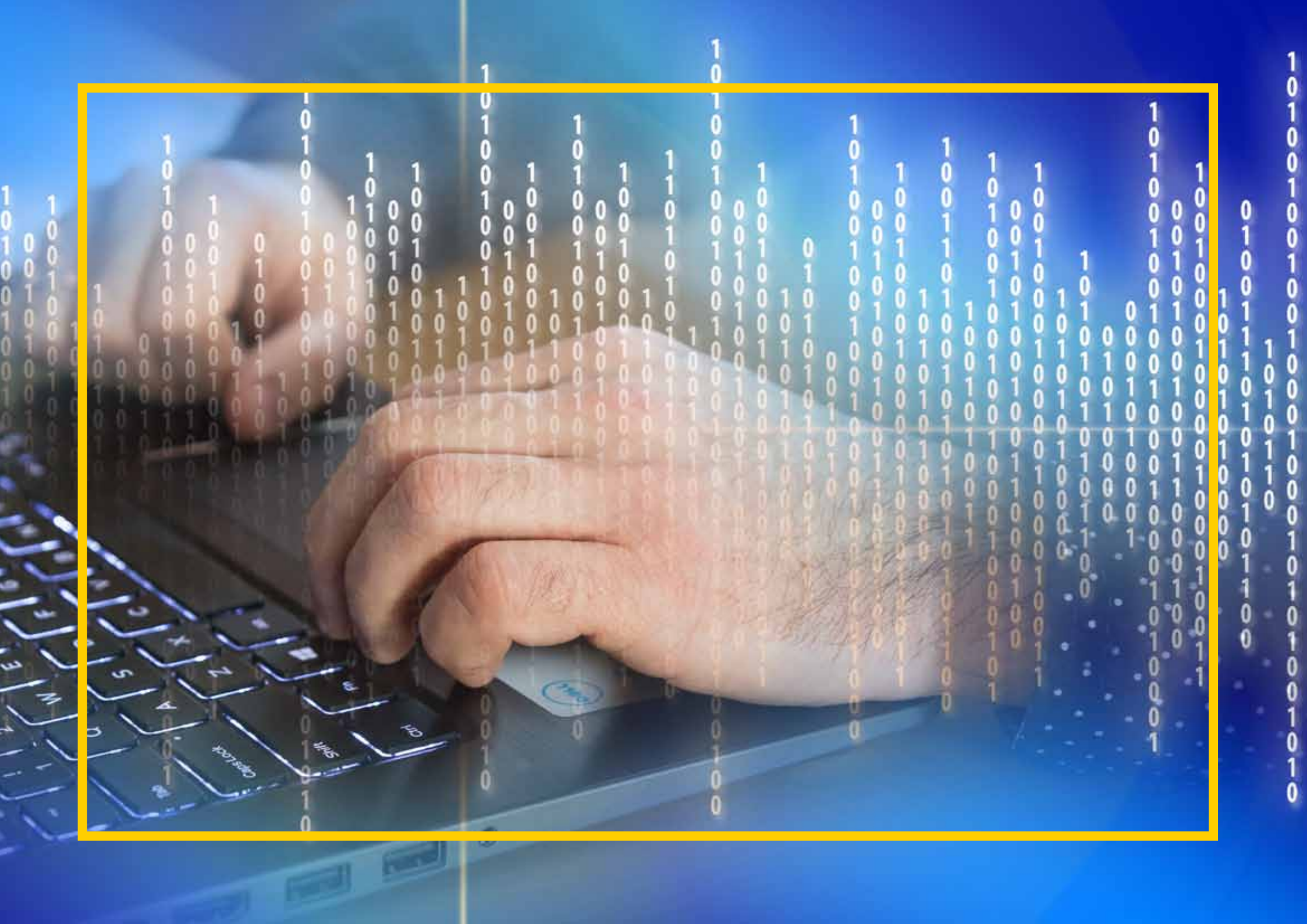
En las empresas existen: Directores de Ciberseguridad, Directores de Sistemas de Información y Directores de Riesgos. ¿Cuál es la información que tiene que llegar al consejo de todo ese proceso de gestión?, para que este pueda estar absolutamente apoyado y respaldado y poder mostrar su conformidad en cómo se están haciendo las cosas en materia de ciberseguridad.

16. Gestión de las situaciones de crisis

El Consejo debe estar informado y ser absolutamente participe. Dado que no es posible proteger a la empresa al 100% de un ciberataque, es muy relevante saber ¿cómo se reacciona? y ¿cómo se gestiona una amenaza o un incidente de seguridad? En estas situaciones de incidentes de seguridad debe tenerse muy en cuenta que ha cambiado totalmente el paradigma. Por ejemplo, cuando sucedió el ataque del *WannaCry (WanaCrypt0r 2.0 o Wannadecryptor*, clasificado como gusano informático del tipo ransomware[53]), en diversas empresas, muchos de sus empleados twittearon y explicaron en Facebook lo que estaba pasando en tiempo real. Sucedió el hecho de que, aunque la empresa no quería publicar el daño de seguridad que se había producido, no pudo evitar que sus empleados lo informaran a través de las redes sociales.

Las compañías tienen que saber gestionar estas situaciones de crisis, deben de estar preparadas y saber exactamente cómo reaccionar porque, estos fallos de seguridad implican grandes deterioros de la imagen ante los clientes. Este deterioro de la imagen tiene un gran impacto en temas económicos. Existe pues un tema reputacional y de confianza, muy relevante, que no se puede eludir en forma alguna y que afectará a la compañía de forma muy importante.

53 El 12 de mayo de 2017 entre las 8 y las 17:08 horas UTC2 se registró un ataque a escala mundial que afectó a las empresas Telefónica, Iberdrola y Gas Natural, entre otras compañías en España, así como al servicio de salud británico, como confirmó el Centro Nacional de Inteligencia. La prensa digital informaba aquel día que al menos 141 000 computadores habían sido atacados en todo el mundo. Los expertos sostienen que WannaCry usó la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense y filtrada por el grupo The Shadow Brokers, que permite atacar computadores con el sistema operativo Microsoft Windows1 no actualizados debidamente. La compañía Microsoft había comenzado a distribuir actualizaciones de seguridad al día siguiente de conocerse esta vulnerabilidad, el 10 de marzo de 2017,12 a través de Windows Update, pero solamente para las versiones de Windows posteriores a Windows Vista. El 13 de mayo de 2017, ante la supuesta gravedad del ataque, publicó un parche separado para Windows 8, Server 2003 y XP.13 Muchos computadores que no tenían aplicadas las actualizaciones de seguridad MS17-010 de marzo de 2017 quedaron gravemente afectados,10 con sus archivos cifrados y mostrando un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descifrar los archivos. En realidad, un experto de Reino Unido evitó en gran medida la expansión del ciberataque global. El autor del blog MalwareTech estaba estudiando el programa dañino cuando se dio cuenta de que el mismo intentaba conectarse a un dominio no registrado: si no lo lograba, cifraba el equipo; si lo lograba, se detenía.2 Una vez que este experto en seguridad registró el dominio, a las 17:08 UTC del 12 de mayo, cesó el ataque. Todas las medidas urgentes que se tomaron a partir de esa hora fueron prácticamente innecesarias. Un análisis del malware ha sido publicado por Microsoft.14 .https://es.wikipedia.org/wiki/WannaCry



17. Mapa regulatorio y las prioridades

a. Mapa regulatorio

Por sectores, hay un volumen regulatorio muy importante que es, casi imposible de gestionar. A nivel de consejo hay que tener mucha información, de cuál es el mapa regulatorio y en qué forma les está afectando.

Por ejemplo, en mayo de 2011, se publicó el "Reglamento de protección de las infraestructuras críticas"[54] y es muy importante conocer que las infracciones que conlleva incumplir el nuevo "Reglamento General de Protección de Datos":

> "Van desde el 2% de la facturación global hasta 10 millones de euros o el 4% de la facturación hasta 20 millones. La vulneración de la normativa implicará sanciones si la Agencia de Protección de Datos considera que se ha sido absolutamente negligente en el tratamiento de datos y en otros casos enviará advertencias para que se puedan corregir"[55].

Estas sanciones económicas podrían quebrar algunas empresas, por lo que el mapa regulatorio debe ser un punto de atención.

b. Las prioridades

El consejo de administración debe focalizarse mucho en aquellos aspectos que pueden ser más relevantes. Los consejos de administración deben marcarse prioridades clave: como garantizar la diversidad en los consejos e impulsar sus conocimientos sobre la transformación digital que se está llevando a cabo en las empresas. También deben conocer las consecuencias que esto produce en cuanto a la ciberseguridad, cuyos riesgos son una amenaza creciente en el siglo XXI.

54 Real Decreto 704/2011, de 20 de mayo, (http://boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf) por el que se aprueba el Reglamento de protección de las infraestructuras críticas. La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Reglamento de ejecución de desarrollo de la mencionada Ley.

55 http://www.agenttravel.es/noticia-030723_-El-reglamento-de-proteccion-de-datos-conlleva-sanciones-de-hasta-el-4-de-la-facturacion-.html

Dentro de las prioridades del consejo está también trabajar niveles de madurez, cooperación y compartir con terceros, cuestión esta última, de una gran importancia. Ahora por ejemplo, con todos los temas de infraestructuras críticas y con la comunicación de incidentes[56] que, por muchas variantes, las empresas tienen que cumplir, es importante establecer criterios comunes y trabajar en marcos que sirvan de comparación, como mínimo, sectorialmente. Al considerar la empresa y su ciberseguridad hay que tener en cuenta el ecosistema donde se desarrolla. En el ecosistema están, por ejemplo, todos los proveedores y las empresas de productos complementarios, etc.

56 "AlertPIC es un instrumento que servirá para la comunicación de incidentes que puedan producirse entre los operadores de infraestructuras críticas y el CNPIC, a través de una novedosa App, que asegura que esta comunicación sea siempre rápida, fiable, segura y fluida". "Esta aplicación, la primera de su clase a nivel internacional, podrá intercambiar información y ficheros en tiempo real como canal de comunicación alternativo ante situaciones de crisis motivadas por un incidente de tipo físico o cibernético, permitiendo realizar llamadas directas para comunicar alertas, notificación de incidencias y difusión de comunicados entre otros servicios". "AlertPIC se caracteriza por su alto nivel de seguridad, al incluir el cifrado de las comunicaciones de extremo a extremo y de su almacenamiento. Y tiene dos plataformas: una de carácter exclusivamente técnico, para la gestión de ciberincidentes por los especialistas de cada organización; y otra de carácter estratégico, para que los responsables de seguridad tengan una vía directa de comunicación con el CNPIC". "La aplicación permitirá reforzar los mecanismos de prevención, gestión y respuesta frente a incidentes de carácter físico y cibernético, aprovechando las capacidades tecnológicas de la Administración, en este caso la experiencia, medios y los sistemas tecnológicos del Ministerio del Interior". http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2017/151117congresoinfraestr.aspx

18. Fiscalía española: Acusación por hechos ilícitos competencia del área de especialización en criminalidad informática

La Fiscalía General del Estado establece, en la "Memoria elevada al Gobierno de S. M. presentada al inicio del año judicial por el Fiscal General del Estado Excmo. Sr. Don José Manuel Maza Martín", los delitos informáticos, las amenazas asociadas y los porcentajes de las mismas, tal y como se expresan en la tabla siguiente:

Delitos informáticos		Calificaciones	%
Delitos contra la libertad	Amenazas / coacciones cometidos a través de las TICs (art. 169 ss y 172 y ss)	242	14,68
	Acoso cometido a través de las TICs (art. 172 ter)	23	1,40
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	36	2,18
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	332	20,15
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	38	2,31
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	22	1,33
Delitos contra la intimidad	Ataques a sistemas informáticos / interceptación transmisión datos (arts. 197 bis y ter)	26	1,58
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	107	6,49
Delitos contra el honor	Calumnias / injurias contra funcionario o autoridad cometidas a través de las TICs (art. 215)	30	1,82
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art. 248 y 249)	633	38,41
	Descubrimiento de secretos empresariales (art. 278 y ss)	16	0,97
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	20	1,21
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	22	1,33
	Delitos contra la propiedad intelectual en la sociedad de la información (arts. 270 y ss)	32	1,94
Delitos de falsedad	Falsificación a través de las TICs	45	2,73
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	13	0,79
Otros		11	0,67
Total		**1.648**	**100,00**

Fuente: Memoria elevada al Gobierno de S. M. presentada al inicio del año judicial por el fiscal general del estado Excmo. Sr. don José Manuel Maza Martín. Madrid 2017. Página 661

a. Acusaciones del Ministerio Fiscal[57]

Durante el año 2016, la Fiscalía española presentó un total de 1.648 escritos de acusación por hechos ilícitos competencia del área de especialización en criminalidad informática. Esta cifra supone un importante incremento[58], cuantificado en un 32,68 % respecto del año precedente, en que dicha cifra fue de 1.242. Se retoma así la tendencia ascendente que venimos constatando, con la excepción del citado año 2015 en que detectamos un ligero descenso de poco más del 2%, desde el inicio de la constitución de la red, en el año 2011, anualidad en la que registramos un total de 906 escritos de esa naturaleza. Quiere decirse con ello, que con independencia de que se haya reducido de forma muy notable el número de procedimientos judiciales incoados por hechos ilícitos vinculados al uso de las TIC, la capacidad de concretar las investigaciones en acusaciones específicas contra personas perfectamente determinadas y por tanto de ofrecer una respuesta adecuada desde el Estado de Derecho frente a estas conductas va mejorando progresivamente.

57 https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/recursos/pdf/MEMFIS17.pdf. Página 660

58 1. Ciberamenazas (To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity). Las amenazas cibernéticas son unos de los riesgos globales emergentes que crecen con mayor rapidez. Durante el foro se ha anunciando el lanzamiento de un Centro mundial para la seguridad cibernética, una plataforma en la que participan distintas partes interesadas con el objetivo de crear un entorno operativo seguro para las nuevas tecnologías como son la inteligencia artificial, la robótica y los drones, los vehículos autónomos y el Internet de las cosas. http://www.transformapartnering.com/conclusiones-davos-que-impactan-en-tu-negocio/

20. La Responsabilidad penal de los miembros del Consejo de Administración

La responsabilidad de los consejos es tener definido el problema de ciberseguridad y establecer:

a. Políticas para gestionar los riesgos
b. Políticas de transparencia
c. Políticas de comunicación
d. Políticas de gestión de crisis
5. Hacer un seguimiento del cumplimiento de todas esas políticas

Es muy importante conocer la responsabilidad penal en las que pueden incurrir, tanto las empresas como los consejeros, porque es la preocupación máxima para los miembros del consejo[59].

Merece la pena resaltar en este panorama organizativo, también la parte jurídica, para que los consejeros sepan a dónde llegar o no llegar con un componente a veces incluso rozando lo ético.

59 "Para establecer en cada caso a quien y de qué modo imputar la responsabilidad, la doctrina se refiere a la "teoría del dominio del hecho", según la cual sólo puede ser autor quien, en atención a la importancia de su aportación objetiva, está en condiciones de dominar el curso del hecho". "En el caso de las compañías mercantiles, lo verdaderamente esencial para el proceso penal -en el que se persigue la verdad material- es determinar quien ostenta el dominio real de la sociedad y la capacidad para utilizarla con fines ilícitos". "la Ley de Sociedades de Capital impone al Consejo de Administración el deber de supervisar las funciones de los órganos delegados, sus miembros ostentan una posición de garante en relación con los riesgos derivados de la actividad empresarial que en su caso puede dar lugar a una responsabilidad penal por omisión". "En esto casos, la jurisprudencia ha venido afirmando que la delegación exonera de responsabilidad penal, siempre que cumpla tres requisitos: que la persona escogida tenga capacidad suficiente para realizar las funciones encomendadas, que se le faciliten los medios e instrumentos necesarios para su realización y que se establezcan mecanismos de control adecuados al riesgo de la actividad". "En relación con el primer requisito, el Consejo de Administración tendrá que escoger a una persona en la toma de decisiones gerenciales y de administración cuyos méritos, experiencia y credenciales acrediten suficientemente su capacitación profesional para dirigir y gestionar la sociedad. Asimismo, será necesario especificar las competencias y funciones que se atribuyen al órgano delegado a fin de delimitar su ámbito de actuación y responsabilidad, haciendo constar igualmente los medios e instrumentos que se ponen a su disposición para el desempeño de sus funciones" "En cuanto al deber de vigilancia, deberán establecerse mecanismos de control adecuados que permitan supervisar eficazmente la actuación de los órganos delegados. En este sentido cobra especial relevancia el programa de cumplimiento normativo o compliance, puesto que, siendo este el principal instrumento para prevenir la comisión de delitos dentro de la empresa, deberá recoger necesariamente los riesgos inherentes a la actividad de los órganos de dirección estableciendo protocolos dirigidos a minimizar dichos riesgos".http://www.legaltoday.com/practica-juridica/penal/penal/la-responsabilidad-penal-del-consejero-el-dificil-manejo-del-dominio-funcional-del-hecho-la-cobertura-legal-del-compliance

¿Hay que comunicar o no comunicar los ciberataques a los inversores? Si durante un tiempo la empresa no comunica, una información privilegiada que los demás no tienen, esto puede llegar a afectar al mercado y por ende a su reputación. Por ejemplo, anteriormente en este documento se ha citado lo siguiente:

> *"La compañía de solvencia crediticia Equifax[60], ha perdido un 27% del valor de su cotización bursátil. Un ciberataque puede llegar a comprometer entre un 25% y un 35% de la capitalización bursátil de una empresa lo que podría tener como consecuencia que, aprovechando estas caídas en la capitalización bursátil, las empresas fuesen sometidas a una OPA. Este hecho podría dar lugar a que una empresa contratase a alguien para que llevara a cabo un ciberataque y hacer posteriormente una OPA. Por tanto, estamos ante un cambio total de paradigma".*

En el seno del consejo, el tema de la transparencia es trascendental, porque desde perspectiva jurídica, a título personal, e institucional, la empresa puede verse implicada. Por lo tanto, surgirán conflictos éticos si alguien, el mercado o los inversores, interpreta que se ha producido una venta determinada de títulos, en el periodo en que la empresa no informó de un ciberataque o que este se produjo de forma artificial para forzar una caída de la acción para favorecer la OPA correspondiente.

Es evidente que cualquier hecho relevante debe ser conocido en el mercado y, un ataque de ciberseguridad que haya tenido consecuencias económicas importantes o de continuidad de negocio importante, tiene que ser comunicado al mercado.

El problema es, hasta donde se llega informando al mercado. Cualquier banco puede tener, por ejemplo, 1.500 ataques diarios o más. Esta información puede generar un pánico realmente innecesario. Esta es una cuestión muy importante que afecta a la reputación de la empresa[61].

60 La compañía de solvencia crediticia Equifax con sede en Atlanta, maneja información de cerca de 820 millones de personas en todo el mundo, y el pasado 7 de septiembre de 2017 reconoció que, entre mayo y julio, había sufrido un ataque informático que pudo exponer datos de 143 millones de personas. Entre los datos a los que accedieron los piratas figuran números de tarjetas de crédito de 209.000 consumidores y documentos con información personal de 182.000 individuos. https://elpais.com/economia/2017/09/26/actualidad/1506447652_267329.html

61 En la era de Internet en la que vivimos, la correcta gestión de la reputación online se ha convertido en una cuestión de capital importancia para todo negocio. Conseguir y mantener una excelente reputación digital es una necesidad especialmente crítica para determinados sectores económicos, como el turístico, ya que tanto la ocupación como la rentabilidad del destino dependen en gran manera de lo que opinen los usuarios. http://www.transformapartnering.com/1950-2/

La ciberseguridad ya ha entrado dentro de los instrumentos de mercado. Por ejemplo, en el caso de Equifax, entre mayo y julio de 2017 sufrió un ataque informático que pudo exponer datos de 143 millones de personas. Estos ataques se descubren el 29 de julio de 2017, y lo comunican el 7 de septiembre de 2017. Es decir, tardan 6 semanas en comunicarlo. Aquí se produjo una falta de transparencia de Equifax, que afectó totalmente a su reputación. Por tanto, la gestión de la cibercrisis es totalmente relevante. Pero, no solo es importante gestionar el ciberataque, sino gestionar también la crisis que se desencadena después del ataque.

Durante el periodo que transcurrió hasta el 7 de septiembre algunos miembros del Consejo de Administración vendieron acciones de Equifax. Esta forma de actuar, por parte de miembros del consejo, constituyo una clara falta de ética y, además, fue claramente delictiva.

La regulación en temas de ciberseguridad todavía tendrá que seguir desarrollándose porque, además de las propias empresas afectadas, están las empresas del ecosistema. Por ejemplo, en el caso de los ordenadores o de los smartphones, hay muchas empresas que constituyen sus ecosistemas, como pueden ser las empresas de hardware y software, por citar dos grandes grupos de actores dentro de los grandes ecosistemas que, en este principio de siglo XXI, se están desarrollando.

En el caso de los coches conectados y sin conductor gracias al IOT (Internet of Things[62]): "Los sistemas informáticos necesarios para hacer funcionar estos automóviles no son ninguna frontera infranqueable para los hackers, por lo que los problemas legales que podría generar este tipo de tecnología sí podrían suponer un serio escollo a su implantación"[63]

En los MBA se están incorporando módulos de riesgo tecnológico, en cuanto que es parte también del conocimiento básico, que tienen que tener los directores de las empresas.

Este es el eterno debate de la especialización. ¿Cuánto hay que saber de algo para gestionarlo? por ejemplo, ¿cuánto tienes que saber de petróleo para ser presidente de una empresa de petróleo? o ¿cuánto tienes que saber de ciberseguridad para controlar los riesgos derivados de ataques cibernéticos o de fallos en el funcionamiento del software o del IOT? Este es un debate no resuelto, y aquí existente dos escuelas de pensamiento, la más generalista y la más específica.

62 Riesgos y retos de ciberseguridad y privacidad en IoT Publicado el 22/12/2017, por Miriam Puente García. https://www.certsi.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

63 http://www.expansion.com/2013/12/12/juridico/1386872371.html

20. Medidas para reducir los riesgos cibernéticos

Hay 3 niveles de medidas para reducción de riesgos cibernéticos.

Primer nivel: **la Prevención**. Es la parte importante. Se está valorando si debe de haber expertos de ciberseguridad entre los consejeros o en otros ámbitos de la Dirección. ¿Qué perfil debe tener quien tome las decisiones?: ¿Un directivo al que se le enseña ciberseguridad o un buen experto en ciberseguridad al que se le enseña a ser directivo? Aquí se arrastra una inercia propiciada por la transformación digital. Hay ejemplos, a nivel internacional, de técnicos muy buenos, que han llegado a ser grandes directivos y que están liderando la transformación digital del mundo. Por ejemplo: Microsoft, Apple, Facebook, WhatsApp. Pero no hay que olvidar que, seguramente, ha habido cientos de miles de grandes técnicos con grandes ideas, que fracasaron, porque no eran buenos directivos.

En muchas organizaciones, el peso en la toma de decisiones de algo tan crítico que afecta, no solo a los riesgos de ciberseguridad, sino a los riesgos de la compañía, se traslada hacia profesionales de la ciberseguridad y, en algunos casos, a hackers blancos. Los hackers blancos son técnicos, no son directivos. Hay algunos hackers blancos que podrían ser buenos directivos, y podrían tener una visión estratégica, y podrían estar involucrados en los comités de dirección e incluso ser consejeros. La tendencia tendría que ser incorporar consejeros con formación en ciberseguridad, Por lo tanto, la parte **preventiva** tiene que ver mucho con la concienciación y la formación a todos los niveles, desde el empleado que utiliza las tecnologías, hasta el consejo de administración. Toda la organización debe entender lo que es la ciberseguridad, qué riesgos entraña y cómo se debe de gestionar.

Segundo nivel: Conjunto de medidas que **tienen un componente técnico**, completo. Son todas las **medidas de detección, de contención, de análisis, de respuesta y de recuperación**. Estas medidas deben ser proporcionadas por personal técnico, por consultoras y empresas especializadas en ciberseguridad.

Defensa en Profundidad

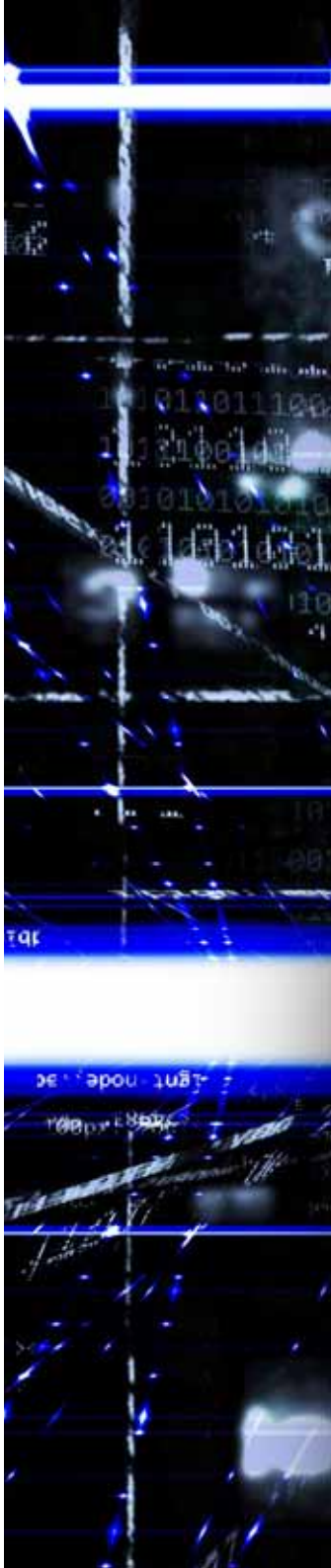
En este caso se está haciendo la **aproximación de la cebolla que equivale a decir que se está haciendo** la defensa en profundidad[64]. Es una estrategia que consiste en aplicar diferentes capas de protección. Evidentemente los ciberataques pueden vulnerar una capa, pero es muy difícil que lleguen a vulnerar todas las capas de protección[65].

Segregación de funciones

La **segregación de funciones**[66], *"está orientada a evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema"*. Es decir, el responsable de informática no puede ser responsable de ciberseguridad. De acuerdo con la segregación de funciones, el responsable de ciberseguridad tiene que estar velando porque los de informática hagan su trabajo de forma segura. La segregación de funciones implica el mínimo privilegio y la mínima funcionalidad, es decir, se proporciona las tecnologías para lo que se necesita, y solamente para eso.

Tercer nivel: **los antivirus**, los firewalls y toda la evolución tecnológica que sólo los expertos de ciberseguridad conocen.

Las nuevas amenazas, que están cambiando continuamente hacen que estas medidas evolucionen también continuamente para adaptarse a los nuevos riesgos que surgen.



64 El término defensa en profundidad, también conocido como defensa elástica, se refiere originalmente a una estrategia de defensa militar que consistía en colocar varias líneas defensivas consecutivas en lugar de colocar una línea única muy fuerte. Una de las ventajas de esta estrategia es que el empuje inicial se va perdiendo al tener que superar las distintas barreras. Además la estrategia puede conseguir que la fuerza atacante se disperse, debilitándola por tanto y pudiendo posteriormente el defensor reorganizarse para atacar el punto más debilitado. La misma idea se utiliza también en aplicaciones civiles, como en las instalaciones nucleares o en computación. https://es.wikipedia.org/wiki/Defensa_en_profundidad

65 El concepto de defensa en profundidad se basa en la premisa de que todo componente de un sistema puede ser vulnerado, y por tanto no se debe delegar la seguridad de un sistema en un único método o componente de protección. De esta forma propone el uso de distintas técnicas que permitan, al menos, duplicar los elementos de protección para limitar los daños en caso de una intrusión en la primera línea de defensa o componente más expuesto. https://es.wikipedia.org/wiki/Defensa_en_profundidad

66 "La segregación de funciones está orientada a evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a la consumación de un fraude. http://marcontrol.blogspot.com/2013/11/la-segregacion-de-funciones-clave-la.html

21. Crisis y su Gestión

Se sabe desde hace mucho tiempo y esto se puso de manifiesto el pasado año con *WannaCry* y con *Petya* que los ciberataques producen **crisis**.

> **Crisis** a nivel nacional como fue *WannaCry* o **crisis** en una entidad o en una organización. Un ciberataque no solo hace perder dinero a las empresas, sino que las mete de lleno en una **crisis**. Estas crisis deben gestionarlas expertos en gestión de crisis y no los expertos en ciberseguridad.

La crisis de WannaCry ofrece varias conclusiones muy interesantes. Por ejemplo, el INCIBE, gestionó la crisis desde el lado de la **comunicación**. Por supuesto, el INCIBE analizó el malware, se coordinó con todos los organismos y empresas que estaban intercambiando información como, por ejemplo: el **Centro Criptológico Nacional (CCN)**, con FCC, con Red Eléctrica de España (REE). Pero **la crisis** se gestionó desde el enfoque de **la comunicación**. Es decir, WannaCry, que era un ransomware, afectó, al menos a 10 empresas importantes y produjo 123.000 incidentes en España en el año 2017.

> El *WannaCry*, además del daño económico, que fue relativamente bajo, produjo una crisis nacional en toda regla. **Telefónica fue una de las grandes afectadas a nivel de imagen**. La gestión de la crisis hubo que hacerla desde el punto de vista de la comunicación porque, lo que había que hacer, era trasladar confianza al mercado dejándole claro que la compañía Telefónica, en este caso, sabía lo que estaba ocurriendo y sabía cómo manejarlo. Telefónica sabía a las 12 de la mañana, que el ataque estaba producido por un ransomware que afectaba a una de las vulnerabilidades conocidas en las que **había solución**. Por tanto, hubo que trasladar al mercado:
>
> 1. “Sabemos lo que pasa”, y “con parchear se soluciona”.
>
> Sin embargo, se estuvo **más de 72 horas viviendo en nuestro país una verdadera crisis con toda la población preocupada**, y con auténticas “bombas” informativas.

INCIBE **“gestionó la comunicación”**. Atendió más de 50 entrevistas en directo en 48 horas. **En España se hicieron “los deberes”. En Reino Unido, sin embargo, lo gestionaron de otra forma**. Reino Unido está dentro de los 5 países con mayor impacto de WannaCry y tenían información que, en España, no se disponía al principio. Todas las empresas, EY, Telefónica y otras empresas, entre las 13 y las 14 horas, tenían toda la información, y se la pasaron a Reino Unido. Reino Unido estuvo más afectado que España.

Por lo tanto, como resumen: la **prevención** (concienciación y formación) ahorra muchísimo a las empresas. De los 123.000 incidentes, gran parte, son incidentes relativos a malware que se desarrolló antes del año 2013. Es decir que, si se hubiesen tenido los sistemas parcheados, las empresas no hubiesen estado afectadas.

Por tanto:

- La estrategia **preventiva** es **fundamental**.
- La **detección, contención, análisis, respuesta y recuperación**, son aspectos puramente técnicos, con departamentos especializados y con empresas especializadas.
- Para **gestionar la crisis** los directores de comunicación deben estar “preparados para contarlo” pues, si lo cuenta un técnico, hablará de ceros y unos, y esto no es hablar de malware ni de servicios NDP. Aquí de lo que se trata es “gestionar crisis”.

El sector financiero vive de la informática y, por lo tanto, en este sector, todo lo relacionado con la seguridad de los procedimientos, está en el ADN de las compañías.

> Sun Tzu[67] decía: “Sí te conoces y conoces al enemigo, no has de temer el resultado de cien batallas. Sí te conoces, pero no conoces al enemigo, por cada victoria alcanzada sufrirás una derrota. Pero sí no te conoces, ni conoces al enemigo, serás derrotado en todas las batallas.”

67 Sun Tzu fue un general, estratega militar y filósofo de la antigua China. https://es.wikipedia.org/wiki/Sun_Tzu

En el sector financiero, los “generales” se conocen bien a sí mismos y conocen bien a sus enemigos, es decir, conocen bien los problemas derivados de la creciente digitalización y de la necesaria ciberseguridad.

Cuando se habla de ciberseguridad es fácil dejarse llevar por la tentación de pensar en *WannaCry*, es decir, lo inmediato es pensar en la agresión exterior. De acuerdo con la experiencia, los incidentes más graves que se han producido, no han sido por agresiones exteriores han sido porque, alguien interno a la compañía, se equivocó.

Entonces, desde el punto de vista práctico es fácil y muy rentable resolver los problemas de seguridad internos. Estos problemas de seguridad se dan frecuentemente porque los procedimientos no están bien diseñados y no están bien controlados.

22. Gestión de crisis en función del tipo de Gobierno Corporativo

Como consecuencia de su concepción del gobierno corporativo, ciertas compañías alemanas tienen una cultura específica que las hace actuar, ante los problemas, de forma que choca con compañías que tienen otra concepción del gobierno corporativo, como son las compañías americanas y las españolas.

En ciertas compañías alemanas, cada vez que hay una crisis, sea de la naturaleza que sea, se monta un grupo de trabajo *ad hoc*, con un miembro del consejo de administración que actúa como sponsor de ese trabajo. Esto quiere decir que, el consejo elige específicamente a uno de sus miembros, para que gestione la crisis surgida. De esta forma, el consejo está directamente involucrado, garantizando que los equipos que están dedicándose a resolver y atender el problema, tienen el apoyo del consejo y, se asegura a su vez, que el consejo tiene toda la información necesaria para la toma decisiones.

En la cultura corporativa española no es factible a día de hoy, un procedimiento como el descrito, porque los equipos de dirección no soportarían que un consejero dictara lo que debe hacerse.

En el mundo corporativo alemán es muy normal que los propietarios de las empresas sean, generalmente, una o dos familias, por lo que la dispersión accionarial prácticamente no existe. El mundo anglosajón es lo contrario. En Estados Unidos, por ejemplo, es impensable la figura del consejero dominical. En los consejos de las empresas americanas no hay uno o dos dueños que están presentes en el Consejo, porque está muy atomizado el accionariado. Por lo tanto, los consejeros que hay, por definición, son todos independientes.

En el entorno alemán se pueden permitir un sponsor como el descrito, que es un sponsor del consejo, pero eso es difícil trasladarlo a la cultura de las empresas con accionariados muy atomizados.

23. Planes de contingencia y cooperación

Es muy importante que existan siempre unos procedimientos de backup, de modo que, si se produce un ataque cibernético en un determinado ámbito el citado backup permite seguir trabajando.

Incluso suelen darse acuerdos con competidores, que están cercanos, para que, por ejemplo, suministren en un momento determinado, porque ellos, a su vez, también se pueden encontrar en el mismo problema en un momento determinado.

La implantación de un sistema de información integrada, donde se conjunten los objetivos de los distintos departamentos de la empresa y se alinee con su estrategia global es **absolutamente clave** para el **éxito de las organizaciones**, inmersas en un contexto económico y de mercado cada vez más globalizado y competitivo.

El problema es que, en la práctica, la mayoría de las compañías se encuentran con **importantes dificultades** para **ejecutar esa integración previamente establecida**. Estos problemas tienen que ver tanto con la propia definición de la estrategia, como con su correcta implantación, donde se alineen los objetivos estratégicos y se puedan evaluar.

Otro problema es la ausencia o uso inadecuado de un software de automatización.

> *"Ninguna empresa, independientemente de su tamaño o sector, está exenta de ser el objetivo de un ataque informático. Vivimos en la era de la información y de la globalización. En el mundo hay más de 10.000 millones de dispositivos conectados a internet, intercambiando y generando datos, cifra que los expertos prevén se multiplique por cinco en las próximas décadas. Cada una de estas conexiones es una puerta de entrada para cualquier ciberdelincuente que quiera utilizar esta información de forma fraudulenta, por la tanto, es importante que estas puertas no sólo estén aseguradas con llave, sino que estén blindadas ante cualquier amenaza.*
>
> *Actualmente, la seguridad informática se ha convertido en uno de los principales retos a los que ha de enfrentarse cualquier compañía. Tal y como afirma el último estudio del Instituto Nacional de Ciberseguridad (INE), el 32% de las empresas admite haber sido víctima de ciberataques en el último año. España, concretamente, ya se ha convertido en el tercer país del mundo que más los ha sufrido y sólo nos superan Estados Unidos y Reino Unido. Casos como el hackeo a CEDRO (Centro Español de Derechos Reprográficos), coincidiendo con el Día Mundial de la Propiedad Intelectual; a El Corte Inglés, en el que se hizo público sus gastos; o el secuestro de información a Telefónica hace tan sólo unos meses, lo demuestran.*

Pero, ¿cuáles son los principales retos a los que nos enfrentamos? ¿Estamos ejecutando las medidas necesarias para evitar un ataque informático?

Movilidad. *Gracias a la tecnología, ahora es posible trabajar prácticamente desde cualquier parte del mundo y a través de cualquier dispositivo móvil. Sin embargo, si protegemos los ordenadores de mesa, ¿por qué no implementamos sistemas de seguridad también en los dispositivos móviles? En este sentido, también hemos de ser conscientes del peligro que supone conectarse a las redes WIFI abiertas ya que su seguridad puede estar comprometida y por tanto, cualquier operación que llevemos a cabo.*

Redes Sociales. *Las redes sociales se han convertido igualmente en otra posibilidad de ataque para los ciberdelincuentes. Cualquiera está expuesto a recibir mensajes que contengan malware, es decir, programas o códigos maliciosos cuyo objetivo sea dañar los sistemas, directamente y sin filtros. Es importante, por ello, saber reconocerlos y no caer en la trampa.*

La nube. *Existe una tendencia en alza a alojar los datos en la nube. Cada vez son más las empresas que se suman a los entornos cloud y, pese a sus múltiples ventajas, hemos de ser conscientes también de que no está libre de riesgos. Crear contraseñas seguras, encriptar los datos, revisar la configuración por defecto o verificar su seguridad con el proveedor es imprescindible para evitar cualquier problema.*

Amenazas internas. *Son muchas las ocasiones en las que el problema se encuentra dentro de la oficina. Un ex-empleado o empleados descontentos con acceso a la información pueden robarla, destruirla o hacer cualquier uso indebido de esta que suponga un punto de inflexión definitivo para cualquier empresa.*

Virus mutantes o polimórficos. *Los virus han evolucionado y mejorado significativamente en los últimos años, tienen la capacidad de mutar, cambiar partes de su código fuente creando miles de copias de diferentes versiones de sí mismos, dificultando así su rastreo por los antivirus convencionales.*

En cualquier caso, existe una variable común en todas estas situaciones, el factor humano. El 80% de los ciberataques tienen su origen en un error humano. Muchos profesionales aún no conocen los riesgos a los que se exponen día a día y mucho menos, como evitarlos. La formación, por ello, ha de convertirse en un pilar clave para sensibilizar a toda empresa que quiera mantener su seguridad intacta. La rápida transformación digital a la que estamos asistiendo, trae consigo una serie de retos que, en muchos casos, las empresas han descuidado, por falta de conocimientos y herramientas para hacerles frente. En este sentido, es vital profesionalizar el cambio y apoyarse en expertos capaces de apoyarlas y acompañarlas en este camino"[68].

 http://www.interempresas.net/Seguridad/Articulos/219364-Estan-nuestras-empresas-seguras-ante-un-ciberataque.html

24. Continuidad de negocio

De acuerdo con el Decálogo de Ciberseguridad de Empresas editado por el INCIBE[69], Las empresas deben estar preparadas para **prevenir, protegerse, y reaccionar** ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario **proteger los principales procesos de negocio** a través de un conjunto de tareas que permitan a la organización **recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad**.

De esta forma se garantiza poder dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes.

Debemos tener en cuenta que el término **continuidad del negocio**[70] no hace referencia exclusivamente a aspectos relacionados con las tecnologías de la información. Aunque podría pensarse que la continuidad del negocio es un ámbito exclusivo de las grandes organizaciones, esto no es cierto. Si bien existe una diferencia significativa, cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastre. Si hablamos del ámbito tecnológico, por ejemplo, mientras que una gran organización puede requerir el despliegue de un **centro de respaldo alternativo**, tanto de comunicaciones, sistemas como servidores en una ubicación remota, en otros casos podría ser más óptimo realizar **copias de seguridad en la nube**, primando el rendimiento frente al coste.

69 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

70 https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

Los planes de continuidad de negocio pueden ayudarnos a:

- **Mantener el nivel de servicio** en los límites definidos.
- Establecer un **periodo de recuperación mínimo**.
- **Recuperar la situación inicial** ante cualquier incidente.
- **Analizar los resultados y los motivos** de los incidentes.
- **Evitar que las actividades** de la empresa **se interrumpan**.

Por todo ello, debemos considerar, desde un punto de vista formal, aquellos factores que pueden garantizar la continuidad de una empresa en circunstancias adversas. Este proceso implica las siguientes fases:

Fase 0. Determinación del alcance. Si nuestra empresa presenta cierta complejidad organizativa, abordar un proceso de mejora de la continuidad puede suponer emplear un número de recursos y un tiempo excesivo. Por tanto, es recomendable comenzar por aquellos departamentos o áreas con mayor importancia y progresivamente ir ampliando la continuidad a toda la organización. Para ello siempre con el compromiso e implicación de la dirección.

Fase 1. Análisis de la organización. Durante esta fase recopilamos toda la información necesaria para establecer los procesos de negocio críticos, los activos que les dan soporte y cuáles son las necesidades temporales y de recursos.

Fase 2. Determinación de la estrategia de continuidad. Conocidos los activos que soportan los procesos críticos, debemos determinar si en caso de desastre, seremos capaces de recuperar dichos activos en el tiempo necesario. En aquellos casos en los que no sea así, debemos establecer las diversas estrategias de recuperación.

Fase 3. Respuesta a la contingencia. A partir de las estrategias de recuperación escogidas, se realiza la selección e implantación de las iniciativas necesarias, y se documenta el **Plan de Crisis** y los respectivos documentos para la recuperación de los entornos.

Fase 4. Prueba, mantenimiento y revisión. A partir de la infraestructura tecnológica de nuestra empresa, desarrollaremos los planes de prueba y mantenimiento.

Fase 5. Concienciación. Además del análisis y la implantación, es necesario que tanto el personal técnico como los responsables de nuestra empresa conozcan qué es y qué supone el Plan de Continuidad de Negocio, así como qué se espera de ellos.

25. Conclusiones

1. Todos los temas de ciberseguridad han empezado a ocupar a los consejos y, de manera intensa por lo menos, a los consejos de las grandes empresas.

2. Fundamentalmente en ciberseguridad hay 3 grandes conceptos que pueden verse afectados:
   - La **confidencialidad de la información**, que es el activo estratégico que, hoy en día, tiene cualquier organización.
   - La **integridad de la información**.
   - La **disponibilidad de la información**, en el momento que la empresa le necesite.

3. Las empresas están en un momento de transformación digital. Esta transformación, es una pieza clave para poder incorporar la revolución digital que está evolucionando radicalmente, (Blockchain, Cloud, Big Data, etc.).

4. Par poder llevar a cabo la transformación digital los temas organizacionales son importantes, pues la ciberseguridad y la gestión de los riesgos en una organización, son claramente una responsabilidad del consejo de administración. Aquí hay que aplicar 3 líneas de defensa.

   a. Primera línea de defensa: **Implantación de las medidas de seguridad**. Esta primera línea está en el ámbito técnico, que solo personas técnicas pueden llevar a cabo porque son las que establecen las soluciones tecnológicas.

   b. Segunda línea de defensa: **Establecer un marco de riesgos que, en materia de ciberseguridad, se están contemplando**. Aquí, las Direcciones de Riesgo tienen que trabajar con estos nuevos conflictos que el mundo de la ciberseguridad impone a las empresas, no solamente por las nuevas tecnologías, sino porque se cambia la forma en que se hacen las cosas.

      i. Antes los desarrollos tecnológicos eran proyectos de 2-3 años. Hoy en día se imponen temas que son resultados de 2-3 semanas.

c. Tercera línea de defensa: **Auditoría periódica y permanente**. En muchas grandes organizaciones, sus equipos de auditoría, no están dotados de, o no están suficientemente asesorados por, especialistas que les puedan apoyar en los aspectos tecnológicos.

5. El consejo debe estar informado y ser absolutamente participe. Dado que no es posible proteger a la empresa, al 100%, de un ciberataque es muy relevante saber ¿cómo se reacciona? y ¿cómo se gestiona una amenaza o un incidente de seguridad? En estas situaciones de incidentes de seguridad debe tenerse muy en cuenta de que ha cambiado totalmente el paradigma. Por ejemplo, cuando sucedió el ataque del *WannaCry* (*WanaCrypt0r 2.0 o Wannadecryptor*, clasificado como gusano informático del tipo ransomware), en diversas empresas, muchos de sus empleados twittearon y explicaron en Facebook lo que estaba pasando en tiempo real. Sucedió el hecho de que, aunque la empresa no quería publicar el daño de seguridad que se había producido, no pudo evitar que sus empleados lo informaran a través de las redes sociales.

6. Por sectores, hay un volumen regulatorio muy importante que es, casi imposible de gestionar. A nivel del consejo hay que tener mucha información, de cuál es el mapa regulatorio y en qué forma les está afectando.

7. El consejo de administración debe focalizarse mucho en aquellos aspectos que pueden ser más relevantes. Los consejos de administración deben marcarse prioridades clave como: garantizar la diversidad en los consejos e impulsar sus conocimientos sobre la transformación digital que se está llevando a cabo en las empresas y las consecuencias que esto produce en cuanto a la ciberseguridad, cuya falta es una amenaza creciente en el siglo XXI.

8. Durante el año 2016, la Fiscalía española presentó un total de 1.648 escritos de acusación por hechos ilícitos competencia del área de especialización en criminalidad informática. Esta cifra supone un importante incremento, cuantificado en un 32,68% respecto del año precedente, en que dicha cifra fue de 1.242.

9. ¿Hay que comunicar o no comunicar los ciberataques a los inversores? Si durante un tiempo no se comunica, si se tiene una información privilegiada que los demás no tienen, esto puede llegar a afectar al mercado y por ende a la reputación de la empresa. Por ejemplo:

    i. *En el caso de Equifax, entre mayo y julio de 2017 sufrió un ataque informático que pudo exponer datos de 143 millones de personas. Estos ataques se descubren el 29 de julio de 2017, y lo comunican el 7 de septiembre de 2017. Es decir, tardan 6 semanas en comunicarlo. Aquí se produjo una falta de transparencia de Equifax, que afectó totalmente a su reputación lo que afectó al 27% del valor de su cotización bursátil. Por tanto, la gestión de la cibercrisis es totalmente relevante. Pero, no solo es importante gestionar el ciberataque, sino gestionar también la crisis que se desencadena después del ataque.*

10. Es evidente que cualquier hecho relevante debe ser conocido en el mercado y, un ataque de ciberseguridad que haya tenido consecuencias económicas importantes o de continuidad de negocio importante, tiene que ser comunicado al mercado.

11. El Reglamento General de Protección de Datos (RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

12. Con anterioridad a la aplicación del RGPD, la obligación de notificar a la Agencia las brechas de seguridad que pudiesen afectar a datos personales se ceñía exclusivamente a operadores de servicios de comunicaciones electrónicas y prestadores de servicios de confianza. Desde el pasado 25 de mayo, esta obligación pasa a ser aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

13. De acuerdo con el Reglamento, cuando el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe notificarlo sin dilación a la autoridad de control competente, y a más tardar en las **72 horas siguientes** a haber tenido constancia de ella. Esta notificación a la Agencia debe realizarse a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

14. La responsabilidad de los Consejos es tener definido el problema de ciberseguridad y establecer:

    i. Políticas para gestionar los riesgos.
    ii. Políticas de transparencia.
    iii. Políticas de comunicación.
    iv. Políticas de gestión de crisis.
    v. Hacer un seguimiento del cumplimiento de todas esas políticas.

15. Todavía hay mucho espacio por recorrer en la transformación de los consejos. Por ejemplo, el caso de Equifax se descubrió el 29 de julio, tardaron 6 semanas en comunicarlo a los mercados, pero la compañía Equifax ya conocía la gravedad del ataque. Durante el periodo que transcurrió hasta el 7 de septiembre algunos miembros del Consejo de Administración vendieron acciones de Equifax. Esta forma de actuar, por parte de miembros del consejo, constituyo una clara falta de ética y, además, fue claramente delictiva.

16. Hay 3 niveles de medidas para reducción de riesgos cibernéticos.

    a. Primer nivel: **la prevención**. Es lo más importante. La prevención tiene que ver mucho con la concienciación y la formación a todos los niveles, desde el empleado que utiliza las tecnologías, hasta el consejo de administración. Toda La organización debe entender lo que es la ciberseguridad, qué riesgos entraña y cómo se debe de gestionar.

b. Segundo nivel: Conjunto de medidas que **tienen un componente técnico, completo**. Son todas las **medidas de detección, de contención, de análisis, de respuesta y de recuperación**. Estas medidas deben ser proporcionadas por personal técnico, por consultoras y empresas especializadas en ciberseguridad.

i. Defensa en Profundidad

1. Es una estrategia que consiste en aplicar diferentes capas de protección. Evidentemente los ciberataques pueden vulnerar una capa, pero es muy difícil que lleguen a vulnerar todas las capas de protección.

ii. Segregación de funciones

1. La **segregación de funciones**, "está orientada a evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema". Es decir, el responsable de informática no puede ser responsable de ciberseguridad. De acuerdo con la segregación de funciones, el responsable de ciberseguridad tiene que estar velando porque los de informática hagan su trabajo de forma segura. La segregación de funciones implica el mínimo privilegio y la mínima funcionalidad, es decir, se proporciona las tecnologías para lo que se necesita, y solamente para eso.

c. Tercer nivel: **los antivirus**, los firewalls y toda la evolución tecnológica que solo los expertos de ciberseguridad conocen.

17. Por tanto:

i. La parte **preventiva** es **fundamental**.
ii. La parte de **detección, contención, de análisis, de respuesta y de recuperación**, son aspectos puramente técnicos, con departamentos especializados y con empresas especializadas.
iii. Para **gestionar la crisis** los directores de comunicación deben estar "preparados para contarlo" pues, si lo cuenta un técnico, hablará de ceros y unos, y esto no es hablar de malware ni de servicios NDP. Aquí de lo que se trata es "gestionar crisis".

18. Se sabe desde hace mucho tiempo y esto se puso de manifiesto el pasado año con *WannaCry* y con *Petya* que los ciberataques producen **crisis**.

i. **Crisis** a nivel nacional como fue WannaCry, **crisis** en una entidad o en una organización. Un ciberataque no solo hace perder dinero a las empresas, sino que las mete de lleno en una **crisis**. Estas **crisis** deben gestionarlas expertos en gestión de **crisis** y no los expertos en ciberseguridad.

19. Cuando se habla de ciberseguridad es fácil dejarse llevar por la tentación de pensar en WannaCry, es decir, lo inmediato es pensar en la agresión exterior. De acuerdo con la experiencia, los incidentes más graves que se han producido, no han sido por agresiones exteriores han sido porque, alguien interno a la compañía, se equivocó.

    i. Entonces, desde el punto de vista práctico es fácil y muy rentable resolver los problemas de seguridad internos. Estos problemas de seguridad se dan frecuentemente porque los procedimientos no están bien diseñados y no están bien controlados.

20. De acuerdo con el Decálogo de Ciberseguridad de empresas editado por el INCIBE[71], Las empresas deben estar preparadas para **prevenir, protegerse, y reaccionar** ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario **proteger los principales procesos de negocio** a través de un conjunto de tareas que permitan a la organización **recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad**.

21. El ataque a la ciberseguridad es un ataque a la continuidad del negocio o a la seguridad nacional por lo que la ciberseguridad debe poder:
    i. **Mantener el nivel de servicio** en los límites definidos.
    ii. Establecer un **periodo de recuperación mínimo**.
    iii. **Recuperar la situación inicial** ante cualquier incidente.
    iv. **Analizar los resultados y los motivos** de los incidentes.
    v. **Evitar que las actividades** de la empresa **se interrumpan**.

22. La prevención y la gestión de las crisis hay que extenderla a todos los niveles: a nivel de compañía, a nivel de país y a nivel de cuerpos de seguridad pues, mientras los ciberataques sigan siendo un gran negocio, las amenazas y los ataques serán continuo.

71 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

GCC

GLOBAL CORPORATION CENTER

EY Fundación España

UNA INICIATIVA DE
Fundación EY e IE Business School

ie Reinventing Higher Education