RESPONSABILIDAD PENAL CORPORATIVA Y CIBERCRIMINALIDAD

El *compliance* penal relativo al Derecho de las Tecnologías de la Información y la Comunicación

Vanessa Mañas Margalef

NIUB: 16446581

Trabajo de Final de Grado

4to Criminología

Curso 2016/17 – 2

Tutor: Víctor Gómez Martín

UNIVERSITAT DE BARCELONA

ÍNDICE

1. Introducción

1.1 Justificación

El binomio formado por el campo de la Criminología y de la Ingeniería Informática, comúnmente conocido por Cibercriminalidad, me ha suscitado mucho interés, tanto académica como profesionalmente. Esto es así debido al auge actual de las Tecnologías de la Información y la Comunicación en prácticamente cualquier ámbito de la sociedad de la información de la cual formamos parte. Y las empresas no son excluidas.

Como consecuencia de la evolución de las nuevas tecnologías, las organizaciones también sufren una permanente transformación, exponiéndose a factores nuevos traducidos en mejores oportunidades de negocio y peores amenazas. En España, se ha observado un ligero descenso en los delitos económicos tradicionales para dar paso al cibercrimen, segunda potencia a nivel mundial (PricewaterhouseCoopers [PwC], 2016). Al mismo tiempo, las entidades reguladoras están aumentando la presión sobre las empresas con el fin de prevenir los delitos llevados a cabo en el seno de su actividad empresarial.

Por este motivo, las áreas de *compliance* y auditoría interna están teniendo cada vez más una mayor relevancia en las organizaciones, debido al incremento de esfuerzos por parte de las empresas en la prevención, detección e investigación de los delitos, cuya responsabilidad penal pueda recaer sobre sí mismas. La preocupación y la concienciación es creciente, pero aún así las medidas siguen sin ser suficientes ante una revolución de ritmo tan cambiante como es la tecnológica.

Por tanto, uno de los principales objetivos de este trabajo reside en mostrar unas cuantas pinceladas sobre dos vertientes diferenciadas. Por un lado, en la parte más general se hablará sobre la cibercriminalidad y las TIC, con el fin de adoptar una perspectiva, a grandes rasgos, de sus particularidades, implicaciones y dificultades en el mundo digital. No obstante, por otro lado se dará un mayor énfasis a la parte específica del *compliance* penal, con el fin de entender la responsabilidad penal de las personas jurídicas, qué supone tener un programa de *compliance* en la empresa, y cuáles son sus elementos clave.

Como valor añadido, me gustaría incorporar una parte práctica y crítica a partir de la experiencia de los profesionales de esta temática sobre aquellas problemáticas más frecuentes con las cuales se encuentran las empresas en el ejercicio de su profesión relativas a las TIC, qué implicaciones tienen las nuevas tecnologías en el modelo de *compliance*, cuáles son los mayores riesgos tecnológicos de *compliance* actuales para las empresas y cómo combatirlos y, sobretodo, qué implicaciones tiene para éstas la presión por el cumplimiento de todas las regulaciones aplicables para demostrar y acreditar un buen gobierno corporativo. Por último, se discutirá acerca de hacia dónde se dirige el mundo del *compliance* y cuáles serán sus retos en el futuro más próximo.

1.2 Metodología

En primer lugar, para poder llevar a cabo las cuestiones expuestas en la justificación del trabajo, se ha realizado una búsqueda de referencias bibliográficas, tanto a nivel nacional como internacional, con el fin de disponer de una base teórica suficientemente amplia del tema expuesto, información procedente de fuentes diversas para así poder aportar una mayor riqueza interdisciplinar al trabajo.

En segundo lugar, como parte práctica del trabajo, se han llevado a cabo tres entrevistas. Éstas tienen como objetivo, a parte de poder contrastar algunos datos obtenidos en el marco teórico, poder entender la problemática del *compliance* relativo a las TIC sufrida por las empresas, y así poder establecer algunas soluciones, fruto de la experiencia. Los entrevistados en el presente trabajo son David Sancho Vidal, asesor jurídico de *compliance* en el despacho de ATGroup, Juan Carlos Ruiloba Castilla, perito informático e investigador tecnológico, y José Ramón Agustina Sanllehi, abogado penalista, profesor en la UIC y consultor jurídico en el despacho Molins & Silva con temas relativos al *compliance* y a la defensa procesal, tanto de personas físicas como jurídicas. Esta elección de los entrevistados es fundamentada en la necesidad de conocer, a través de la esfera profesional y académica, la opinión respecto del modelo de *compliance* de las empresas relativo a las TIC.

2. Marco teórico

2.1 Bloque I: Cibercriminalidad y ciberespacio

2.1.1 Definición del concepto y contextualización

El imponente desarrollo y expansión de Internet como vía de comunicación y relación interpersonal y a la vez medio de intercambio masivo de información le ha otorgado estos últimos años y de forma progresiva una extraordinaria trascendencia social, adquiriendo con ello un rol esencial para el desarrollo de todo tipo de actividades de carácter lúdico, cultural, financiero o comercial (Fernández Teruelo, 2007, 2011). La criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación (en adelante, TIC) sigue siendo totalmente novedosa y por ello parcialmente incomprendida por la sociedad en general y, en particular, por las instituciones necesitadas de prevención para poder afrontar esta amenaza (Miró, 2012). La sociedad no estaba preparada para esta globalización propiciada por la computación (Nava Garcés, 2007).

La difusión de la informática en todos los ámbitos de la vida social ha determinado su uso como instrumento para la comisión de actividades lesivas de bienes jurídicos e indicativas del consiguiente peligro social o su ser como objeto de atentados criminales (Luño, 1996). Estos cambios sociales provocados por las TIC resultan decisivos en todos los ámbitos y, por supuesto, también tienen su repercusión en el campo del Derecho Penal (Mata y Martín, 2001).

En 1984 William Gibson acuñó el término *cybercrime,* cuya configuración se ha realizado de forma paralela al mundo físico como espacio comunicativo e interactivo modificador de las relaciones económicas, políticas, sociales y personales (Brenner, 2010; Miró, 2012). Desde una concepción amplia, Yar (2006) contempla el cibercrimen como aquel delito cuya característica esencial es el rol central jugado por las TIC en su comisión. De la misma forma pero en otras palabras, Miró (2012) lo determina como cualquier delito llevado a cabo en el ciberespacio con las particularidades criminológicas, victimológicas y de riesgo penal derivadas de ello. Por lo tanto, el binomio ciberespacio y crimen constituye el concepto de cibercrimen.

Cuando terminó la primera década del siglo XXI, el cibercrimen se había convertido en un amplio negocio a gran escala (Arnott, 2008; Finjan Malicious Code Research Center [FMCRC], 2008). Asimismo, el derecho penal se había ido expandiendo para abarcar nuevos tipos de actividades delictivas (Brenner, 2010), siendo la ciberdelincuencia económica uno de los primeros ámbitos de delincuencia en Internet abarcadora de múltiples tipologías de conducta diferentes entre sí (Miró, 2012). La mayoría del cibercrimen observable hoy en día representa la migración de los crímenes del mundo real al ciberespacio, lugar convertido en la herramienta utilizada por los cibercriminales para cometer, mediante el uso de las TIC, los antiguos crímenes de formas nuevas (Brenner, 2010).

Aunque el riesgo de todo avance tecnológico siempre ha sido el hombre a merced de la tecnología y no al revés (Nava Garcés, 2007), la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas (Miró, 2012). Así lo están evidenciando diferentes estudios revisados (Centro Criptológico Nacional – Computer Emergency Response Team [CCN-CERT], 2014, 2015; Ponemon Institute, 2015; United Nations Office on Drugs and Crime [UNODC], 2013).

2.1.2 Características del ciberespacio

El impacto social causado por el desarrollo de las TIC es innegable (Morris y Higgins, 2010). Nuevas formas de comunicación surgen con el advenimiento de Internet, caracterizadas por una capacidad sin precedentes de cambiar información de manera instantánea y en un marco general de ausencia de normas claras (Agustina y Gómez-Duran, 2016), a su vez facilitadora de material normalmente prohibido, la inyección de costumbres ajenas quebradoras de los patrones de vida existentes en una población (Nava Garcés, 2007). Las TIC simplemente reflejan la cultura, la cosmovisión y los valores de la sociedad reproductora (Mafla, 2011).

Esta sociedad de la información se caracteriza por el impulso de múltiples cambios en la misma por parte de las TIC (Miró, 2012), tanto en una mejora drástica de la calidad de vida de los individuos (Morris y Higgins, 2010), como posibilitando una multiplicidad muy variada de escenarios de amenaza y ataque (Konradt, Schilling y Werners, 2016). Así, el ciberespacio como

nuevo entorno de interacción social (Mafla, 2011) y de oportunidad delictiva (Miró, 2012) creado gracias a las TIC es un ámbito de comunicación paralelo al espacio físico (Miró, 2013), caracterizado por un sinfín de actuaciones contra la confidencialidad, la integridad o la disponibilidad de datos o sistemas de computación (UNODC, 2013).

En los últimos años, la penetración de las tecnologías sobre las cuales se construye este ciberespacio se ha acelerado dramáticamente, lo cual ha traído consigo un aumento en el nivel de violencia en el mundo digital (Mafla, 2011). A su vez, esta nueva era digital ha conllevado importantes transformaciones (Agustina y Gómez-Duran, 2016) por ser Internet, además de un medio para la intercomunicación de sistemas informáticos con finalidad económica, un medio para la interacción personal entre usuarios, para la comunicación íntima entre personas o para la cesión voluntaria de esferas de intimidad (Miró, 2013).

La problemática en el ciberespacio se complica aún más, según Mafla (2011), por las características peculiares de las TIC utilizadas para su construcción. En primer lugar, debido a la desestabilización del orden establecido producido por las TIC; han modificado significativamente la forma de comunicación e interacción social creando nuevas y más complejas oportunidades, así como nuevas formas de comportamientos violentos o antisociales. Y, en segundo lugar, a causa de la inmediatez del efecto globalizador en el ciberespacio; por un lado, ante una delincuencia informática con tendencia a trascender los límites locales, nacionales o regionales, existe la posible generación de violencia desde cualquier parte del mundo, así como el aprovechamiento de Internet por parte de los ciberdelincuentes para compartir sus conocimientos, habilidades y herramientas delictivas y para formar asociaciones ilícitas globales.

A esta problemática se le suma la dificultad para delimitar el ámbito de la definición de ciberespacio porque ésta puede cambiar en el futuro debido a la influencia incisiva de la evolución de las TIC (Mafla, 2011). Estos espacios virtuales, al inicio, fueron adoptados por los ciudadanos sin la existencia de una regulación formal sobre los mismos; más tarde, mediante un proceso lento y no siempre acertado, estos espacios virtuales de interacción social se incorporaron al marco jurídico de las instituciones y los países (Mafla, 2011). En resumidas cuentas, los cibercrímenes llevados a cabo en este espacio están y continuarán evolucionando con la nueva tecnología y las mentes

criminales versátiles (binti Mohamed, 2013). Por tanto, el ciberespacio es de carácter cambiante y novedoso (Miró, 2012).

Por otro lado, Grabosky (2001) se pronuncia mediante la metáfora *old wine in new bottles*, referenciada a su vez por Brenner (2004) y binti Mohamed (2013), en la posición intermedia conforme a la cual la cibercriminalidad comparte con la delincuencia todos los elementos definitorios del concepto de crimen pero dándose los mismos de una forma tal en el nuevo ámbito del ciberespacio, influyente, en mayor o menor medida, significativamente en la explicación del delito y en su prevención. Miró (2012), además, también expone, por un lado, la visión más extrema, en la cual la ciberdelincuencia es un tipo de delincuencia nueva para la cual no son válidas las teorías tradicionales creadas para explicar el espacio físico, así como su polo opuesto, en el cual el cibercrimen es idéntico estructuralmente al delito cometido en el espacio físico cambiando solamente el aspecto del mismo pero en ningún caso sus caracteres configuradores.

Finalmente, siguiendo las directrices expuestas por Miró (2012), los caracteres configuradores del ciberespacio determinantes para cualquier fenómeno social llevado a cabo en él son varios:

• En primer lugar, el ciberespacio es transnacional, ya que el ciberespacio no está situado en un sitio concreto sino en todos a la vez (en sentido funcional) y en ninguno (en sentido físico). Esta inexistencia de fronteras o distancias permite el acceso a sus servicios desde cualquiera de los Estados nacionales por no pertenecer a ninguno en concreto. Aumentan a su vez las facilidades en el ciberespacio para la multicomunicación social entre personas.

• En segundo lugar, la neutralidad de la red referente a la libertad del usuario a la hora de transitar por el mismo sin fronteras pero sin censuras de acceso por parte de nadie, tan sólo las impuestas por el propio usuario. En el ciberespacio, a pesar de haber constancia o huella de lo comunicado y de su capacidad para causar daño a bienes esenciales, hay mayor capacidad de la información para difundirse en un espacio universal y popularizado.

• En tercer lugar, el ciberespacio no está centralizado debido a la inexistencia de nodos, tanto centrales como locales, en Internet. Nadie ejerce control de la información circulante ni Internet está sometido a leyes nacionales de un único país así como tampoco a unas normas propias aceptadas por todos los integrantes y esto conlleva poca efectividad por parte de los controles gubernamentales.

• En cuarto lugar, el ciberespacio es anonimizado. Pese al esfuerzo desde algunos sectores para construir algún tipo de sistema identificativo de los usuarios en Internet, al menos de momento, es inconcebible imaginar un ciberespacio donde todos o la gran mayoría de los usuarios estén identificados.

• Y, en quinto y último lugar, el ciberespacio está sujeto a revolución permanente y abierto al cambio por las propias características dinámicas de las TIC. Esto supone, por una parte, la ineficacia de las barreras de protección para los intereses personales y sociales en muy poco tiempo, bienes aparentemente intocables frente a las TIC pueden pasar a ser susceptibles de ataque en un instante; en definitiva, el derecho camina totalmente a remolque de un contexto social cambiante haciendo parecer obsoletas a las soluciones jurídicas cuando entran en vigor. Por otra parte, se deben tener en cuenta los cambios en el ciberespacio procedentes de los usuarios, quienes acaban decidiendo cuáles son las normas sociales básicas de funcionamiento interno. En el entorno social del ciberespacio, por tanto, destaca la no definición de ética o moral imperante, porque son los propios usuarios con sus conductas quienes la pueden cambiar. Como consecuencia, se hace evidente la disminución de la capacidad de influencia reguladora del Derecho.

En conclusión, los caracteres singulares de este nuevo lugar de comunicación transnacional, anónimo y sujeto a revolución permanente, en el cual las dimensiones espacio-temporales incrementan las posibilidades de contacto entre potenciales agresores y víctimas, tomando en cuenta, tal como establecen Cohen y Felson (1979), la producción del crimen únicamente cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y la ausencia de un guardián capaz de darle protección al primero, ha hecho del ciberespacio un ámbito de oportunidad delictiva distinto al espacio físico, en el cual la víctima adquiere especial relevancia para la explicación y prevención del delito (Miró, 2012).

2.1.3 Precisiones político-criminales y conceptuales sobre la intervención penal en Internet

Ante la nueva realidad emergida con la cibercriminalidad y la incertidumbre, las cuales plantean hechos socialmente considerados dañinos e incluso ilícitos desde una perspectiva general, se suscita la duda sobre las repercusiones jurídico-penales de los mismos, cuyos conceptos deben ser abordados desde la perspectiva de la Política Criminal y la Criminología como instrumentos al alcance del Derecho Penal (Mata y Martín, 2001).

En relación con las aplicaciones y procedimientos informáticos y las redes de transmisión de datos e Internet, según González Rus (2007), la intervención del Derecho Penal debe realizarse en un triple sentido: primero, sobre qué premisas de carácter valorativo debe apoyarse la intervención, conducente a la determinación de los bienes jurídicos requeridos de protección; segundo, qué tipo de ataques deben ser considerados penalmente relevantes; y tercero, qué instrumentos de técnica legislativa resultan preferibles para articular la tutela penal.

Más concretamente, para Meján (1994), el encuentro entre Derecho e Informática es bidireccional: por un lado, el Derecho sirve a la Informática (por ej. para proteger los derechos de autor del bien informático o el derecho a la intimidad del dueño de la información, o bien para castigar los delitos cometidos con motivo de la informática, entre otros); por otro, la Informática sirve al Derecho mediante la provisión de procesos ágiles a la impartición de la justicia y la recopilación de datos jurídicos relevantes para su ejercicio.

Para González Rus (2007), los "nuevos" riesgos aparecidos gracias a Internet son tres: el comportamiento realizado en Internet (delito informático) puede incrementar y multiplicar los efectos lesivos del bien jurídico producidos por los delitos "tradicionales"; Internet supone la aparición de nuevos soportes y elementos relacionados con las nuevas tecnologías, cuya existencia no gozaba de protección; e Internet ha hecho aparecer nuevas formas de atentar contra intereses individuales y sociales adaptadas al medio informático.

La difusión de la informática en todos los ámbitos de la vida social ha determinado su utilización como instrumento para la comisión de actividades lesivas de bienes jurídicos relevantes, tales como el patrimonio, la privacidad, el honor o la vida de las personas (Nava Garcés, 2007), y entrañan el consiguiente peligro social o el hecho de ser la propia informática objeto de atentados criminales (Luño, 1996; Mata y Martín, 2001). Por lo general, para la ejecución de estas conductas constituyentes de una peculiar adaptación al espacio virtual de actuaciones lesivas más o menos clásicas se aprovecha el enorme potencial de este canal de comunicación, aunque no todas se han limitado a la mera adaptación al medio de conductas clásicas, como las estafas, pues en otras

ocasiones el medio las ha convertido en hechos delictivos masivos, como es el caso de la pornografía infantil (Fernández Teruelo, 2011). A su vez, permite la intercomunicación entre grupos organizados para delinquir y fomenta conductas antisociales (Nava Garcés, 2007). Por ello y su carácter clandestino, la utilización de Internet representa la posibilidad de desplegar una conducta con un elevado desvalor de acción (Mata y Martín, 2001).

Actualmente, se mantienen dos criterios con respecto a la intervención penal en Internet y en las redes de transmisión de datos (González Rus, 2007). El primero, partidario del "Derecho Penal Informático", además de incorporar a la tutela penal los "nuevos" bienes jurídicos nacidos como consecuencia de la generalización y consolidación de los medios y procedimientos informáticos y con la suficiente importancia para merecer de intervención penal, teniendo en cuenta la insuficiencia de las previsiones penales actualmente disponibles para afrontar los problemas punitivos presentados por Internet y las redes de transmisión de datos. En cambio, otro sector, mayoritario en el derecho comparado, partidario de agotar las posibilidades de protección ofrecidas por el derecho vigente sobre la base de los bienes jurídicos "tradicionales" sin perjuicio de introducir, en la medida precisa cuando sea imprescindible, las modificaciones concretas necesarias.

Picotti (2004) defiende la intervención penal apoyada en bienes jurídicos "nuevos" de naturaleza informática, es decir, el primer postulado. En este caso, serían considerados como bienes jurídicos la seguridad informática, la intangibilidad o indemnidad de los datos informáticos y la libertad informática. No obstante, si se realiza un paralelismo con el derecho español, estas consideraciones cambian. Según González Rus (2007), la seguridad informática no es apreciada para el logro de una tutela eficaz ante peligros de comportamientos realizados en Internet, si bien es posible lograrla adelantando el momento de la protección de otros bienes como la intimidad (artículo 18 CE) o el patrimonio. En el caso de la intangibilidad o indemnidad de los datos, se reconoce el delito contra la integridad o la libre disponibilidad de los datos, en el artículo 264 CP, como una modalidad específica de daños. Y, finalmente, la libertad informática es el único bien jurídico propiamente informático cuyo reconocimiento se encuentra en el artículo 197.2 CP como derecho a controlar el uso de los datos de carácter personal y familiar informáticamente recogidos y tratados (*habeas data*).

Siendo el reto político-criminal el hecho de adaptar todas las estructuras políticas, jurídicas y sociales a la necesidad de protección de nuevos y viejos intereses frente a nuevas formas delictivas cambiantes debido al carácter dinámico del ámbito social donde las mismas se producen (Miró, 2012), la solución político-criminal y técnica más conveniente para dar respuesta penal a las necesidades de tutela surgidas del desarrollo de la informática, Internet y las redes de transmisión de datos, según González Rus (2007), resulta de utilizar y complementar las figuras delictivas actualmente disponibles, solución adoptada por el Código Penal de 1995 y mayoritaria en el derecho comparado. De esta forma, se abordan los delitos informáticos desde las modalidades delictivas ya existentes; tan sólo cuando exista una "laguna" de punición, es decir, cuando ninguno de los bienes jurídicos ya protegidos penalmente es capaz de cubrir adecuadamente la demanda de protección surgida en relación con el uso de medios, procedimientos informáticos o redes, como ha ocurrido con el derecho a la protección de los datos personales, estará justificada la incorporación de un nuevo bien jurídico. En definitiva, la valoración de los objetos jurídicos de protección y la de los comportamientos lesivos de los mismos debe hacerse en términos semejantes a la valoración recibida cuando la protección se produce fuera de Internet.

Más específicamente, las "demandas punitivas" para los "nuevos" riesgos de Internet anteriormente mencionados pueden solventarse mediante tres formas distintas respectivamente: la primera, creando tipos agravados o circunstancias calificadoras las cuales tomen en cuenta el incremento del desvalor de acción o de resultado de figuras del delito ya existentes; la segunda, ampliando la protección penal a los nuevos elementos o soportes resultantes de eventuales objetos materiales de delitos ya también previstos y castigados; y, la tercera, considerando punibles particulares formas de conducta lesivas de bienes jurídicos, asimismo ya contemplados y tutelados penalmente (González Rus, 2007).

Sin embargo, debido a las peculiaridades criminológicas y a la incidencia de esta amenaza real en múltiples aspectos sociales, las necesidades de intervención político-criminal frente al cibercrimen pasan por, además de una correcta política legislativa sustantiva nacional, la adaptación

de las estructuras procesales y técnicas necesarias, especialmente a nivel internacional, para la prevención de su realización y la mejor investigación procesal de las mismas (Miró, 2012).

2.1.4 Clasificación de la ciberdelincuencia: tipologías delictivas

Como se ha visto, el concepto cibercriminalidad. por un lado, define el ámbito de riesgo particular y específico derivado del uso de las TIC para bienes jurídicos esenciales y, por otro, engloba tipologías de conducta peligrosas para dichos bienes caracterizados por la utilización de redes telemáticas y demaś sistemas, terminales y servicios de las TIC con los riesgos asociados en lugar de tipos penales (Miró, 2012).

No obstante, no existe una clasificación única de tipologías delictivas en relación a la ciberdelincuencia. En este sentido, se tomará como punto de referencia básico aquello establecido por la legislación pero, a su vez, también se expondrán varias clasificaciones posibles de diferentes autores al respecto.

Según Hilbert (2013), el cibercrimen, tal como lo entendemos hoy en día, puede dividirse en cuatro categorías: cibercrimen, ciberespionaje, ciberguerra y ciberactivismo. La primera, en esencia, se refiere al uso de un ordenador o una red informática para cometer un acto criminal motivado por alguna forma de beneficio, generalmente monetaria, o alguna otra ganancia; son los mismos delitos cometidos en el mundo terrestre pero con otros métodos en los cuales los perpetradores pueden ser absolutamente desde individuos hasta grupos organizados. Ejemplos de ello son el robo de identidad, fraude, *stalking*, extorsión *online*, *spam* y *phishing*. La segunda, en cambio, aunque el espionaje industrial también tenga como motivación el dinero, está motivado por el robo de información; se trata de acceder a un sistema o red ajeno, construyendo diferentes maneras dentro y fuera de éste generando pequeñas cantidades de datos a la vez. Es a largo plazo y a menudo perpetrado por importantes grupos de hackers, rivales económicos competidores y Estados-nación, por eso son muy difíciles de detectar. La tercera, tiene como objetivo la destrucción de los sistemas. Este arma cibernética creado puede ser utilizado no sólo por los gobiernos sino también por la competencia empresarial rival y los empleados descontentos mediante la bomba lógica, un *software* diseñado para eliminar o corromper las bases de datos corporativas. Finalmente, la cuarta categoría es una modalidad nueva consistente en la utilización de una web por parte de un individuo o grupo

de individuos para dar a conocer su causa, en este caso, mediante los ataques de denegación de servicio (DoS).

Por otro lado, basándose en las definiciones realizadas por *Serious and Organised Crime Strategy*[1], Furnell, Emm, y Papadaki (2015) exponen la distinción entre dos modalidades de cibercrimen: por un lado, los *cyber-dependent* crimes, ciberdelitos dependientes necesariamente de computadores ya que su comisión sólo es posible utilizando un ordenador, una red de ordenadores o cualquier otra TIC y, por otro, los *cyber-enabled crimes*, ciberdelitos tradicionales cuyo alcance se incrementa mediante el uso de las TIC. En el primer caso se incluyen la propagación de virus y otros programas maliciosos, *hacking* y ataques de denegación de servicio distribuido (DDoS). Son ataques contra ordenadores u otros recursos de la red aunque también pueden tener resultados secundarios como fraudes. En el segundo caso, estos ataques pueden ser realizados sin el uso de las TIC e incluyen ejemplos como fraude (*phishing* y otros), robo y abuso sexual contra niños.

Desde otra perspectiva, Brenner (2010) describe el cibercrimen en tres categorías definidas por los agentes del orden público, cuya clasificación se remonta a mediados de los años 90. En primer lugar, los *target cybercrimes*, crímenes en los cuales el objetivo del delito es el ordenador. Destacan en esta modalidad el *hacking*, *malware* y el ataque de denegación de servicio distribuido (DDoS). En segundo lugar, los *tool cybercrimes,* crímenes en los cuales los computadores son utilizados como herramientas para cometer el delito. Destacan en esta modalidad el fraude, la malversación, *stalking*, falsificación, amenazas, extorsión, calumnias, el juego, terrorismo, homicidio y la propagación de la pornografía infantil. En tercer y último lugar, los *computer incidental*, crímenes en los cuales el ordenador juega un rol accidental en la comisión del delito. Destacan en esta categoría los narcotraficantes, los delincuentes de cuello blanco, otros asesinos, chantajes o extorsión.

Y, por último, se muestra una clasificación más detallada de las diferentes tipologías delictivas de la ciberdelincuencia. Siendo la utilización de sistemas de información y comunicación para la comisión de conductas delictivas dentro del ciberespacio el elemento común a todas las tipologías de cibercrimen, Miró (2012) realiza una tabla tipológica - criminológica de la delincuencia en el ciberespacio atendiendo, en primer lugar, al aspecto incidente de las TIC en el comportamiento

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

criminal y, en segundo lugar, al propósito criminal de la actuación y al contexto de incidencia del ciberespacio afectado por los delitos. La tabla resultante es la siguiente:

Tabla 1. Clasificación de la ciberdelincuencia atendiendo a la incidencia de las TIC en el comportamiento delictivo.

	Ciberataques puros	*Ciberataques réplica*	*Ciberataques de contenido*
CIBERCRÍMENES ECONÓMICOS	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupación red • *Antisocial networks*	• Ciberfraudes (*phishing, pharming, scam, auction fraud*…) • *Cyberspyware* (uso de *sniffers* y demás *spyware*, ciberespionaje de empresa) • *Identify theft* • *Spoofing* (DNS *spoofing*, ARP *spoofing*, IP *spoofing, web spoofing*) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en Internet • Ciberpiratería intelectual
CIBERCRÍMENES SOCIALES		• *Spoofing* • *Cyberstalking* • *Cyberbullying* • *Online harassment* (ciberamenazas, coacciones, injurias, etc.) • *Sexting* (y extorsión con imágenes de *sexting*) • *Online grooming*	
CIBERCRÍMENES POLÍTICOS	• Ataques DoS (*cyberwar*) • Ataques DoS (*Cyberhacktivism*) • *Malware* intrusivo	• Ciberespionaje terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Nota. Extraído de Miró, F. (2012). Tipos de cibercrimen y clasificación de los mismos. Dentro *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. (p. 47-143). Madrid: Marcial Pons.

Los *ciberataques puros* son aquellos delitos únicamente posibles en el ciberespacio. La problemática se derivará de la total novedad de los comportamientos con la consiguiente falta de estrategias preventivas de carácter criminológico frente a ellas, así como de la inexistencia de preceptos permisivos de la incriminación de los mismos. Por otro lado, los *ciberataques réplica* son aquellos delitos tradicionales cuya realización será en el ciberespacio. El problema será la potenciación del riesgo para los intereses sociales derivado del nuevo medio, vasto e inmenso como es el ciberespacio, donde se ejecuta la infracción, así como la dudosa capacidad de los tipos penales

existentes para dar cabida a conductas similares en lo injusto pero cambiantes en su forma de realización. Y, por último, los *cibercrímenes de contenido* plantean dificultades de contenidos en el ciberespacio como con la compleja cuestión de atribuir responsabilidad a todos los intervinientes en tal proceso.

Como se puede observar, la clasificación de las diferentes tipologías delictivas del cibercrimen resultante va a depender del objetivo de enfoque puesto por el analista. Asimismo, se considera la clasificación más completa y detallada de las expuestas la de Miró (2012).

2.1.5 Normativa nacional e internacional

Mafla (2011) nos habla de los problemas relacionados con los derechos digitales, los cuales definen los privilegios de los ciudadanos usuarios de computadores y redes, tales como el derecho a la privacidad de las comunicaciones, la libertad de expresión, la protección de datos personales, etc. Para solucionarlo, se plantea la necesidad de establecer un sistema de gobernanza de Internet aunque lamentablemente, especifica el autor, los Gobiernos, las corporaciones, los entes judiciales, la sociedad civil y los organismos internacionales no han logrado mayores consensos sobre los mencionados temas. La gobernanza de Internet es el desarrollo y la aplicación, por parte de los Gobiernos, el sector privado y la sociedad civil, en sus respectivas funciones, de principios compartidos, normas, reglamentos, procedimientos de toma de decisiones y programas configuradores de la evolución y uso de Internet (de Bossey, 2005). Por ejemplo, en el caso de España existe la Agencia Española de Protección de Datos[2], cuya función es velar por el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

A pesar de ser la jurisdicción nacional la principal autoridad reguladora en la definición, investigación y sanción de los ciberdelitos, es importante establecer el margen de maniobra otorgado a los Estados-Nación no solo en ser apropiado sino también proporcional a las protecciones otorgadas por los instrumentos multilaterales (Kamal, 2017). En este caso, tomando en consideración la necesidad de garantizar el equilibrio entre acción penal y respecto a los derechos humanos fundamentales, la necesidad de aplicar una política penal común con la finalidad de

2 http://www.agpd.es/portalwebAGPD/LaAgencia/index-ides-idphp.php

proteger a la sociedad frente a la cibercriminalidad, así como la necesidad de cooperación entre Estados y sector privado en la lucha contra ésta, el 23 de noviembre de 2001 en Budapest se celebra el conocido Convenio sobre la Ciberdelincuencia del Consejo de Europa. Este Convenio actualmente está ratificado por 52 países; concretamente, España lo ratificó el 3 de junio de 2010, entrando en vigor el 1 de octubre de ese mismo año.

El Convenio contempla expresamente los delitos informáticos y define los tipos penales a considerar para cada uno de ellos (Cap. II Sec. 1), representados en la siguiente tabla:

Tabla 2. Clasificación de los delitos informáticos y sus tipos penales según el Convenio sobre la Ciberdelincuencia.

Título	**Tipo/s penal/es con artículo/s**
1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Acceso ilícito (art. 2), Interceptación ilícita (art. 3), Ataques a la integridad de los datos (art. 4), Ataques a la integridad del sistema (art. 5), Abuso de los dispositivos (art. 6)
2. Delitos informáticos	Falsificación informática (art. 7), Fraude informático (art. 8)
3. Delitos relacionados con el contenido	Delitos relacionados con la pornografía infantil (art. 9)
4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10)

Nota. Elaboración propia a partir de la clasificación de los ciberdelitos y los tipos penales a considerar para cada uno de ellos extraída de Convention of Cybercrime, ETS núm. 185.

Esta clasificación del Convenio plantea distintas propuestas político-criminales (Rueda Martín, 2010). Por un lado, se distingue entre la protección de los sistemas informáticos (arts. 2, 5 y 6) y la protección de los datos o de la información contenida en dichos sistemas. Por otro, aunque se proponga la tipificación como delito del simple acceso intencional sin autorización a la totalidad o parte de un sistema informático, los Estados, con carácter facultativo, podrán establecer algunas exigencias en la configuración de esta infracción penal: a) el acceso sea cometido infringiendo medidas de seguridad; b) el acceso se realice con la finalidad de obtener datos u otra finalidad deshonesta; o bien c) los sistemas informáticos vulnerados se encuentren conectados a otros sistemas informáticos.

Asimismo, el 28 de enero de 2003 en Estrasburgo se promulgó el Protocolo Adicional al Convenio sobre la Ciberdelincuencia respecto a la criminalización de los actos xenófobos y racistas relacionados con las nuevas tecnologías.

En el marco europeo, la Unión Europea (en adelante, UE) publicó la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información con la finalidad de establecer unas normas mínimas relativas a la definición de infracciones penales y sanciones aplicables, así como mejorar la cooperación entre autoridades competentes; luego, se incluye a la policía y otros servicios especializados encargados de aplicar la ley en los Estados Miembro, así como organismos especializados de la propia UE, como Eurojust[3], European Cybercrime Centre (EC3)[4] de la Europol y la European Union Agency for Network and Information Security (ENISA)[5].

Finalmente, en nuestro ordenamiento jurídico no se contempla expresamente el concepto de ciberdelito o delito informático; luego, en ciertos supuestos se deberá acudir a la legislación complementaria reguladora de la sociedad de la información, como la LOPD, la LSSI, la Ley General de Telecomunicaciones, etc. No obstante, son tipificadas en el Código Penal (en adelante, CP) aquellas conductas delictivas en las cuales interviene de alguna forma una actividad relacionada con las TIC. Así, se identifica como delito informático aquel cuyo nexo común alrededor del cual se produce es un ordenador o dispositivo electrónico con conexión a Internet, porque (Rayón Ballesteros y Gómez Hernández, 2014): a) el objeto sobre el cual recae la conducta es el propio sistema, el programa informático o el equipo; b) ese sistema es utilizado como medio a través del cual se realiza la conducta delictiva; o bien c) el bien jurídico protegido es la integridad de la información, la confidencialidad de la misma o los datos y los sistemas o programas informáticos.

3 http://www.eurojust.europa.eu/about/background/Pages/history.aspx
4 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
5 https://europa.eu/european-union/about-eu/agencies/enisa_en

Según la Instrucción FGE 2/2011 sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías, el área de criminalidad informática se distingue en tres categorías distintas representadas en la siguiente tabla:

Tabla 3. Clasificación del área de criminalidad informática y su correspondencia con el Código Penal según la Instrucción FGE 2/2011.

Categoría	**Delitos correspondientes en el CP**
A. Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs	• Delitos de daños, sabotaje informático y ataques de denegación de servicios (art. 264) • Delitos de acceso sin autorización a datos, programas o sistemas informáticos (art. 197.3) • Delitos de descubrimiento y revelación de secretos (art. 278) cometidos a través de las TIC o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos. • Delitos contra los servicios de radiodifusión e interactivos (art. 286)
B. Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs	• Delitos de estafa (art. 248.2 a, b y c) siempre que, en los supuestos a) y c) se utilicen las TICs para llevar a cabo la transferencia u operación de cualquier tipo en perjuicio de otro. • Delitos de acoso de menores de 13 años, *child grooming* (art. 183 bis), cuando se lleven a efecto a través de las TICs. • Delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas (art. 189) cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TICs. • Delitos contra la propiedad intelectual (arts. 270 y ss.) cuando se cometan utilizando las TICs.
C. Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia	• Delitos de falsificación documental (arts. 390 y ss.) cuando para la ejecución del delito se hubieran empleado las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad técnica en la investigación criminal. • Delitos de injurias y calumnias contra funcionario público, autoridad o agente de la misma (arts. 211 y ss.) cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal. • Delitos de amenazas y coacciones (arts. 169 y ss.) cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal. • Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

Nota. Elaboración propia a partir de la clasificación del área de criminalidad informática extraída de Instrucción FGE 2/2011 sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías.

Aunque clasificados de distinta forma, se puede observar la correspondencia de algunos tipos penales del Código Penal con los del Convenio del Cibercrimen. No obstante, en las últimas reformas del Código Penal, Ley Orgánica 1/2015 y 2/2015, hubo modificaciones relevantes en materia de delitos informáticos. Aunque Virumbrales (2015) realiza una versión extendida, a continuación se expone una versión más reducida de aquellos aspectos más relevantes:

- Delito de descubrimiento y revelación de secretos. Se tipifica como nuevo delito la divulgación no autorizada de grabaciones o imágenes íntimas obtenidas con el consentimiento de la víctima sin que ésta lo sepa cuando afecten gravemente a su intimidad (art. 197.7 CP). Se introducen una serie de modificaciones en el delito de intrusión informática (art.bis.1 CP): se penará el simple acceso aunque no se haya accedido a los datos; en cuanto a medidas de seguridad, se debe estar al adecuado estado de la técnica, usos o costumbres; hay colaboración cuando se facilita a un tercero el acceso al conjunto o a una parte del sistema de información. Se tipifica como nuevo tipo penal el delito de interceptación de transmisiones de datos informáticos (art. 197.bis.2 CP) con el cual se pretende criminalizar la interceptación de transmisiones no públicas de datos informáticos y ceñirse en exclusiva a la transmisión de estos. Asimismo, se tipifica también el supuesto, antes atípico, de castigar a la persona creadora de programas informáticos o proporcionadora de contraseñas o códigos permisivos y facilitadores para llevar a cabo las conductas anteriores (art. 197.ter CP), así como a la persona facilitadora a un tercero de cualquiera de esos medios por los cuales se comete el delito. Además, se incorpora como subtipo agravado el supuesto de actuar en el seno de una organización o grupo criminal (art.197.quater CP). Por último, se regula la responsabilidad penal de la persona jurídica (art. 197.quinquies CP) y del funcionario público (art. 198 CP) en esta tipología de delitos.
- Delito contra la propiedad intelectual. Se castigan las conductas de reproducción, plagio, distribución y comunicación de la obra (arts. 270 y ss. CP). Se prevé el ánimo de obtener un beneficio económico directo o indirecto en lugar del ánimo de lucro (art. 270.1 CP), así como se contemplan las páginas web de enlaces como nuevo supuesto, castigando tanto a quien realiza la vulneración directamente como a quien la facilita (art. 270.2 CP). Asimismo, se faculta al juez a retirar los contenidos ilícitos de los servidores de Internet e incluso para acordar el bloqueo el acceso al portal, y se añade como posibilidad de realizar medidas cautelares durante el transcurso

del proceso a fin de no esperar a la sentencia y evitar la producción de más vulneraciones en este derecho (art. 270.3 CP). Por último, se incluyen otras conductas como la importación, exportación o facilitación del acceso (art. 270.5 CP).

- Delito de amenazas. Se tipifica la modalidad de *stalking* como nuevo delito de acoso, acecho u hostigamiento mediante llamadas telefónicas continuas, seguimientos o cualquier otra fórmula con capacidad para lesionar gravemente la libertad y el sentimiento de seguridad de la víctima aunque no se produzca violencia (art. 172.ter CP).
- Delito de daños informáticos. Se añade como supuesto el castigo del daño al sistema informático en su conjunto y no al dato, programa o documento (art. 264.bis CP), artículo en el cual también se incorpora la circunstancia agravante para cuando el sistema informático dañado pertenezca a una empresa, negocio o Administración pública. Se tipifica como supuesto, antes atípico, castigar a quien crea el programa informático utilizado para producir el delito aunque posteriormente no se llegue a cometer materialmente el delito, pues basta con su intención de realizarlo más adelante (art. 264.ter CP). Finalmente, se regula la responsabilidad penal de la persona jurídica en esta materia (art. 264.quater CP).
- Delito de pornografía infantil. Se tipifica como supuesto, antes atípico, al particular asistente a espectáculos exhibicionistas o pornográficos sabiendo ser partícipes menores o persones con discapacidad necesitadas de especial protección (art. 189.4 CP). Asimismo, se incluyen como supuestos nuevos, por un lado, el castigo a la posesión y adquisición para uso privado de pornografía infantil y, por otro, a quien acceda de forma puntual aunque intencional a pornografía infantil por cualquier medio, incluida las TIC (art. 189.5 CP). Por último, también se añade la posibilidad de los jueces de cerrar páginas web de pornografía infantil o bloquear su acceso a ciertos usuarios (art. 189.8 CP).
- Delito de *child grooming*. Se amplía el art. 183.bis con el contenido de los artículos 183.ter y 183.quater CP. En el primero, cuyo supuesto es el castigo de la conducta de embaucamiento, se sube la edad del menor de 13 a 16 años. En el segundo, se añade el supuesto de exención de responsabilidad penal para cuando medie el consentimiento libre de la víctima y el autor sea próximo en edad y madurez o grado de desarrollo, para dar cabida a exigencias internacionales (entre otras, la Directiva 2011/92/UE) y la pedofilia en la red.
- Delito de ciberterrorismo. Se considerará como tal cuando una organización terrorista cometa delitos contra la intimidad y daños informáticos (art. 573.2 CP). De esta forma, se contempla este delito de forma mucho más exhaustiva, específicamente en los artículos 575 y 578

CP. En el primero, se tipifican las actividades terroristas realizadas en la red para captar, adoctrinar y adiestrar a nuevos miembros. En el segundo, se castiga el delito de enaltecimiento del terrorismo.

Asimismo, respecto a la investigación de tales delitos en España destacan por su relevancia la Brigada de Investigación Tecnológica (BIT)[6] del Cuerpo Nacional de Policía y la Unidad de Delitos Telemáticos (UDT)[7] de la Guardia Civil. Además, en 2011 se creó la Fiscalía de Criminalidad Informática surgida como una necesidad constatada en la práctica habitual de las Fiscalías al detectarse un progresivo aumento en el número de casos de investigaciones criminales vinculadas a las TIC, tal como establece la propia Instrucción FGE 2/2011 sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías. También destaca el Instituto Nacional de Ciberseguridad (INCIBE)[8], el Centro Criptológico Nacional (CCN)[9], así como el Centro Nacional de Excelencia en Ciberseguridad (CNEC)[10].

En conclusión, la fenomenología delictiva vinculada a las TIC es cada vez más variada y abundante: así, cualquier regulación queda pronto anticuada, puesto que la realidad delictiva siempre va por delante de la regulación legal y penal. Sin embargo, ello no se traduce en la irrelevancia de la regulación existente o el innecesario apoyo cooperativo.

2.1.6 Proceso de investigación y enjuiciamiento: fases y problemática

La sociedad de la información se caracteriza por la ausencia de fronteras y la inmaterialidad de la comunicación, evidencia de la inexistencia de límites temporales y espaciales dificultando la detección, investigación y persecución de estas conductas (Rayón Ballesteros y Gómez Hernández, 2014). El alcance geográfico global de los ciberdelitos dificulta enormemente la persecución de los ciberdelincuentes, así como también las innumerables barreras jurídicas interpuestas para llevar a los ciberdelincuentes ante la justícia una vez identificados y localizados (Mafla, 2011). Internet determina una notable dificultad para la detección y persecución del cibercrimen, según Fernández Teruelo (2011), debido al anonimato potencial del autor y la ejecución a distancia, ambos propios de este medio.

6 https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
7 https://www.gdt.guardiacivil.es/webgdt/la_unidad.php
8 https://www.incibe.es/que-es-incibe/que-hacemos
9 https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es
10 http://www.cnec.university/cnec/

El establecimiento de la competencia jurisdiccional para su enjuiciamiento plantea problemas muy graves, ya que el principio de territorialidad (art. 23 LOPJ), con algunas excepciones también reguladas en este mismo artículo, choca con la dimensión trasnacional propia de Internet. Por tanto, este problema de extraterritorialidad evidencia la necesaria cooperación internacional para combatir esta tipología de delitos (Nava Garcés, 2007) traducida en una armonización entre las legislaciones de distintos países (convenios de colaboración) y en la necesidad de mecanismos de cooperación (Viota Maestre, 2007). En otras palabras, se precisa realizar un enfoque supranacional con unidades policiales de investigación especializadas y dotadas de medios técnicos necesarios, así como de un enjuiciamiento rápido y especializado en este tipo de conductas (Rayón Ballesteros y Gómez Hernández, 2014).

En el caso de los delitos a distancia, la determinación del lugar donde se ha cometido el delito (*locus commisi delicti*) es clave para concretar este principio. La doctrina se ha manifestado favorable a la teoría del resultado, según la cual el delito se comete donde tiene lugar el resultado externo (Fernández Teruelo, 2011). No obstante, esta solución no siempre será válida dado que la teoría de la ubicuidad, según la cual el delito se da por cometido donde se realiza la actividad o manifiesta el resultado, ha sido admitida por el Tribunal Supremo en ATS de 20 de mayo de 1992 (RJ 1992\4195), cuando acción y resultado no tengan lugar dentro de la misma jurisdicción.

Cárdenas Aravena (2008) realiza una revisión crítica de los criterios imperantes en doctrina poniendo de relieve los problemas presentados al expandir este principio en aras de una mayor eficiencia en la persecución de tales delitos. Asimismo, Rayón Ballesteros y Gómez Hernández (2014) exponen en más detalle la conducta delictiva a efectos procesales.

Según Brenner (2010), los delitos trasnacionales crean dos tipos de desafíos para los agentes del orden: recolectar evidencias del extranjero y obtener la custodia de un sospechoso hallado en ese momento en el extranjero. En el primer caso, se puede confiar en los dispositivos formales utilizados tradicionalmente para recolectar evidencias en casos criminales transnacionales, o bien, la cooperación informal entre agentes policiales. En el segundo caso, se puede confiar en el dispositivo formal de la extradición, o bien, la acción informal y unilateral del país en busca del sospechoso. No obstante, revela como única estrategia alternativa hasta ahora, desarrollada y en proceso de implementación, para facilitar la cooperación transnacional en las investigaciones del cibercrimen la del Consejo de Europa.

En relación al procedimiento de investigación propio de esta tipología delictiva, Rayón Ballesteros y Gómez Hernández (2014) exponen las fases generales de la investigación en el ámbito de la delincuencia tecnológica, teniendo en cuenta el rastro dejado por nuestra actividad en la Red (Viota Maestre, 2007). Suele sintetizarse en las siguientes tres fases:

A) Fase previa: comprender qué ha pasado, en qué ha consistido el delito y cómo se ha podido perpetrar. Se inicia con el conocimiento del delito por parte de las autoridades y organismos encargados de la investigación criminal, generalmente a través de denuncia presentada por las víctimas, afectados o perjudicados por el delito. Se suele solicitar ayuda a los servidores de red por ser una de las fases más complejas. El ordenador de la víctima, el del autor y los sistemas intermedios (Viota Maestre, 2007), en este caso el proveedor de servicios de Internet, suelen guardar un registro de sucesos de lo ocurrido llamado *log*, cuyo contenido es información relevante de gran utilidad en la investigación. Se trata de archivos de registro cuya finalidad es comprobar en cada momento la coherencia entre el funcionamiento del sistema y su diseño, y verificar si funciona de forma prevista, sin interferencias ni internas ni externas (Viota Maestre, 2007). No obstante, es importante destacar la necesidad de realizar *back-up's* para detectar las evidencias del delito en los ordenadores personales puesto que estos no suelen guardar *logs*. Además, el limitado espacio de los discos duros donde se almacenan estos archivos de registro hace necesaria la sustitución, transcurrido un tiempo, de los más antiguos por otros más nuevos (Viota Maestre, 2007).

B) Fase de investigación (propiamente dicha): esclarecer quién es el responsable y si ha perpetrado alguna acción punible. Se realizan una serie de operaciones técnicas para identificar sus conexiones y precisar los datos de tráfico afectados para identificar al abonado titular de la conexión; se identifican a un equipo y un abonado pero no a quién presuntamente cometió el acto ilícito puesto que la dirección IP (*Internet Protocol*) asignada al ordenador, un conjunto de cuatro números separados por puntos cuyo valor puede oscilar entre 0 y 255 (Viota Maestre, 2007), puede ser manipulada. Por tanto, todos estos aspectos tan solo serán un indicio de uso de un equipo informático y no prueba objetiva en un juicio. No obstante, es posible aportar cierto anonimato a la comunicación mediante un *proxy*, un sistema intermediario instalado para aislar de cierta manera una red interna del resto de Internet, de manera que el destinatario desconoce cuál es la dirección IP real del solicitante (Viota Maestre, 2007).

Para conseguir los datos de tráfico es necesario conocer el número IP en el momento de conectarse a Internet (la familia de protocolos TCP/IP - *Transmision Control Protocol / Internet Protocol –*

hacen posible la interconexión y tráfico de red en Internet), el momento concreto de acceso para la comisión del hecho dañoso, así como identificar el ordenador, su ubicación, el abonado de la línea telefónica o el contrato de acceso.

Viota Maestre (2007) menciona la posibilidad recuperar de forma exitosa archivos teóricamente eliminados mucho tiempo antes cuando la parte del disco donde se almacenaban los datos no haya sido ocupada por otros, aunque existen formas de eliminar ficheros utilizando protocolos de seguridad, dificultando, hasta incluso imposibilitando, su recuperación. Asimismo, la autora realiza un análisis del riesgo, detallado y enumerado, de los factores causantes de la destrucción o no existencia de evidencias, algunos de ellos ajenos a la voluntad de la víctima o del propio autor. Concluye ser la mejor forma de eliminar el contenido de un soporte informático la destrucción física del mismo.

A su vez, debe tenerse en cuenta la importante consideración de estos datos como datos reservados de carácter personal; luego, es de obligado cumplimiento su tratamiento conforme a la LOPD. Asimismo, también es necesaria la incautación y posterior estudio de los *routers* utilizados para la conexión a Internet para poder descartar la existencia de otros sospechosos de las conductas investigadas, puesto que las conexiones *wifi* se comportan como un sistema de anonimato en las comunicaciones (Viota Maestre, 2007).

C) Fase incriminatoria: obtener y asegurar las pruebas del delito para la posterior fase de enjuiciamiento. Se intervienen y aprehenden los ordenadores generalmente mediante la entrada y registro domiciliario en el lugar donde se encuentren, así como la redacción de los informes periciales. Esto se lleva a cabo con un mandamiento judicial: por un lado, se interviene el material y dispositivos informáticos susceptibles de contener indicios de criminalidad, siendo necesario intervenir todo el equipo completo y vital mantener la integridad de tal equipo intervenido, para lo cual se realizará su precintado y su plena identificación en el acta de entrada y registro confeccionada por el secretario judicial; por otro lado, se interviene sobre indicios vinculables al usuario y al equipo correspondiente, así como sobre instrumentos y efectos relacionados.

No obstante, existe una gran dificultad en la adopción de medidas restrictivas de derechos fundamentales, como es el caso de la intervención de las comunicaciones (Narváez Rodríguez, 2007) o entradas y registros, sobre todo cuando la gravedad del delito no es tan elevada para justificar una diligencia tan gravosa y la misma es denegada por el juez (Viota Maestre, 2007); luego, la investigación se daría por finalizada.

Por su parte, el juez puede llevar a cabo una inspección ocular para reconocer el lugar donde se encuentran los indicios materiales del delito o lugares por donde haya podido circular la comunicación delictiva. En todo caso, conviene aislar el lugar del crimen y el ordenador o dispositivo electrónico desde donde se ha producido la comunicación. Por este motivo son fundamentales las primeras horas de intervención de los equipos y las primeras declaraciones obtenidas del entorno del sospechoso para la justificación de la detención y la obtención de indicios necesarios. Se realizan interrogatorios para el esclarecimiento de la comisión delictiva y posteriormente se sigue con el análisis de los efectos intervenidos para lo cual se lleva a cabo un *volcado*, es decir, la realización de una copia previa de la información salvaguardando siempre la original, tanto del software como del hardware. Se realiza esta operación para conocer, en el momento de la intervención judicial, el contenido real del ordenador intervenido y para evitar no perder, deteriorar o alterar por cualquier causa este contenido, puesto que al juez se le debe entregar el auténtico cuerpo del delito (art. 334 LECrim). Resulta a su vez determinante garantizar la cadena de custodia de este *volcado*, realizado en presencia del secretario judicial. Posteriormente, debe mantenerse el precintado de los equipos intervenidos para garantizar esta cadena de custodia de la prueba.

Se realizará el análisis pericial y se almacenarán los discos duros para garantizar su integridad, para lo cual es importante guardar una serie de precauciones mínimas. Para la realización de este análisis no existen herramientas preestablecidas judicialmente, luego cada Cuerpo de Seguridad del Estado utiliza las suyas propias por lo cual se genera cierta inseguridad jurídica tanto para procesados como investigadores. Este análisis no siempre es concluyente porque los indicios obtenidos por separado no significan nada pero la interpretación conjunta de ellos de manera interrelacionada puede constituir una prueba para juicio. Con este conjunto de indicios obtenidos en los análisis efectuados se elabora un informe técnico de naturaleza policial para explicar la comisión del hecho delictivo por una persona concreta y las operaciones practicadas para llegar a esas conclusiones finales. El informe pericial debe practicarse según los art. 723 a 725 de la LECrim. A su vez, a causa de diferentes lagunas legales al respecto, es necesario acudir a los art. 456 y ss. de la misma ley respecto a la pericial realizada en fase de instrucción o investigación. Para que sea considerado prueba de cargo es necesaria su práctica en el juicio oral, directamente o ratificado por su autor.

Por otro lado, el perito informático se considera una persona tal que, sin ser parte del proceso, emite declaraciones sobre hechos con carácter procesal en el momento de su captación, para cuyo conocimiento o apreciación son necesarios convenientes conocimientos informáticos. Será en el

juicio cuando ratifique su informe para ser tenido en cuenta por el juez a efectos de valor probatorio. Este tipo de pruebas suelen ser realizadas por organismos oficiales dependientes de las Fuerzas y Cuerpos de Seguridad del Estado, así gozan de la presunción de neutralidad e imparcialidad, y serán tenidos en cuenta siempre y cuando se confeccionen por ingenieros o informáticos distintos a quiénes han realizado la intervención del material o equipo informático.

Cuando se trata de aplicar la normativa de carga de la prueba en un proceso penal de un delito vinculado a la Red, se presentan una serie de dificultades tanto si son delitos puramente informáticos o delitos tradicionales en su vertiente tecnológica, aunque en ambos casos la clase de actividad desplegada para desvirtuar la presunción de inocencia y hacer creíbles los hechos de la acusación más allá de toda duda razonable, es la misma (Sanchís Crespo, 2007) y, en muchas ocasiones, insuficiente (Sentencia 110/2005 del Juzgado de lo Penal n.º1 de Madrid, de 29 de julio). Así, debe señalarse la necesidad de establecer un marco normativo europeo específico regulador de la prueba electrónica, tal como también exponen de forma muy detallada Insa, Lázaro, y García (2008) evidenciando la carencia de formación, cualificación y regulación específicas para una mejor actuación profesional. En el enjuiciamiento, la prueba electrónica se convierte en la única solución para evidenciar la comisión de un hecho delictivo de tales características; consistirá en cualquier información obtenida a partir del dispositivo electrónico intervenido para adquirir convencimiento de la certeza de un hecho (Rayón Ballesteros y Gómez Hernández, 2014).

Con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones se pretende hacer frente a las dificultades de persecución de esta tipología delictiva. A su vez, es planteada como una transposición de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. El propósito de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por éstos, con el objetivo de posibilitar su disposición a los agentes facultados. Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores prestadores de servicios de comunicaciones electrónicas disponibles al público o explotadores de redes públicas de comunicaciones, conforme a la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

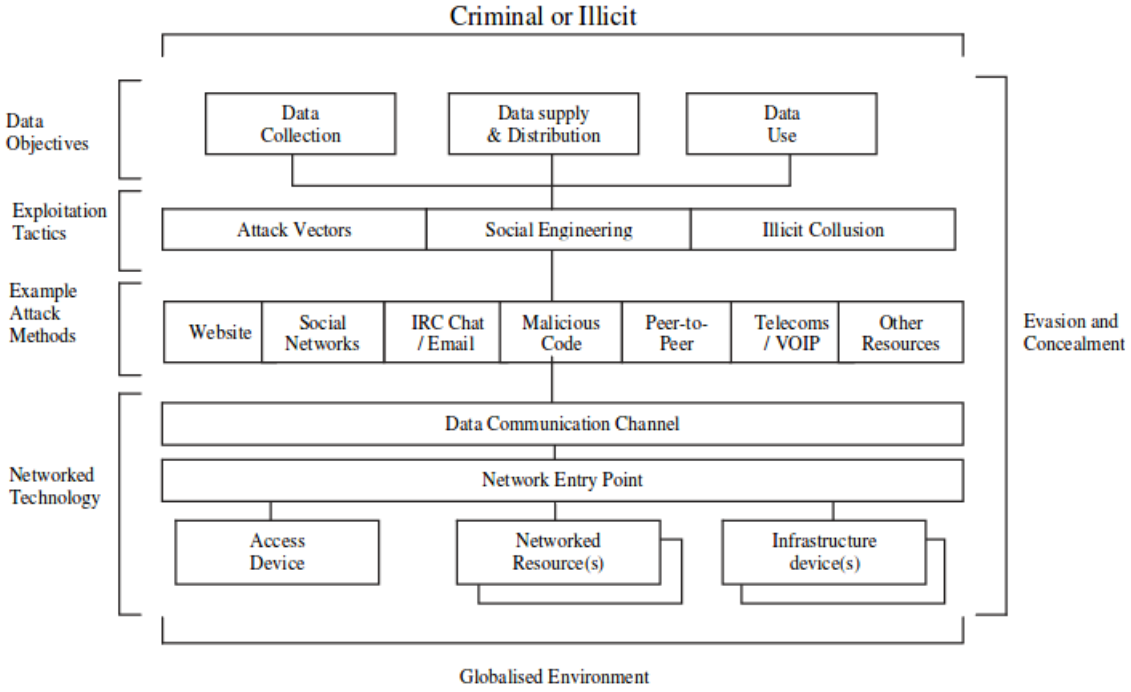
En relación a los prestadores de servicios de la sociedad de la información, sus obligaciones se encuentran reguladas en los arts. 9 y ss. y su régimen de responsabilidad en los arts. 13 y ss., ambas de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). Estos se pueden clasificar en ("Proveedores de servicios", n.d.): 1) Empresas brindando conexión a Internet a sus clientes (ISP), 2) Prestadores de servicios de alojamiento de datos, y 3) Buscadores y proveedores de enlaces. Al respecto, Ortiz Márquez (2007) realiza un análisis muy detallado de los proveedores de enlaces y también una comparativa entre proveedores de acceso y proveedores de servicios.

Sin embargo, se ha planteado la posible vulneración del artículo 18.1 y 3 CE respecto a la garantía del secreto de las comunicaciones, relacionando el concepto con la privacidad (Narváez Rodríguez, 2007), en aquellos casos en los cuales los agentes policiales inician la investigación a raíz de la denuncia de un particular, consiguiendo por medios extrajudiciales la IP del acusado (Fernández Teruelo, 2011). Esto supondría una vulneración de la Ley 25/2007 puesto que exige para la cesión de estos datos, con carácter general, la autorización judicial previa y los datos a conservar son los del objeto a tratar.

No obstante, la jurisprudencia se contrapone y establece la dirección IP de un usuario como, en cierta medida, pública por lo cual no sería necesaria autorización judicial; tan solo lo sería para determinar a qué sujeto fue asignada (STS 236/2008, 292/2008, 739/2008, 680/2010). Asimismo, cabe mencionar la existencia de una base de datos de dominio público, cuya consulta puede ser realizada por cualquier persona, donde se almacena un registro de las direcciones IP y a qué proveedor de servicios se encuentran asignadas tales direcciones (Viota Maestre, 2007).

Finalmente, Hunton (2009) define un modelo de investigación del ciberdelito demostrando las oportunidades de la aplicación de la ley en este proceso. El modelo está destinado a permitir la transferencia de modelos policiales convencionales a un entorno a menudo abstracto y técnico. En el modelo gráfico, *Cybercrime investigation and analysis framework*, resalta la interacción lógica de los siete principales componentes distintos al examinar las actividades generales comunes en el ciberdelito y sus características:

Tabla 4. *Cybercrime investigation and analysis framework.*



Nota. Extraído de Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), 528-535. doi:10.1016/j.clsr.2009.09.005

El objetivo del modelo es simplificar la complejidad de la investigación del delito cibernético y proporcionar al investigador puntos específicos de referencia técnica para conceptualizar los componentes comunes y las actividades abstractas donde se puede encontrar evidencias confiables e inteligencia criminal. Además, el modelo proporciona un enfoque flexible intermedio el cual permitirá el comienzo de una investigación en su punto más apropiado y considerará cada componente relevante a su vez, así como está destinado a ser aplicado de forma iterativa. En resumen, este modelo pretende ser una herramienta de investigación práctica con la finalidad de ayudar a la policía a planificar investigaciones complejas relacionadas con el cibercrimen técnico, considerando formalmente la tecnología y las técnicas utilizadas, identificando las habilidades y conocimientos especializados, y asegurando la recuperación de pruebas fidedignas y admisibles.

En estudios posteriores, los conceptos del modelo básico del anterior gráfico aplicados en el entorno policial del Reino Unido son presentados siguiendo las diferentes etapas de investigación del cibercrimen (Hunton, 2011) y también se discuten los diferentes roles técnicos en los procesos de investigación en la interacción entre agentes policiales y otros cuerpos tecnológicos implicados (Hunton, 2012).

2.1.7 Teorías criminológicas aplicadas al ciberespacio

Durante estos últimos años ha habido estudios sugestivos de criminología aplicada a la cibercriminalidad, cuyo manejo se centra en teorías como la del aprendizaje social (Young y Zhang, 2005), el etiquetamiento (Turgeman-Goldschmidt, 2008), la del autocontrol (Higgins, Fell, y Wilson, 2007), el control social (Svensson y Bannister, 2004) o la decisión racional (Beebe y Rao, 2005). Gran parte de los estudios de este tipo tienen en consideración para su investigación la teoría de las actividades cotidianas de Cohen y Felson (Bossler y Holt, 2009; Choi, 2008; García-Guilabert, 2016; Holt y Bossler, 2009; Hutchings y Hayes, 2009; Miró, 2013; Yar, 2005).

Cohen y Felson (1979) consideran el delito producido en un tiempo y espacio determinados sin exigir a este último ser físico, aunque implícitamente se presuponga. Asimismo, el delito se produciría durante las actividades cotidianas del día a día, cuando en el espacio-tiempo se unen un objetivo adecuado, un delincuente motivado y la inexistencia de un guardián capaz de proteger al blanco; luego, estos tres elementos forman el conocido "triángulo del crimen". Ahora bien, cuando el lugar tenido en cuenta es el ciberespacio, éste altera la concreta expresión de los factores del crimen a tener en consideración en aras a la prevención del delito (Miró, 2012, 2013). A continuación, se expone de manera muy resumida el paralelismo detallado del triángulo del crimen con este nuevo espacio realizado por este último autor mencionado.

Así pues, el ámbito potencial de oportunidad criminal de un agresor motivado se expande debido a la inexistencia de barreras físicas, aumentando al mismo tiempo considerablemente el número de personas involucradas (agresores y objetivos adecuados). También se incrementan las posibilidades de motivación de éste, ya que la realización de un ciberdelito tendrá un coste temporal mayor o menor en función del tipo y son inexistentes los costes de desplazamiento y de huida. A su vez, la multiplicación de potencialidad lesiva de las TIC permite al agresor motivado seleccionar entre varias víctimas cuál va a ser el objetivo de su agresión, así como la contracción de distancias le ofrece la posibilidad de atacar a varias con una única conducta. Desde la visión de la teoría de la decisión racional, el cibercriminal incluiría dentro de los riesgos potenciales a sopesar frente a los beneficios de su agresión la gran dificultad, en términos judiciales probatorios, de ser identificado (Pittaro, 2007).

Por otro lado, son condiciones determinantes para ser un objetivo adecuado de un cibercrimen, también citadas por García-Guilabert (2016): 1) introducción de la persona o alguno de sus bienes en el ciberespacio, 2) valor apetecible de éstos para el ciberdelincuente, e 3) interacción de la persona titular del bien con Internet, haciéndolo visible y con posibilidad de contactar con el agresor motivado. Alshalan (2006) trabaja la hipótesis de la importancia predictora de la victimización en el ciberespacio de la víctima en función de su comportamiento en éste y concluye mediante su estudio empírico de regresiones logísticas lo siguiente: a mayor frecuencia de acceso a Internet, mayor riesgo de victimización.

Finalmente, el ciberespacio disminuye la capacidad potencial del guardián de evitar el crimen debido a su evolución permanente. Los guardianes de los objetivos adecuados pueden ser cualesquiera otros sistemas personales o no, ajenos a la propia víctima o impuestos por ella misma, en calidad de forma de protección, tales como los antivirus u otros sistemas de seguridad (Bossler y Holt, 2009), además de los programas *antispyware* y *firewall* (Choi, 2008). La víctima vuelve a jugar un papel primordial, ya que en parte de ella depende su propia autoprotección. Aunque los sistemas de autoprotección no son los únicos existentes, actualmente, ante la inexistencia de formas de control formal más institucionalizadas, la autodefensa sigue siendo la mejor forma de protección frente a estos delitos (Grabosky, 2001).

2.1.7.1 Medidas de prevención situacional aplicadas al cibercrimen

Generalmente, el agresor suele ser el núcleo para una mayor comprensión del crimen, dado que el objetivo de su agresión y las condiciones de defensa de las cuales dispone están también definidas en su motivación. *The random fallacy* es el término utilizado por Felson y Boba (2010) para dar explicación a la posible creencia por parte de la víctima de ser un objetivo aleatorio y a una elección por parte del agresor de ésta independientemente de su actuación. No obstante, existen estudios con evidencias de la especial importancia del comportamiento de la víctima en la victimización por la cibercriminalidad informática, confirmando todos ellos la idea antes ya mencionada sobre la víctima como definidora del ámbito de riesgo accesible para el agresor motivado (Alshalan, 2006; Choi, 2008; García-Guilabert, 2016).

A su vez, también se pone de manifiesto, no solo de los elementos del triángulo del cibercrimen, la incidencia de factores demográficos en la cibervictimización (Alshalan, 2006; Pratt, Holtfreter, y Reisig, 2010). En Estados Unidos se confirma un mayor riesgo de victimización de los varones frente a las mujeres, hecho relacionado con una mayor frecuencia y duración de uso de Internet aunque la primera no sea estadísticamente significativa y deba atenderse al tipo de actividad realizada por ambas partes (Alshalan, 2006), así como un mayor riesgo de victimización para los jóvenes debido a un tiempo de uso en Internet significativamente mayor frente a los más mayores (Pratt et al., 2010). En cambio, según un estudio publicado por el Ministerio del Interior del Gobierno de España (2015), en general sufren mayor victimización los hombres (55.45%) menos cuando son menores puesto que entonces las mujeres duplican en cifras a los varones, pero el rango de edad predominante para ambas edades es de 26 a 40 años. Por tanto, se pueden observar ligeras diferencias entre ambos países al respecto.

De ello se puede deducir también la idea de la víctima como condicionante para la prevención del cibercrimen. A tales efectos, Miró (2012) consideran las primeras medidas a adoptar: la educación de la víctima en seguridad informática, su concienciación para la adopción de *software* de protección y de rutinas seguras en su actuar cotidiano en el ciberespacio, también citada por Morris y Higgins (2010) y Miró (2013), y la información real sobre los riesgos en éste, también citada por García-Guilabert (2016). Además, Newman (2010) dice no ser necesario un uso complejo de sistemas informáticos para la prevención del cibercrimen, ya que la mayoría de cibercrímenes se realizan debido a debilidades humanas. Por añadidura, se evidencia una distorsión en la percepción sobre los riesgos existentes en el ciberespacio por desconocimiento puesto que Vozmediano, San Juan, y Vergara (2008) comprueban el exiguo miedo de las personas al ciberdelito frente a otros crímenes cuya probabilidad de ocurrencia sobre la víctima es claramente inferior. En el estudio realizado por Bossler y Holt (2010) y centrado en estudiantes universitarios, una de las implicaciones políticas más importantes derivadas de éste fue la necesidad de promover los riesgos a los cuales se verían enfrentados como consecuencia de la exposición a criminales en el ciberespacio. Así pues, comentan por un lado la importancia de desarrollar por parte de las universidades programas para educar a su cuerpo estudiantil y, por otro, la necesidad de identificar por parte de los administradores de seguridad a las personas involucradas en cualquier

comportamiento desviado y bloquear o eliminar su conectividad a Internet para reducir el riesgo de victimización de la comunidad en general.

Por otro lado, Jones (2007) nos habla de la posibilidad de utilizar las posibilidades brindadas por el *open source software* para la modificación de códigos fuente de programas informáticos como forma de sustitución del control policial reactivo frente al cibercrimen al estilo *community policing model*, es decir, con una vigilancia de los propios usuarios de la Red. El autor destaca la gran cantidad de ventajas ofrecidas por los sistemas de *software* libre para luchar contra este fenómeno, dado que para la mejora de la seguridad de sistemas se descentraliza tanto la detección de riesgos como la aplicación de parches. Se trataría de trasladar los sistemas de prevención comunitaria informal al ciberespacio.

Respecto al agresor motivado, siguiendo la idea del crimen como comportamiento instrumental orientado a la obtención de necesidades básicas del agresor de Cornish y Clarke (1986), se trata de analizar cómo puede influirse en su decisión para no cometer el delito. Consiste en modificar el ámbito de oportunidad para cambiar la percepción de éste e incidir sobre su conducta, específicamente aumentando los costes para lograr el objetivo deseado (en términos judiciales, el ser capturado) y reduciendo la obtención de los posibles beneficios. Por tanto, la perspectiva preventiva adoptada para éste es de cariz psicológico – motivacional, siendo relevantes en el ciberespacio por un lado las medidas de autoprotección del usuario y, por otro, la cooperación judicial y la armonización de la justicia.

El modelo de prevención situacional del delito da importancia a los factores ambientales, centrándose en espacio-tiempos propiciadores de una concentración de delitos determinada, hecho permisivo de intervención sobre la oportunidad para reducirla y evitar la comisión del delito por parte del agresor motivado (Cornish y Clarke, 2003). Por tanto, se trata de mejorar la protección de la víctima aumentando el esfuerzo necesario para llevar a cabo el delito. Así pues, se adecua la prevención situacional al ciberespacio porque, como bien ya se ha mencionado, el ciberespacio es un nuevo ámbito de oportunidad delictiva y, a su vez, un ambiente de cambio constante.

Especialmente en las medidas de prevención situacional en las cuales haya intervención de la víctima puede producirse un desplazamiento del objetivo deseado por el ciberdelincuente (Miró, 2012): elección de un objetivo con menor esfuerzo delictivo y para un menor riesgo de ser identificado y poder aumentar sus beneficios. Además, como consecuencia del éxito de una política de prevención situacional, es posible un aumento en la difusión de beneficios, o reverso del desplazamiento, consistente en una reducción inesperada de delitos no destinatarios directos de la acción preventiva llevada a cabo (Clarke y Weisburd, 1994).

Finalmente, considero interesante la aportación de Miró (2012) por ofrecer una transposición del catálogo de posibles medidas preventivas desde un enfoque situacional a este nuevo ámbito de oportunidad delictiva, la cual tan solo espera ser una orientación, ya que muchas de las medidas de prevención situacional pueden no reducir en exceso las cifras de la cibercriminalidad aunque sí complicar el éxito del ciberdelincuente. Las diferentes medidas se recogen en la siguiente tabla:

Tabla 5. Veinte tipos de medidas de prevención situacional de la cibercriminalidad.

Reducción del ámbito de incidencia	**No introducir objetivos** Separación de discos duros con acceso y sin acceso al sistema; sistemas de control parental; filtros de contenido; controladores de seguridad ActiveX; no acceso a salas de chat (*grooming*).	**Identificación de zonas de riesgo** Campañas de información sobre riesgos; aviso en red de infección de *spam*; sistemas de control de banca electrónica.	**Descontaminación / limpieza de residuos** Borrado y destrucción de virus latentes; desinfección de *bots*.
Aumentar el esfuerzo percibido	**Controlar el acceso al sistemas** *Firewall*; actualización de los sistemas operativos; claves de acceso al sistema; claves de acceso a las redes; renovación de claves; sistemas de perfiles en redes sociales.	**Detectar e impedir el ataque** Antivirus; *antispyware*; *antispam*; sistemas de control de banca electrónica.	**Retirar transgresores** Cierre de webs; solicitud de retirada de contenido ilícito; mecanismos de denuncia en redes sociales; cortar el acceso a una IP.
Aumentar el riesgo percibido	**Aumentar el número de guardianes** Moderadores de foros; sistemas Echelon, Enfopol, Carnivore y Dark Web.	**Reducción del anonimato** Identificar las IP; registro en foros web; sistemas de identificación del usuario; identificación y autentificación biométrica.	**Reforzar la vigilancia formal** Control de webs a través de *proxy*; equipos especializados de persecución del cibercrimen.
Disminuir las ganancias percibidas	**Ocultar objetivos** Utilización de sistemas de encriptación; ocultar datos personales en redes sociales; no utilización de claves bancarias; perfeccionamiento	**Desplazar objetivos** Discos duros extraíbles; sistemas de pago alternativos (Paypal); cambio de direcciones web, direcciones de dominio y demás.	**Eliminar beneficios** Persecución a compradores de contenidos ilícitos; persecución del blanqueo capitales.

	sistemas e-comercio.		
Eliminar excusas	**Establecer reglas** Armonización internacional del Derecho; Nitequette.	**Fijar instrucciones** Avisos web de licencias; *copyright* y *copyleft*; avisos sobre privacidad en redes sociales.	**Fortalecer la conciencia moral** Concienciación en materia de propiedad intelectual; reforzar moralmente los negocios lícitos.

Reducción del ámbito de incidencia	*Aumentar el esfuerzo percibido*	*Aumentar el riesgo percibido*	*Disminuir las ganancias percibidas*	*Eliminar excusas*
Separación de objetivos Internet2, creación de subredes locales de seguridad.	**Controlar facilitadores** Obligaciones de vigilancia para IPPS; control de datos por RSS.	**Facilitar la vigilancia** Mejora de los sistemas de identificación de IP; reconstrucción de la arquitectura con fines defensivos.	**Trastornar los mercados delictivos** Ofrecer sistemas de intercambio de archivos económicos (Spotify y demás); control de páginas de descarga directa de archivos.	**Facilitar la conformidad** Nuevos modelos de negocio (Apple); competiciones legales de *hackers*; fortalecimiento del *software* libre.

Nota. Extraído de Miró, F. (2012). Ciberespacio y oportunidad delictiva. Dentro *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. (p. 143-227). Madrid: Marcial Pons.

2.2 Bloque II: Delincuencia corporativa, Seguridad de la Información y *Compliance*

2.2.1 Delincuencia corporativa

El mundo empresarial apareció por primera vez en la investigación criminológica en el artículo de Edwin Sutherland sobre "La delincuencia de cuello blanco" en 1940, a la cual vinculó con el mundo de los negocios (Garrido, Stangeland, y Redondo, 2006). Así, aplicando su teoría de la asociación diferencial a la delincuencia económica, según Sutherland, las prácticas delictivas de grandes empresas eran aprendidas, directa o indirectamente de quienes ya las practicaban. Generalmente, la delincuencia de cuello blanco se ha caracterizado por (Friedrichs, 2010): ocurrir en un contexto laboral legítimo, estar motivada por el objetivo de ganancia económica o éxito ocupacional; y la inexistencia de violencia directa e intencional.

A pesar de usarse indistintamente los conceptos "delincuencia de cuello-blanco" y "delincuencia corporativa" (Lynch, McGurrin, y Fenwich, 2004), la segunda se define como aquellos actos ilícitos y dañinos realizados por directivos y empleados de empresas con el fin de promover los intereses corporativos (Friedrichs, 2010). En otras palabras, se habla de criminalidad corporativa cuando empresas u organizaciones legalmente establecidas cometen infracciones, generalmente en busca de una mejor situación económica, aprovechándose de las oportunidades

brindadas a quienes ejercen la profesión, viniendo determinada esta "personalidad delictiva" de la corporación por el tipo de actividad realizada y las oportunidades ofrecidas para transgredir las normas, independientemente de las personas ocupantes de cargos de responsabilidad (Garrido et al., 2006). Por tanto, la criminalidad corporativa es una forma de delincuencia de cuello-blanco. Ambos tipos de delitos son más perjudiciales y costosos para la sociedad que la delincuencia convencional, aunque son tratados con más indulgencia, pero por otro lado resulta evidente su inadecuada representación en la literatura criminológica[11] (Lynch et al., 2004).

Del mismo modo, también encaja en la delincuencia corporativa la teoría de la oportunidad delictiva de Cloward y Ohlin (Garrido et al., 2006), puesto que una empresa persigue el beneficio, un objetivo claramente definido socialmente aceptable. En este caso, si son más elevados los gustos que los ingresos, la empresa quiebra. Cuando la empresa no puede ganar dinero de forma legítima, lo conseguirá con falsificación o adulteración de productos, o bien, con fraudes o subvenciones públicas fraudulentas. Así, la criminalidad corporativa podría ser considerada como forma ilegítima de conseguir este beneficio empresarial.

Muy interesante es el estudio realizado por Steffensmeier, Schwartz, y Roche (2013) sobre la inclusión del género a la delincuencia corporativa mediante el desarrollo de un marco enfocado a preocupaciones de género y oportunidades criminales predictivo de la participación mínima y marginal de las mujeres en las redes criminales corporativas. Así, los resultados obtenidos evidencian al hombre mayormente como delincuente corporativo; menos de uno de cada diez es una mujer. Cuando participan mujeres, el papel desempeñado es menor, mientras que los hombres suelen ser cabecillas. Esto evidencia la probabilidad de exclusión de las mujeres en las conspiraciones criminales lucrativas o su utilización en las formas tipificadas por sexo consideradas más efectivas para la empresa. Esta diferencia de roles refleja en parte la mayor representación de las mujeres en posiciones subordinadas en las empresas. Estos hallazgos plantean una intrigante cuestión: ¿reducirían más mujeres en puestos de liderazgo y poder corporativo el fraude corporativo? La respuesta parece ser afirmativa, puesto que las ejecutivas pueden ser más éticas en la toma de decisiones, más propensas a respetar las leyes fundamentales del riesgo financiero y

11 Para un análisis más extenso sobre la explicación de delincuencia corporativa mediante teorías criminológicas, el punto 1 de la Lección II, "Cumplimiento normativo, criminología y responsabilidad penal de personas jurídicas", en Nieto Martín, A. (2015). *Manual de cumplimiento penal en la empresa*. Valencia: Tirant Lo Blanch., Nieto Martín, A. (2015).

evitar los excesos de riesgo, tanto dentro como fuera del entorno corporativo, y menos propensas a fomentar una cultura organizativa criminal.

Clinard y Quinney (1994), en términos genéricos, distinguieron entre la delincuencia corporativa, en cuyo alcance se encuentran los delitos cometidos por representantes de grandes empresas con el fin de mejorar la situación económica de éstos, y la delincuencia ocupacional, cuya comprensión admite los delitos cometidos por personas en su interés individual, con frecuencia dirigidos contra la misma empresa, aprovechándose de su posición en ella. De igual modo, Friedrichs (2010) nos ofrece una clasificación más exhaustiva de ambos tipos de delincuencia. En función del tipo de actividad, podemos clasificar a los crímenes corporativos en violencia corporativa, o bien, en abuso corporativo de poder, fraude o explotación económica. Asimismo, si estos dos tipos se clasifican por tipo de víctima, en el primero encontramos la violencia corporativa contra consumidores (productos inseguros), contra trabajadores (condiciones de trabajo inseguras) o contra el público (prácticas medioambientales inseguras) y, en el segundo, delitos contra ciudadanos y contribuyentes (defraudación del gobierno y evasión de impuestos corporativos), contra consumidores (fijación de precios, agudización de precios, publicidad falsa y falsa representación de productos), contra empleados (explotación económica, robo corporativo, prácticas laborales desleales y vigilancia de empleados), contra competidores (prácticas monopolísticas y robo de secretos comerciales), contra franquiciados y proveedores (fraudes por descuento y compensación), o finalmente contra dueños o acreedores (fraude contable de gestión, autocontrol y quiebra estratégica). Por otro lado, la delincuencia ocupacional se puede clasificar en crímenes cometidos por pequeñas empresas (delincuencia de venta al por menor -*retail crime*- y fraude de servicios), crímenes cometidos por profesionales (médico, legal, académico y religioso) o crímenes cometidos por empleados.

Con el tiempo, la conversión de la tecnología de la información en la industria más grande del mundo ha supuesto la aparición del cibercrimen y, asimismo, la aparición de una nueva modalidad de comisión del delito de cuello-blanco (Parker, 1980), puesto que el coste y la sofisticación de la alta tecnología proporcionan nuevos medios y oportunidades para este tipo de delito (Schlegel y Cohen, 2007). Por ejemplo, los ordenadores tienen un rol fundamental en el abuso de información privilegiada ayudando a ocultar ganancias ilegales y posiciones de mercado. Al mismo tiempo, también han aparecido nuevas formas de comisión de delitos informáticos, como el robo de

identidad y el robo de información confidencial, para defraudar de diversas maneras a las empresas usuarias de Internet (Grabosky, 2007), o incluso delitos llevados a cabo por o a través de empresas o personas dentro del contexto de una ocupación legítima, victimizando a consumidores e individuos. Por ejemplo, un empleado podría usar un ordenador con el fin de extraer secretos comerciales para posteriormente venderlos a competidores estando motivado por el deseo de venganza por los malos tratos recibidos por parte del empleador. En muchos casos, las víctimas de estos delitos son reacias a denunciar su victimización, como por ejemplo los bancos, puesto que existe un posible perjuicio en su reputación, tienen poca confianza en el sistema de justicia penal, o bien, el posible escándalo público puede generar desconfianza para sus clientes por el hecho de publicar la vulnerabilidad de sus sistemas informáticos y de la información contenida en ellos.

Actualmente, en un contexto donde un 70-89% de trabajadores autónomos, puestos directivos u de otro tipo son los más propensos a utilizar Internet en su lugar de trabajo (Eropean Comission [EC], 2015), y donde el cibercrimen es un desafío creciente (United Nations Office on Drugs and Crime [UNODC], 2013), las empresas deben asegurarse de disponer de una ciberseguridad adecuada al momento y también de aumentar la resistencia informática, en particular de su capacidad de detectar, contener y corregir las infracciones, intencionales o deliberadas, y otros incidentes informáticos (National Crime Agency [NCA], 2016). Entre las fechas enero 2015 – abril 2016 un 43% de las organizaciones fueron víctimas de un ataque *ransomware*, así como un 57% de los ataques fueron dirigidos a consumidores, ataques traducidos en pérdidas globales de cientos de millones de dólares (Symantec, 2016). Para este 2017 se predice como uno de los puntos clave necesarios la protección de la información (*data protection*), debido a posibles recopilaciones de datos por parte de hacktivistas o por ataques *ransomware* (McAfee Labs, 2016), incluso por el probable incremento de los ataques a la integridad de los datos tanto en el sector público como privado (Stroz Friedberg, 2017), entre muchos otros; luego, la aplicación y cumplimiento de la Normativa General de Protección de Datos (*General Data Protection Regulation,* GDPR) aumentará los costos administrativos entre organizaciones (Trend Micro, 2016).

2.2.2 Ciberseguridad y Seguridad de la Información

Instituciones, organizaciones, empresas y ciudadanos están expuestos a los riesgos del ciberespacio y a unas amenazas exigentes de una respuesta global; así, se incluyen en el término

Ciberseguridad todas aquellas actividades orientadas a responder a determinadas amenazas, cuyo alcance pueda verse amplificado debido al uso de la tecnología e Internet como medio (PricewaterhouseCoopers [PwC], 2015).

Se define la Ciberseguridad como la protección de activos de información a través del tratamiento de amenazas, las cuales ponen en riesgo la información procesada, almacenada y transportada por los sistemas de información interconectados (Information Systems Audit and Control Association [ISACA], 2016). Por tanto, la finalidad es proteger la información digital de los sistemas interconectados. Asimismo, está comprendida por cinco campos (European Union Agency for Network and Information Security [ENISA], 2015): Seguridad de las Comunicaciones (protección contra una amenaza a la infraestructura técnica de un sistema informático cuyos resultados no fueron planeados por diseñadores, propietarios o usuarios), Seguridad Operativa (protección contra la corrupción prevista de los procedimientos o flujos de trabajo con resultados no planeados por diseñadores, propietarios o usuarios), Seguridad de la Información (protección contra la amenaza de robo, eliminación o alteración de datos almacenados o trasmitidos dentro de un sistema informático), Seguridad física (protección contra amenazas físicas con posibilidad de influir o afectar el bienestar de un sistema informático) y Seguridad pública / nacional (protección contra una amenaza cuyo origen es el ciberespacio pero puede poner en peligro los activos físicos o informáticos generando un beneficio político, militar o estratégico para el atacante).

Para la Comunidad de Estándares, la Organización Internacional de Normalización (*International Organization for Standardization*, en adelante, ISO) y la Comisión Electrónica Internacional (*International Electrotechnical Commission*, en adelante, IEC), el concepto Ciberseguridad incluye la protección contra la variedad de posibles riesgos padecidos por organizaciones y datos, especialmente cuando éste es considerado sinónimo de "Seguridad de la Información". Así, la familia de estándares ISO/IEC 27000[12] ayuda a las organizaciones a mantener los activos de información seguros.

Por otro lado, la Seguridad de la Información es definida por la norma ISO/IEC 27001 como la preservación de la confidencialidad, integridad y disponibilidad de la información, entendiendo por información aquel conjunto de datos organizados en poder de una entidad cuyo valor sea

12 https://www.iso.org/isoiec-27001-information-security.html

relevante para la misma, independientemente de la forma cómo se guarde o transmita, de su origen o de la fecha de elaboración (Asociación Española de Normalización y Certificación [AENOR], 2009; "Sistema de Gestión de la Seguridad de la Información", n.d.). Así, para garantizar una buena gestión de la Seguridad de la Información se deben identificar los aspectos trascendentales, conocidos como CIA: 1) la información no es dispuesta ni revelada a individuos, entidades o procesos no autorizados (*confidentiality*); 2) el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso (*integrity*); y 3) el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de individuos, entidades o procesos autorizados cuando lo requieran (*availability*).

La norma ISO/IEC 27001 es la más conocida de la familia ISO/IEC 27000, puesto que proporciona los requisitos necesarios para un Sistema de Gestión de la Seguridad de la Información. La norma UNE-ISO/IEC 27001:2007 anuló la UNE 71502:2004, Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), hasta entonces vigente en España (Asociación Española de Normalización y Certificación [AENOR], 2008).

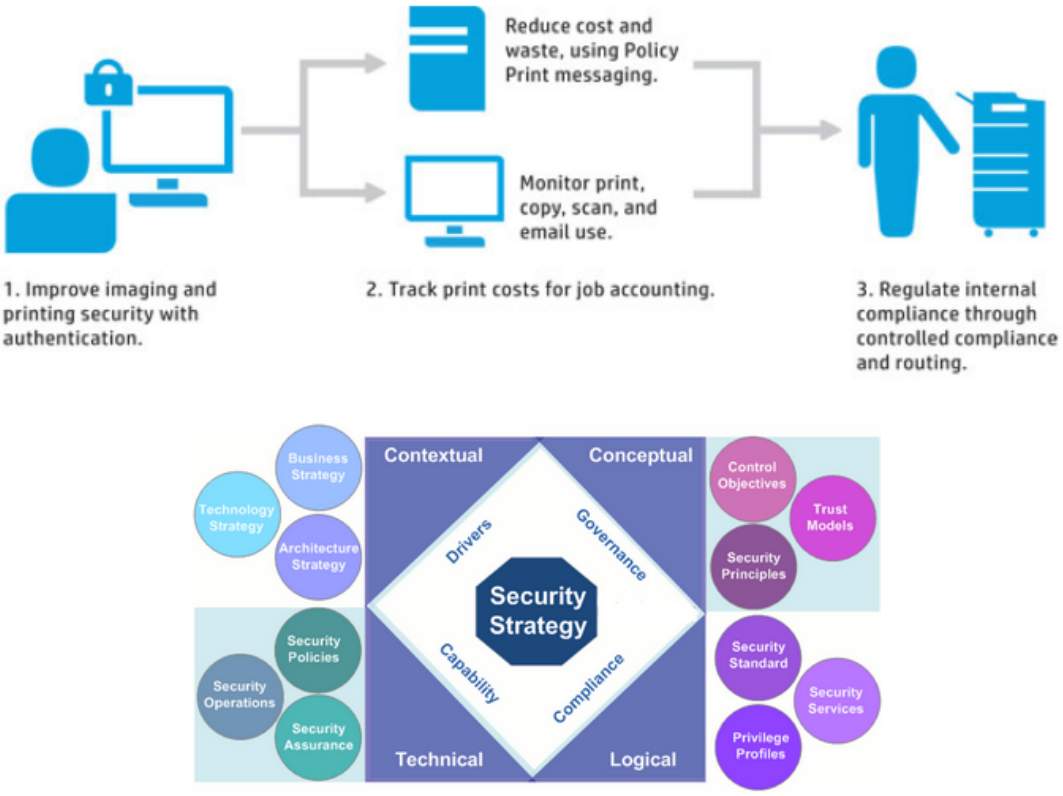
2.2.2.1 Sistemas de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (*Information Security Management Systems*, en adelante, ISMS) es el proceso sistemático, documentado y conocido por toda la organización cuya finalidad es gestionar la seguridad de la información. Así, garantizar un nivel de protección total es virtualmente imposible aun disponiendo de un presupuesto ilimitado; luego, el propósito de dicho sistema es garantizar el conocimiento, gestión, minimización y adquisición de los riesgos de la seguridad de la información por la organización de manera documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios producidos en los riesgos, el entorno y las tecnologías ("Sistema de Gestión de la Seguridad de la Información", n.d.).

Fundamentalmente se distinguirán dos tipos de procesos (Gómez Fernández y Fernández Rivero, 2015): 1) Procesos de gestión, los cuales controlan el funcionamiento del propio sistema de gestión y su mejora continua; y 2) Procesos de seguridad, los cuales se centran en los aspectos relativos a la propia seguridad de la información. EISA se relaciona más ampliamente con la práctica de la seguridad de la optimización del negocio, tal como se puede ver en la siguiente figura,

puesto que se refiere a la arquitectura de seguridad empresarial, a la gestión del rendimiento y a la arquitectura de procesos de seguridad (ValueLinked, 2013).

Tabla 6. Gráfico representativo de la idea fundamental de EISA.



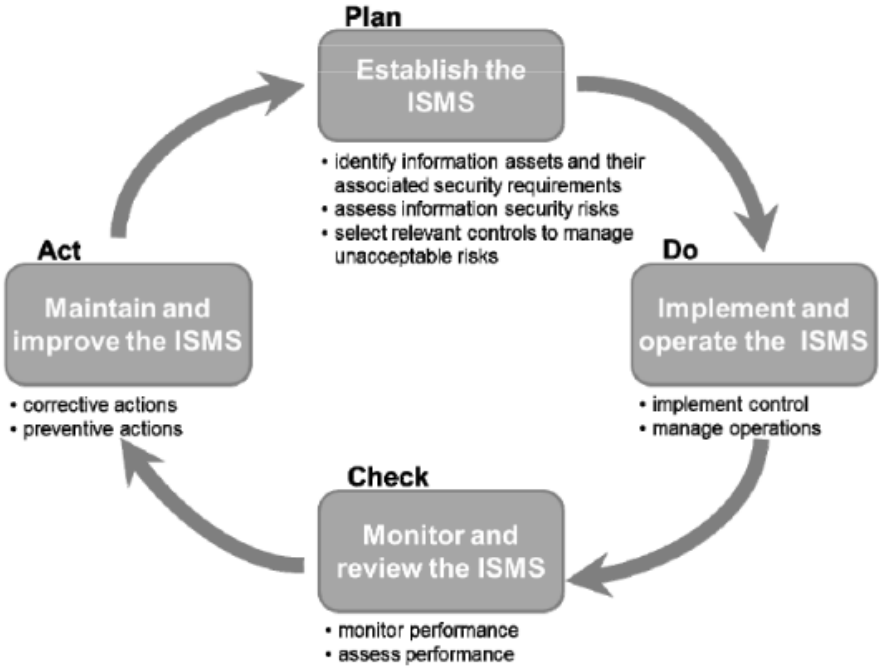
Nota. Extraído de ValueLinked. (2013). *Services*. Consultado 29 marzo 2017, desde https://sites.google.com/a/valuelinked.com/www/services

Así, el objetivo clave de crear una EISA es garantizar la alineación de la estrategia empresarial y la seguridad de la tecnología de la información, ya que por definición EISA supone la práctica de aplicar un método para describir una estructura y comportamiento/s actual/es o futuro/s de los procesos de seguridad, sistemas de información, personal y subunidades organizativas de la empresa, todos ellos alineados con los objetivos fundamentales de la organización y la dirección estratégica (ValueLinked, 2013).

Asimismo, la familia ISO 27000 hace referencia al ciclo "Plan-Do-Check-Act" (en adelante, PDCA) o ciclo de Deming, mostrado en la siguiente figura, cuyo énfasis recae en la necesidad de orientación del proceso y la integración de la planificación operativa y comprobación constante de

la aplicación de la planificación y el compliance (Disterer, 2013). Es una estrategia de mejora continua de la calidad usada mucho por ISMS.

Tabla 7. Gráfico representativo del ciclo de Deming o PDCA.



Nota. Extraído de Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4(2), 92-100. doi:10.4236/jis.2013.42011

En resumen, en la fase de planificación (*Plan*) de un ISMS se definen los requisitos para la protección de la información y los sistemas de información, se identifican y evalúan los riesgos y se desarrollan procedimientos y medidas adecuados para reducirlos, cuya implementación se dará en la fase de realización (*Do*). Finalmente, los informes generados mediante el monitoreo continuo de las operaciones en la fase de comprobación (*Check*) se utilizarán para obtener mejoras y el posterior desarrollo del ISMS en la fase de actuación (*Act*). Es un ciclo cerrado y de retroalimentación. Esta explicación más detallada relacionada con la familia de estándares ISO 27000 se expone en Disterer (2013).

2.2.3 Responsabilidad penal de las personas jurídicas

Por primera vez en España la LO 5/2010 previó la responsabilidad penal de las personas jurídicas (en adelante, RPPJ), cuyos fundamentos esenciales se regulan en el artículo 31.bis CP. La doctrina justifica esta decisión político-criminal, según señala Díez Ripollés (2012), con: a) Una necesidad de intervención penal en corporaciones debido a dificultades para exigir

responsabilidades individuales en el seno de empresas complejas con tendencia a tener una responsabilidad diseminada; b) Un escaso efecto preventivo en la organización de la responsabilidad individual o de la propia del derecho administrativo sancionador, repercutiendo solamente de forma eficaz y efectiva sobre la organización la responsabilidad penal; y c) sanciones penales a personas jurídicas buscan implicar de forma efectiva a las propias organizaciones en la detección y prevención de delitos cometidos en su seno por parte de personas físicas, introduciendo la vinculación de la responsabilidad penal con la promoción de la autorregulación en la esfera empresarial a través de los *Compliance Programs*.

Antes de esta reforma, explica del Moral García (2016), las personas morales no podían sufrir penas pero sí medidas de seguridad caracterizadas como consecuencias accesorias (art. 129 CP). A su vez, debido al interés del Derecho Penal por comportamientos humanos, eran condenadas las personas físicas intervinientes en la comisión del delito o contribuyentes a él a través de alguna forma de participación, bien con su colaboración activa, bien con su indebido dejar hacer u omisión de quien es garante. Pues, este mismo objetivo se persigue con la reforma de 2010. Según la Circular 1/2011 FGE y otros autores (Boldova Pasamar, 2013; Urruela Mora, 2012), se abandona el principio *societas delinquere non potest*, esto es, la persona jurídica no puede cometer delitos, y también el principio *societas puniri non potest*, es decir, la sociedad no puede ser penada (del Moral García, 2016; Gómez Martín, 2012; Mir Puig, 2014); en contrapuesta, los mismos autores citados en apoyo al segundo principio se mantienen en una posición divergente en relación al primero.

Tal regulación, además de incorporar el artículo del Código Penal anteriormente mencionado, es completada con las disposiciones de los artículos 33.7 (penas imponibles a las personas jurídicas), 50.3 y .4 (extensión y cuota diaria de la pena de multa), 53.5 (posibilidad de pago fraccionado), 52.4 (multas sustitutivas de la multa proporcional cuando el cálculo de ésta no sea posible), 66.bis (determinación de la pena aplicable), 116.3 (responsabilidad civil) y 130 (supuestos de transformación y fusión de sociedades).

Aunque la reforma del Código Penal no facilite una definición de persona jurídica penalmente responsable, los sujetos pasivos del proceso penal referidos, quienes necesariamente deben ser personas jurídicas, son personas jurídico privadas de Derecho civil y mercantil y determinadas personas jurídico públicas aludidas en el apartado 2 de la Circular 1/2011 FGE. Para aquellos otros

entes colectivos carentes de la misma naturaleza, la Ley prevé un régimen diverso establecido en el artículo 129 CP. Asimismo, se excluyen a las personas jurídicas de Derecho Público por considerarse no estar sujetas a responsabilidad penal en el apartado 5 del artículo 31.bis CP, y a los partidos políticos y sindicatos, aunque esta última consideración fue derogada por la LO 7/2012, de 27 de diciembre, pudiendo ya ser responsables penalmente. Por lo tanto, el objetivo principal de la introducción de la RPPJ en la Ley son los entes colectivos de Derecho Privado.

Se establece un sistema normativo dualista de atribución de la responsabilidad vicarial o por transferencia (Boldova Pasamar, 2013; Circular 1/2011 FGE; Mir Puig, 2014; Nieto Martín, 2015; Urruela Mora, 2012), de manera que las personas jurídicas pueden resultar penalmente responsables de los hechos cometidos por determinadas personas físicas cuando concurran los requisitos necesarios referidos en el apartado 1 del artículo 31.bis CP, esto es, de delitos cometidos en nombre o por cuenta de las personas jurídicas y en su provecho, o bien por sus representantes legales y administradores de hecho o de derecho (art. 31.bis 1 a) CP), o bien de delitos cometidos estando sometidos a la autoridad de las personas físicas del anterior inciso dentro del mismo apartado 1, en el ejercicio de sus funciones y por cuenta y en provecho de las personas jurídicas, por no haberse ejercido sobre ellos el debido control en el caso concreto (art. 31.bis 1 b) CP). Así, en el primer caso, cuando la persona física haya actuado al margen de sus funciones, en provecho propio o incluso en perjuicio de la persona jurídica no cabrá la responsabilidad penal de ésta, y en el segundo caso, queda excluida la RPPJ en los supuestos en los cuales el empleado haya actuado exclusivamente en provecho propio o al margen de las actividades sociales, y cuando se haya ejercido sobre la misma el debido control y/o la necesaria prevención del delito (Boldova Pasamar, 2013).

Por tanto, se trata de una responsabilidad no independiente pero autónoma y susceptible de apreciarse exclusivamente o de forma acumulativa respecto de la persona física, como así resulta del contenido de los apartados 2 y 3 del artículo 31.bis CP. No solo se eliminan lagunas punitivas sino también se minimizan los previsibles intentos de desplazamiento de la carga desde la persona jurídica a la física, y al revés. Ambos apartados son, en palabras de Urruela Mora (2012), factores de desvinculación de la responsabilidad penal de la empresa respecto del delito de la persona física, es decir, el camino hacia una autorresponsabilidad empresarial. En el apartado 2, la RPPJ será exigible en cualquier caso cuando se haya constatado la comisión de un hecho delictivo cometido

por los sujetos referidos en el apartado 1 del artículo 31.bis CP aun cuando la concreta persona física no haya sido individualizada ni haya sido posible dirigir un procedimiento contra ella. Por otro lado, en el apartado 3 se dispone de vías de no exclusión ni modificación de la responsabilidad penal para cuando concurran, en los sujetos autores de los hechos delictivos o aquellos responsables de no haber ejercido el debido control sobre los autores mismos, circunstancias modificantes de la culpabilidad del acusado o agravantes de su responsabilidad, el fallecimiento de dichas personas o se hubieran sustraído a la acción de la justicia. En consecuencia, nos encontramos ante una responsabilidad vicarial limitada porque la persona jurídica responde penalmente aunque la persona física se encuentre en alguna de las circunstancias mencionadas anteriormente (Boldova Pasamar, 2013).

En casos en los cuales se deba proceder a la acusación tanto de personas físicas como jurídicas, se atiende a la norma del apartado 2 del artículo 31.bis CP para la modulación de las cuantías de las respectivas sanciones pecuniarias cuya imposición se solicite, garantizando el principio de proporcionalidad (Circular 1/2011 FGE). La regulación legal de las penas para personas jurídicas sólo las admitirá sin infringir gravemente el principio de culpabilidad si se hace una clara distinción con las penas para personas físicas y se las priva del significado simbólico caracterizador de gran reproche (Mir Puig, 2011).

La única pena para sancionar a la persona jurídica en todo caso es la multa, salvo por consejo de razones de prevención especial, o gravedad y especiales circunstancias de la conducta imputada (Circular 1/2011 FGE). La LO 5/2010 establece un catálogo de sanciones específicas para las organizaciones y una serie de reglas penológicas y, a su vez, modifica el texto del artículo 129 CP y deroga el apartado 2 del artículo 31. En el artículo 33.7 CP se establece un catálogo de penas con carácter grave aplicables a las personas jurídicas. Tal y como expone del Moral García (2016), las consecuencias accesorias del artículo 129 CP y las sanciones administrativas son bautizadas como *penas* en el artículo 33 CP y, con este cambio, más simbólico que de contenidos, varía considerablemente el procedimiento para su imposición.

En relación a los delitos, se ha optado por configurar un sistema de *numerus clausus* (Urruela Mora, 2012), es decir, la responsabilidad penal no será susceptible de generarse con respecto de cualquier ilícito penal sino únicamente en aquellos casos previstos por la ley en el apartado 1 del

artículo 31.bis CP. En otras palabras, la RPPJ se rige por el principio de excepcionalidad y por tanto se contrae a un número cerrado de infracciones penales (Boldova Pasamar, 2013). La reforma del CP de 2010 circunscribe la RPPJ al siguiente catálogo de delitos:

Tabla 8. Catálogo de delitos circunscritos a la RPPJ en la reforma del CP de 2010.

Delito	**Artículo del Código Penal**
Tráfico ilegal de órganos	156 bis
Trata de seres humanos	177 bis
Delitos relativos a la prostitución y la corrupción de menores	189 bis
Delitos contra la intimidad y allanamiento informático	197
Estafas y fraudes del artículo 251	251 bis
Insolvencias punibles	261 bis
Daños informáticos	264
Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores	288
Blanqueo de capitales	302
Delitos contra la Hacienda Pública y la Seguridad Social	310 bis
Delitos contra los derechos de los ciudadanos extranjeros	318 bis
Delitos de construcción, edificación o urbanización ilegal	319
Delitos contra el medio ambiente	327, 328
Delitos relativos a la energía nuclear y a las radiaciones ionizantes	343
Delitos de riesgo provocado por explosivos	348
Delitos contra la salud pública en la modalidad de tráfico de drogas	369 bis
Falsedad en medios de pago	399 bis
Cohecho	427
Tráfico de influencias	430
Corrupción de funcionario extranjero	445
Financiación del terrorismo	576 bis

Nota. Extraído de Circular 1/2011 de la Fiscalía General del Estado, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.

Por otro lado, el objeto de proceso penal en caso de imputación de una persona jurídica es la acreditación, a través de los medios de prueba correspondientes en cada caso, de la comisión del hecho delictivo por parte de las personas físicas referidas en el apartado 1 del artículo 31.bis CP, esto es, representantes, gestores de hecho o de derecho y subordinados en la jerarquía empresarial, en las concretas circunstancias establecidas en la Ley (Circular 1/2011 FGE; Urruela Mora, 2012).

El apartado 4 del artículo 31.bis CP contiene un catálogo cerrado de atenuantes de aplicación a las personas jurídicas, con lo cual se impide la aplicación de aquellas circunstancias contenidas en el artículo 21 CP por referirse a comportamientos exclusivamente humanos. Cabe destacar el carácter postdelictivo de todas estas circunstancias modificadoras de la RPPJ y la exigencia de una actuación de los representantes legales de la entidad, excluyendo la actuación de otros posibles sujetos (Urruela Mora, 2012). Asimismo, la atenuación recogida en la letra d) del artículo 31.bis 4 CP enlaza con los programas de cumplimiento corporativo, *Compliance Programs*, dirigidos a estimular un buen gobierno corporativo mediante la autorregulación empresarial, hecho criticable, nos dice el mismo autor, cuando dicho efecto atenuante se circunscriba a los casos de implementación *ex post* de dichas medidas, sin tener previsto ningún efecto atenuante o eximente de la RPPJ cuando concurra en el misma realización de los actos ilícitos la existencia de programas de cumplimiento corporativo eficaces y efectivos.

Los programas de autorregulación corporativa, *compliance guide* o *corporate defense,* podrán ser utilizados para la evaluación del contenido real del mandato cuyo titular es el representante o gestor, y todo el conjunto integrante del *debido control* de la actividad empresarial en el caso concreto, pero en ningún caso son constituyentes de fundamento de imputación de la persona jurídica ni de substrato de *culpabilidad de empresa*; no existe referencia a ello en el artículo 31.bis CP (Circular 1/2011 FGE). Por tanto, la elaboración y el cumplimiento del *compliance guide* o normas de autorregulación de la empresa solo son relevantes en la medida en que traduzcan una conducta.

Esta necesidad de implementación de un sistema de prevención de delitos es referida en la LO 5/2010, aunque la misma no regula de forma expresa los mecanismos mediante los cuales las personas jurídicas pueden reducir el riesgo de ser consideradas responsables penalmente por los delitos establecidos en el apartado 1 del artículo 31.bis CP. Sin embargo, la reforma del CP de 2015 intenta poner fin a las dudas interpretativas planteadas por la anterior regulación, mediante la identificación exacta y clara de los requisitos necesarios de un correcto sistema de debido control o prevención de delitos en la organización.

Así, la Ley Orgánica 1/2015, de 30 de marzo, realiza una modificación importante respecto del artículo 31.bis, parcialmente el artículo 66 e incorpora tres nuevos artículos, 31.ter, 31.quater y

31.quinquies CP, reproductores del contenido anteriormente regulado en los apartados 2º, 3º, 4º y 5º del antiguo artículo 31.bis CP. La Circular 1/2016 FGE no afecta a la vigencia de la Circular 1/2011 FGE, la cual será de aplicación en todo aquello no modificado por la LO 1/2015.

La persona jurídica podrá carecer de responsabilidad penal cuando demuestre tener implantado un plan de cumplimiento eficaz, antes contemplado como atenuante de la RPPJ y ahora como eximente en su incorporación en la LO 1/2015, fortaleciendo así su papel con la reforma. Es precisamente en el segundo inciso del artículo 31.bis 1 CP donde cobra pleno sentido el planteamiento de posible exención de la RPPJ si logra probar el implemento de las medidas de control oportunas con la finalidad de evitar la producción de actividades ilícitas en su seno; luego, esto conecta con los *Compliance Programs*. Los modelos de organización y gestión deberán observar las condiciones y requisitos establecidos en los apartados 2 y 5 del artículo 31.bis CP. ¿Es más eficaz y disuasorio este sistema? El tiempo lo dirá. Una primera valoración de los efectos psicológicos a nivel de directivos de empresa, expone del Moral García (2016), parece indicar una respuesta afirmativa como fórmula preventiva para evitar la criminalidad en la entidad, no por miedo a sufrir una pena sino por el riesgo de reputación posiblemente conllevado, puesto que las repercusiones económicas negativas pueden ser mucho mayores que la cuantía de la multa.

Asimismo, la reforma del 2015 respalda la visión de un sistema de heterorresponsabilidad, apoyado a su vez por la Circular 1/2011 FGE, pues se confiere a los programas de cumplimiento eficaces en todo caso *ex ante* un valor absolvente también cuando el autor es un directivo del ente; hacia esta dirección apunta también la STS 514/2015, de 2 de septiembre. Cuando determinados sujetos actúen como directivos o empleados en beneficio de la organización, se tendrá obligación de imponer una pena también a la persona jurídica, salvo existir un programa de cumplimiento eficaz burlado por el autor (artículo 31.bis CP). Esta cláusula de exención de la RPPJ incorporada constituye una causa de exclusión de la punibilidad, a modo de excusa absolutoria, cuya carga probatoria incumbe a la persona jurídica, quien deberá acreditar el cumplimiento de las condiciones y requisitos legales de los modelos de gestión y organización (Circular 1/2016 FGE).

Más particularmente, en las letras a) y b) del artículo 31.bis 1 CP se mantiene el fundamento de atribución de la RPPJ de tipo vicarial exigiendo, como antes de la reforma, la previa comisión de un delito por una persona jurídica en las concretas circunstancias establecidas; en el primer caso,

por personas con responsabilidades mayores en la empresa y, en el segundo, por personas indebidamente controladas por las primeras. Asimismo, como ya se ha adelantado, esta reforma reconoce la responsabilidad autónoma de la persona jurídica mediante la regulación de los programas de organización y gestión, cuyo valor es eximente bajo determinados requisitos.

Por un lado, con respecto a la letra a) del apartado primero del artículo 31.bis CP, se amplía notablemente el círculo de sujetos añadiendo, sin ser propiamente administradores o representantes legales de la sociedad, a quienes forman parte de órganos sociales con capacidad para tomar decisiones, así como a mandos intermedios, apoderados singulares y a otras personas en quienes se haya delegado determinadas funciones, incluidas las de control de riesgos ostentadas por el oficial de cumplimiento (Circular 1/2016 FGE).

Por otro lado, respecto de la letra b) del apartado primero del artículo 31.bis CP, se sustituye la expresión *en su provecho* por *en su beneficio directo o indirecto*, conservando así la misma naturaleza objetiva de la acción, tendiente a conseguir un beneficio sin exigencia de la producción del mismo sino con la suficiente actuación de la persona física dirigida de manera directa o indirecta a beneficiar a la empresa. Además, ello permite extender la RPPJ a aquellas entidades cuyo objeto social no persigue intereses estrictamente económicos, así como la inclusión clara de los beneficios obtenidos por medio de un tercero interpuesto, los beneficios para ahorrar costes y todo aquel estratégico, intangible o de reputación; tan solo se excluyen las conductas idóneas para reportar a la entidad beneficios llevadas a cabo por personas físicas para su uso exclusivo y propio beneficio o para terceros (Circular 1/2016 FGE).

De la misma manera, en este mismo último inciso se sustituye el *debido control* por *haberse incumplido gravemente los deberes de supervisión, vigilancia y control*, evidenciando así una disminución de intervención punitiva, cuyo alcance penal permite excluir incumplimientos no graves frente a aquellos en los cuales tan solo caben sanciones administrativas o mercantiles (Circular 1/2016 FGE). Por tanto, no es necesario el establecimiento de una vinculación directa con la empresa, quedando incluidos autónomos, trabajadores subcontratados y empleados de empresas filiales, siempre que se hallen integrados en el perímetro de su dominio social. El incumplimiento grave de estos deberes ha de valorarse *atendidas las concretas circunstancias del caso*, expresión ya utilizada anteriormente, lo cual remite a los programas de organización y gestión objetos de una

inicial valoración en relación con este criterio de imputación para evaluar el alcance y contenido del mandato de dichos sujetos.

En relación a los delitos, se incorporan algunos al catálogo, subrayados de color en la siguiente tabla gráfica. Así, el actual listado de delitos se extiende a:

Tabla 9. Catálogo de delitos circunscritos a la RPPJ en la reforma del CP de 2015.

Delito	**Artículo del Código Penal**
Tráfico ilegal de órganos	156 bis.3
Trata de seres humanos	177 bis.7
Delitos relativos a la prostitución y la corrupción de menores	189 bis
Delitos contra la intimidad y allanamiento informático	197 quinquies
Estafas	251 bis
Frustración de la ejecución	258 ter
Insolvencias punibles	261 bis
Daños informáticos	264 quater
Contra la propiedad intelectual e industrial, el mercado y los consumidores	288
Blanqueo de capitales	302.2
Financiación ilegal de los partidos políticos	304 bis.5
Contra la Hacienda Pública y la Seguridad Social	310 bis
Contra los derechos de los ciudadanos extranjeros	318 bis.5
Urbanización, construcción o edificación no autorizables	319.4
Contra los recursos naturales y el medio ambiente	328
Relativos a las radiaciones ionizantes	343.3
Riesgos provocados por explosivos y otros agentes	348.3
Contra la salud pública	366
Contra la salud pública (tráfico de drogas)	369 bis
Falsificación de moneda	386.5
Falsificación de tarjetas de crédito y débito y cheques de viaje	399 bis
Cohecho	427 bis
Tráfico de influencias	430
Delitos de odio y enaltecimiento	510 bis
Financiación del terrorismo	576

Nota. Extraído de Circular 1/2016 de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

Asimismo, el régimen del artículo 129 CP es aplicado en los delitos previstos para personas jurídicas cuando se hayan cometido en el seno, con la colaboración, a través o por medio de

organizaciones carentes de personalidad jurídica, y es contemplado también para los siguientes delitos, ya reprochados con anterioridad en esta doble vía sancionadora por la Circular 1/2011 FGE:

Tabla 10. Lista de delitos contemplados conforme el artículo 129 CP a raíz de la reforma del CP de 2015.

Delitos	**Artículos CP**
Relativos a la manipulación genética	162
Alteración de precios en concursos y subastas públicas	262
Negativa a actuaciones inspectoras	294
Delitos contra los derechos de los trabajadores[13]	318
Falsificación de moneda	386.4
Asociación ilícita	520
Organización y grupos criminales y organizaciones y grupos terroristas	570 quater

Nota. Extraído de Circular 1/2016 de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

Finalmente, en caso de personas jurídicas de pequeñas dimensiones, según el artículo 31.bis 3 CP, podrán demostrar su compromiso ético mediante una razonable adaptación a su propia dimensión de los requisitos formales del apartado 5 del mismo artículo, en coherencia con las menores exigencias contables, mercantiles y fiscales.

En consecuencia, tras la LO 1/2015, el *debido control,* ahora *deberes de supervisión, vigilancia y control,* sigue atribuido a las personas físicas de las letras a) y b) del artículo 31.bis 1 CP y no a la propia persona jurídica, con lo cual los modelos de organización y gestión ni definen la culpabilidad de la empresa ni constituyen el fundamento de su imputación. Debido a la exclusión de la responsabilidad penal de la empresa ofrecida por estos modelos bajo determinadas condiciones, el objeto del proceso penal se extiende ahora también a la valoración de la idoneidad del modelo adoptado por la entidad (Circular 1/2016 FGE).

Además, por otro lado, tras la Reforma del Código Penal de 2015, la FGE publicó la Circular 8/2015 sobre los delitos contra la propiedad intelectual cometidos a través de los Servicios de la Sociedad de la Información, cuyo objetivo es establecer pautas para la interpretación y aplicación

13 Para un mayor análisis y debate acerca de los derechos de los trabajadores en materia de *compliance*, ver Gómez Martín, V. (2014). *Compliance* y derechos de los trabajadores. En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p. 421-458). Madrid: Edisofer.

de los nuevos tipos penales incorporados en la reforma, y, a su vez, de ofrecer soluciones y criterios de actuación respecto de algunas cuestiones jurídicas planteadas en los procesos incoados con anterioridad a la entrada en vigor de ésta. Así, algunos de los elementos clave a destacar en esta Circular son: la comunicación pública como elemento normativo del art. 270 CP; el ánimo de lucro comercial, requisito el cual ha sido sustituido por el de obtener un beneficio económico directo e indirecto; y el hecho de mantener fuera de persecución penal las conductas de los motores de búsqueda y de los usuarios.

2.2.4 *Compliance* penal

El análisis de riesgos y la prevención con respecto a los delitos de las personas jurídicas cobra un papel relevante para las empresas socialmente responsables, como así se pone de manifiesto en la Comunicación de la Unión Europea de 25 de octubre de 2011 sobre la Estrategia renovada de la Unión Europea para 2011-2014 sobre la responsabilidad social de las empresas, en su lucha contra el fraude y la corrupción dentro de este mismo concepto. Esta conveniente adopción de programas de prevención de delitos, en cuyo contenido se incorporan esquemas organizativos y protocolos dirigidos a este mismo fin, están alineados con la Responsabilidad Social de las Empresas (en adelante, RSE) y al mismo tiempo, pueden estar integrados en las estrategias y políticas de RSE de la empresa con el fin de buscar su implementación y mantenimiento en el tiempo. Asimismo, se deben reformular las cuestiones legales como oportunidades de negocio, puesto que es un factor crucial para lograr una ventaja competitiva de la ley (Klynveld Peat Marwic Goerdeler [KPMG], 2016; Peterson, 2013), mediante: compromiso a considerar la ley como un activo estratégico; selección de un marco adecuado para guiar ese compromiso; esbozo de acciones específicas para cumplir ese compromiso; implementación de las acciones elegidas (fomento de una mayor lealtad y reducción de rotación del personal); e conducción a mejoras a lo largo de la cadena de valor. En la RSE fundamentada en las empresas como ciudadano responsable (*good citizens corporations*), la ética de empresa juega también un papel fundamental, puesto que es la encargada de detectar los valores existentes, proponer de nuevos, y establecer el *management* adecuado para introducirlos en la empresa (Nieto Martín, 2015).

Por un lado, con la implantación de programas de prevención de riesgos penales se busca advertir qué riesgos penales son previsibles objetivamente y así adecuar medidas de control y

reacción ante su puntual ejecución, y por otro lado, se pretende atenuar o incluso exonerar a la empresa de su responsabilidad penal, aunque evidente es la no existencia de una herramienta garantizadora de riesgo 0 (Gallego Soler, 2014; Peterson, 2013). Por tanto, esta herramienta sirve para demostrar no encontrarse en un supuesto de irresponsabilidad organizada por parte de la organización por haberse llevado a cabo todos los medios a su alcance para prevenir el delito. En otras palabras, con la implementación de un *criminal compliance* en la empresa se pretende realzar el valor de la adquisición de conocimiento, puesto que se persigue asegurar mayor posesión de información por parte del órgano de dirección, el cual en empresas estructuralmente complejas suele estar al margen de la vida operativa (Montaner Fernández, 2015).

Los programas de *compliance* tienen su origen en los Estados Unidos, en pleno apogeo con la aprobación del *Chapter Eight*[14] de las *Federal Sentencing Guidelines for Organizations* (en adelante, FSGO) a partir del 1 de noviembre de 1991. Estos programas aparecen en un contexto caracterizado por la desconfianza hacia el poder empresarial y la creencia de una mayor eficacia conseguida por la autorregulación empresarial en lugar de la regulación estatal (Artaza Varela, 2013).

Según la United States Sentencing Commission (USSC, 2016), un programa eficaz de *compliance* debe implicar la actuación de la empresa con la diligencia debida, con el objetivo de detectar y prevenir delitos, además de promover una cultura organizacional estimulante de comportamientos éticos y respetuosos con la normativa. Para ello, como elementos básicos mínimos se requiere de:

• Establecimiento de códigos de conducta y procedimientos internos de cumplimiento. Aunque todos los interesados coincidan en la implicación de motivaciones éticas, cada actor enfatiza un motivo económico precedente de una postura ética diferente, identificando así una jerarquía aparente en la etiología de la responsabilidad ambiental corporativa (Bisschop, 2010). Son elementos clave de una cultura organizacional (Ethics & Compliance Initiative [ECI], 2016a): a) estrategia de la alta dirección *(tone from the top)* hacia el compromiso de hacerlo bien y poniendo en acción los valores organizacionales (por líderes y empleados); b) apoyo y refuerzo del supervisor abriendo comunicaciones a través y hacia abajo de la organización; c) capacidad para plantear inquietudes; d) ser responsable y responsabilizarse de sus actos (*accountability*); y e) presión de los

14 http://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8

otros. Por tanto, serían características de una cultura no ética (Ethics & Compliance Initiative [ECI], 2016b): a) pensamiento a corto plazo; b) identificación débil del empleado de la compañía, sus clientes o sus productos/servicios; c) indicios de "riesgo moral" (no alineación de incentivos y riesgos) y recompensa por mala conducta cuando produce ganancias comerciales a corto plazo; d) dificultad en hacer preguntar / cuestionar inquietudes y falta de equidad; e) estilo de gestión cuestionable; y f) presión irrazonable para cumplir.

• Órgano de gobierno informado adecuadamente sobre el contenido y extensión de los programas de *compliance,* y obligado a ponerlo en práctica de forma eficaz. Con el fin de garantizar esta eficacia, debe designar un miembro de la dirección para ser el *compliance officer.* Debe haber una delegación adecuada de aquellos aspectos relacionados con el cumplimiento legal por parte de la administración (Blumenberg y García-Moreno, 2014; Gómez-Jara Díez, 2012; Nieto Martín, 2015). El consejo directivo y la alta dirección necesitan capacitar y proveer adecuadamente recursos a las personas con responsabilidades cotidianas para mitigar riesgos y construir confianza organizacional; luego, *tone at the top* infunde a la organización una cultura de integridad (Deloitte, 2015). El *chief compliance officer* tiene la responsabilidad diaria de supervisar la administración de cumplimiento y los riesgos de reputación, creando así una ventaja competitiva para su empresa (Blumenberg y García-Moreno, 2014 ; Deloitte, 2015).

• Adopción de sistemas de auditoría y monitorización diseñados con el fin de detectar conductas delictivas de empleados y otros. A pesar de la adopción de programas de cumplimiento y el pago de buenos salarios sean estrategias sustitutas de un seguimiento perfecto, ambas pueden ser sustitutas en empresas pequeñas y complementarias en las grandes corporaciones cuando la tecnología de monitorización es imperfecta (Polidori y Teobaldelli, 2016). En este mismo estudio, se prevé poco probable la adopción de programas de monitorización cuyo coste sea alto y fijo por parte de pequeñas empresas. Para asegurar un ambiente de control efectivo, el proceso comienza con la implementación de controles apropiados, los cuales deben ser probados y monitorizados y auditados de forma regular, asegurando así su salud continua (Deloitte, 2015).

• Reforzamiento constante de estándares de conducta mediante formación continua de toda la plantilla de la empresa y adopción de un régimen sancionador. Estas actividades de formación y sensibilización crean consciencia sobre los riesgos a los cuales están expuestos y facilitan la tarea al órgano de *compliance* (Blumenberg y García-Moreno, 2014). En general, las regulaciones más eficaces son las sanciones legales creíbles y la certeza y severidad del descubrimiento informal por parte de otras personas significativas en la empresa (Simpson et al., 2013); luego, los resultados

destacan la simbiosis entre el control formal e informal, siendo necesaria una combinación de enfoques cooperativos y coercitivos para lograr mejores niveles de cumplimiento de las leyes por parte de las empresas (Yeager, 2016). El mayor riesgo de *compliance* es la deshonestidad, ya sea por pecados de omisión (e. g. no decir nada si se tiene sospecha de una actividad delictiva), por informes falsos, exageraciones de clientes, proyecciones surrealistas y optimistas sobre costos o entregas, etc., por este motivo en las empresas, por ejemplo, donde la seguridad es un alto riesgo, los procedimientos excelentes están incrustados en las prácticas de trabajo para mejorar el cumplimiento (ECI, 2016b). No obstante, se debe evitar el *hipercompliance,* puesto que un exceso de reglas y sanciones no conducirá a un lugar de trabajo más seguro (Rebbit y Erickson, 2016). Por otro lado, es necesario el reconocimiento de la diferenciación entre los distintos actores, empresas y niveles abordando el problema central teniendo en cuenta estas diferencias, pero sin permitir la paralización de la comunicación por culpa de éstas (Bisschop, 2010). Asimismo, dar incentivos, esto es, sanciones positivas (Nieto Martín, 2015), como sistema de compensación y promoción de recursos humanos puede ser un método eficaz, aunque los gerentes deben estar capacitados para saber por qué a las personas les gustan este tipo de estímulos y cómo haberlo (ECI, 2016b); luego, sus posibilidades de satisfacción serán mayores cuando está integrado dentro de la cultura organizacional. El uso de fondos para aumentar la certeza de las sanciones formales o de reputación puede ser más importante que financiar programas de cumplimiento voluntario (Rorie, 2015).

• Publicación del sistema de canales (*hotlines*) de denuncia mediante el cual el personal de la empresa puede denunciar conductas delictivas sin pavor a represalias por parte de la entidad. Estos sistemas de denuncias o *whistleblowing* (de denunciantes cívicos) deben cumplir con la normativa relativa a la protección de datos a fin de proteger la confidencialidad de la línea mediante la implantación de medidas de seguridad de alto nivel (Gómez-Jara Díez, 2012). En este sentido, la Agencia Española de Protección de Datos en su Informe Jurídico 0128/2007[15] se posicionó a favor de las denuncias confidenciales. En el II Congreso Nacional de Compliance, los ponentes coincidieron en no considerar como elemento suficiente por sí solo para poder aplicar la atenuante el hecho de contar con este canal (“El 'II Congreso Nacional de Compliance' hace incapié en la importancia de los canales de denuncia”, 2016). A pesar de la existencia de esta herramienta, en un 57% de las ocasiones son receptores de denuncias el supervisor o los *managers* y tan solo un 7% son reportadas por el *hotline* (Ethics & Compliance Initiative [ECI], 2015).

15 https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf

• Actualización periódica de los programas de *compliance* con el fin de evitar la comisión de conductas delictivas similares futuras. Para la evaluación del programa es importante documentar toda la actividad realizada por el mismo porque ayudará en cualquier investigación y además porque las conclusiones de ésta puede ayudar a prevenir posibles recortes en el programa en un futuro (ECI, 2016b); esta documentación podrá contener normativa interna de la empresa en materia de cumplimiento, o bien, mostrar la vida y funcionamiento diario del sistema (Nieto Martín, 2015), puesto que es aquello más interesante para el juez. Deben identificarse las amenazas estratégicas, los activos y las vulnerabilidades de los procesos y la efectividad actual de los controles de seguridad, puesto que ayuda a gestionar la evaluación de riesgos[16] y a adoptar controles de riesgo organizacionales, administrativos y técnicos (KPMG, 2016).

• Modelo de *compliance* personalizado teniendo en cuenta las particularidades de cada empresa en concreto *(tailoring),* puesto que los factores de riesgo de cada una son únicos (Blumenberg y García-Moreno, 2014). Una de las razones por la cual las personas son falibles con el riesgo es el *recency affect*, es decir, dar más prioridad a los primeros ítems de una lista y obviar los últimos (ECI, 2016b). Variables como el tamaño de la organización, su productividad y su poder de mercado son determinantes clave de si se previenen las conductas delictivas y de la estrategia de prevención utilizada, como por ejemplo supervisar a los gerentes o pagarles salarios más elevados (Polidori y Teobaldelli, 2016). También las actitudes de los empleados son indicadores clave de la salud de la organización y pueden ofrecer información temprana sobre áreas de debilidad o vulnerabilidad (Hess y Broughton, 2014). Las evaluaciones de riesgo no se refieren tan sólo al proceso, sino también a la comprensión de los riesgos a los cuales se enfrenta una empresa; luego, no se puede mitigar un riesgo si no se conoce de su existencia (Deloitte, 2015).

A todos estos elementos comunes a los programas de cumplimiento Nieto Martín (2015) añade:

• Protocolos de reacción: la denuncia de los hechos, la reparación o la colaboración con las autoridades públicas deben basarse en valores coherentes con los del resto del sistema de cumplimiento, fijándose de antemano cómo la empresa debe actuar en estas situaciones.

• Institucionalización: determinar a través de un sistema de delegaciones quiénes son los responsables de controles dicho riesgo. Se trata de determinar quién va a ocuparse de la supervisión

16 Para un análisis más exhaustivo acerca de la evaluación de riesgos, el punto 3 de la Lección IV, "Código ético, evaluación de riesgos y formación", en Nieto Martín, A. (2015). *Manual de cumplimiento penal en la empresa*. Valencia: Tirant Lo Blanch., Nieto Martín, A. (2015).

y coordinación de las áreas singulares de cumplimiento, responsabilizarse de la constante actualización del programa y gestionar sus elementos transversales.

El plan de respuesta y el conocimiento de una no total evitación de las violaciones legales mitigarán el nivel de interrupción de las operaciones diarias, además de reducir la tentación de dedicar recursos excesivos de la empresa a resolver cualquier cuestión jurídica; luego, los costos de incumplimiento superan claramente el costo del cumplimiento (Peterson, 2013). En conclusión, un programa de cumplimiento normativo eficaz está adaptado a las características de la organización y a los riesgos propios de su actividad, implementado efectivamente en la estructura organizativa de la entidad, y revisado y actualizado de forma periódica por un ente autónomo respecto del órgano de administración; luego, si la empresa cuenta con uno previamente a la comisión delictiva pone de manifiesto una gestión con la debida diligencia de sus propios riesgos. Por esta razón, la certificación sólo servirá para acreditar la eficacia del programa cuando ésta recopile evidencias acreditadas de una implementación efectiva del programa por ser el organismo certificador garante de independencia y profesionalidad (Neira Pena, 2016). Como ejemplo, el marco de Ética y Compliance de la empresa Deloitte, mostrado en el siguiente gráfico, reconoce como elemento central del programa una cultura ética y obediente, en el cual si ésta no apoya el desarrollo de la actividad empresarial basada en principios, todas las personas, procesos y tecnologías puestos en marcha para mitigar los riesgos de *compliance* no van a ser optimizados.

Tabla 11. Marco de Ética y Cumplimiento de la empresa Deloitte.

Nota. Extraído de Deloitte. (2015). *Building world-class ethics and compliance programs: Making a good program great. Five ingredients for your program.* Consultado 28 abril 2017, desde https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-g2g-compendium.pdf

Las empresas pueden optar por dos modelos de organización (Blumenberg y García-Moreno, 2014): basado en la vigilancia de los trabajadores y en el establecimiento de estrictas medidas de control, colocando a la entidad en una especie de "estado policial" y poniendo en riesgo los derechos fundamentales de estos; o bien, crear en la compañía una cultura de legalidad basada en dinámicas de transparencia e integridad (código de conducta como base), el cual previene de sanciones por conductas irregulares de sus empleados, asegura medidas de control de cumplimiento respetuosas con la normativa (e. g. selección de personal, control de pagos e instrumentos de pago, *due diligence* a la hora de contratar agentes comerciales), así como con los derechos de los trabajadores. La mejor manera efectiva de determinar el nivel óptimo de cumplimiento es usar una metodología consistente en la forma de un *compliance management system*, la cual permita un desarrollo coherente y una evaluación de las medidas de cumplimiento en términos de diseño, implementación y efectividad operativa (KPMG, 2016). Se trata de: 1) definir los requisitos; 2) evaluar y responder a las conductas de riesgo; 3) implementarlo en toda la empresa; 4) formar y orientar; 5) evaluar; y 6) remediar. Una de las metodologías más conocidas es la publicada por el Committee of Sponsoring Organizations of the Treadway Commission[17] (en adelante, COSO), la cual define un modelo común de control interno contra los cuales estas organizaciones pueden evaluar sus propios sistemas de control en relación a las operaciones, informes financieros y *compliance*.

Los programas de cumplimiento normativo penal, programas de *compliance* o *corporate compliance* son referidos en el Código Penal como «modelos de organización y gestión», a pesar de no haber ninguna definición legal establecida; aun así, existe cierta correspondencia de la legislación española con la praxis internacional. Estos programas recogen el plan de prevención de riesgos penales, los principios generales y las políticas de la organización ante tales riesgos, el ámbito y los responsables de su aplicación, y las actividades de control y supervisión para su correcta aplicación. De este modo, estos modelos de organización y gestión deben cumplir los siguientes requisitos legales (art. 31.bis 5 CP):

17 https://www.coso.org/Pages/default.aspx

1. Mapa de riesgos penales: identificar actividades en cuyo ámbito puedan ser cometidos los delitos a prevenir.

2. Código ético y protocolos de actuación: establecer protocolos o procedimientos definidores del proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas respecto de aquéllos.

3. Plan de acción de recursos financieros: disponer de modelos de gestión de los recursos financieros adecuados para impedir la comisión de delitos a prevenir.

4. Canal de denuncias: imponer la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

5. Sistema disciplinario: establecer un sistema disciplinario adecuado de sanciones para cuando se incumplan las medidas establecidas por el modelo.

6. Realizar una verificación periódica del modelo y su eventual modificación cuando se manifiesten infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, la estructura de control o en la actividad desarrollada en la cual se necesiten.

Aunque todavía no haya analizado los requisitos legales, el Tribunal Supremo ha sido tajante en la STS 154/2016, de 29 de febrero, la primera sentencia condenatoria a personas jurídicas, estableciendo como causa de justificación eximente de responsabilidad la presencia de "adecuados mecanismos de control" por formar parte de los elementos objetivos del tipo. Por su parte, la Circular 1/2016 FGE desglosa detalladamente cada uno de estos requisitos, expone el contenido obligatorio de un programa de cumplimiento normativo penal y, además, define cuáles deben ser los criterios a considerar para valorar la eficacia de dichos programas.

Para la elaboración, implementación y gestión de Programas de Compliance, disponer de herramientas tecnológicas, como *Complylaw*[18], *e-CAS*[19], o *GlobalSUITE*[20], entre muchas otras, facilita una solución eficaz en el establecimiento de una política apropiada de prevención frente a supuestos de riesgo penal y de cumplimiento normativo (nacional e internacional).

18 https://landings.wolterskluwer.es/complylaw/
19 https://complianceabogados.es/wp-content/uploads/2017/03/hojaPRODUCTO_eCAS.pdf
20 http://www.globalsuite.es/wp-content/uploads/2016/03/GlobalSUITE-Compliance-Penal.pdf

2.2.4.1 Criterios para valorar la eficacia del modelo y su calidad

La redacción legal no facilita su tarea al juez, aunque éste dispone de un margen de discrecionalidad en la valoración de la idoneidad del programa de cumplimiento y en la comprobación de la adopción y ejecución por parte del órgano de administración de estos modelos (Cugat Mauri, 2015). Según la Circular 1/2016, para valorar la eficacia de los modelos de organización y gestión, se atiende a:

• Su regulación debe interpretarse de manera que el régimen de RPPJ no quede vacío de contenido y sea de imposible apreciación en la práctica.

• Su objeto es, además de evitar la sanción penal, promover una verdadera cultura ética corporativa, de tal modo que su verdadera eficacia reside en la importancia adoptada por éstos en la toma de decisiones de los dirigentes y empleados y en qué medida constituyen una verdarera expresión de cumplimiento. Así, en el estudio realizado por Sturdivant y Ginter (1977) las empresas socialmente responsables prevalecieron por una notable mejora de sus resultados económicos y sus *managers* fueron quienes se preocupaban más por los derechos individuales y por una mayor capacidad de respuesta a las demandas sociales y económicas de cambio.

• Las certificaciones sobre la idoneidad del modelo expedidas por empresas o asociaciones evaluadoras y certificadoras de cumplimiento de obligaciones, mediante las cuales se manifiesta el cumplimiento del modelo de condiciones y requisitos legales, podrán apreciarse como un elemento adicional más de la adecuación del modelo pero en modo alguno acreditan su eficacia, ni sustituyen la valoración competente y exclusiva al órgano judicial.

• Cualquier programa eficaz depende del inequívoco compromiso y apoyo de la alta dirección para trasladar una cultura de cumplimiento al resto de la compañía. Si son los principales responsables de la entidad quienes incumplen el modelo de organización y de prevención o recompensan o incentivan, directa o indirectamente a los empleados que lo incumplen, difícilmente puede admitirse la existencia de un programa eficaz, cuyo reflejo es una verdadera cultura de respeto a la ley en la empresa, de tal modo que, en estos casos, se presumirá de la ineficacia del programa. No obstante, existe una clara confianza en los líderes senior de la organización, puesto que un 91% de los hombres y un 86% de mujeres creen en la aportación satisfactoria de información por parte de éstos sobre las distintas ocurrencias en la empresa, así como un 94% de los hombres y un 89% de mujeres creen en ellos como un buen ejemplo a seguir (ECI, 2016a).

• La responsabilidad corporativa debe ser más exigente en los supuestos en los cuales la conducta criminal redunda principalmente en beneficio de la sociedad que en aquellos otros en los

cuales dicho beneficio resulta secundario o meramente tangencial al directa y personalmente perseguido por el delincuente. En estos casos, cabe exigir a la persona jurídica la adecuación de la contratación o promoción de quién delinquió a unos protocolos y procedimientos garantes de altos estándares éticos en la contratación y promoción de directivos y empleados.

• Se concederá valor especial al descubrimiento de los delitos por propia corporación. Detectada la conducta delictiva por la persona jurídica y puesta en conocimiento de la autoridad, deberán solicitar la exención de pena al evidenciarse no solo la validez del modelo sino su consonancia con una cultura de cumplimiento corporativo.

• Si bien la comisión de un delito no invalida automáticamente el modelo de prevención, este puede quedar seriamente en entredicho a tenor de la gravedad de la conducta delictiva y su extensión en la corporación, el alto número de empleados implicados, la baja intensidad del fraude empleado para eludir el modelo o la frecuencia y duración de la actividad criminal.

• También se atenderá al comportamiento de la corporación en el pasado. Se valorará positivamente la firmeza de la respuesta en situaciones precedentes y negativamente la existencia de anteriores procedimientos penales o en trámite, aunque se refieran a conductas delictivas diferentes de la investigada, o previas sanciones en vía administrativa.

• Las medidas adoptadas por la persona jurídica tras la comisión del delito pueden acreditar el compromiso de sus dirigentes con el programa de cumplimiento. Así, la imposición de medidas disciplinarias a los autores o la inmediata revisión del programa para detectar sus posibles debilidades, la restitución y la reparación inmediata del daño, la colaboración activa con la investigación o la aportación al procedimiento de una investigación interna, sin perjuicio del posible valor atenuante de alguna de estas actuaciones. Operarán en sentido contrario el retraso en la denuncia de la conducta delictiva o su ocultación y la actitud obstructora o no colaboradora con la justicia.

Por otro lado, aunque a veces se formulan conjuntamente con los elementos del programa, los criterios de calidad podrían condensarse en los siguientes aspectos (Nieto Martín, 2015):

• Implicación de los directivos. Si los dirigentes no se comprometen, no asumen una responsabilidad directa y visible en la ejecución del programa, éste no será del todo efectivo. El *tone from the top* o *tone from the middle* debe mostrarse en el día a día del programa. También deben ser los responsables de vigilar la implantación efectiva de las medidas de cumplimiento.

• Participación de los trabajadores y de los grupos de interés. La eficacia de un sistema de cumplimiento equivale en gran medida a su legitimidad.

• Coherencia. La política de cumplimiento debe ser coherente con la cultura de la empresa, y las políticas y prácticas en materia de recursos humanos.

• Independencia, capacidad y formación de los responsables de cumplimiento. Deben tener la cualificación necesaria para abordar esta tarea, pero sobre todo un alto grado de independencia, indicador de eficacia y solvencia del programa, dentro de la entidad.

• Recursos adecuados. Un programa de cumplimiento sólo es eficaz si cuenta con recursos materiales y humanos adecuados. Se debe evitar sobredimensionar el departamento de cumplimiento, y crear controles innecesarios y exagerar riesgos, puesto que pueden deslegitimar el programa.

• Vigencia del programa. Los empleados de todos los niveles deben conocer sus específicas funciones y obligaciones dentro del sistema. También se demuestra su vigencia por que las sanciones disciplinarias son realmente impuestas y ejecutadas. La existencia de controles sobre el papel no garantiza efectivamente el respeto a éstos.

2.2.4.2 Beneficios de la implantación del modelo

En una entrevista realizada al sr. Bonatti Bonet (Círculo de Mujeres de Negocios TV, 2013), el abogado penalista comenta los beneficios del administrador cuando tiene implantado un modelo de compliance:

• Los empresarios tienen más claro qué riesgos asumen con su toma de decisiones. Permite ser conscientes de las consecuencias y evaluar los riesgos, así como priorizar decisiones.

• Evitar riesgos latentes, del entorno, de consecuencia directa. Con un plan de prevención se coordinan las diferentes obligaciones legales, tales como prevención de riesgos laborales, protección de datos, prevención de blanqueo de capitales, entre otros. Después de un programa de prevención, los riesgos estáticos dejan de existir.

• Se consigue alinear a toda la empresa en una filosofía de seguridad. La empresa es más consciente de los riesgos del día a día, de la importancia de los riesgos laborales, de la protección de datos de la empresa, de la confidencialidad, de la prevención de blanqueo de capitales.

• Otorgamiento de un valor importante a nivel de protección de la marca (e. g. actuación para evitar la RPPJ cuando un empleado hace uso personal del ordenador de la empresa para una búsqueda de archivos de carácter pedófilo).

• Añade valor a la empresa en términos de reconocimiento, más calidad y más competencia en el mercado.

2.2.4.3 *Compliance Officer*

La figura del *compliance officer*[21] no se encuentra definida en nuestro ordenamiento jurídico, motivo por el cual es de difícil valoración su responsabilidad penal (Montaner Fernández, 2015); el Código Penal tan solo prevé las funciones de supervisión, vigilancia y control (art. 32.bis 2.2º CP), cuyo ejercicio debe realizarse con poderes autónomos de iniciativa y control pero solamente en las grandes corporaciones darán lugar a departamentos de *Compliance.* Aun así, no van a existir dos departamentos iguales ni los responsables de cumplimiento van a tener las mismas funciones en todas las empresas. En resumen, tan solo se podrá hablar de funciones de cumplimiento. No obstante, el 52% de las empresas españolas tienen implantado un programa formal de ética empresarial y cumplimiento normativo y, de estas, el 43% afirma contar con un *compliance officer* como responsable de su programa (PwC, 2016).

Respecto de los órganos de cumplimiento, existen dos modelos (Blumenberg y García-Moreno, 2014): el primero, previsto en las US Sentencing Guidelines y más extendido en la práctica, busca blindar al órgano de cumplimiento habiéndolo depender única y directamente del Consejo; y el segundo, recogido en el Código Penal, pretende la independencia del órgano de cumplimiento incluso del propio Consejo, puesto que entre sus tareas se encuentra supervisar a los directivos y administradores de la entidad.

El Código Penal en su artículo 31.bis deja abierta la posibilidad de ser funciones asumidas por departamentos preexistentes, tales como el de auditoría interna, sin haber necesidad de crear ninguna figura nueva dentro de la empresa; luego, puede no existir una figura de tales características sin implicar el incumplimiento del deber de control ejercido por la empresa (Lascuraín Sánchez, 2014). Asimismo, el artículo 31.bis 5 CP permite delegar estas funciones en el Órgano de Administración cuando se trate de personas jurídicas las cuales puedan tener cuenta de pérdidas y ganancias abreviada (art. 258 LSC). Es necesario destacar la independencia de todo oficial de cumplimiento con respecto del Órgano de Administración, aunque debe contar con los

21 Para un mayor análisis y debate acerca de la figura del *compliance officer*, ver Lascuraín Sánchez, J.A. (2014). Salvar al oficial Ryan (Sobre la responsabilidad penal del oficial de cumplimiento). En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p. 301-336). Madrid: Edisofer.

recursos suficientes para conseguir la eficacia del modelo de prevención de delitos (Gallego Soler, 2014). En efecto, siempre y cuando no se esté ante supuestos de adaptación dolosa a la conducta delictiva de terceros, son muy reducidas las posibilidades de atribución de responsabilidad penal a esta figura por incumplimiento de sus funciones (Montaner Fernández, 2015).

El oficial de cumplimiento, individual o colegiado, debe tener una formación acorde con el contenido de aquellos riesgos de los cuales va a advertir, prevenir y reaccionar (Gallego Soler, 2014). Por tanto, va a ser una figura de apoyo a la función de control genérica del empresario, no como sujeto delegado del empresario sino como profesional privado con determinados conocimientos técnicos relacionados con la función de supervisión encargado de llevar a cabo (Montaner Fernández, 2015).

Inicialmente, a esta figura le compete (Dopico Gómez-Aller, 2013): a) diseñar del programa de prevención, cuya aprobación debe ser realizada necesariamente por la dirección de la empresa y debe cumplir los estándares de calidad propios del sector de actividad; b) implementar el programa para conseguir los fines preventivos; c) controlar y hacer el seguimiento del programa, y establecer sus reformas; d) si no hay previsión de una gestión externa del canal de denuncias, está obligado a investigar y reportar sobre éste; en caso contrario, debe estar informado puntualmente de sus resultados y tiene la obligación de reportar sobre ellos a los directivos (Nieto Martín, 2013); y e) informar de aquellos riesgos generadores de responsabilidad penal relevantes para la posterior corrección de conductas o situaciones detectadas (Silva Sánchez, 2013). Por el contrario, no le compete la ejecución material de hechos concretos de cumplimiento, puesto que el oficial de cumplimiento de normal tiene capacidad y deber de control y supervisión pero no así competencias ejecutivas; luego, resulta necesaria la contemplación de la delegación funciones concretas a terceros (Robles Planas, 2013).

Los oficiales de ética y cumplimiento demuestran una aparente legitimidad de su papel visto desde fuera de la organización pero también deben demostrarla de sí mismos a nivel interno a través de tácticas distintas (Klebe Treviño, den Nieuwenboer, Kreiner, y Bishop, 2014): *making the business case* (intentar demostrar el encaje de su trabajo con la filosofía de maximización de accionistas dominante, de valor instrumental para lograr el éxito empresarial); *relabeling ethics and compliance* (intentar influir en la legitimidad moral y cognitiva, es decir, la primaria compartida);

leveraging synergies between ethics and compliance (aprovechamiento de las sinergias entre su trabajo y la cultura y valores de la organización); y *creating trusting connections* (invertir en la creación de relaciones personales, positivas, confiables y puramente procedimentales con el personal de la organización). Por otro lado, Hess y Broughton (2014) recomiendan a estas figuras considerar formas de construir prácticas éticas de toma de decisiones en sus empresas desde abajo hacia arriba y hacia afuera, y al mismo tiempo en estrecha colaboración con los oficiales de riesgo, con el fin de encontrar maneras de integrar las medidas de cultura y otros indicadores de ética organizacional en los programas de gestión de riesgos.

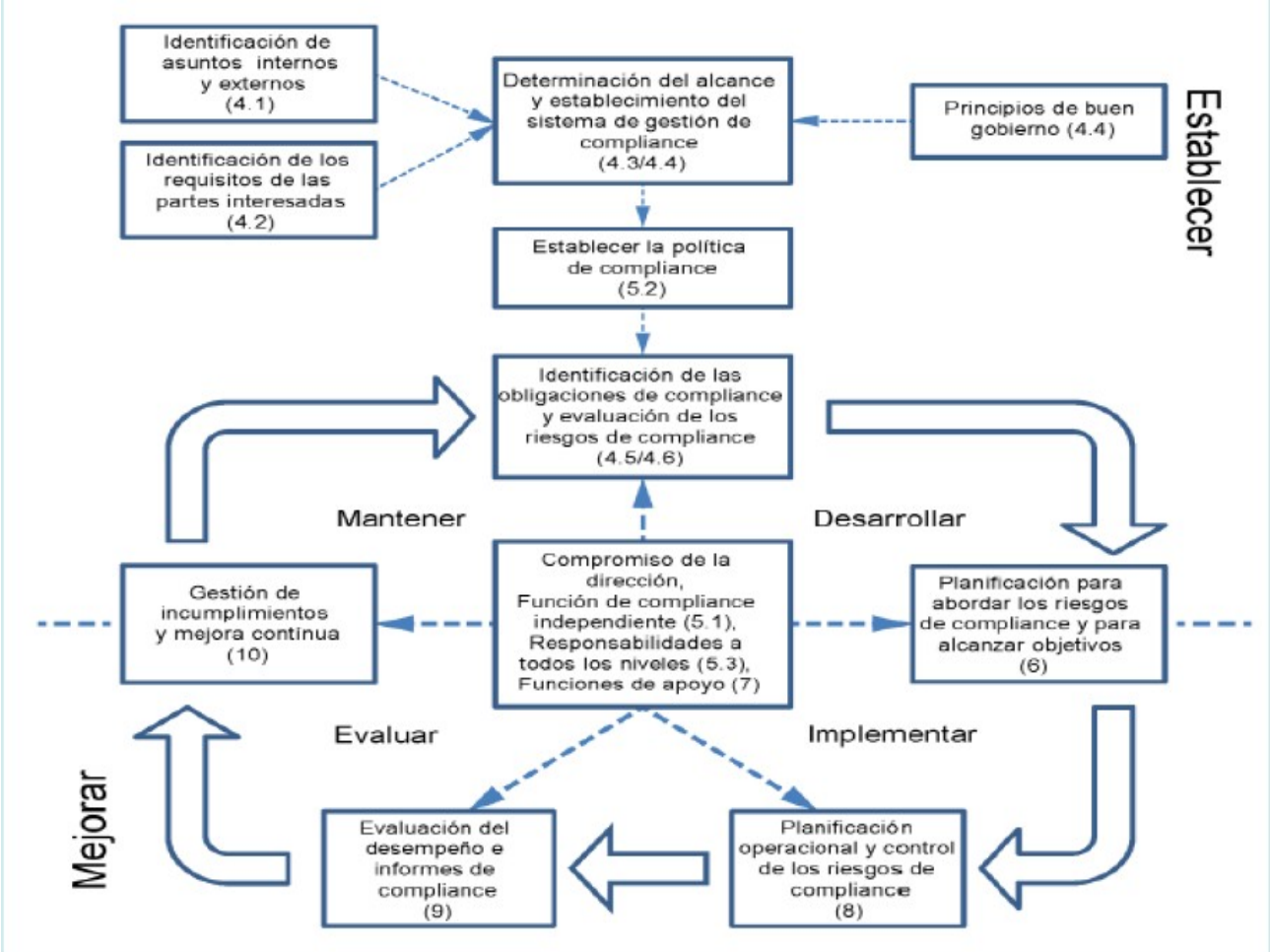
2.2.4.4 Normalización y estandarización

Respecto de la normativa internacional, se debe atender a la norma ISO 19600[22] sobre Compliance Management Systems, cuyo contenido recoge buenas prácticas y recomendaciones para ayudar a las organizaciones a desarrollar un sistema de gestión, cuya función sea identificar, controlar y cumplir con los requisitos legales requeridos; luego, se pretende homogeneizar los sistemas de gestión para la prevención de delitos en las empresas. A pesar de ofrecer esta amplia gama de prácticas para cada organización independientemente de su tamaño, las PYME siguen encontrándose con el desafío de cómo validar su sistema de compliance. El cumplimiento normativo y los programas de cumplimiento son fenómenos surgidos en las grandes empresas, por eso uno de los principales problemas de *compliance* es no haber determinado cuáles son las medidas de organización idóneas en las PYME, sujetas en muchos sectores a iguales requisitos legales que las grandes (Nieto Martín, 2015). Asimismo, la norma ISO 37001[23] sobre Anti-Bribery Management Systems utiliza la certificación como mecanismo para orientar el diseño e implementación del modelo y para acreditar la concordancia entre el resultado del trabajo de la empresa con el estándar. Esta última norma se adelanta a la publicación de la UNE 19601[24] sobre Sistemas de Gestión de Compliance Penal en España, pendiente aún de publicación oficial, la cual pretenderá ofrecer una pauta certificable para los requerimientos penales del modelo. Así, este triángulo normativo facilitará a las PYME un grupo de instrumentos cualificados y flexibles, facilitadores del correcto diseño e implementación de los Sistemas de Compliance.

22 https://www.iso.org/standard/62342.html
23 https://www.iso.org/standard/65034.html
24 http://www.aenor.com/revista/pdf/feb17/14feb17.pdf

El Sistema de Gestión de Compliance referido en la ISO 19600, basada en el método de los cuatro-pasos usado para el control y la mejora continua de los procesos, es decir, el *plan-do-check-act* (Ernst & Young [EY], 2015), desarrolla una cultura de la integridad en todos los aspectos de la empresa: gobierno corporativo, finanzas, comercial, legal y riesgos. Así, según Cerem Business School (2015), las mejorías se otorgan a un nivel interno, puesto que la plantilla tendrá unas bases cuyo uso servirá para desempeñar la acción de la empresa de manera óptima (e. g. código de conducta), y a nivel externo, dado que la reputación de la empresa aumentará por las buenas prácticas observables en su desempeño diario (e. g. confianza con la empresa). En resumidas cuentas, serán los grandes beneficios de un meticuloso cumplimiento de la legalidad la supresión de la arbitrariedad y la discrecionalidad. Siguiendo este estándar, el modelo de *compliance* podría estructurarse de la siguiente manera:

Tabla 12. Relación entre los elementos de la gestión del *compliance* de acuerdo con la ISO 19600.



Nota. Extraído de Bleker, S., y Hortensius, D. (2014). ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT. *Journal of Business Compliance,* 2, 1-12. Consultado 27 abril 2017, desde

http://www.esv.info/download/zeitschriften/BUCO/leseprobe_2.pdf , Intercer. (n.d.). *UNE-ISO 19600:2015. COMPLIANCE: Implantación del Sistema de gestión Compliance*. Consultado 27 abril 2017, desde http://www.intercer.es/files/MODELO%20CONSULTORIA%20ISO%2019600%20COMPLIANCE.pdf , y TÜV Rheinland. (2016). *UNE-ISO 19600 SISTEMAS DE GESTIÓN DE COMPLIANCE*. Consultado 27 abril 2017, desde https://www.tuv.com/media/spain/actos/2006/20160519_cogag/ISO_19600_Compliance_Management_System_rev_1.pdf

La implementación de la ISO 19600 tiene como potenciales beneficios (EY, 2015): a) simplifica el enfoque; b) incorpora con cierta flexibilidad elementos críticos de otros estándares aceptados; c) proporciona una razón para revisar su programa; d) demuestra a los reguladores la búsqueda de su organización de alineación con los últimos estándares; e) el estándar es de orientación personalizable para poderse beneficiar de ello todas las organizaciones y sigue un enfoque basado en el riesgo. Los riesgos identificados, obligaciones de cumplimiento, son la base para el establecimiento e implementación de controles; y, d) tiene como objetivo crear una cultura organizacional en la cual el cumplimiento se convierta en la norma general.

Por otro lado, aunque todavía no ha sido publicada oficialmente, la norma UNE-19601 destaca por su aportación en la estandarización de la terminología utilizada en Compliance Penal (Cuevas Sarmiento, 2017): la Política de Compliance Penal y el Sistema de Gestión. En el primer caso, se trata de un documento marco facilitador de un contexto idóneo para la definición, revisión y consecución de los objetivos del *compliance*, convirtiéndose en la traducción del *tone at the top.* Para su realización, las empresas deberán ayudarse de asesores externos o de un *compliance officer* con conocimientos técnicos. Deberá fijar el entorno de la empresa, concretar la legislación penal vigente aplicable y reconocer aquellos ámbitos en cuyo entorno puedan ser cometidos los delitos a prevenir. En el segundo caso, se trata de un conjunto de elementos de una empresa, interrelacionados o interaccionados con el fin de medir y precisar el nivel de consecución de objetivos del *compliance*, así como las políticas, procesos y procedimientos para conseguirlos. Se compone de evaluaciones de riesgos penales y controles existentes, modelos de gestión, protocolo de conservación de evidencias, y de objetivos específicos sobre cualquier bloque normativo, cuyo impacto pueda ser relevante. Mientras la política de *compliance* permite a la alta dirección u órgano de gobierno fijar las pautas, el Sistema de Gestión de Compliance es un componente dinámico construido mediante la acción de la organización y, por tanto, ambos deben coexistir. Asimismo, sobre dicha norma, Bonatti Bonet (2017) ofrece una exploración más detallada aunque, a grandes rasgos, la misma exige como factores internos y externos relevantes mínimos a considerar para

lograr los objetivos de *compliance*: i) tamaño y estructura de la organización; ii) ubicaciones y sectores donde opera; iii) naturaleza y complejidad de sus actividades y operaciones; iv) entidades sobre las cuales ejerce control; v) miembros de la organización y sus socios de negocio; vi) naturaleza y extensión de las relaciones con funcionarios públicos; y vii) obligaciones y compromisos legales, contractuales o profesionales.

2.2.4.5 Retos del *compliance*

Uno de los mayores retos del *compliance* es la gestión del riesgo de *compliance* de terceros. De hecho, más de una tercera parte de los negocios no identifican formalmente el grave riesgo de terceros (Klynveld Peat Marwic Goerdeler [KPMG], 2015). En términos legales, existen dos piezas, ambas prescribiendo la obligación de las organizaciones de aplicar procedimientos de diligencia debida basada en el riesgo sobre terceros cuyos servicios los realizan con o para su nombre: US Bribery Act[25] y US Foreign Corrupt Practices Act[26].

La mayoría de violaciones de cumplimiento provienen de comportamientos humanos, siendo estos una de las mayores prioridades de regulación. En un contexto donde la actividad legal es creciente y los *stakeholders* expresan su creciente intolerancia hacia actitudes corporativas pobres, las firmas están pagando por las malas conductas de los empleados.

La amenaza interna, es decir, los riesgos de cumplimiento desde dentro de la organización, evidencia los ataques más devastadores, los cuales pueden ser de forma intencional (fraude) o no intencional (negligencia o accidente). De hecho, el fraude interno, con un 67% del cual un 80% es cometido por personal interno con acceso autorizado a datos, es más frecuente que el fraude externo, con un 33% (Winterman, 2016), siendo el más aumentado el fraude relacionado con la fuga de información de carácter confidencial. Los ataques perpetrados por *insiders* (individuo autorizado con privilegios de acceso roba datos) para robar información pueden estar motivados, frecuentemente por más de uno a la vez, por dinero, ideología, coerción y ego (Trend Micro, 2015). Las características más comunes de los defraudadores son hombres, de 41 a 50 años, con estudios universitarios, ostentando cargos intermedios y con más de 10 años de antigüedad en la empresa (PwC, 2016). Este tipo de amenazas son más complicadas de asesorar (KPMG, 2016), puesto que

25 https://www.gov.uk/government/publications/bribery-act-2010-guidance
26 https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

existe menos tecnología en comparación a las amenazas externas, hay mucha más gente implicada y está orientado al proceso, por tanto, detectar y manejar estos requerimientos va a necesitar de una verdadera coordinación y una buena cultura organizacional. Los factores fomentadores de este tipo de amenazas son (Winterman, 2016): connivencia dirección/empleados/terceros; excesiva presión por alcanzar objetivos corporativos; falta de control por parte de la dirección; inadecuación o inexistencia de mecanismos de control interno; y cambios regulatorios o de procesos internos. Aplicando el modelo de vinculación social de Hirschi (1969), el cual incluye como elementos básicos el apego, el compromiso, la participación y la creencia, Sims (2002) intenta explicar la mala conducta específica del empleado de romper reglas éticas. Así, los resultados indicaron poder ser utilizados el apego, medido por la satisfacción en el trabajo y de la organización, y la participación, ligada a la permanencia en la empresa, para comprender mejor esta posible ruptura de reglas.

Otro gran reto es la protección de datos con la introducción del nuevo Reglamento General de Protección de Datos (en adelante, GDPR), de obligado cumplimiento para todas las organizaciones de los Estados Miembro a partir de 2018. Esta normativa deberá ser un punto clave en la agenda de las empresas, puesto que va a suponer un gran impacto en la privacidad y la protección de datos, por (KPMG, 2016):

• Sanciones mayores para el no cumplimiento.

• Obligación de notificar una brecha de información dentro de las 72 horas posteriores a la consciencia de la existencia del suceso, así como también a aquellos sujetos quienes se vean afectados por estos datos, conllevando por un lado haber de dar una mayor importancia a los procesos y tecnología para gestionar estas brechas de información en lugar del seguimiento, y por otro lado, el daño en la imagen y la reputación de la empresa conllevado.

• Protección de datos por diseño, es decir, las organizaciones necesitarán adecuar medidas y herramientas organizacionales apropiadas para la protección de datos y demostrar la constante revisión y actualización de estas. Asimismo, necesitan demostrar el procesamiento de datos de carácter personal tan sólo cuando sea estrictamente necesario.

• El ciclo de vida de la gestión de los datos tendrá fecha límite porque el reglamento acoge el derecho de un sujeto a pedir la eliminación de todos sus datos, siendo las organizaciones generalmente responsables de buscar y borrar todos los datos personales relevantes relacionados con el sujeto concreto, tanto de la propia organización como de aquellos datos compartidos con terceros.

Existe otro reto sobre cómo transformar los datos en ideas útiles (KPMG, 2016), es decir, usar el análisis de datos en aquellos riesgos hasta el momento desconocidos, por ejemplo, con modelos estadísticos avanzados basado en tiempo real o para buscar patrones. Esto permitiría al *compliance officer* pasar más tiempo en tareas generadoras de mayor valor y, por tanto, obtener un mejor y más eficiente *compliance*.

Finalmente, como reto futuro, o no tan futuro, desde una perspectiva de seguridad, los accesos remotos al servidor para mejorar las condiciones de trabajo de los empleados promocionando un saludable balance de vida de trabajo mientras se intenta salvar a la compañía, además de costar dinero, puede causar una pérdida de control de datos confidenciales. Un ejemplo de ello sería el BYOD o *Bring Your Own Device* (Eriksen-Jensen, 2013), una política empresarial consistente en el acceso por parte de los empleados a los recursos de la empresa a través de sus dispositivos personales de uso privado. En relación a los riesgos de seguridad tecnológica, los empleados deben ser educados para fortalecer su conciencia de seguridad IT y enseñarles cómo reducir los riesgos, por eso la decisión y actuación de la alta dirección es un factor clave, además del comportamiento de los *insiders* y su conciencia, pues también pueden aumentar o disminuir los riesgos (Lin, 2014).

3. Resultados

En este tercer apartado se pretenderá contrastar la documentación bibliográfica obtenida con la realización de las tres entrevistas a profesionales de la materia, con el fin de realizar una mayor aproximación a la problemática sufrida por las empresas en la implementación del modelo de *compliance* en la búsqueda de su eficacia, haciendo especial mención a las PYME y a las TIC. Por otro lado, se pretende recopilar algunas medidas básicas en la prevención y monitorización de las TIC. Finalmente, se discutirá hacia dónde se dirige el *compliance* en términos de retos futuros. Todo ello conformará el valor añadido del trabajo (Anexos I/II/III).

3.1 Importancia de la eficacia del modelo de cumplimiento normativo

En el transcurso del segundo bloque del marco teórico se ha hablado de cuáles son los elementos clave para un modelo de *compliance* y sobre qué se entiende por eficacia y calidad del modelo. Consecuentemente, la primera pregunta a plantearse debería ser ¿Qué conlleva y qué significa tener implantado un modelo eficaz de *compliance*?

El modelo de cumplimiento normativo nace con el fin de entender la situación en la cual se encuentra la empresa, esto es, aparece con el objetivo de aprender a interpretar los códigos éticos, la responsabilidad social corporativa y el diseño de la cultura empresarial. La persona jurídica crea peligros a consecuencia o inherentes a su propia actividad empresarial, por tanto, se busca responsabilizar a la empresa cuando no se ha dotado de las suficientes medidas no facilitadoras del delito (fenómeno de la irresponsabilidad organizada relativa a la delincuencia corporativa), es decir, no ha neutralizado la potencialidad criminógena de ciertas dinámicas de grupo. Por ello, en este fundamento jurídico de la responsabilidad penal corporativa de reducir delitos se busca el mejor resultado jurídico exigible a la empresa, generando menos costes para ésta. En resumen, un *corporate compliance program* debe tener en cuenta la reducción de los riesgos (minimizar el impacto del hecho delictivo sucedido, aunque no se prevendrá el delito en su totalidad – riesgo 0 inexistente –) y la autorregulación regulada por parte de la empresa (demostrar las medidas impuestas para limitar los riesgos). Así, será considerado un defecto de organización cuando la empresa favorezca o incentive el riesgo de comisión de determinados delitos.

Actualmente, se hace patente la falta de jurisprudencia acerca de jueces valorando qué modelos de *compliance* son adecuados y cuáles no (las pocas sentencias habidas son sencillas,

puesto que suelen ser a empresas sin ningún plan de *compliance*). Así lo transmitieron los tres entrevistados. El hecho anterior, sumado al de no haber en España ningún tipo de empresa, privada o pública, certificadora de estos modelos para dar garantía de su efectividad, nos lleva a una situación de desinformación y desorientación respecto de una correcta implementación del modelo. Lamentablemente, por ahora no hay forma de saberlo exactamente ni tener la certeza de ello.

Por el momento, solamente se hace hincapié en quién va a valorar la validez e idoneidad del modelo. Así, la empresa deberá demostrar al juez la excepcionalidad del delito en la prueba procesal, esto es, el cumplimiento de su programa de *compliance* con todas las medidas adecuadas y razonables para la prevención de ese delito concreto, aunque quien haya podido cometer o haya cometido el delito haya eludido todos los controles eficazmente. Para ello, la empresa se deberá enfrentar a las dificultades para descubrir el delito, a aquellas para identificar a los partícipes del delito, y a aquellas para perseguir y recuperar los efectos del delito. Pero, ¿cómo va a proceder exactamente para adoptar un modelo adecuado de cumplimiento?

Por un lado, una empresa debe disponer de un modelo de cumplimiento normativo personalizado. Esto implica una individualización del modelo: un modelo para una empresa concreta de un tipo concreto, cuya actividad empresarial pertenece a un sector determinado del mercado. Por tanto, dos empresas no van a tener el mismo modelo de cumplimiento; luego, no sirve de nada comprar un modelo de *compliance* a otra empresa que ya lo tenga implantado en la suya y le funcione porque, como se acaba de mencionar, el modelo debe tener las particularidades propias de la empresa concreta, debe estar adaptado a las problemáticas de su actividad empresarial, así como a sus concretos riesgos. En otras palabras, debe estar adaptado al objeto social, dimensión y estructura de la persona jurídica.

Por otro lado, aunque parezca obvio, el modelo de cumplimiento normativo debe prevenir los delitos establecidos por el Código Penal español en los cuales puede ser responsable penalmente una persona jurídica, y no otros. Esta especificidad es totalmente necesaria, puesto que de nada servirá ante un juez tener implementado en una empresa española un modelo de *compliance* comprado (ya sea para reducir costes o para evitar tener un modelo alejado de los estándares de *compliance*), aunque sea con una gran cantidad de dinero, a una empresa extranjera porque se entenderá el delito prevenido con otra legislación diferente a la española y eso no es competencia de

ningún juez español. Esta práctica suscita serias reservas sobre la propia idoneidad del modelo adoptado y el verdadero compromiso de la empresa en la prevención de conductas delictivas. Al Derecho Penal no le va a interesar tanto una certificación para acreditar la eficacia del modelo como la adecuada prevención del delito concreto llevada a cabo por el mismo.

En resumen, sin duda muchas empresas se han dotado o se dotarán de completos y costosos modelos de cumplimiento con la única finalidad de eludir el reproche penal, pero más allá de su adecuación formal tal y como está establecida en el Código Penal, tales programas deberán enfocarse a promover una verdadera cultura ética corporativa de respeto a la normativa, donde la comisión de un delito conforme un suceso accidental y la exención penal, una consecuencia de dicha cultura. De esta manera, la Circular 1/2016 FGE y Nieto Martín (2008) atienden a la valoración de estas medidas previstas en el modelo con la finalidad de valorar el nivel de compromiso con el cumplimiento. No obstante, se sigue corriendo el riesgo en el seno de la organización de percibir estos programas como una garantía certera frente a la acción penal.

Es muy importante querer hacer las cosas bien y tener predisposición a ello. Esta cuestión enlaza con el compromiso de la alta dirección (*tone at the top*) y la cultura organizacional, ambos pilares determinantes del éxito y eficacia de un modelo de cumplimiento. En el modelo de organización y gestión, la realidad merecedora de ser protegida es la transparencia de la estructura organizativa, ya que dicho modelo no es un valor en sí mismo para la empresa sino un instrumento apto para alcanzar dicha estructura transparente penalmente exigible. Un programa eficaz dependerá del apoyo e innegable compromiso de la alta dirección de la compañía, puesto que en caso de ser el autor del delito un administrador o un alto directivo de la corporación, se pone en entredicho la seriedad del programa en revelarse el menor compromiso ético de la sociedad. Por este motivo, se presumirá de programa ineficaz cuando un alto responsable de la compañía participe, consienta o tolere el delito. A su vez, este es un punto donde el programa flaquea, así se remarcó en la entrevista (Anexo I), puesto que se entiende al órgano de administración como el corazón de la empresa y éste no se va a controlar a sí mismo; luego, en este caso, no hay solución posible.

3.2 Problemática relativa a la implementación diaria del modelo de *compliance*

Cada vez más, en esta búsqueda de un mundo transparente donde abunda un gran volumen de regulaciones, a veces contraproducente, las empresas están más presionadas y obligadas a acreditar

constantemente un buen gobierno corporativo y un buen funcionamiento en el transcurso de la actividad empresarial. Se hace patente el incremento de empresas pidiéndose entre ellas el código de conducta o, de alguna manera, la acreditación certificadora de estar implementando un plan de *compliance* en su organización, aunque sea cada una a su propia medida o simplemente tenga los requisitos mínimos básicos establecidos en el Código Penal. Sin embargo, estos códigos de conducta no parecen ser suficientemente sólidos ni estar instaurados en su completa totalidad; tan sólo alrededor de un 50% de los programas de ética empresarial y cumplimiento normativo cuentan, entre otras medidas, con un código de conducta, cuya cobertura abarca áreas claves de la política de riesgo, y establece valores de la organización, de forma clara y entendible, así como los comportamientos esperados de sus miembros (PwC, 2016).

Principalmente, el problema central reside en la no concienciación de los delitos por parte de las empresas. Claramente, éstos son una cuestión definida como "ésto aquí no pasa" o "aquí en la empresa todos somos de confianza, nos conocemos y nunca va a pasar nada", incluso a veces la pregunta "¿alguna vez se ha cometido algún delito en esta empresa?", asusta. Este asunto está totalmente sesgado, es erróneo y está equivocado. Esta primera reacción, aparecida en todas las entrevistas, es una cuestión relevante a la hora de valorar e invertir en la implantación de un modelo preventivo de delitos en una empresa.

Siguiendo la teoría de la prevención situacional del delito, cuando se tiene una consciencia elevada del delito porque cabe la posibilidad de ser descubierto, se podrá disuadir mucho al potencial infractor; luego, si no se tiene, difícilmente se podrá hacer frente a esos riesgos de forma eficiente. En este sentido, el mundo digital ofrece una ventaja, puesto que cualquier acción realizada dentro del mundo digital suele dejar rastro. Hacia esta misma línea sigue la concienciación de los empleados, dado que si éstos tienen conocimiento del registro de toda su acción realizada en el contexto empresarial, de alguna manera serán disuadidos.

En este sentido, toma relevancia la cultura y educación de los usuarios de las TIC, esto es, la formación y concienciación de éstos. La empresa debe enseñar a estos usuarios, en este caso refiriéndose al personal de la misma, cómo deben actuar, cuáles son sus derechos, deberes y responsabilidades, así como advertirles de la posibilidad de ser objeto de responsabilidades en caso

de incumplimiento (e. g. sanciones disciplinarias), y de poder ser monitorizados. Esta es la mejor forma de fortalecer el eslabón del ser humano de ser víctima (Anexo II).

Concretamente, la Seguridad de la Información va a ser un ítem valorado o no en función de la identificación realizada por cada empresa de sus bienes más sensibles, de cómo los proteja, del tipo de información poseída, pero sobretodo de quiénes dirijan la empresa. Hay empresas protegiendo la seguridad tradicional pero obviando completamente proteger su información. La concienciación de este riesgo parece tender a aumentar, así se concluye en las entrevistas, pero no parece ser suficiente por dos motivos. En primer lugar, si aflorara la verdadera cantidad de ataques constantes actuales, las empresas tomarían conciencia a un ritmo más drástico. Aun así, es necesario comentar el inconveniente supuesto de la existencia de noticias silenciadas, una especie de *cifra negra* (Anexo III), debido a la no voluntad de trascendencia de los ataques sufridos por parte de las empresas, normalmente de cierto renombre. Y, en segundo lugar, cuando este riesgo se concibe como lejano o con la idea de no ser a uno mismo a quién afecta, si no hay una ayuda o "pequeño empujón" en forma de obligación legal, las empresas son reacias a invertir en seguridad y cuesta, más si no han sido nunca víctimas de ningún tipo de delito relativo a las TIC (Anexo II).

3.3 ¿De qué deben protegerse las empresas, cómo deben hacerlo y con qué herramientas?

Cuando el Código penal recomienda la adopción de un modelo de prevención de delitos (debemos recordar su no obligatoriedad), no lo hace pensando exclusivamente en utilizarlo para evitar la responsabilidad penal de la empresa, sino para fomentar en la organización tener mecanismos de protección contra ataques a la misma (ser capaz de detectar los riesgos, curarse en salud y protegerse contra los mismos), no porqué sean responsables sino por ser víctimas (Anexo III).

Pero, ¿de qué deben protegerse las empresas? Los tipos delictivos frecuentemente sufridos por las empresas suelen ser los daños informáticos (e. g. borrar información de la empresa), el descubrimiento y revelación de secretos (e. g. fuga de información), o más a menudo, la falsificación de documentos, mientras que el delito económico no sale a la luz con una simple auditoría (Anexo I). Asimismo, también son frecuentes los ciberataques (e. g. ataques de denegación de servicio), el *phishing*, o bien los delitos contra la propiedad intelectual (Anexo III).

En este sentido, una empresa puede ser víctima de dos acciones (Anexo II). Por un lado, víctima directa de la actividad contra ella y/o su sistema de información. Por otro, puede ser autora porque alguno de sus empleados ha utilizado servicios de la misma para cometer un delito, con lo cual también podría ser la persona jurídica responsable penalmente si ese delito concreto está contemplado dentro de los posibles delitos estipulados en el Código Penal en los cuales puede la persona jurídica ser responsable penalmente.

¿Cómo gestionar las amenazas? Las amenazas internas y las externas se gestionan de forma similar (Anexo II). El primer paso es conocer cuáles son los activos de la empresa, cuáles son los potenciales riesgos posibles de estos activos (probabilidad de producirse una amenaza o ataque a un activo y se consiga el objetivo), y quiénes pueden ser las personas beneficiadas de su destrucción, robo o modificación, sabiendo qué posibilidades tienen y de qué posibles formas pueden realizar ese ataque. Para la producción de un hecho es necesaria la conjunción de tres elementos: poseer un activo, tener una vulnerabilidad, y haber un atacante. Entonces, es imprescindible analizar cuáles son los riesgos y protegerlos en su justa medida, aunque este análisis sea la cuestión más complicada. No es tan importante la gestión de la información en sí misma como la de los riesgos de la información.

Ahora bien, no es suficiente con valorar el riesgo, sino también resulta necesario valorar el posible impacto producido en la empresa. Con la ponderación de tales situaciones, se establecen unas prioridades, de las cuales las más altas serán aquellas con posible mayor impacto. De esta manera, se debe actuar sobre ellos en función del riesgo con el fin de fortificarlos y reducirlos, pero con un coste asumible para la empresa. En otras palabras, sabiendo la imposibilidad de existencia de un riesgo 0, en caso de producirse cualquiera de los riesgos posibles, el impacto en la empresa debe necesariamente poder ser asumido por la misma, sino supondría impedir a la empresa el seguimiento de su actividad normal. Sin embargo, resulta ser una de las vías más conflictivas el hecho de disponer en la compañía de servicios de tecnología externalizados, puesto que esto supone un descontrol absoluto por parte de la empresa de sus sistemas (Anexo I).

En este sentido, para una efectiva gestión de riesgos y control, resultará interesante el seguimiento del modelo de las tres líneas de defensa (The Institute of Internal Auditors [IIA], 2013), en el cual la alta dirección y los órganos de gobierno corporativo, de nuevo, tendrán un papel

fundamental para llevarla a cabo de forma correcta. En la primera línea de defensa (propiedad / gestión de riesgos) destaca el control de la gerencia operativa. La segunda línea de defensa (control de riesgos y cumplimiento) destaca en sus varias funciones de supervisión de riesgos, controles y cumplimiento establecidas por la administración. Y, por último, en la tercera línea de defensa (aseguramiento de riesgos) destaca el aseguramiento independiente y la auditoría interna.

Para establecer un sistema de gestión, control y monitorización de todas las acciones, primero se realiza la gestión de los riesgos y, en ella, se analiza la probabilidad de ocurrencia de los mismos en o a los sistemas de información de la empresa. Además, se deben fortalecer las medidas con un bastionado (*hardering*) de la seguridad, esto es, asegurar los sistemas disminuyendo sus vulnerabilidades, para las cuales se está más propenso cuanto más funciones se desempeñan (un sistema con una única función es más seguro que uno con muchas). Siguiendo esta línea, también deben tener un sistema para controlar en todo momento si se ha está produciendo un incidente, pues aún habiendo implementadas medidas de seguridad, no eximen de poder romperse.

Sin embargo, una empresa no se puede proteger de un riesgo desconocido, así como tampoco puede fortalecer una vulnerabilidad hasta el momento desconocida para ella. Para estos casos, la única solución existente para la empresa es crear alertas de sucesos inusuales en la actividad empresarial para, posteriormente, analizarlas. Esto va a permitir a la empresa conocer si se está atacando a un riesgo desconocido hasta el momento, o bien, se está atacando el sistema por una vulnerabilidad hasta el momento no protegida. En definitiva, se trata de conocer bien el funcionamiento diario de la empresa y comprobar la inexistencia de actividades fuera de éste. Pero, ¿cómo se crean estas alertas?

Se trata de establecer un procedimiento propietario de la propia empresa para controlar las actividades inusuales, sospechosas o fuera de la lógica empresarial, y detectarlas. No se trata de disponer de ninguna herramienta conocida, puesto que entonces también lo será para el atacante y podrá eludir sus controles, sino de llevar a cabo medidas propietarias de seguridad complementarias (Anexo II). La figura encargada de llevarlas a cabo sería el *hacker ético* o *hacker blanco*, entendido como una persona experta con altos conocimientos, tanto en informática como fuera de aquello ya establecido. Su función en la empresa, o para la investigación de un caso concreto, sería implementar medidas solamente exclusivas para esa empresa, medidas no establecidas en ninguna

normativa ni estándar. Esta medida ofrece dos ventajas a la empresa: por un lado, supone un plus en términos de valor diferencial frente a la competencia; y por otro, podría servirle de defensa a la empresa en el supuesto de querer defenderse ante un ataque contra ella por haber sido negligente o por no tener las medidas de seguridad pertinentes en los casos en los cuales puede ser acusada de tener responsabilidad penal, puesto que puede alegar no solamente haber seguido el *check-list* recomendado en los estándares ISO sino haber añadido este plus para fortalecer sus medidas de seguridad. Ahora bien, a esta figura del *hacker ético* se le debe dar una cobertura, no puede actuar por libre ni con iniciativa propia dentro de la empresa, sino debe de estar atado de pies y manos por un contrato con la misma, necesariamente, estableciendo de forma clara todo aquello incluido dentro de su poder de actuación, dejando claro no poder extralimitarse en sus funciones ni poder vulnerar ningún derecho fundamental; esto no quiere decir dar un balance a cada rato de cada paso avanzado por el mismo. De esta manera, estas medidas propietarias quedarán establecidas en el protocolo de seguridad de esa empresa, pero en ningún otro. Las oficinas financieras ya están implementando estos sistemas de perfiles de actividad de los propios usuarios y de funcionamiento, con el fin de combatir los ataques desde el exterior de usuarios no habituales.

En relación a la seguridad, la empresa debe buscar un equilibrio. Si implementa mucho en ella, disminuirá en usabilidad y funcionalidad, además de generar en el empleado una sensación, quizás contraproducente, de presión y constante control. Para evitar ésto, se deben buscar sistemas en los cuales el propio usuario sea partícipe en la implementación de esas medidas de seguridad, y eso no se consigue solamente imponiéndoles, sino convenciéndoles, y autoconvenciéndose ellos mismos, de la validez de esas medidas, tanto en la seguridad de la empresa como en la suya propia (la de su puesto de trabajo).

Evidentemente, este control al usuario es fundamental pero no el único. No se deben olvidar las medidas de seguridad tradicionales, así como tampoco el resto de medidas de seguridad y control, como podría ser el establecimiento de una solución *endpoint* (Anexo II). La seguridad *endpoint* se ocupa de los riesgos presentados por los dispositivos conectados a una red empresarial, asegurando cada dispositivo, como punto de entrada para amenazas, para bloquear los intentos de acceso y otras actividades de riesgo en estos puntos de entrada. A medida que las empresas adoptan políticas empresariales como BYOD (*Bring Your Own Device*) o BYOT (*Bring Your Own Technology*), el perímetro de seguridad de la red empresarial se ha ido disolviendo esencialmente.

Particularmente, en la implementación de BYOD se debe llevar aunado el control del dispositivo concreto o de la parte del dispositivo a utilizar para el nivel corporativo. Es decir, un mismo dispositivo podrá tener dos perfiles a la vez, uno personal y otro corporativo. Para no poner en peligro los activos de la empresa, el perfil corporativo debe estar cifrado, tan sólo se le está permitido descargar aplicaciones desde la tienda de la misma empresa, puesto que son aquellas controladas y monitorizadas por la misma, y el acceso desde el dispositivo únicamente se dará a aquellas áreas de la empresa con menor nivel de impacto.

Recogiendo todas las anteriores medidas de seguridad mencionadas, se revelan los tipos de seguridad debidos de tener en cuenta por la empresa (Anexo II): una seguridad preventiva (antes del incidente, para evitar su posterior suceso); una seguridad detectiva (descubrir el incidente cuando se está produciendo); una seguridad reactiva (plan de contingencias); y, finalmente, una seguridad holística (sistemas considerados para alcanzar en conjunto el mayor nivel de seguridad).

Respecto de las amenazas internas, la primera medida fundamental es la protección y el control del usuario (Anexo II), por los dos principales problemas de los *insiders*: por un lado, con el perfil de atacantes, conocen y tienen privilegios de acceso a la información y, a su vez, conocen los activos y cuáles son las medidas de seguridad, con lo cual pueden saber cómo eludirlas para acceder a esa información; y por otro, son usados como el puente intermedio hacia la información. Además de monitorizar los sistemas, actividades y acciones de los usuarios, en todas las entrevistas aparece la necesidad de educarlos y concienciarlos mediante un plan de formación para evitar verse involucrados en cualquier tipo de incidente, tanto en el perfil de víctima como de atacante. Es importante haber arraigado el conocimiento de sus obligaciones y limitaciones en el marco de la empresa, de esa manera podrán tomar conciencia de sus responsabilidades (civiles, penales, administrativas) en caso de incumplimiento. En este sentido, es de vital importancia evitar generar en los empleados la sensación de ser el modelo de prevención de delitos, simplemente, una declaración de buenas intenciones, pues entonces tan sólo quedará en papel mojado; ellos deben tener la sensación de una verdadera ejecución y efectividad del mismo.

Poder controlar y monitorizar las actividades de los empleados, significa incidir en la esfera de su privacidad, es decir, en sus derechos fundamentales. A sabiendas de la dicotomía existente

entre la seguridad y la privacidad (si aumenta la primera, disminuye la segunda), se debe encontrar un equilibrio. Una posible solución, no regulada ni estipulada en ningún sitio, podría ser el establecimiento de un sistema garantista de la privacidad de los trabajadores, en el cual esta información monitorizada se guardara cifradamente, aunque no siempre supervisada ni analizada, pero no fuera accesible ni para los empleados ni para los administradores (Anexo II); tan sólo en caso de haberse producido un incidente y necesitar conocer los detalles sobre qué ha pasado, a partir de una autorización judicial podría pedirse la verificación y examen de tal información, garantizando así únicamente la invasión a la privacidad del trabajador en ese caso concreto. A pesar de haber cierta tolerancia al principio, si en el convenio colectivo de la empresa aparece como infracción el supuesto en el cual un trabajador utiliza las herramientas del trabajo con fines particulares (fines privados indirectamente), el control de estos dispositivos por parte del empresario queda justificado, puesto que estas herramientas son consideradas propiedad de la empresa (Anexo III).

Aunque a veces el empleado roba información para venderla a la competencia, muchas otras veces es por negligencia del mismo. Por ejemplo, la empresa informa al personal sobre cuáles son los canales seguros de envío de información y el trabajador no los utiliza. En estos casos, la empresa tiene la obligación de informar sobre las medidas básicas relativas a las TIC (e. g. prohibir el uso de memorias USB, prohibir dar la contraseña privada a nadie, informar sobre cada cuánto tiempo se debe cambiar la contraseña de usuario, etc.) y debe prever todo tipo de supuestos en las políticas TIC de la empresa de los diferentes incidentes posibles; de otra manera, la empresa será responsable penalmente de ese incidente debido a la posible alegación del empleado de no tener conocimiento de esa medida. Esta cuestión enlaza con la especificidad comentada anteriormente de los modelos de *compliance*, porqué en caso de disponer de un programa de *compliance* extranjero, este tipo de particularidades en los diferentes supuestos no estarían previstos.

Generalmente, la empresa suele despedir, directamente y sin duda alguna, al empleado (Anexo I), concretamente en un 72% de los casos (PwC, 2016). En muchas ocasiones, antes de denunciar al mismo, la empresa obtiene las pruebas del delito cometido para evitar generarse cualquier tipo de perjuicio innecesario (e. g. demandas por parte del empleado despedido). Con ello, evitan denunciar por ese incidente posteriormente al empleado y el delito se queda "en el aire"; luego, esto mismo va en contra del espíritu del *compliance.* En estos casos, si algún trabajador

incumple el código ético es importante la respuesta de la empresa y la documentación de la misma (e. g. sanción disciplinaria amparada por la normativa laboral), dado que eso sirve para demostrar la voluntad y capacidad de respuesta de la empresa ante cualquier incidente.

Además del decálogo de orientaciones prácticas para un buen gobierno de las TIC ofrecido por Agustina (2013), en el Anexo II se adjunta una lista extensa de medidas básicas de prevención y monitorización a tener en cuenta por la empresa, destacando el control de accesos y las copias de seguridad (Anexo I). A su vez, en el Anexo III se destaca la existencia de una normativa informativa dirigida al trabajador sobre todas sus responsabilidades, deberes y obligaciones, con el fin de tomar consciencia de la monitorización y control de sus acciones, y también de las consecuencias de las mismas. Por último, también resulta destacable el protocolo de actuación en el despido de un trabajador, puesto que se han dado muchos casos de pérdidas de información por olvidar dar de baja las credenciales o el acceso remoto del usuario (Anexo I).

Con respecto del canal de denuncias o sistema de *whistleblowing*, los empleados no suelen hacer un uso razonable de esta herramienta, concretamente tan sólo es usado en un 7% de las ocasiones (PwC, 2016). La causa de este asunto podría ser la falta de concienciación de los empleados en este tema debido al miedo a sufrir algún tipo de represalia. Por este motivo, resulta clave la confianza entre cargos (Anexo I), especialmente con el departamento de recursos humanos de la empresa, donde acuden los trabajadores cuando tiene algún problema o no entienden alguna cuestión. O, puede haber poco uso del canal simplemente porqué no hay delito alguno. De todas formas, no es propenso a haber denuncias falsas de ningún tipo, cuestión más peligrosa si el canal fuera anónimo, puesto que el anonimato dificulta el descubrimiento del delito, la identificación y persecución de los partícipes, y la recuperación de sus efectos. En estos casos, probablemente la investigación ni siquiera se llevara a cabo por falta de información acerca del incidente.

El hecho de haber extendido el objeto del proceso penal ahora también a valorar la idoneidad del programa de cumplimiento adoptado por la corporación, denota la importancia de la documentación aportada al juez sobre la implantación del modelo de *compliance* y no solamente eso, sino también la demostración de la realización del mismo. Es necesario dejar rastro de toda la actividad empresarial, puesto que así la empresa demuestra su consciencia con respecto de aquello sucedido en la misma.

Todas las políticas y planes de seguridad deben documentar toda la casuística correspondiente, esto es, el análisis de activos, el análisis de posibles riesgos, las medidas de seguridad implementadas y sus correspondientes responsables (implementación, mantenimiento, control y auditoría), en caso de haber cualquier incidente la determinación de quién ha sido o cuál es su tratamiento, y finalmente, la modificación constante (evolución) de las medidas conforme se va realizando un seguimiento del funcionamiento de todo ello (apariencia "viva" y actualizada diariamente).

El juez debe tener acceso a toda esa información, a todas las auditorías realizadas por la empresa, y a todo el catálogo de medidas, cuya implementación se está realizando en ese momento en la organización. No es suficiente con disponer de un documento escrito, sino además es necesario su cumplimiento, es decir, un análisis del incidente. Resulta importante medir la capacidad de respuesta del departamento IT ante un incidente (Anexo III). Si el incidente se produce en una modalidad no contemplada en la misma documentación sobre las medidas de seguridad, la empresa no sería responsable si tenía implementadas unas medidas de seguridad adecuadas y mínimas. Sin embargo, si se produce el incidente pero no se debería de haber producido porque en el plan de seguridad así decía estar implementándose, evidentemente esto se consideraría un engaño por parte de la empresa y entonces sí sería responsable penalmente. En este sentido, el delito no puede invalidar necesariamente un programa de prevención, pudiendo haber sido diseñado e implementado adecuadamente sin llegar a tener una eficacia absoluta.

Además de la prueba documental como medio de prueba debido de aportar por la persona jurídica para acreditar en un proceso penal la eficacia de su plan de cumplimiento normativo, también existe la prueba testifical. Es importante porqué en su caso un perito informático valorará la seguridad informática del modelo y un perito de *compliance* valorará la adecuación de las medidas adoptadas para la prevención del delito concreto, aunque en este segundo caso se desconoce qué figura exactamente va a hacer de experto en peritaje de *compliance*. Este tipo de pruebas no suelen ser muy amigables cuando estos testigos resultan ser los empleados de la propia empresa (Anexo I/II), puesto que no hay garantías certeras de no estar beneficiando a la empresa con sus declaraciones.

3.4 El lugar de las PYME en el mundo del *compliance*

Los modelos de cumplimiento normativo aparecen con el fin de poner fin a la delincuencia corporativa de las grandes corporaciones, pero ¿qué lugar ocupan las PYME, empresa más frecuente en España, en este mundo del *compliance*? En un principio, son todas las personas jurídicas aquellas afectadas al respecto.

En este sentido, hay empresas multinacionales donde el plan de *compliance* lleva tiempo implantado y dónde se tiene una cultura corporativa muy desarrollada. Esto es así porque en otros países hace mucho más tiempo de la exigencia del mismo, como por ejemplo en el caso anglosajón o italiano. Entonces, esta cuestión pasa a ser completamente una novedad para las empresas, cuya operación no se extendía al ámbito externo, es decir, para las PYME, las cuales frecuentemente suelen ser proveedores de las grandes empresas, las cuales empiezan a exigirles tener implantados un programa de *compliance*.

Puesto que las características en términos de complejidad de una gran empresa no pueden compararse con las peculiaridades de una PYME, tan sólo les queda adaptar a su propia estructura organizativa su modelo de *compliance* (Anexo I). De esta manera, a pesar de tener un programa con sólo los elementos más básicos, el juez valorará esta sencillez y la adecuación de las medidas implementadas correspondientes para la evitación de aquellos delitos concretos con los cuales pueda verse más afectada la empresa, en caso de tenerse una actividad empresarial muy específica. Y, por otro lado, esta adaptación para las PYME también va a suponer un reto para las consultoras, puesto que tiene mayor dificultad realizar un plan de *compliance* simplificado, cuyo disfrute sea gozando de todas las garantías necesarias pero a la vez a un nivel y presupuesto mucho menor.

Siguiendo esta línea, las sanciones a las PYME deben ser equitativas en función al daño posiblemente originado a la empresa, es decir, deben ser proporcionales a la facturación de la empresa (Anexo II). No tiene ningún sentido poner una sanción de millones de euros a una PYME si probablemente esa sea la facturación de un mes o incluso de todo un año; en cambio, sí lo tendría para una gran empresa, para cuyo presupuesto es nada. Además, se debería considerar la sanción como una segunda oportunidad para la empresa, ya que no sólo va a servirle de advertencia y castigo, en su justa medida, para evitar el mismo suceso en un futuro, sino debe ayudarla a recuperarse y enderezarse con el fin de mejorarla.

En este mundo de las Big Four y con gran competencia de mercado, el problema va a ocasionarse cuando tener implantado un modelo de *compliance* sea obligatorio, puesto que habrá muchos oportunistas queriéndose aprovechar de la situación ofreciendo servicios, tal vez bien de precio, cuya utilización en la práctica no sirva para nada porqué en realidad el servicio resulta ser pésimo o un engaño (Anexo II/III); no por ser el más barato, o incluso el más caro, es el mejor ni el cual mejor se adapta a las necesidades de la empresa. Las PYME deben tener mucho cuidado con a quién delegan ese servicio, pero sobretodo, deben exigir en todo momento el servicio que están pagando y deben supervisar toda la documentación aportada por parte de quién han contratado, ya que en caso de incidente la empresa podría incurrir en una negligencia por no haberlo controlado de forma más exhaustiva. Aún así, indudablemente para las PYME es mejor disponer de un servicio externo; en contra, para las grandes empresas es mejor tener un departamento interno especializado.

Con el fin de poder disponer de un buen servicio de seguridad TIC, hay soluciones corporativas posibles para las PYME. En este sentido, una consultoría externa puede unir a empresas de la misma tendencia o similitudes para ofrecerles una solución corporativa conjunta, o incluso ofrecerles un servicio de seguridad, sin ser a tiempo completo, acorde con sus necesidades (Anexo II). En resumen, si no puedes asumir el gasto, compártelo.

3.5 Conclusiones: Retos futuros para el *compliance*

El crecimiento de las nuevas tecnologías y el acceso a Internet, se han traducido en un incremento en el riesgo de exposición de las organizaciones a determinados delitos, particularmente los ciberdelitos, con una probabilidad de ocurrencia del 37% a escala mundial y de un 24% a nivel estatal (PwC, 2016); luego, cada vez está teniendo más relevancia la seguridad de la información en el contexto empresarial. Aun así, siendo lo más idóneo para las empresas estar cercanas a la máxima seguridad, la realidad es totalmente contraria: están más cercanas a la inseguridad.

En este mundo digitalizado e interconnectado y ante esta nueva avalancha de amenazas, sin apenas control alguno, el cumplimiento normativo está teniendo también un papel muy relevante. Sin embargo, el gran volumen de regulaciones a las cuales están sometidas y obligadas las corporaciones, con indiferencia del tipo, y la gran presión por demostrar un buen gobierno corporativo, muchas veces puede resultar contraproducente. En su caso, el programa de *compliance*

en España todavía es muy reciente y apenas se ha asimilado, sobretodo en las PYME, cuya adaptación les va a suponer un gran reto, hasta el momento asustadizo. Asimismo, tampoco ayuda la falta de jurisprudencia con respecto a la eficacia de estos modelos.

A todo ello, se le suma, a partir de mayo de 2018, la entrada en vigor del Reglamento General de Protección de Datos, una normativa europea aparecida con mucha fuerza y desgarre. A diferencia de las facilidades ofrecidas por el programa de *compliance*, este nuevo reglamento está repleto de nuevas cuestiones y de cambios a los cuales, por el momento, en general no se tiene muy claro cómo afrontar. Entre otras modificaciones, cambia el sistema de protección de datos y se obliga a la empresa a tener un plan de actuación, aparece el principio de responsabilidad activa (*accountability*) y con él una nueva figura, muy parecida al *compliance officer* (independiente, individuo/grupo, interno/externo), llamada *data protection officer*, la empresa deberá notificar a la autoridad de control y a los respectivos sujetos particulares posiblemente afectados si ha sufrido una fuga de información, y habrá un régimen sancionador muy poco garantista. Todo ello, hará evidente el aumento de presión entre empresas y profesionales, quienes deberán pedir más recursos, y aumentará la carga de gestión de la empresa, la cual deberá ser muy proactiva al respecto. Por tanto, ante esta gran inseguridad jurídica con tipificaciones poco claras e imprecisas y acuerdos de compromiso, se esconden grandes retos, tanto para la autoridad de control como para todos los demás.

Ahora, por ser el principio, hay mucha reacción y animadversión al respecto, pero con el tiempo, esta primera reacción se irá apaciguando hasta dejar de ser novedad para convertirse en normalidad; así lo manifestaron los entrevistados. Entendiendo el plan de *compliance* como una adición de valor competitivo a la empresa, además de mejorar la imagen corporativa (dan caché), primero se irán implementando en grandes corporaciones y, una vez estén, las PYME, aunque se desconoce a qué ritmo. Probablemente, cuando comiencen a aumentar los casos de empresas sancionadas en sentencias por este motivo, en demostración de su verdadero cumplimiento, esto servirá como punto de alerta para las organizaciones para empezar a tomar realmente conciencia de ello y entonces llevar a cabo la implantación del modelo de *compliance*. Sin embargo, cuando se quiere hacer un cambio disruptivo total, se debe hacer ayudando mediante la formación, la concienciación y el apoyo; luego, para llevar a cabo correctamente este funcionamiento, se debe

tener una estrategia de implementación y, en caso de no tenerla, lo cual es muy probable, las empresas se seguirán manteniendo como han estado hasta ahora (Anexo II).

Finalmente, a título personal me gustaría añadir mi sorpresa ante la buena noticia para las PYME con respecto de los posibles problemas en la implementación de un modelo de cumplimiento normativo. Esto ha de servir a este tipo de empresas como una forma de empuje para tomar un mayor valor competitivo en el mercado y concienciarse de los posibles riesgos y del valor de sus sistemas de información, o incluso simplemente de la misma información contenida en ellos, para posteriormente aprender a utilizarlo como valor diferencial con respecto de las otras empresas, pues ni una falta de seguridad en los dispositivos y equipos de la empresa ni una falta de implantación de un modelo de *compliance* son problemas de implementación. Y, por último, me agradaría mostrar mi especial asombro por haber descubierto mi gusto e interés por esta nueva área de trabajo, donde la figura del criminólogo tiene aún mucho por decir.

4. Referencias

Referencias bibliográficas

Agencia Española de Protección de Datos. (n.d.). *Transparencia: La Agencia*. Consultado 16 febrero 2017, desde http://www.agpd.es/portalwebAGPD/LaAgencia/index-ides-idphp.php

Agencia Española de Protección de Datos. (2007). *Creación de denuncias internas en las empresas (mecanismos de "whistleblowing")*. Consultado 30 abril 2017, desde https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf

Agustina, J. R. (2013). ¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa?. *IDP. Revista de Internet, Derecho y Política*, 16, 7-26. doi:10.7238/idp.v0i16.1806

Agustina, J. R., y Gómez-Duran, E. (2016). Factores de riesgo asociados al *sexting* como umbral de diversas formas de victimización. Estudio de factores correlacionados con el *sexting* en una muestra universitaria. *Revista de Internet, Derecho y Política,* 22, 32-58. doi:10.7238/idp.v0i22.2970

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of A National Survey*. Mississippi: Mississippi State University.

Arnott, S. (2008, agosto 13). How Cyber Crime Went Professional. *Independent.* Consultado 21 noviembre 2016, desde http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html

Artaza Varela, O. (2013). *La empresa como sujeto de imputación de responsabilidad penal: Fundamentos y límites*. Madrid: Marcial Pons.

Asociación Española de Normalización y Certificación. (2008). *UNE 71502:2004*. Consultado 07 febrero 2017, desde http://www.ca.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0030656#.WL8HrFeKzCJ

Asociación Española de Normalización y Certificación. (2009). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. Consultado 07 febrero 2017, desde http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

Asociación Española de Normalización y Certificación. (2017). *UNE 19601 ayudará a prevenir delitos en las organizaciones*. Consultado 27 abril 2017, desde http://www.aenor.com/revista/pdf/feb17/14feb17.pdf

Atgrupchannel. (2017, abril 6). *Comentarios a la Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas* [Vídeo]. Consultado 6 abril 2017, desde https://www.youtube.com/watch?v=TxJWBrRGiGw

Audisec. (2016). *GlobalSUITE – Compliance Penal*. Consultado 05 abril 2017, desde http://www.globalsuite.es/wp-content/uploads/2016/03/GlobalSUITE-Compliance-Penal.pdf

Beebe, N. L., y Rao V. (2005). *Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security*. Consultado 23 enero 2017, desde http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.509.1358&rep=rep1&type=pdf

binti Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law and Security Review*, 29(1), 66-76. doi:10.1016/j.clsr.2012.11.005

Bisschop, L. (2010). Corporate environmental responsibility and criminology. *Crime, Law and Social Change,* 53(4), 349-364. doi:10.1007/s10611-009-9227-8

Bleker, S., y Hortensius, D. (2014). ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT. *Journal of Business Compliance,* 2, 1-12. Consultado 27 abril 2017, desde http://www.esv.info/download/zeitschriften/BUCO/leseprobe_2.pdf

Blumenberg, A-D., y García-Moreno, B. (2014). Retos prácticos de la implementación de programas de cumplimiento normativo. En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p.273-300). Madrid: Edisofer.

Boldova Pasamar, M. A. (2013). La introducción de la responsabilidad penal de las personas jurídicas en la legislación española. *Estudios Penales y Criminológicos*, 33, 219-263.

Bonatti Bonet, F. (2017, febrero 26). Primera aproximación a la UNE 19601. [Entrada blog]. Consultado desde http://www.bonattipenal.com/primera-aproximacion-a-la-une-19601/

Bossler, A. M., y Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology,* 13 (1), 400-420.

Bossler, A. M., y Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227-236. doi:10.1016/j.jcrimjus.2010.03.001

Brenner, S. (2004). Cybercrime Metrics: Old Wine, New Bottles?. *Virginia Journal Of Law and Technology*, 9(13).

Brenner, S. (2010). *Cybercrime: Criminal Threats From Cyberspace.* Santa Barbara: Praeger.

Cárdenas Aravena, C. (2008). El lugar de comisión de los denominados ciberdelitos. *Política Criminal: Revista Electrónica Semestral de Políticas Públicas de Materias Penales*, 6, 1-14.

Centro Criptológico Nacional. (n.d.). *¿Quiénes somos?*. Consultado 16 febrero 2017, desde https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es

Centro Criptológico Nacional – Computer Emergency Response Team. (2014). *Ciberamenazas 2014. Tendencias 2015*. Consultado 29 noviembre 2016, desde https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html

Centro Criptológico Nacional – Computer Emergency Response Team. (2015). *Ciberamenazas 2015. Tendencias 2016*. Consultado 29 noviembre 2016, desde https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

Centro Nacional de Excelencia en Ciberseguridad. (n.d.). *Institucional*. Consultado 16 febrero 2017, desde http://www.cnec.university/cnec/

Cerem Business School. (2015, agosto 17). ISO 19600, novedosa herramienta enfocada al cumplimiento legal. [Entrada blog]. Consultado desde https://www.cerem.es/blog/iso-19600-novedosa-herramienta-enfocada-al-cumplimiento-legal

Círculo de Mujeres de Negocios TV. (2013). *Responsabilidad penal de la empresa y de los empresarios, LegalTV programa 9* [Vídeo]. Disponible en: https://www.youtube.com/watch?v=uUzpS4cE1cc

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2(1), 308-333.

Clarke, R. V., y Weisburd, D. (1994). Diffusion of crime control benefits: observations on the reverse of displacement. *Crime Prevention Studies*, 2, 165-183.

Clinard, M. B., y Quinney, R. (1994). *Criminal behaviour systems: A typology*. Cincinnati: Anderson Publishing Co.

Cohen, L., y Felson M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608. doi:10.2307/2094589

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Welcome to COSO*. Consultado 30 abril 2017, desde https://www.coso.org/Pages/default.aspx

Cornish, D. V., y Clarke, R. V. (1986). *The Reasoning Criminal. Rational Choice Perspectives on Offending*. Nueva York: Springer.

Cornish, D. V., y Clarke, R. V. (2003). Opportunities precipitator and criminal decisions: A reply to Wortley's critique of situacional crime prevention. *Crime Prevention Studies,* 16, 41-96.

Cuerpo Nacional de Policía. (n.d.). *BIT - ¿Quiénes somos?*. Consultado 16 febrero 2017, desde https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

Cuevas Sarmiento, J. A. (2017, marzo 14). UNE 19601: Política de Compliance vs. Sistema de Gestión. [Entrada blog]. Consultado desde http://www.garberipenal.com/une-19601-sistema-gestion-compliance/

Cugat Mauri, M. (2015). La reforma de la responsabilidad penal de las personas jurídicas: el papel del juez ante el peligro de hipertrofia de las compliance. *Estudios Penales y Criminológicos*, 35, 919-963.

de Bossey, C. (2005). *Report of the Working Group on Internet Governance*. Consultado 16 febrero 2017, desde http://www.wgig.org/docs/WGIGREPORT.pdf

Del Moral García, A. (2016). *La responsabilidad penal de las personas jurídicas: Societas delinquere non potest ..., sed puniri potest!*. Consultado 30 marzo 2017, desde http://www.abogacia.es/2016/01/18/la-responsabilidad-penal-de-las-personas-juridicas-societas-delinquere-non-potest-sed-puniri-potest/

Deloitte. (2015). *Building world-class ethics and compliance programs: Making a good program great. Five ingredients for your program.* Consultado 28 abril 2017, desde

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-g2g-compendium.pdf

Díez Ripollés, J. L. (2012). La responsabilidad penal de las personas jurídicas. Regulación española. *InDret: Revista para el Análisis del Derecho*, 1, 1-33.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4(2), 92-100. doi:10.4236/jis.2013.42011

Dopico Gómez-Aller, J. (2013). Posición de garante del compliance officer por infracción del "deber de control": una aproximación tópica. En Nieto Martín, A., y Arroyo Zapatero, L. (dirs.), *El Derecho penal económico en la Era Compliance* (p. 165-190). Valencia: Tirant lo Blanch.

eCompliance Consultores&Abogados, y Borak ITsolutions (2017). *e-CAS, Compliance Assisting Solution*. Consultado 05 abril 2017, desde https://complianceabogados.es/wp-content/uploads/2017/03/hojaPRODUCTO_eCAS.pdf

"El 'II Congreso Nacional de Compliance' hace incapié en la importancia de los canales de denuncia". (2016, diciembre 2). *LegalToday*. Consultado 27 abril 2017, desde http://www.legaltoday.com/actualidad/noticias/el-ii-congreso-nacional-de-compliance-hace-hincapie-en-la-importancia-de-los-canales-de-denuncia

Eriksen-Jensen, M. (2013). *Holding back the tidal wave of cybercrime*. Computer Fraud & Security, 2013(3), 10-16. doi:10.1016/S1361-3723(13)70028-9

Ernst & Young. (2015). *ISO 19600 – International standard of compliance management*. Consultado 27 abril 2017, desde http://www.ey.com/Publication/vwLUAssets/EY-iso-19600-international-standard-for-compliance-management/$FILE/EY-iso-19600-international-standard-for-compliance-management.pdf

Ethics & Compliance Initiative. (2015). *Encouraging Employee Reporting Through Procedural Justice*. Consultado 27 abril 2017, desde https://connects.ethics.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=2961d73f-3dd2-4cc5-a449-57f0276d536c&forceDialog=0

Ethics & Compliance Initiative. (2016a). *Men, Women & Ethical Leadership. Gender's Influence on Tone at the Top*. Consultado 27 abril 2017, desde https://connects.ethics.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=91324409-3699-b5a7-5b99-0c85f2c26ad2&forceDialog=0

Ethics & Compliance Initiative. (2016b). *Ethics Exchanged: Conversations with Jeff Kaplan & Steve Priest on Behavior, Culture, Ethics and Compliance*. Consultado 28 abril 2017, desde https://higherlogicdownload.s3.amazonaws.com/THEECOA/f6d550cf-32d7-4c33-9101-9b760815c04a/UploadedImages/Articles/EthicsExchangePrint.pdf

Eurojust. (n.d.). *History of Eurojust*. Consultado 16 febrero 2017, desde http://www.eurojust.europa.eu/about/background/Pages/history.aspx

European Comission. (2015). Cybersecurity Report. Consultado 27 marzo 2017, desde http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

European Union. (n.d.). *European Union Agency for Network and Information Security (ENISA)*. Consultado 16 febrero 2017, desde https://europa.eu/european-union/about-eu/agencies/enisa_en

European Union Agency for Network and Information Security. (2015). *Definition of Cybersecurity. Gaps and overlaps in standardisation*. Consultado 07 marzo 2017, desde https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Europol. (n.d.). *European Cybercrime Centre – EC3.* Consultado 16 febrero 2017, desde https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Felson M., y Boba, R. (2010). *Crime and everyday life*. Thousand Oaks: Sage.

Fernández Teruelo, J. G. (2007). *Cibercrimen: delitos cometidos a través de Internet*. Oviedo: Constitutio Criminalis Carolina.

Fernández Teruelo, J. G. (2011). *Derecho penal e internet: Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Valladolid: Lex Nova.

Finjan Malicious Code Research Center. (2008). *Web Security Trends Report.* Consultado 21 noviembre 2016, desde https://observatorio.iti.upv.es/media/managed_files/2008/09/01/maliciouspageofthemonth_finjan_munjul2008.pdf

Friedrichs, D. O. (2010). *Trusted criminals. White Collar Crime in Contemporary Society*. Wadsworth: Cengage Learning.

Furnell, S., Emm,f D., y Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud and Security*, 2015(10), 5-12. doi:10.1016/S1361-3723(15)30093-2

Gallego Soler, J-I. (2014). Criminal Compliance y proceso penal: reflexiones iniciales. En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p. 195-229). Madrid: Edisofer.

García-Guilabert, N. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. En Tamarit Sumalla, J. M. (coord.), Ciberdelincuencia y cibervictimización. *Revista de los Estudios de Derecho y Ciencia Política*, 22, 48-61. doi:10.7238/idp.v0i22.2969

Garrido, V., Stangeland, P., y Redondo, S. (2006). *Principios de Criminología*. Valencia: Tirant lo Blanch.

Gómez Fernández, L., y Fernández Rivero, P. P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el esquema nacional de seguridad*. Consultado 08 marzo 2017, desde http://www.aenor.es/aenor/normas/ediciones/fichae.asp?codigo=11248

Gómez-Jara Díez, C. (2012). La culpabilidad de la persona jurídica. En Bajo Fernández, M., Feijoo Sánchez, B. J., y Gómez-Jara Díez, C. (coords.), *Tratado de responsabilidad penal de las personas jurídicas: adaptado a la Ley 1/2015, de 30 de marzo, por la que se modifica el Código Penal* (p. 153-180). Cizur Menor: Civitas Aranzadi.

Gómez Martín, V. (2012). Falsa alarma. O sobre por qué la Ley Orgánica 5/2010 no deroga el principio *societas delinquere non potest*. En Mir Puig, S., y Corcoy Bidasolo, M. (dirs.), *Garantías constitucionales y Derecho penal europeo* (p. 331-383). Madrid: Marcial Pons.

Gómez Martín, V. (2014). *Compliance* y derechos de los trabajadores. En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p. 421-458). Madrid: Edisofer.

González Rus, J. J. (2007). Precisiones conceptuales y político-criminales sobre la intervención penal en Internet. En Echano Basaldua, J. I. (dir.), *Delito e informática: algunos aspectos* (p. 13-40). Bilbao: Publicaciones de la Universidad de Deusto.

Government of the United Kingdom. (2012). Bribery Act 2010 guidance. Consultado 30 abril 2017, desde https://www.gov.uk/government/publications/bribery-act-2010-guidance

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles?. *Social & Legal Studies,* 10 (2), 243-249.

Grabosky, P. N. (2007). *Electronic Crime*. Upper Saddle River: Pearson.

Grupo de Delitos Telemáticos de la Guardia Civil. (n.d.). *La unidad*. Consultado 16 febrero 2017, desde https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Her Majesty's Government. (2013). *Serious and Organised Crime Strategy*. Consultado 21 noviembre 2016, desde https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

Hess, M. F., y Broughton, E. (2014). Fostering an ethical organization from the bottom up and the outside in. *Business Horizons*, 57(4), 541-549. doi:10.1016/j.bushor.2014.02.004

Higgins G., Fell B., y Wilson, A. (2007). Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States. *Social Science Computer Review*, 25(3), 339-357. doi:10.1177/0894439307299934

Hilbert, E. (2013). Living with cybercrime. *Network Security,* 2013(11), 15-17. doi:10.1016/S1353-4858(13)70126-0

Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.

Holt, T. J., y Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behaviour*, 30(1), 1-25. doi:10.1080/01639620701876577

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), 528-535. doi:10.1016/j.clsr.2009.09.005

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, 7(3-4), 105-113. doi:10.1016/j.diin.2011.01.002

Hunton, P. (2012). Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. *Public Money & Management*, 32(3), 225-232. doi:10.1080/09540962.2012.676281

Hutchings, A., y Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the "Net"?. *Current Issues in Criminal Justice*, 20(3), 1-20.

Information Systems Audit and Control Association. (2016). *Ciberseguridad ¿Una moda pasajera o una realidad que influirá en nuestras vidas?*. Consultado 07 marzo 2017, desde http://www.isacavalencia.org/eventos/wp-content/uploads/2016/02/CharlaUPV-ISACA-Ciberseguridad_febrero_2016.ppt.pdf

Insa, F., Lázaro, C., y García, N. (2008). Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo. *Revista Venezolana de Información, Tecnología y Conocimiento*, 5(2), 139-152.

Intercer. (n.d.). *UNE-ISO 19600:2015. COMPLIANCE: Implantación del Sistema de gestión Compliance*. Consultado 27 abril 2017, desde http://www.intercer.es/files/MODELO%20CONSULTORIA%20ISO%2019600%20COMPLIANCE.pdf

International Organization for Standardization. (n.d.). *ISO/IEC 27000 family – Information security management systems*. Consultado 07 marzo 2017, desde https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization. (2005). ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems - Requirements.

International Organization for Standardization. (2014). *ISO 19600:2014. Compliance management systems – Guidelines*. Consultado 27 abril 2017, desde https://www.iso.org/standard/62342.html

International Organization for Standardization. (2016). *ISO 37001:2016. Anti-bribery management systems – Requirements with guidance for use*. Consultado 27 abril 2017, desde https://www.iso.org/standard/65034.html

Instituto Nacional de Ciberseguridad. (n.d.). *Qué hacemos*. Consultado 16 febrero 2017, desde https://www.incibe.es/que-es-incibe/que-hacemos

Jones, B. R. (2007). Comment: Virtual Neighborhood Watch: Open Source Software and Community Policing against Cybercrime. *The Journal of Criminal Law & Criminology*, 97(2), 600-630.

Kamal, D. (2017). Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill.

Klebe Treviño, L., den Nieuwenboer, N. A., Kreiner, G. E., y Bishop, D. G. (2014). Legitimating the legitimate: A grounded theory study of legitimacy work among Ethics and Compliance Officers. *Organizational Behaviour and Human Decision Processes*, 123(2), 186-205. doi:10.1016/j.obhdp.2013.10.009

Klynveld Peat Marwic Goerdeler. (2015). *Anti-Bribery and Corruption: Rising to the challenge in the age of globalization*. Consultado 30 abril 2017, desde https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/anti-bribery-corruption-2015.pdf

Klynveld Peat Marwic Goerdeler. (2016). *Clarity on compliance: The future of compliance*. Consultado 28 abril 2017, desde https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ch-clarity-on-compliance-en.pdf

Konradt, C., Schilling, A., y Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, 58, 39-46. doi:10.1016/j.cose.2015.12.001

Lascuraín Sánchez, J.A. (2014). Salvar al oficial Ryan (Sobre la responsabilidad penal del oficial de cumplimiento). En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (Dirs.), *Responsabilidad de la Empresa y Compliance* (p. 301-336). Madrid: Edisofer.

Lin, Y. (2014). *IT Risk Management: Case study*. (Tesis doctoral, Lahti University of Applied Sciences, Finlandia). Consultado 30 abril 2017, desde http://www.theseus.fi/bitstream/handle/10024/76744/Lin_Yimei.pdf?sequence=3

Luño, A. (1996). *Ensayos de Informática Jurídica.* México: Fontamara.

Lynch, M. J., McGurrin, D., y Fenwich, M. (2004). Disappearing act: The representation of corporate crime research in criminological literature. *Journal of Criminal Justice*, 32, 389-398. doi:10.1016/j.jcrimjus.2004.06.001

Mafla, E. (2011). *Seguridad ciudadana en el ciberespacio.* Consultado 27 noviembre 2016, desde http://repositorio.flacsoandes.edu.ec/bitstream/10469/6502/1/BFLACSO-CS44-04-Mafla.pdf

Mata y Martín, R. (2001). *Delincuencia Informática y Derecho Penal.* Madrid: Edisofer.

McAfee Labs. (2016). *2017 Threats Predictions*. Consultado 06 marzo 2017, desde https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf#1807_0916_rp_threats-predictions-2017.indd%3A.134685%3A727

Meján, L. (1994). *El Derecho a la Intimidad y la Informática.* México: Porrúa.

Ministerio de Educación, Cultura y Deporte del Gobierno de España. (n.d.). *Ficha de Tesis*. Consultado 20 mayo 2017, desde https://www.educacion.gob.es/teseo/mostrarRef.do?ref=480009

Ministerio del Interior del Gobierno de España (2015). *Estudio sobre la cibercriminalidad en España*. Consultado 27 enero 2017, desde

http://www.interior.gob.es/documents/10180/3066430/Informe+Cibercriminalidad+2015.pdf/c10f398a-8552-430c-9b7f-81d9cc8e751b

Mir Puig, S. (2011). *Bases constitucionales del Derecho penal*. Madrid: Iustel.

Mir Puig, S. (2014). Las nuevas "penas" para personas jurídicas: una clase de "penas" sin culpabilidad. En Mir Puig, S., Corcoy Bidasolo, M., y Gómez Martín, V. (dirs.), *Responsabilidad de la Empresa y Compliance* (p. 3-14). Madrid: Edisofer.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Miró, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica*, 11(5), 1-35.

Montaner Fernández, R. (2015). El *criminal compliance* desde la perspectiva de la delegación de funciones. *Estudios Penales y Criminológicos*, 35, 733-782.

Morris, R., y Higgins, G. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice,* 38(4), 470-480. doi:10.1016/j.jcrimjus.2010.04.016

Narváez Rodríguez, A. (2007). Tutela de la privacidad e interceptación pública de las comunicaciones. En Echano Basaldua, J. I. (dir.), *Delito e informática: algunos aspectos* (p. 297-373). Bilbao: Publicaciones de la Universidad de Deusto.

National Crime Agency. (2016). Cyber Crime Asessment 2016. Consultado 27 marzo 2017, desde http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

Nava Garcés, A. (2007). *Delitos informáticos*. México: Porrúa.

Neira Pena, A. M. (2016). La efectividad de los *criminal compliance programs* como objeto de prueba en el proceso penal. *Política criminal*, 11(22), 467-520. Consultado 30 abril 2017, desde http://www.politicacriminal.cl/Vol_11/n_22/Vol11N22A5.pdf

Newman, G. R. (2010). Cybercrime: Prevention of. En Fisher, B. S., y Lab, S. P. (eds.), *Encyclopedia of Victimology and Crime Prevention.* Los Ángeles: Sage.

Nieto Martín, A. (2008). *La Responsabilidad Penal de las Personas Jurídicas: Un Modelo Legislativo*. Madrid: Iustel.

Nieto Martín, A. (2013). Problemas fundamentales del cumplimiento normativo en el Derecho Penal. En Kuhlen, L., Montiel, J. P., y Ortiz de Urbina Gimeno, I. (eds.), *Compliance y teoría del Derecho Penal* (p. 21-50). Barcelona: Marcial Pons.

Nieto Martín, A. (2015). *Manual de cumplimiento penal en la empresa*. Valencia: Tirant Lo Blanch.

Ortiz Márquez, J. M. (2007). Responsabilidad penal de los proveedores de enlaces. En Echano Basaldua, J. I. (dir.), *Delito e informática: algunos aspectos* (p. 259-276). Bilbao: Publicaciones de la Universidad de Deusto.

Parker, D. B. (1980). Computer-related white-collar crime. En Geis, G., y Stotland, E. (Eds.), *White-collar crime: Theory and research* (p. 199-200). Beverly Hills: Sage.

Peterson, E. A. (2013). Compliance and ethics programs: competitive advantage through the law. *Journal of Management & Governance,* 17(4), 1027-1045. doi:10.1007/s10997-012-9212-y

Picotti, L. (2004). *Il diritto penale della'informatica nell'epoca di Internet*. Padova: CEDAM.

Pittaro, M. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, 1(2), 180-197.

Polidori, P., y Teobaldelli, D. (2016). Corporate criminal liability and optimal firm behaviour: internal monitoring versus managerial incentives. *European Journal of Law and Economics*, 1-34. doi:10.1007/s10657-016-9527-2

Ponemon Institute. (2015). 2015 *Cost of Cyber Crime Study: Global*. Consultado 29 noviembre 2016, desde http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

Pratt, T. C., Holtfreter, K., y Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267-296. doi:10.1177/0022427810365903

PricewaterhouseCoopers. (2015). *Temas candentes de la Ciberseguridad. Un nuevo espacio lleno de incógnitas*. Consultado 07 marzo 2017, desde https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/temas-candentes-ciberseguridad.pdf

PricewaterhouseCoopers. (2016). *Encuesta sobre fraude y delito económico 2016.* Consultado 29 abril 2017, desde http://www.pwc.es/es/publicaciones/transacciones/assets/pwc-forensic-encuesta-fraude-empresarial-y-delito-economico-2016-spain.pdf

Proveedores de servicios. (n.d.). Consultado 18 febrero 2017, desde http://www.lssi.gob.es/proveedores-servicios/Paginas/proveedores.aspx

Rayón Ballesteros, M. C., y Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, 47, 209-234.

Rebbit, D., y Erickson, J. (2016). Hypercompliance. *Professional Safety*, 61(7), 31-37.

Robles Planas, R. (2013). El responsable de cumplimiento ("Compliance Officer") ante el Derecho Penal. En Silva Sánchez, J-M. (dir.), *Criminalidad de empresa y compliance. Prevención y reacciones corporativas* (p. 319-336). Barcelona: Atelier.

Rorie, M. (2015). An integrated theory of corporate environmental compliance and overcompliance. *Crime, Law and Social Change*, 64(2), 65-101. doi:10.1007/s10611-015-9571-9

Rueda Martín, M. A. (2010). Los ataques contra los sistemas informáticos: Conductas de Hacking. Cuestiones político-criminales. En Romeo Casabona, C. M (ed.), *La adaptación del Derecho Penal al desarrollo social y tecnológico* (p. 347-379). Granada: Editorial Comares.

Sanchís Crespo, C. (2007). El levantamiento de la carga de la prueba en Internet: ¿ficción o realidad?. En Echano Basaldua, J. I. (dir.), *Delito e informática: algunos aspectos* (p. 375-390). Bilbao: Publicaciones de la Universidad de Deusto.

Schlegel, K., y Cohen, C. (2007). The impact of technology on criminality. En Byme, J. M., y Rebovich, D. J. (Eds.), *The new technology of criminal law and social control* (p. 23-47). Monsey: Criminal Justice Press.

Silva Sánchez, J-M. (2013). *Fundamentos del Derecho penal de la Empresa*. Montevideo - Buenos Aires: BdeF.

Sims, R. L. (2002). Ethical Rule Breaking by Employees: A Test of Social Bonding Theory. *Journal of Business Ethics*, 40, 101-109.

Simpson, S. S., Gibbs, C., Rorie, M., Slocum, L. A., Cohen, M. A., y Vandenbergh, M. (2013). An Empirical Assessment of Corporate Environment Crime–Control Strategies. *The Journal of Criminal Law & Criminology*, 103(1), 231-278.

Sistema de Gestión de la Seguridad de la Información. (n.d.). Consultado 07 marzo 2017, desde http://www.iso27000.es/download/doc_sgsi_all.pdf

Steffensmeier, D., Schwartz, J, y Roche, M. (2013). Gender and Twenty-First-Century Corporate Crime: Female Involvement and the Gender Involvement and the Gender Gap in Enron-Era

Corporate Frauds. *American Sociological Review*, 78(3), 448-476. doi:10.1177/0003122413484150

Stroz Friedberg. (2017). *2017 Cybersecrity Predictions*. Consultado 27 marzo 2017, desde https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-Report.pdf?__hssc=151509478.1.1490611960991&__hstc=151509478.afb3010341c3b81fd2725b1a0c3ea4f8.1490611960991.1490611960991.1490611960991.1&__hsfp=1089580748&hsCtaTracking=d55e3826-9853-4c20-a525-aa8dd662b642|bd412063-f249-44de-800f-1583fd96dbd9

Sturdivant, F. D., y Ginter, J. L. (1977). Corporate Social Responsiveness: Management Attitudes and Economic Performance. *California Management Review*, 20, 30-39.

Svensson, J, y Bannister, F. (2004). Pirates, sharks and moral crusaders: Social control in peer-to-peer networks. *First Monday Peer-Reviewed Journal on the Internet*, 9(6), 1 y ss. doi:10.5210/fm.v9i6.1154

Symantec. (2016). An ISTR Special Report: Ransomware and Businesses 2016. Consultado 27 marzo 2017, desde http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

The Institute of Internal Auditors. (2013). *IIA Declaración de Posición: Las tres líneas de defensa para una efectiva gestión de riesgos y control*. Consultado 20 mayo 2017, desde https://na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Spanish.pdf

The United States Department of Justice. (2017). Foreign Corrupt Practices Act. Consultado 30 abril 2017, desde https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

Trend Micro. (2015). *Follow the Data: Dissecting Data Breaches and Debunking Myths*. Consultado 30 abril 2017, desde https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf

Trend Micro. (2016). *The Next Tier. Trend Micro Security Predictions for 2017*. Consultado 06 marzo 2017, desde https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-next-tier.pdf

Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. *International Journal of Cyber Criminology*, 2(2), 382-396.

TÜV Rheinland. (2016). *UNE-ISO 19600 SISTEMAS DE GESTIÓN DE COMPLIANCE*. Consultado 27 abril 2017, desde https://www.tuv.com/media/spain/actos/2006/20160519_cogag/ISO_19600_Compliance_Management_System_rev_1.pdf

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*. Consultado 27 noviembre 2016, desde https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

United States Sentencing Commission. (2016). *2016 CHAPTER 8: CHAPTER EIGHT – SENTENCING OF ORGANIZATIONS*. Consultado 27 abril 2017, desde http://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8

Urruela Mora, A. (2012). La introducción de la responsabilidad penal de las personas jurídicas en derecho español en virtud de la LO 5/2010: perspectiva de *lege lata*. *Estudios Penales y Criminológicos*, 32, 412-468.

ValueLinked. (2013). *Services*. Consultado 29 marzo 2017, desde https://sites.google.com/a/valuelinked.com/www/services

Viota Maestre, M. (2007). Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros). En Echano Basaldua, J. I. (dir.), *Delito e informática: algunos aspectos* (p. 237-257). Bilbao: Publicaciones de la Universidad de Deusto.

Virumbrales, A. (2015). *Regulación penal de la delincuencia informática: Especial referencia a la reforma del Código Penal en materia de ciberdelincuencia tras la Ley Orgánica 1/2015, de 30 de marzo*. Universidad de Valladolid, Castilla y León.

Vozmediano, L., San Juan, C., y Vergara, A. I. (2008). Problemas de medición del miedo al delito: Algunas respuestas teóricas y técnicas. *Revista Electrónica de Ciencia Penal y Criminología*, 10-07, 07:1-07:17. Consultado 27 enero 2017, desde http://criminet.ugr.es/recpc/10/recpc10-07.pdf

Winterman. (2016). *Informe anual de fraude corporativo 2016.* Consultado 30 abril 2017, desde http://www.winterman.com/wp-content/uploads/2017/03/estudio-winterman-2016.pdf

Wolters Kluwer. (n.d.). *Complylaw, la herramienta definitiva para identificar y gestionar los riesgos penales de una organización*. Consultado 05 abril 2017, desde https://landings.wolterskluwer.es/complylaw/

Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407-427. doi:101177/147737080556056

Yar, M. (2006). *Cybercrime and society*. London: Sage.

Yeager, P. C. (2016). The Elusive Deterrence of Corporate Crime. *Criminology & Public Policy*, 15(2), 439-451. doi:10.1111/1745-9133.12201

Young, R., y Zhang, L. (2005). *Factors Affecting Illegal Hacking Behaviour*. Consultado 23 enero 2017, desde http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1979&context=amcis2005

Legislación

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS núm. 189.

Auto del Tribunal Supremo de 20 de mayo de 1992 (RJ 1992\4195).

Circular 1/2011 de la Fiscalía General del Estado, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.

Circular 8/2015 de la Fiscalía General del Estado, sobre los delitos contra la propiedad intelectual cometidos a través de los servicios de la sociedad de la información tras la reforma operada por Ley Orgánica 1/2015.

Circular 1/2016 de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 1/2015.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia renovada de la UE para 2011-2014 sobre la responsabilidad social de las empresas, DOUE, COM/2011/0681 final.

Constitución Española, BOE núm. 311 § 31229 (1978).

Convention of Cybercrime, ETS núm. 185.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de las

comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DOUE núm. 105 § 80647 (2006).

Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, DOUE núm. 335 § 82637 (2011).

Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, DOUE núm. 218 § 81648 (2013).

Instrucción FGE 2/2011 sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, BOE núm. 157 § 12666 (1985).

Ley Orgánica 10/1995, de 23 noviembre, del Código Penal, BOE núm. 281 § 25444 (1995).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE núm. 298 § 23750 (1999).

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm. 166 13758 (2002).

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, BOE núm. 251 § 18243 (2007).

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE núm. 152 § 9953 (2010).

Ley Orgánica 7/2012, de 27 de diciembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en materia de transparencia y lucha contra el fraude fiscal y en la Seguridad Social, BOE núm. 312 § 15647 (2012).

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, BOE núm. 114 § 4950 (2014).

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE núm. 77 § 3439 (2015).

Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo, BOE núm. 77 § 3440 (2015).

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, BOE núm. 260 § 6036 (1882).

Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, BOE núm. 161 § 10544 (2010).

Jurisprudencia

Sentencia 110/2005 del Juzgado de lo Penal n.º1 de Madrid, de 29 de julio.

Sentencia del Tribunal Supremo 236/2008, de 9 de mayo.

Sentencia del Tribunal Supremo 292/2008, de 28 de mayo.

Sentencia del Tribunal Supremo 680/2010, de 14 de julio.

Sentencia del Tribunal Supremo 739/2008, de 12 de noviembre.

Sentencia nº514/2015 de TS, Sala 2º, de lo Penal, 2 de Septiembre de 2015.

Sentencia nº154/2016 de TS, Sala 2ª, de lo Penal, 29 de Febrero de 2016.

ANEXOS

ANEXO I

ENTREVISTA I: DAVID SANCHO VIDAL

PREGUNTA: ¿Cuál es su perfil profesional y a qué se dedica actualmente?

"Me he formado en derecho y criminología, y desde hace aproximadamente dos años estoy en este despacho, en ATGroup.

Inicialmente, este despacho empezó con temas de protección de datos pero a raíz de la reforma de 2015, la parte del compliance y la responsabilidad penal de las personas jurídicas, un poco mejor definida que antes, tomó importancia. A partir de ahí, este despacho quiso ofrecer esta parte de servicio, a parte del de protección datos, aunque ya se daba pero de una forma más específica a nivel internacional de alguna empresa que lo pedía y nos íbamos adaptando. Al no estar prácticamente regulado, se podía hacer de una manera más libre, aunque desde este despacho se iba estudiando otros modelos, específicamente el italiano. El modelo italiano es el que ha clonado el español. Hubo mucha suerte. Así, ya teníamos mucho trabajo hecho.

Fue cuando en ese momento en este despacho hubo un hueco para personas que se pudieran dedicar a ello y yo me dediqué, junto con mi compañero Jorge, que es el inventor de este todo este sistema. Nosotros hemos estado haciendo diversas implementaciones y auditorías de compliance desde un papel en blanco, que era un poco la idea que teníamos, a como lo estamos implementando."

PREGUNTA: En un entorno creciente de regulaciones, de necesidad de acreditar el buen gobierno corporativo y una actividad empresarial adecuada, ¿cómo se consigue llevar a cabo un efectivo programa de *compliance* penal en la empresa?

"Podríamos empezar por la respuesta más deseable que podríamos buscar a esto: porque hay una entidad certificadora que certifica. Esto como primera opción, que existiera en España algún tipo de empresas privadas o públicas que certificasen estos modelos y dieran la garantía que son los adecuados y que por ahora están bien, o que tuviéramos más información en sentido de jurisprudencia. Si tuviéramos más sentencias de este tipo, de jueces valorando los programas de compliance podríamos saber si una empresa podría tener la certeza de que eso funciona.

Sin embargo y lamentablemente, ahora mismo no hay forma de saberlo. ¿Por qué no? Porque estamos en un parámetro en el cual nos perdemos en derecho penal. Y al derecho penal le va a importar bien poco que esté certificado o no. Es decir, tú como empresa me puedes dar los papeles de todas las empresas privadas del mundo que digan que tu programa funciona pero lo que está claro es que si ha cometido un delito, en el caso de que se hubiera cometido uno, y el juez tiene que discernir, a mi juicio,

se entiende que esto no funciona. Por tanto, si una entidad te ha certificado pero tú no me demuestras que tu programa de compliance era suficientemente robusto para prevenir ese delito, no me lo voy a creer. Es decir, al juez se le tiene que demostrar que el programa de compliance cumplía con todas las medidas razonables y adecuadas para prevenir ese delito y que la persona, quien lo ha cometido o lo ha podido cometer, se ha saltado todos los controles eludiéndolos de forma muy eficaz, pues se lo ha trabajado muchísimo, pero aun así todos los controles que se tenían eran buenos.

En síntesis, quien debe valorar esto es un juez de lo penal, no otro juez ni otra entidad administrativa ni privada. Ha habido un delito en tu empresa y te he imputado, he investigado a quien ha cometido el delito y a la empresa, y entonces la empresa debe sacar sus herramientas de defensa, en este caso el compliance. Por lo tanto, el único que va a valorarlo es el juez. Creemos que es difícil que a la larga salga algún tipo de empresa certificadora que valide estos programas, puesto que se demostrará en algún momento en el juicio si era válido o no.

Respecto de AENOR, ésta emite certificados para una parte pero eso no certifica los delitos del Código Penal español. De hecho, hay muchos programas de compliance ya hechos y muchas entidades certificadoras que ya llevan tiempo ejerciendo, pero son de otras legislaciones. La especificidad de los delitos del Código Penal español son específicos, valga la redundancia, son nuestros, son de España, con nuestra jurisprudencia y con nuestras historias de nuestro país. Entonces, puedes poner un plan de compliance extranjero y lo aplicas aquí pero puede ser que el juez entienda que lo estás aplicando en base a una normativa extranjera que no prevé el delito fiscal como se prevé en España, por ejemplo. Entonces, tú te has comprado ese modelo, te has gastado mucho dinero en un programa extranjero que no prevé bien lo que al juez le interesa que prevenga. Tienes que prevenir delitos españoles, y estos son particulares.

Otras normativas, como las mercantiles o las civiles, podrían ser equiparables entre países, pero cuando hablamos de delitos, los delitos establecidos en el Código Penal (CP) deben estar interpretados como así se establece en el mismo, porque al fin y al cabo, te puede depender de ir a la cárcel o no. Por lo tanto, la conclusión es que los planes de compliance tienen que estar muy bien orientados a los delitos españoles y no a otras cuestiones porque al fin y al cabo lo que estamos previniendo son estos artículos que están escritos en el CP y el único que lo controla es el juez."

PREGUNTA: ¿Con qué problemática se encuentran las empresas en su día a día? ¿Podría darme algún ejemplo práctico de algún caso de responsabilidad penal corporativa por un delito informático?

"En cuanto a su implementación, yo creo que el problema central es que la gente entienda de qué va todo esto. Parece que es muy obvio pero de hecho es un problema porque la gente no puede creer que tú les vayas allí y le preguntes sobre delitos, porque mucha gente lo tiene como "esto aquí no pasa", "esto aquí no va a pasar nunca". Un ejemplo muy curioso fue cuando les estábamos dando una

formación y se lo tomaban todo a broma, pero después cuando se van todos te viene uno y te dice "oye, aquí una vez pasó…" y te cuenta un caso. Para algunos es una realidad muy distinta porque nunca lo han visto pero cuando te toca, te toca, y tú ves que ese que me vino después no se estaba riendo cuando te lo contaba.

A nivel de empresas, los delitos más típicos son siempre daños informáticos, gente que borra información de la empresa, revelación de secretos, o habitualmente nos encontramos certificados falsos. Los delitos económicos son mucho más complicados de surgir, al menos en las primeras auditorías (e. g. alguien está haciendo transacciones económicas que no debe).

Quizá el primer elemento complejo para que todo ese plan de compliance se vaya permeabilizando en toda la institución es que la gente entienda que los delitos pueden pasar, algo tan sencillo como eso. Es importante perder un tiempo en leer ese protocolo que te dieron (e. g. protocolo sobre la protección de la información) para entender de qué va y que cosas como los delitos pueden pasar, y cada vez van a exigir más desde fuera. De hecho, cada vez más las empresas se piden entre ellas el código de conducta o de alguna manera se le pide a la empresa que certifique estar implementando un plan de compliance, aunque se haga cada uno como quiere y sólo se tengan los elementos básicos establecidos en el artículo del CP.

Entonces, si tuviera que decirte algo difícil sería la primera reacción. Desde finales de 2015, en todas las empresas con las cuales hemos trabajado ha sido la primera vez. Entonces, con el tiempo iremos viendo cuando hagamos más auditorías si la gente ya se va concienciando un poco más de esta prevención, yo imagino que sí.

Actualmente, los códigos de conducta no suelen ser suficientemente sólidos ni están instaurados por completo. Nosotros insistimos mucho en que puedas demostrar que tú lo estás llevando a cabo. Insisto, al juez deberás documentarle, vía documental o vía testifical, que tú a esa persona que acaba de cometer un delito la has informado de todo lo que tenía que hacer y aun así lo ha cometido. Entonces, toda esa documentación, que anteriormente te firmó, lo tienes que conservar y tiene que ser creíble. Siempre recomendamos que si es electrónico que esté firmado electrónicamente, si es en digital con algún tipo de precinto sellado. El juez debe creerse que la empresa lleva desde el 2015 haciendo ese modelo de compliance, que vea que es un intento de ahora mismo porque se ha cometido un delito. No descartamos que si no se hace bien no se consiga demostrar la existencia de un modelo, pero dependerá más de testigos que vengan a corroborar la implementación del plan; en este caso, de empleados de la propia empresa o el encargado de departamento.

Aun así, no somos amigos de las testificales. Mejor dejar rastro con documentación de absolutamente todo aquello que se pueda para acreditar que la empresa es consciente de todo aquello que se está realizando en ella. Sobre todo, si algún trabajador incumple el código ético, que siempre haya una respuesta, aunque sea una amonestación; así lo dice el CP en su inciso sobre el sistema disciplinario. Si algún trabajador comete alguna irregularidad, de alguna manera dar una respuesta y documentarla. Cualquier respuesta está amparada en la normativa laboral, la cual da a la empresa,

generalmente, bastante libertad para atribuir sanciones en base a determinadas conductas; solo con que te desobedezcan, si es una orden razonada ya tiene potestad para llevarla a cabo. Lo mismo ocurriría para una normativa interna de la empresa de compliance si hay incumplimiento, pero eso también tiene que quedar reflejado en las actas del comité.

Lo importante es la documentación que tú puedas aportar, porque en el juicio es donde se va a poner en tela de juicio tu programa de compliance y ahí tienes que aportar todo lo que puedas para que el juez se lo crea y diga "tienes un plan de compliance, bien, ahora puedo valorar que te ponga una pena de responsabilidad penal de persona jurídica o no", porqué el juez puede decir que sí tienes responsabilidad. Eso también nosotros lo decimos, puede exonerar de responsabilidad a la persona jurídica el plan de compliance pero no es seguro. Es decir, puede el juez valorar que está muy bien que tengas eso pero al final lo ha valorado por otras cosas que no faltan en el mismo. Aún no hemos visto suficientemente casos, pero en todo caso no es seguro. Así lo dice el CP "podrá exonerar o atenuar la responsabilidad penal...", pero no es objetivo, no se tiene medido.

Nos ponemos en el caso de que eso irá por un delito concreto, porque ahora la mayoría de condenas de las personas jurídicas están siendo muy sencillas desde este punto, puesto que no tienen planes de compliance, entonces el juez sólo valora eso y cuánta multa o qué pena le impone. No ha entrado demasiado en eso, pero por el momento imaginamos que todo irá por informes periciales, que por el momento no sabemos quién va a ser el experto en programas de compliance que los haga, pero imaginamos que será un perito que valorará las medidas de seguridad concretas. Así, si hubiera habido un delito de revelación de secretos y la empresa tuviera un plan de compliance y dentro de ese plan tuviere un protocolo de protección de la información, el perito se encargará de valorar ese protocolo con lo que ha pasado y verá si ese protocolo era suficientemente potente como para evitar ese delito. El protocolo existía, todos los testigos así han dicho conocer de su existencia, pero alguien aun así ha decidido incumplirlo. Entonces dirá que era suficientemente fuerte, considerando que la empresa ya ha hecho todo lo que tendría que hacer, esto es, hasta donde era razonable llegar la empresa ha llegado, aunque una persona se haya saltado todos los controles.

Todo ello se hará con peritajes, puesto que un juez solo es experto en derecho penal. A un juicio irían el perito informático de la empresa y aquél pedido por el fiscal a la oficina judicial. En el interrogatorio no habrá variedades, el juez se fiará de los peritos y eso también dependerá de la perspicacia de los abogados en las preguntas que les darán credibilidad o no a los peritos. Pero en todo caso, a pesar del vocabulario técnico inteligible para no expertos en la materia, abogado y perito deben ponerse de acuerdo para que lo que ha pasado allí se entienda y quede claro. Eso funcionará como siempre, traerán un perito para valorar la seguridad informática y otro para valorar el compliance."

PREGUNTA: En relación a la información tratada y custodiada por la empresa, en 2018 será de obligado cumplimiento para todas las empresas de los Estados Miembro el

nuevo Reglamento Europeo de Protección de Datos. ¿Qué implicaciones va a tener la entrada en vigor de este nuevo reglamento para la empresa? ¿Va a suponer un incremento en los costes de la empresa? ¿Este nuevo reglamento supone un paso adelante o hacia atrás?

"Creo que aquí la clave va a ser nuestra Agencia de Protección de Datos si se pone las pilas. En teoría, están impulsando una nueva LOPD española, cuyo Proyecto de Ley ya están haciendo. Esta ley en principio lo que va a hacer es regular las dudas que se generen del reglamento, porque el reglamento se va a aplicar sí o sí directamente sin necesidad de trasponer nada. Pero entiendo que convivirán las dos normativas, la nueva LOPD pensada para convivir con el reglamento y, en base a esto, la Agencia Española de Protección de Datos imagino que en cuanto salga va a estar emitiendo constantemente Circulares sobre cómo se regula esto y aquello, haciéndonos el favor a los ciudadanos de entender cómo va a funcionar todo este reglamento.

Nosotros estamos valorando si ya empezar a decirles a los clientes sobre ello, pero creemos que es una imprudencia ponernos ahora a asesorar sobre cosas que no es que no entendamos sino que no tenemos cómo encajarlo en una empresa. Lamentablemente, estamos esperando a tener algo más sólido para proponerles un plan de incorporación al nuevo Reglamento. Porque hay empresas que han hecho un gasto bastante importante en toda la materia de compliance y tienen una estructura muy bien organizada. Entonces, esta gente que tiene ya esta estructura creada, hay que ser muy cuidadosos con qué les modificamos. Sólo habrá que modificar aquellas cosas contrarias al nuevo reglamento, por ejemplo, lo de los ficheros, que se tenían que declarar ante la Agencia Española y ya no será necesario porque ahora se guardarán desde un registro interno que tienes que tener a disposición de una inspección por si se te requiere."

PREGUNTA: Pero, por ejemplo, a partir de ahora se deberá notificar ante la Agencia si por una brecha de seguridad se ha sufrido una fuga de información, así como también a aquellos sujetos cuyos derechos puedan haberse visto vulnerados.

"La clave va a ser cómo va a sancionar la Agencia a alguien que no haya hecho esto, es decir, ante un incumplimiento de notificación y que lo haya arreglado todo "en casa", a ver cómo se va a solucionar. Pero no me acabo de creer yo esto, no me creo que una empresa se atreva a desnudarse así. En la LOPD existía un registro de incidencias de todo lo que te estaba pasando y las medidas de seguridad que habías adoptado para que no te volviera a pasar. Pero ahora no, ahora te hacen avisar a la Agencia para que ellos vengan a mirarte y avisar a los afectados. Tú puedes intentar solucionar el problema pero la notificación ya está hecha; esto sirve de excusa para que la Agencia venga a "ver como lo tienes todo, ya de paso".

Hasta ahora, está siendo una Agencia que se financia con sus propias sanciones. En teoría podrían ir a todo tipo de organizaciones, pero a la práctica, de oficio van a grandes empresas y a las pequeñas van por denuncia. Generalmente, a las PYME que hemos tenido aquí no las sancionan, además, aunque no siempre, avisan con dos días de antelación y te da tiempo a reorganizarlo todo un poco. Pero en el momento que existe una denuncia, ya no hay nada que hacer, van a ir y aprovechando, mirarán otras cosas.

Recuerdo un caso de una auditoría, que me pareció un poco de locura, que hablábamos con un informático sobre cuando un usuario te hace un derecho de cancelación para que borres todos sus datos de la base de datos, tienes que borrarlo también de la parte del código, no basta con que no aparezca para un usuario en pantalla porque los inspectores de la Agencia son informáticos y con que tan sólo aparezca un nombre que no debe, ya está. Pero a veces pasa algo y otras no, son arbitrarios. A veces se hace este control tan exhaustivo y otros días no, por interés. Al menos, lo importante es tener lo evidente bien hecho."

PREGUNTA: Todas estas exigencias y regulaciones mencionadas anteriormente parecen estar pensadas única y exclusivamente para las grandes corporaciones. Por ejemplo, la posible sanción impuesta por incumplir la protección de datos en el nuevo reglamento. Entonces, ¿cómo pueden afrontar las PYME con sus recursos todos estos cambios?

"Por un lado, está claro lo que planteas, pero por otro lado hay que recordar que igualmente están afectadas todas las personas jurídicas. Entonces, te puedo decir lo que dijo el Fiscal hace poco cuando estuvo aquí en una conferencia sobre la Circular 1/2016 FGE[1], que vino a decir que deberán adaptarse. En principio, todo es teóricamente, el juez va a valorar que el plan de compliance sea bastante sencillo, que tenga los cuatro elementos básicos y que si tienes una actividad muy específica que solo te mires el delito concreto que va a afectar a tu actividad concreta y si hay que hacer un protocolo de seguridad sobre ello pues uno porque sois muy pequeños.

Entonces ahí también está un poco el reto para las consultoras. Un poco, para los que nos dedicamos a esto, saber adaptarnos a este plan de compliance simplificado que tenga todas las garantías necesarias pero que sea a un nivel y un presupuesto mucho más bajo para que todo el mundo pueda llegar, porque tiene que llegar todo el mundo. Además, estas PYME en ocasiones son proveedores de grandes empresas y estas grandes empresas tendrán un plan de compliance potente y lo que van a hacer es pedirles a todos sus proveedores que también lo tengan.

Nosotros entendemos que la siguiente ola del compliance va a venir cuando todas las grandes empresas lo tengan ya instaurado, porque de momento casi todos los que nos los piden son grandes empresas o empresas pequeñas que tienen miedo o han tenido algún problema y nos llaman, como por

1 https://www.youtube.com/watch?v=TxJWBrRGiGw

ejemplo alguna que se dedica a colegios o empresas con riesgos medioambientales. Por defecto, lo suelen hacer las grandes empresas, las cuales se lo pueden permitir de entrada. Entonces, cuando estas grandes ya lo tengan, la siguiente ola va a ser pedir que lo tengan las pequeñas, pero no será exigible tener uno muy complejo sino simple para que pueda ser asumido.

Eso va a ser más complicado que hacerlos para las grandes empresas, aunque creo que será posible: acreditar que todo el mundo lo conoce, acreditar que todo el mundo cumple las medidas de seguridad, hacer un estudio concreto de la actividad que tienes y en base a eso dibujar tu mapa de riesgos y centrarse solo en aquellos delitos que puedan suceder, haciendo protocolos si se requieren, aunque muchas veces las empresas ya tienen controles preventivos delictivos pensados para eso. Por ejemplo, la LOPD ya previene delitos, entonces indirectamente ya estás previniendo que haya delitos de revelación de secretos, de daños informáticos, etc. Por lo tanto, todo lo que ya tenga implementado la empresa se mantiene y si es necesario algún refuerzo se refuerza, y simplemente se documenta para acreditarlo si alguna vez se está en un escenario donde se deba demostrar algún día."

PREGUNTA: Uno de los elementos básicos del programa de *compliance* es el mapa de riesgos. En relación a las nuevas tecnologías, ¿cuáles son las mayores preocupaciones que tienen las empresas respecto de los riesgos tecnológicos de *compliance*? ¿Cómo pueden afrontarlos?

"Sobretodo, encaminado a los delitos que tienen que ver con los delitos informáticos, mayoritariamente revelación de secretos y daños informáticos, lo que nos estamos encontrando en ocasiones es que muchas empresas tienen los servicios de tecnología externalizados, y yo sí que te destacaría esto porque es una de las vías más conflictivas, porque ellos tienen un descontrol absoluto de sus sistemas. Lo que estamos haciendo nosotros es auditar a la persona externa que se encarga de ello, y le preguntamos por su empresa, cómo funciona, si tiene compliance instalado, y es una forma de darles un toque a estas empresas para que documenten asegurar tener las medidas necesarias, tener un código de conducta en su empresa, y eso es aportado por el responsable de sistemas de esa empresa externa. Y a los de la misma empresa, pues un poco como siempre, vincularlo al sistema de entrevistas, que el responsable informático de la empresa nos certifique que no ha cometido ningún delito, que todas sus implementaciones están correctas, es decir, un poco por el proceso habitual."

PREGUNTA: Entonces, sobre lo que comenta, para las PYME es más fácil tener un servicio de consultoría externo que no tener un órgano mismo de *compliance* dentro de la empresa, aunque para las grandes corporaciones es al revés. ¿Me equivoco?

"No, claro, esto es un problema pero allí el CP ha sido bastante claro, puesto que tiene que ser un órgano de la persona jurídica, es decir, el oficial de cumplimiento tiene que ser alguien de la empresa.

Aunque, hay un matiz para las empresas pequeñas, debido a que tienen que presentar el balance de cuentas simplificado, con lo cual puede ser que el órgano de compliance sea el mismo órgano de administración.

Esto entra en conflicto con la figura del oficial de cumplimiento tradicional porque tiene que ser independiente pero vinculado a la alta dirección. Nosotros la solución que hacemos a veces es que el oficial de cumplimiento sea una persona que no esté vinculada a la alta dirección pero que trimestralmente, mensualmente o cada seis meses tenga una reunión con un representante de la alta dirección y que reporte todo lo que está haciendo, para que se acredite que la alta dirección está enterada, que supervisa, y que si hubiera algo flagrante lo cambiaría.

Nosotros entendemos la independencia como que él nunca podrá ser despedido mediante unos estatutos del oficial de cumplimiento, donde se establezca que nunca puede ser despedido o sancionado con motivo de las actuaciones que lleve a cabo como oficial de cumplimiento. Entonces, en principio allí se garantiza que va a poder actuar independientemente. En la práctica, es mucho más complicado que eso pero jurídicamente no hay más solución que esa; está protegido como si fueras un delegado sindical."

PREGUNTA: ¿Qué ocurre entonces si en el mismo órgano de administración está el oficial de cumplimiento y el delito se produce desde la misma administración?

"Allí es donde el modelo empieza a ser imperfecto porque el órgano de administración al fin y al cabo será como el propio corazón de la empresa y se entiende que si lo cometen ellos pues sobre ellos no lo puede controlar nadie, puesto que el dios supremo de la empresa es el órgano de administración, o en su caso los socios. Pero si se comete allí, es que no hay otra, no se podrán controlar a sí mismos. Podrán auditarse, podrán acreditar que se están auditando por alguien externo, que eso siempre queda bien, pero al final el propio CP dice que para garantizar que se puedan acabar cumpliendo estos planes de compliance no se puede exigir que exista un oficial de cumplimiento. Está claro que es uno de los puntos donde el programa flaquea."

PREGUNTA: Prácticamente en una empresa el mayor número de incidentes provienen del interior de la misma, es decir, del personal. Esta falta de lealtad y concienciación del cumplimiento, esta motivación de venganza tal vez, se ponen en relación con una buena cultura y ética empresarial. ¿Cómo puede hacer frente la empresa a esta tipología de amenazas? ¿Qué respuestas acostumbra a tener la empresa una vez el delito es descubierto?

"Cuando la empresa generalmente despide directamente, por lo que hemos visto no les tiembla nunca el pulso. Cuando ven algo extraño, llaman al detective, perito informático, abogados, y recogen

todo lo que pueden de información, y proceden al despido. En muchas ocasiones, para que el empleado no les de problemas cuando lo despiden (demandas, por ejemplo), le ponen todas las pruebas del delito encima de la mesa y le dicen "no lo voy a denunciar si te vas tranquilamente"; recordemos que hay delitos que es obligado denunciar y otros que no. Entonces la empresa utiliza estas pruebas de delitos para despedir al trabajador pero no denuncian. Y el delito se queda allí, lo que va en contra del espíritu del compliance, aunque eso depende del delito también.

Puede ser que el empleado robe información para venderla a la competencia pero hay veces que es por negligencia. El empleado envía algo por WeTransfer o por el correo personal. La empresa te dice cuáles son los canales seguros de envío de información y los empleados no lo utilizan. Si es accidental, hay mucha gente que interpreta negligencia como accidental, justificando que es un error que se hubiera podido evitar si estuvieras más atento. Yo entiendo que entonces ahí la empresa se moderaría un poco con el empleado, pero técnica y jurídicamente tendrían que darle un aviso.

De hecho, una de las primeras preguntas cuando estamos ante una violación de secretos es "¿la empresa te ha informado?". Es obligación por parte de la empresa informar sobre medidas básicas como por ejemplo sobre contraseñas (no se pueden decir a nadie, cada cuánto tiempo se tienen que cambiar). Todas estas cuestiones deben ser dadas por la empresa desde un primer momento, en un papel que tienes que firmar. En cualquier caso, cuando un cliente nos viene a explicar qué ha pasado, la primera pregunta que les formulamos es ¿tú a este trabajador le explicaste qué tenía que hacer en este caso? Si todo ello está escrito en un papel, en un código de medidas informáticas por ejemplo, que además está firmado por el trabajador, la culpa es toda suya, tanto si alega habérselo leído como si no. Ahora bien, si el código de medidas no llega hasta tales supuestos, el incidente es responsabilidad de la empresa. El empleado entonces podrá alegar perfectamente que él no tenía conocimiento de ello. Se debe prever todo tipo de matices en cada supuesto, de ahí el problema de los programas de compliance extranjeros, que son básicos debido a que no tienen la particularidad de prever los delitos del Código Penal español."

PREGUNTA: Respecto al conocimiento de los incidentes en la empresa, ¿cuál es el canal por el cual se tiene más conocimientos de los incidentes sucedidos en ella? ¿Son los canales de denuncia o *whistleblowing* una herramienta en uso actual por parte del personal de la empresa o simplemente existe pero los empleados temen a "ser chivatos"? ¿Es positivo que los canales de denuncia sean confidenciales o cabe la posibilidad de "efecto rebote", es decir, facilitar la realización de denuncias falsas?

"Aquí tenemos implementado este sistema con algunas empresas y por ahora hemos recibido muy pocas denuncias. Por lo tanto, de momento creemos que la gente aún se tiene que concienciar. Por mucho que les expliques que hay un juez externo, que no le va a traer represalias, yo creo que la vía más clara es la confianza entre cargos. La clave está en la persona de recursos humanos, en la credibilidad

que tienen en la empresa, puesto que allí es donde acuden los trabajadores cuando sucede algo que no entienden o hay algún problema. Si esa figura tiene la confianza de los trabajadores, es lo más importante y a partir de ahí se puede reaccionar. Pero en lo que refiere al canal de denuncias creo que aún le queda tiempo, tiene que estar más asimilado. Pero también pueden no llegar denuncias no porque no se fían sino porque simplemente no hay delitos.

Por ahora no hemos visto denuncias falsas por parte de los empleados, aunque supongo que esto sería más peligroso si fuese anónimo. Como no se define nadie sobre si tiene que ser anónimo o confidencial, lo único que tenemos es que fuera confidencial por el hecho de que si es una persona que denuncia un hecho, no es un policía, luego para investigarse debo saber qué has visto, debo informarme y por tanto te tengo que tener fichado. Como hasta el momento nadie dice nada sobre que no pueda ser anónimo, nosotros lo que hacemos es dejar la opción de no poner el nombre, aunque ya se advierte que si no se pone el nombre, posiblemente la investigación finalice antes de empezar a no ser que se adjunte toda la documentación y pruebas al respecto. Por tanto, lo único que generaría ser anónimo es que la investigación no se acabaría llevando a cabo.

Nosotros lo que hacemos es que la información del denunciante tan solo la vemos nosotros que la recibimos y desde aquí, en caso de que tenga indicios delictivos lo remitimos al oficial de cumplimiento de allí para ver hasta dónde continúa. Pero es que al fin y al cabo esto se hace para evitar que para comunicarlo se tenga que ir al superior, porque muchas veces es el superior quien está "manchado". Al final, se trata de crear una ilusión de independencia al empleado. Si ha pasado algo, la dirección se acabará enterando."

PREGUNTA: En relación al proceso de auditoría y seguimiento, ¿qué papel juegan los profesionales de la seguridad informática al respecto? ¿Entre ellos se incluye al *hacker ético* o se considera que estaría irrumpiendo en algún tipo de ilegalidad? ¿Únicamente se debería contar con profesionales de la seguridad de la información o también con profesionales de otros campos?

"En el hacker blanco no veo problema siempre y cuando eso quede muy claro y sea una relación contractual entre el hacker y la empresa que el hacker puede testear los niveles de seguridad y hasta qué punto. Pruébalo, documéntamelo y sobretodo que quede claro a qué se accede y qué estás mirando, y hasta qué punto concreto puedes llegar, que el hacker quede limitado.

Respecto del concepto de intromisiones, siempre vendrá ligado por si hay consentimiento o no, y cuando lo hay ya no se consideraría así. Es más, si es la empresa quien contrata, de vez en cuando se suele tener permiso para testear y hackear la red. Todo esto siempre que quede bien documentado y dentro de un contrato, con normas definidas previamente. Entrar sin permiso, como el hacker gris o el negro, eso sí que no está permitido.

Lo más básico es que abogados e informáticos se pongan de acuerdo. Los primeros no saben de la parte técnica ni los segundos de regulaciones, o no al menos por norma, y así se podría tener claro en qué consiste el delito exactamente. Los demás departamentos deberán influir en función de lo que les afecte. A veces, el departamento de informática tiene información que no funcionan sistemas informáticos de otros departamentos."

PREGUNTA: Si tuviera que realizar un plan de respuesta a incidentes para hacer frente a ciberdelitos, ¿me podría relatar un decálogo de medidas preventivas o buenas prácticas que debería llevar a cabo la empresa y también su personal durante el día a día?

"Sobretodo como principal los accesos, que en todo momento quede identificado quién entra dónde, y que en todo momento la empresa pueda saber quién accede y qué pasa en ella. Hay veces que los propios trabajadores saben las contraseñas de los demás compañeros y te dicen que "es que sino no podemos trabajar", porque uno envió una factura a un cliente con nombre de otro, puesto que este último estaba de vacaciones. Legal no es, pero la empresa va a tener un problema como algún día suceda algo. ¿Realmente es necesario correr ese riesgo?

Por otro lado, el tema de las copias de seguridad. Tradicionalmente se hacían en las propias empresas, y ahí se almacenan datos personales, con lo cual si no estaban en otro sitio, estos datos no se podían recuperar. Por tanto, se debe velar por la seguridad física de los datos. Está muy regulado si lo haces internamente, y si lo haces externamente, pedir todo tipo de acreditaciones a la empresa externa para asegurarse de que se está haciendo bien.

En relación a los delitos de daños informáticos, uno de los delitos más comunes es despedir a un empleado que borra antes de irse datos importantes porque se cree que la información es suya porque la ha trabajado él. Hay que tener un protocolo de actuación, tanto a nivel administrativo como laboral. En el momento que despides al trabajador, ya no debe tener acceso a nada. Hemos tenido casos que se olvidan de cambiar usuario y contraseña y de quitarle la conexión remota. Si esa información supera los 400 € estamos entrando en un delito si esa información se ha realizado y trabajado en la empresa, puesto que es propiedad de la empresa. Para esto entonces se debe tener un buen protocolo de salida de personal, pero también hay que estar muy bien coordinado con los informáticos para saber qué tiempo necesitan para quitar todo el acceso al empleado a despedir. Ha habido casos de despidos a última hora del viernes y el informático ya no está o el informático es externo y está cerrado y no le pudieron tramitar la baja del usuario ni del remoto. Hubo uno concretamente en el cual se hizo así y en ese fin de semana la persona borró la información, pero la empresa no se dio cuenta hasta un mes más tarde, con lo cual el ordenador usado por ese empleado ya había sido utilizado por otros y era imposible hacer un peritaje allí."

PREGUNTA: En un futuro, ¿hacia dónde cree que evolucionará o se dirigirá el *compliance*? ¿Contra qué retos cree que deberán enfrentarse las organizaciones? Por ejemplo, cómo se podría gestionar la política empresarial *Bring Your Own Device*.

"El caso del remoto es el más peligroso y el más fácil de sacar información, porqué al menos en los sistemas de la empresa no se permite pinchar pendrives y se puede controlar. Esto es una decisión de empresa, es decir, darles acceso remoto a aquellos cargos en los que se confíe o altos directivos que lo necesiten, pero sobretodo tener blindado a qué se puede acceder y a qué no. Pero que todo esto esté en un contrato que fue firmado antes de disponer del acceso remoto. Si asumen sus obligaciones, si pasa algún día algo, te cubres las espaldas como empresa.

Yo creo que es muy similar a la protección de datos, que empezó como una locura pero ahora todo el mundo más o menos lo conoce. Si ha calado a empresas que han implementado y concienciado de la protección de datos, creo que compliance no va a ser menos. El plan de compliance tiene la ventaja que la regulación de la empresa sea adecuada pero no que se aplique, puesto que la empresa lo puede hacer tan sencillo como pueda y puedes hacérselo muy a medida. No es como en el caso de la protección de datos, que tienes muchas medidas y además el reglamento que está por venir.

Creo que le va a dar mucha competitividad a las empresas españolas, puesto que en el extranjero ya se lleva haciendo desde hace años esto, como por ejemplo en Italia, donde ya hace once años que se lleva haciendo esto. EEUU e Inglaterra llevan muchísimo tiempo, ya que lo inventaron ellos. Va a acabar insertándose como una normativa más, como fue el caso de la prevención de riesgos laborales o la contratación laboral en su momento. Poco a poco, primero las grandes, luego las pequeñas, pero el ritmo no sé cuál será. Se meterá prisa o no en función de los jueces, de si empiezan a haber casos de sanciones a empresas por esto. De momento, las sentencias que van saliendo lo hacen muy "a trompicones". A nivel de empresa, muchas tienen el plan de compliance por imagen, por sentirse iguales a empresas inglesas, da mucho caché, y lo consideran una inversión muy buena. Las PYME están asustadas, de momento."

ANEXO II

ENTREVISTA II: JUAN CARLOS RUILOBA CASTILLA

PREGUNTA: ¿Cuál es su perfil profesional y a qué se dedica actualmente?

"Yo soy perito informático e investigador tecnológico. Me dedico a dar respuestas a incidentes y compromisos informáticos cuando ya han sucedido, adquirir las evidencias, analizarlas y presentarlas ante las propias autoridades correspondientes o ante el cliente si es un procedimiento estándar."

PREGUNTA: La Circular 8/2015 establece las conductas de los usuarios atípicas puesto que, según la misma, a pesar de acceder a obras protegidas de forma irregular, no llevan a cabo ningún tipo de explotación económica. Entonces, en tal situación ¿cuál es la protección que reciben los derechos de la propiedad intelectual?

"El tipo tiene varios elementos, uno de ellos es el ánimo de lucro y, si no hay, evidentemente no se cumplen todos los elementos del tipo y por tanto es atípico.

En el caso de usuarios, hay dos procedimientos, no solamente el derecho penal, para proteger la propiedad intelectual. Se establecen otras vías jurisdiccionales para poder perseguir esas invasiones al derecho. Por otro lado, si hay connivencia por parte de quien está proviniendo el servicio y hay un ánimo de lucro que está en esta empresa, aunque sea indirecto, podría cumplirse en esta figura todos los tipos del derecho delictivo y podría ser condenado por lo mismo.

Es decir, imagínate yo estoy dando un servicio de contenidos de obras de propiedad protegidas con derecho intelectual sin permiso del verdadero propietario y me estoy beneficiando porque en mi plataforma donde estoy ofreciendo ese servicio estoy cobrando por una suscripción a los usuarios que están haciendo uso, a través de publicidad, o cualquier otro tipo de beneficio indirecto que pudiera obtener con esas obras. Evidentemente, estoy explotando esa propiedad intelectual de otro y me estoy beneficiando económicamente, con lo cual sería responsable aunque mis usuarios no tuvieran ningún beneficio si consideramos que no es beneficio obtener la obra y no comprarla."

PREGUNTA: Se sabe por estudios que las empresas se ven muy afectadas en términos económicos cuando son víctimas de un ciberdelito, mayoritariamente por fraude. ¿Como empresa, qué es lo que tendríamos que hacer para que no se volviera a repetir en un futuro? ¿Basta con tenerlo en cuenta en nuestro modelo de organización y gestión? ¿Cuál es la mayor problemática a la que se enfrentan hoy en día las empresas?

"La empresa puede ser víctima de dos acciones. Por un lado, víctima directa de la actividad contra ella y/o su sistema de información, pero también puede ser autora porque alguien de sus empleados utilice servicios de la empresa para cometer un delito extra de la empresa, con lo cual también podría ser responsable la persona jurídica si el delito concreto está dentro de los delitos estipulados en que penalmente puede ser responsable la persona jurídica. En otras palabras, no solamente se tiene que proteger de ataques desde el exterior sino de ataques desde el interior.

¿Cómo puede protegerse? Evidentemente, establecer un sistema de gestión, control y monitorización de todas las acciones, es decir, establecer medidas de seguridad para que esos delitos no sean cometidos ni contra ellas ni desde ellas y a un tercero; luego, serían las primeras medidas a implementar. Para ello, tienen que hacer una gestión de todos los riesgos posibles y evidentemente tienen que analizar la probabilidad de que esos riesgos se lleven a cabo en sus sistemas de información o a sus sistemas de información. No solamente hace falta hacer ese estudio, sino luego es necesario un bastionado de la seguridad, es decir, un fortalecimiento de las medidas de seguridad, y también se debe tener en cuenta que aunque esas medidas de seguridad sean implementadas, no eximen de que en algún momento se puedan romper y se puedan producir los ilícitos. Entonces, las empresas tienen que tener un sistema para controlar en todo momento si se ha roto ese sistema y si se está produciendo el hecho.

En resumen, una empresa debe tener una seguridad preventiva, una seguridad detectiva para poder detectar cuando se está produciendo, y una seguridad reactiva, es decir, tener un plan de contingencias sobre cómo tienen que actuar en caso de que se produzcan los hechos, como capturar las evidencias, preservarlas y presentarlas. Asimismo, también deben tener una seguridad holística con el fin de recuperarse del incidente y preservar la continuidad del negocio.

Esa seguridad no solamente tiene que ser tecnológica, también administrativa, analógica, etc., es decir, debe implementar todos los sistemas de seguridad, los cuales deben estar en concordancia con la seguridad general de la empresa y acorde con otros departamentos también, no solamente la figura de los técnicos informáticos, sino el departamental, el departamento administrativo y los propios usuarios, puesto que los últimos son aquellos que principalmente pueden ser objetos del ataque desde el exterior o ser ellos mismos los que realicen el objeto hacia el exterior o hacia la propiedad de empresa.

También se tienen que monitorizar, además de los sistemas, las actividades y acciones de los propios usuarios, y educarlos y concienciarlos para que ellos no sean víctimas de esas acciones o no sean ellos los autores de esas acciones, conociendo cuáles son sus obligaciones y sus limitaciones. Así, de esa manera podrán tomar conciencia de las responsabilidades que puedan tener (civiles, penales, administrativas) que pudieran incurrir en caso de incumplimiento de esas obligaciones.

Evidentemente, las políticas y planes de seguridad se deben documentar, es decir, es necesario disponer de una documentación donde quede estipulada toda la casuística: análisis de todos los activos, de los riesgos posibles, las medidas de seguridad que se implementan y quienes son los responsables de implementarlas, mantenerlas, controlarlas y auditarlas, en caso de que se produzcan los incidentes quienes son o cómo se debe tratar esos incidentes, y luego hacer un seguimiento de que todo eso está

funcionando, y dinámica y automáticamente ir evolucionando las medidas conforme van cambiando situaciones de la empresa, que es constante (cambiar actualizaciones de las aplicaciones de los sistemas de los firewalls, cambian los usuarios, cambian las obligaciones de los usuarios, cambian los roles, hay personas que se van fuera de la empresa o están de baja y otras que se incorporan, etc.).

Por ejemplo, en la política de seguridad de la empresa está estipulado que a una persona cuando esté de baja se le tiene que quitar las credenciales de acceso para no poderse conectar a los equipos. Todo eso deberá quedar recogido en la documentación, pues alguien tendrá que tendrá que supervisar que eso se está realizando y se ha llevado a cabo durante toda la vida de la empresa.

En el caso del juez, tendría que tener acceso a toda esa información, a todas esas medidas y también acceso a todo lo que se ha venido haciendo en esas auditorías. No basta con que estén por escrito sino que además se deben cumplir, y es necesario que alguien diga que realmente se estaban cumpliendo, y sobretodo, es necesario un análisis del incidente. Si el incidente se ha producido de una forma que no estaba recogida en las medidas de seguridad, evidentemente la empresa no sería responsable si tenía las medidas de seguridad adecuadas y mínimas. Ahora bien, si el incidente se ha producido y no se debiera haber producido porque en la política de seguridad decía que eso ya se estaba haciendo y no se estaba haciendo, evidentemente sería un engaño por parte de la empresa.

Por ejemplo, si te dice en una política de seguridad que se hace una salvaguarda semanalmente, que las copias de seguridad se van fuera de la empresa, y luego le entra un malware que le cifra la información y no tienen copias de seguridad, evidentemente pues aquí sería responsable la empresa que realmente dice que está teniendo una copia de seguridad pero no está monitorizando que se estaban haciendo. En cambio, si la empresa tiene contratado ese servicio a una empresa tercera y cada mes está pagando una mensualidad para que le salgan las copias de seguridad, y la empresa tercera le dice que la estaba haciendo y luego no la estaba haciendo, que es un caso real que pasó con un malware y llevaba la empresa tercera más de un año sin hacer las copias de seguridad y cobrando a la empresa mes a mes por ese servicio, evidentemente la empresa no sería responsable, estaba pagando una seguridad y ahí todo puede ser una negligencia de no supervisar que realmente esa empresa estaba haciendo el servicio que le estaba vendiendo."

PREGUNTA: Uno de los mayores riesgos para las empresas son sus propios empleados. Es conocido que los *insiders* son quienes más daño pueden hacer a la organización por disponer de permisos autorizados con acceso a datos confidenciales. Frente a este tipo de amenazas, se habla de disponer de una buena cultura ética y de cumplimiento pero, ¿qué técnicas o herramientas en las TIC puede utilizar la empresa para combatirlas? ¿Basta con solo tener un modelo de *compliance* adecuado?

"Los insiders tienen dos problemas. Por un lado, ellos conocen y tienen privilegios para la información; conocen los activos, cuales son las medidas de seguridad, con lo cual puede saber cómo sortearla y poder acceder a esa información. Asimismo, también son parte de ataques desde el exterior, es decir, también utilizan los usuarios para poder acceder a la información. En otras palabras, pueden ser atacantes o pueden ser ellos el puente intermedio hacia la información. Por este motivo, proteger y controlar al usuario es la primera medida fundamental.

De momento, como no podemos volver a programar los cerebros humanos con parches de seguridad para que estén al día y no sean vulnerables, lo único que nos queda es la concienciación y formación de estos usuarios. Enseñarles cómo tienen que actuar y enseñarles cuáles son sus derechos, sus deberes y sus responsabilidades, advertirles que pueden ser objetos de responsabilidades en caso de no cumplimiento y que pueden ser monitorizados. Esa cultura y educación a los usuarios no es más ni menos que extrapolar el Código Penal adentro de la empresa. El Código Penal establece una serie de leyes de obligado cumplimiento que se sabe que si las infringen pueden caerles las conductas sancionadoras que estén en el tipo. Más o menos, en la empresa viene a ser lo mismo, es decir, educarles y enseñarles lo que pueden incumplir. De esa manera, es la mejor forma de fortalecer ese eslabón de ser víctima el ser humano.

En relación a la seguridad, se tiene que buscar un equilibrio. Si implementas mucho en seguridad, bajas en funcionalidad y usabilidad y además el usuario se puede ver con una espada de Damocles que esté encima y quizás pueda ser contraproducente. Es decir, hay que buscar sistemas en los que sea el propio usuario el que participe también en esa seguridad, saber que él es algo importante dentro de la seguridad y dejarle participar en la implementación de esas medidas. Evidentemente, si los usuarios son partícipes en implementar esas medidas serán más fácilmente susceptibles de seguirlas, más que si son impuestas obligadamente. Para ello, hay que establecer no solamente medidas técnicas sino también medidas psicológicas para que se sienta formando parte de la empresa. No solamente hay que imponerles sino convencerles, y él tiene que ser el propio que se tiene que autoconvencer que eso es correcto por seguridad de la empresa y por seguridad de su puesto de trabajo, puesto que si la empresa desaparece o va mal, va mal contra él. Él se tiene que sentir parte de la empresa y tiene que participar también en la seguridad.

Evidentemente, ese control al usuario es importante pero no es el único. Hay que establecer las medidas de seguridad tradicionales. No hay que olvidar el resto de medidas de seguridad y control, no hay que olvidar meter soluciones endpoint a los sistemas y poder proteger a las empresas tanto de los ataques externos como internos.

Hoy en día se viene diciendo que los antivirus han dejado de ser eficaces, puesto que la mayoría de la ciberdelincuencia lo que buscan son formas que no sean detectadas por el sistema de seguridad. Entonces, hay que establecer sistemas de seguridad que sean más inteligentes y que vayan aprendiendo actividades sospechosas o actividades fuera de la lógica o de la actividad de la empresa. Tiene relación con la inteligencia artificial, es un poco conocer los hábitos normales de funcionamiento de la empresa

para detectar que hay algo fuera de lo habitual. Por ejemplo, yo tengo estudiado que de mi empresa las comunicaciones hacia el exterior no pueden pasar de x gigabytes a la semana, si un día ve un pico que se duplica por tres es que algo está pasando, o si no tengo trabajadores los fines de semana y encuentro que hay actividad en mi sistema el fin de semana es que alguien se está conectando a mi equipo. Es decir, ver cosas fuera de los hábitos normales y alertar al usuario o empresario. Un poco como lo que están implementando las oficinas financieras para combatir los ataques desde el exterior de usuarios no habituales.

Esta medida ya se está implementando. Las empresas que invierten en seguridad también invierten en sistemas digamos de perfiles de actividad de los propios usuarios y de funcionamiento, y cuando detectan algo anormal, por ejemplo, si un usuario se conecta siempre desde dos rangos de IP pero un día se conecta desde una IP que es de un país extranjero, pues va a pedir un pin adicional o una medida adicional de seguridad porque no es lo habitual. Claro que puede ese usuario haber viajado al extranjero, pero ya como es una cosa extraña, para protegerlo evidentemente si detecta algo distinto de lo habitual se tiene que establecer un mecanismo mayor de seguridad, solamente en situaciones extremas, y un poco se tiene que tender a eso."

PREGUNTA: En relación a las amenazas externas, se sabe que existen pero en menos cantidad. Aun así, ¿qué tipo de medidas respecto de sus sistemas puede la empresa utilizar para protegerse de tales riesgos?

"Son similares. Lo importante es conocer qué activos tengo. En el momento que conozco los activos que tengo, tengo que conocer quienes son las personas o qué cosas pueden amenazar esos activos. Saber cuáles son los activos y saber cuáles son los potenciales riesgos que pueden tener esos activos, y si hay gente que saldría beneficiada destruiéndolos o robándolos o modificándolos, y esa gente qué posibilidades tiene y de qué forma lo podría realizar. Solamente conociendo medio bien cómo estoy, en qué situación y cómo es mi seguridad, puedo defenderme de las amenazas externas. No podemos partir diciendo "voy a fortalecer mi perímetro de seguridad y lo protejo en todas las medidas" sino hay que proteger, y es a lo que se tiende ahora y de hecho así lo hace la modificación del reglamento de protección de datos, se habla más bien no de la información sino de los riesgos de la información. Un poco tenemos que ir analizando cuáles son los riesgos y proteger cada riesgo en su medida. ¿Cómo?

Cuando hablamos de un riesgo, estamos hablando de un porcentaje de probabilidades de que se produzca una amenaza, ataque a un activo y consiga el objetivo. Entonces, puede ser que tenga un activo, puede ser que tenga una vulnerabilidad, y puede ser que tenga un atacante, pero debo tener los tres para que se produzca el hecho. Es decir, si tengo el activo, tengo la vulnerabilidad pero no tengo atacantes que quieran explotar la vulnerabilidad o ese activo, entonces no tengo riesgo, y viceversa. Hay que analizar el riesgo, eso es lo complicado, puesto que se debe establecer el porcentaje de que eso se

produzca y una vez lo tengo, dar valor a ese riesgo en el impacto que puede producir. Entonces, no solamente hay que valorar el riesgo sino también el impacto que puede producir en mi empresa.

Ponderando esas situaciones, se deben establecer unas prioridades, de las cuales las más altas son aquellas que puedan hacer más impacto en mi empresa. En función del riesgo se debe actuar, fortificándolos y reduciéndolos para conseguir un equilibrio con el cual la empresa pueda asumir cualquier tipo de impacto. El riesgo 0 es imposible pero si se produce cualquiera de los riesgos posibles, el impacto debe ser asumible y no debe impedir poder seguir con la actividad normal de la empresa; luego, la empresa podrá asumir ese riesgo. Ese cálculo y ese análisis de esa situación es lo complicado.

Por otro lado, la empresa no se puede proteger de un riesgo que desconoce. No puede fortificar una vulnerabilidad que desconoce. Entonces, para ello solamente puede crear alertas, es decir, cosas que están pasando que no son normales. Si tú detectas algo inusual en tu empresa, tienes que estudiarlo también porque quizás está atacando un riesgo que desconoces o están atacando un sistema por una vulnerabilidad que no tienes protegida, con lo cual no la estabas monitorizando ni mirando.

Entonces, para esas cosas que desconocemos tenemos que establecer otras medidas, que son las medidas de actividad distinta a la habitual. Se trata de conocer bien cómo está funcionando día a día la empresa y comprobar que todo sigue igual. Si hay algo que cambia, deberemos examinar qué está pasando aquí y por qué esto es distinto. Allí ya no hay reglas, hay que establecer un procedimiento propietario de la propia empresa para controlar las actividades y detectarlas. En caso de haber una herramienta que haga eso, esa herramienta será conocida por los atacantes y lo harán de una forma distinta para que la herramienta no los detecte; entonces, tiene que ser algo totalmente desconocido y ajeno, por lo tanto, se trataría de medidas complementarias de seguridad propietarias."

PREGUNTA: Una de las fases de un modelo de *compliance* es la de la monitorización y seguimiento. Así, normalmente se acostumbra a llevar a cabo por profesionales de la seguridad informática con el fin de evitar brechas de seguridad. Así, ¿esta fase tan solo es revisada por este tipo de profesionales o bien hay o debería haber otros implicados? ¿Podríamos poner como sinónimo de *hacker ético* al profesional que busca brechas de seguridad en la empresa o se consideraría así algo ilícito?

"En la figura del compliance officer, que los abogados dicen que tienen que ser ellos y los técnicos dicen que son los técnicos, o que tiene que ser una figura interna de la empresa o externa, entra en juego no solamente la tecnología. Hemos hablado también de psicología, de seguridad holística, de derechos fundamentales, con lo cual esa figura o es un superhombre que maneje todas las ciencias y artes o tiene que ser un equipo heterogéneo, formado, como mínimo, por ejemplo por un letrado, un técnico, un responsable de seguridad, un psicólogo, un especialista en derecho procesal, etc.

En el caso del hacker ético, independientemente de la definición de la RAE o de las intromisiones en el Código Penal, yo entiendo la palabra hacker como un experto. Si bien es cierto que tiene bastante influencia en el mundo informático, un hacker podría ser especialista en cualquier arte o ciencia. Entonces, podrían haber hackers informáticos, a nivel legal, o a nivel de cualquier otra ciencia. Qué papel emplea?

Emplea un papel muy importante. Un hacker lo tenemos que definir como una persona que tiene unos conocimientos especiales fuera de lo habitual, fuera de lo que está escrito o lo que la gente normal sabe. Cuando te he comentado antes que parte de las medidas de seguridad que debemos implementar en una empresa deben ser medidas propietarias distintas porque los atacantes no se las van a esperar y de esa manera no se podrán defender ni saltárselas, sería esta figura el encargado de llevarlas a cabo. La función del hacker ético en la empresa sería implementar medidas propietarias, medidas que no tienen otras empresa, con lo cual si el atacante no sabe que están estas medidas, va a ir ocultándose a todas las medidas de seguridad normales pero va a ser detectado o monitorizado por medidas propietarias. Eso sí, tienen que ser cosas que no estén escritas, que no puedan encontrar, que no sean medidas normales, deben ser otras medidas realizadas por esa persona. También si ese atacante ha realizado las acciones, ya ha borrado la información o la ha cambiado para que no sea perseguido, ese hacker ético puede dar respuesta, mirar más allá, por ejemplo, se le puede ocurrir realizar una búsqueda de información donde ha estado el atacante cuando ha ido a borrar la información.

En un caso que hemos llevado hace poco, habían atacado, modificado una serie de documentos, habían cambiado los datos de los ficheros y los meta-datos de los ficheros, pero el atacante no había cambiado las copias de seguridad interiores que se habían hecho. Entonces, ahí tienes que tener una figura que se le ocurra algo más. El papel de la figura del hacker ético sería imprescindible tenerlo para las medidas propietarias o para buscar respuestas a problemas que se susciten de forma propietaria. Si no tiene ese hacker ético en la empresa, se tendría que contratar para implementar esas medidas ad-hoc solo para ella o para investigar un caso, a parte de los expertos con conocimientos o titulados en esas artes, que podrían seguir las recomendaciones de la ISO correspondiente paso por paso o la reglamentación que estuviera en un reglamento que se tenga que cumplir. Esas personas metódicas y que siguen el libro y lo que ya se ha establecido por un grupo de expertos realizan lo mínimo, pero no es suficiente. Nos hace falta ese plus más, que es lo que daría diferencia a la empresa.

Sería una ventaja para la empresa que quisiera defenderse ante un ataque contra ella de que ha sido negligente o de que no tenía las medidas de seguridad correspondientes, puesto que no podría ser acusada de tener responsabilidad porque podría defenderse diciendo que no solamente ha seguido el check-list y las instrucciones que están regladas sino además ha añadido como plus estas medidas para fortalecer.

Si una empresa contrata el servicio de un hacker ético, le tiene que dar una cobertura, no le puede dejar hacer ni campar por su aire, pero eso no quiere decir que esa persona te tenga que dar un balance de todo lo que realice o todo lo que hace. No puede actuar por iniciativa propia, lo que haga lo tendrá

que justificar, deberá quedar plasmado, pero quedará solamente en posesión de la empresa, es decir, la seguridad que implemente propietaria estará en el protocolo de seguridad de esa empresa pero no estará en el protocolo de seguridad de otra empresa.

Claro, alguien que pudiera acceder al protocolo de seguridad de esa empresa podría ver qué medidas de seguridad hay y podría saltárselo, eso sí, pero también podría quedar incorporado en el protocolo de seguridad, cifrado para que no lo pudiera ver cualquiera que pudiera acceder a ese protocolo de seguridad. Ese protocolo de seguridad podría estar custodiado de una forma garantista para evitar que se pudiera violentar, pero todo tiene que estar reglado y tiene que haber contratos de poder de actuación que establezcan que esa persona no se puede extralimitar, que no puede violar ningún derecho fundamental. Aunque sea un hacker, tiene que ser ético, no puede ir realizando cosas que sean ilegales; se pueden hacer muchas cosas éticas distintas y que no son ilegales. Todo lo que puedo hacer que no sea ilegal, lo puedo implementar; lo que es ilegal, no lo puede implementar aunque lo deje por escrito."

PREGUNTA: Cada vez es más frecuente el uso y la presencia de dispositivos tecnológicos en la empresa. Por un lado, aportan un mayor valor competitivo a la empresa pero por otro, aumentan la probabilidad de amenaza. Así, por ejemplo, la política empresarial BYOD empieza, o empezó hace unos años, a ser muy frecuente. ¿Cómo puede gestionar la empresa este tipo de situaciones sin incurrir en un "sistema policial" de monitorización constante de la actividad en los sistemas de sus empleados, de sus correos electrónicos, etc.? ¿Esto no chocaría con los derechos de los trabajadores?

"Ahí tenemos un problema. Para controlar las actividades significa entrar en la esfera de la privacidad de las personas, es decir, monitorizar un poco todo lo que hacen. Entonces, siempre está la dicotomía que si aumenta la seguridad se pierde la privacidad y se tiene que buscar un equilibrio. Estas monitorizaciones no tienen por qué ser constantemente supervisadas o miradas por una persona, es decir, se puede guardar esa información y ser usada solamente en caso necesario.

Es como el tema de monitorizar todos los actos que hace una persona. En un momento determinado, si se produce un incidente nos hace falta saber qué ha pasado (por dónde han entrado, qué es lo que han estado haciendo, qué se han llevado, qué han añadido, qué han modificado, por dónde se han escapado). Para poder tener esa información significa haber monitorizado todo, pero si monitorizas todo significa también monitorizar las actividades normales de los usuarios. Eso no quiere decir que si yo estoy grabando toda la información que entra y sale y se genera en mis equipos, esté mirando constantemente todo lo que hacen mis usuarios.

Se tendría que establecer un sistema en que esa información se guardara pero que no fuera accesible ni por los propios empleadores / administradores. Esa información quedará registrada pero también cifrada, y solamente ante un incidente alguien con mayor poder decisorio o una autoridad judicial en un momento determinado podría ordenar descifrarla para verificarla y examinarla con garantías de no invasión de la privacidad, solamente en el incidente que se estuviera investigando. Entonces, se tendrían que buscar soluciones como ésta: que se monitorizara todo pero que solamente fuera accesible en caso de seguridad, y en ese caso, sólo accediendo a información relacionada al incidente de seguridad.

Esto se tiene que estipular y reglamentar muy bien y no se puede dejar a decir a la buena fe del empresario, es decir, no basta con que éste te diga "no, no, esto está cifrado y la clave solamente la sé yo pero no voy a entrar", puesto que un día ese empresario puede sentir curiosidad por fisgonear qué está haciendo un empleado cualquiera. Entonces, tiene que haber medidas que no se puedan romper ni por el empresario. Esto no está reglamentado ni estipulado pero yo creo que sería la forma correcta de hacerlo.

Por ejemplo, también podría haber tres llaves, entonces tres personas distintas se tendrían que poner de acuerdo en un momento determinado para poder abrir la cerradura si quisiéramos ver esa información en un momento determinado. Es decir, establecer algún mecanismo que fuera garantista y que garantizara la privacidad de los propios trabajadores.

Cuando se implementa BYOD o BYOT en la empresa, tiene que llevar aunado el control de ese dispositivo o de la parte del dispositivo que vas a utilizar para el nivel corporativo. Hoy en día, los dispositivos permiten tener varios dispositivos virtuales, lo cual permite generar un segundo dispositivo para la empresa dentro de tu dispositivo, y ese dispositivo con información de la empresa tiene que estar protegido, controlado y monitorizado por la empresa. Yo te puedo dejar traerte tu móvil y tú me tienes que dejar acceso a tu móvil para configurártelo adecuadamente y no poner en peligro mis activos, porque sino no puedo poner en riesgo mis activos en tu móvil, porque tu móvil lo puede coger tu hijo, tu mujer, tu marido, quién sea, y tú puedes ser muy consciente de lo que puedes instalar o no, pero si tú le dejas el móvil a tu hijo, él puede bajarse una aplicación o un juego que puede ser un malware y si allí está la cuenta de correo corporativo puede acceder a ella, o al control remoto de mi empresa o a la VPN.

Entonces, ese dispositivo si se permite utilizar en la empresa, tiene que tener dos perfiles, un perfil suyo y un perfil corporativo. Y las aplicaciones que se carguen en un perfil no pueden ver la información que sea corporativa, y viceversa. Hay soluciones para configurar los dispositivos que necesitamos en la esfera personal y esfera laboral con garantías de seguridad. La medida más estricta es utilizar las aplicaciones que quiera instalar el empleado en el dispositivo a través de la tienda de la empresa, debido a que la empresa auditará sus aplicaciones y el empleado en lugar de conectarse a la tienda del sistema operativo de su móvil, lo hará a la tienda de la empresa y así solamente el dispositivo podrá instalar aplicaciones auditadas por la empresa.

Asimismo, ese dispositivo tampoco se conectará a toda la infraestructura tecnológica de la empresa, sino a unas parcelas concretas y serán aquellas áreas de menor riesgo de impacto, es decir, si

solamente necesita el dispositivo para el correo, solamente se podrá conectar con el dispositivo propio al correo, pero a lo mejor no puede acceder a la contabilidad, a la cartera del cliente, a los proyectos, al I+D. De ahí que el empleado tenga que dejarse auditar el dispositivo, puesto que se considera que si la empresa te deja utilizar tu dispositivo, también debes dejarla poder supervisarlo. Hoy en día, se pueden tener dos o más teléfonos o en un mismo dispositivo tener distintos perfiles, áreas que no pueden interactuar entre ellas y de las cuales la de la empresa está cifrada. No es problema de implementación.

En empresas nos vamos a encontrar con un gran rango de tipos, puesto que puede haber empresas muy estrictas en seguridad y otras totalmente ajenas a la seguridad. ¿Qué es lo idóneo? Todas cercanas a la máxima seguridad pero, ¿cuál es la situación de la realidad? Que están casi todas cercanas a la inseguridad."

PREGUNTA: En términos de cumplimiento, una empresa debe de acreditar constantemente su buen funcionamiento y actuación, pero este volumen de regulaciones parece a veces actuar en contra. ¿Cómo pueden las empresas gestionar sus recursos correctamente e implantar un buen modelo de *compliance* eficaz pero asimismo gastar en medidas preventivas de seguridad? ¿Es la seguridad de la información un ítem valorado y tenido en cuenta por las empresas o simplemente actúan en el caso de que hubiera habido algún incidente porqué consideran que "a mí esto no me va a pasar"?

"Hay empresas que conciben estos riesgos como un riesgo lejano o algo que no les va a pasar a ellos, entonces hasta que no les pasa no se lo creen y por eso son reacios a invertir en seguridad. Dependerá de la empresa, hay empresas que invierten en seguridad tradicional y en cambio no protegen su información.

La seguridad de la información será un ítem valorado en función de las personas que dirijan la empresa. La tendencia es que cada vez aumente esa seguridad de la información, pero si no hay ayuda por parte de una obligación legal para cumplir, cuesta. Mientras no hubo la Agencia de Protección de Datos ni la LOPD, la gente con los datos personales hacía y deshacía lo que quería y eso provocaba una gran inseguridad con los datos. Al sancionar si no los tenías regulados y protegidos, evidentemente eso ayudó a que las empresas se protegieran, declarasen sus datos y solamente tuvieran aquellos datos necesarios para su actividad. Pero si no hay esa ley que ayude un poquito, cuesta. A veces, tenemos que usar esa espada de Damocles, que ya he mencionado antes."

PREGUNTA: Normalmente, esta estandarización y normalización del sistema de gestión de la seguridad de la información y del sistema de gestión de *compliance* y para la protección de datos están pensadas para grandes corporaciones, pero me preocupan

las PYME, tipo de empresa más frecuente en España. ¿En qué lugar quedan a la hora de poder combatir con todos estos riesgos y cómo pueden acreditar su buen funcionamiento si muchas veces piensan que cuesta mucho dinero, no tienen percepción de poder ser víctimas de un ciberdelito y por lo tanto no es una prioridad en la que invertir, o incluso a veces simplemente no tienen tanto dinero para gestionarlo?

"La prioridad de invertir o no para una PYME es porcentual a la facturación de la empresa. Si factura menos, el porcentaje de la sanción también se reduce. Esas son las tendencias, que hayan sanciones también porcentuales a nivel de la facturación.

Primero, hay que saber, determinar y fijar quienes están obligados a hacer una evaluación de impacto, qué empresas van a estar obligadas a implementar una serie de medidas que impone el reglamento. En el momento que se sepa, por la información, por el volumen, por ciertos indicadores, entonces las empresas estarán más o menos obligadas a implementarlas. A mí eso me parece contraproducente, puesto que la seguridad tendría que ser igual para todos. Se habla de que si son pocos datos no van a estar obligadas. Pero, ¿por qué se decide eso si es igual de grave para una persona que le roben únicamente sus datos como si se hace a cincuenta mil personas más a su vez? Entonces, esto tendría que estar regulado igual para todas las empresas.

En el caso de las sanciones, tienen que ser equitativas en función al daño que pueda originar a la empresa. Si es una multinacional y fuera una sanción fija, a lo mejor para una multinacional 50.000 euros es nada y entonces 50.000€ no serían una sanción. Pero para una PYME ,esa cantidad podría llegar a suponer la facturación de un mes o de todo un año incluso, entonces evidentemente no sería justo; luego, tiene que ser proporcional. A mí me parecen adecuadas las medidas que hay cuando se hacen sanciones proporcionales a la facturación de la empresa. Ahora bien, desconozco si todas van por ahí o solamente van algunas.

Lo justo sería que la justicia fuera en concordancia a lo que se pretende. Muchas veces se habla que las sanciones sirven para recuperar, para enderezar, para mejorar, no para castigar. Entonces, se trata de que sea así, que cuando se sanciona a alguien le des una segunda oportunidad y para que le sirva como un toque de atención porqué lo ha hecho mal y se le está advirtiendo para que en un futuro no se vuelva a repetir, por ello se le aplica la sanción, sanción que debe ser constructiva; luego, se debe tender a una reglamentación que aplique una serie de sanciones no para hundir la empresa sino para reconducirla, para castigarla pero en su justa medida. Por este motivo, no puede haber sanciones cuantitativamente igual que en vez de cualitativas. Es difícil pero hay soluciones.

Se pueden buscar soluciones corporativas, como por ejemplo aunar empresas de la misma tendencia o similitudes con una misma solución corporativa para todas ellas. Por ejemplo, imagínate que una solución fuera un centro de back-up (en caso de incidente, tengas un replicado toda la tecnología de la empresa). Para una empresa sola podría ser un coste considerable pero si se unen 20 empresas pequeñas y tienen el centro de back-up para cuando les haga falta, como no van a ser atacadas

las 20 a la vez, comparten gastos y disponen de esa solución. Igual puede hacerse con un sistema de incidentes o una serie de personas que le controlen la seguridad a una empresa, puesto que a una PYME no le sale a cuenta disponer de un departamento especializado y por ello deberá contratarlo externamente. Evidentemente, si tienes tres equipos no vas a pagar los mismos sueldos que si tienes cien. Si tienes cien, necesitarás más horas de ingeniería para supervisar tu sistema. A lo mejor para una empresa de 10 personas con que vaya un técnico tres horas a la semana es suficiente para mantener, revisar y adecuarle el sistema, con lo cual tiene que ser equilibrado. En resumen, si no puedes asumir el gasto, compártelo.

Este servicio lo estamos ofreciendo a empresas pequeñas, así como también servicios temporales acorde a su situación. Estamos fortaleciendo su estructura tecnológica implementando medidas de seguridad igual que si fuera una grande empresa pero no estamos full-time; en algunas un día por semana y en otras uno cada quince días, depende del tamaño de la empresa, con lo cual son gastos asumibles. Tener un trabajador a tiempo y jornada completa le saldría mucho más caro a una PYME, puesto que debería pensar en tener repuestos en vacaciones o por si se pone de baja, con lo cual todo se duplica.

En el caso de las grandes empresas, les sale más a cuenta tener su propio equipo interno. Entonces, tienes que ver en qué situación estás como empresa, hacer números, y quedarte con aquello que te penalice menos y te sea más efectivo. Evidentemente, como ya se ha dicho antes, en el caso de las PYME siempre será mejor externalizar el servicio, pero siempre supervisando que te cubra, garantice y te de toda la información, que te tenga al día de todo aquello que hace, no se puede depender. Así, no puedes contratar al más barato y pensar que te lo está haciendo todo bien, pero tampoco al más caro porqué no significa que te lo haga bien. Hay que buscar aquel que haga lo que necesitas y a la vez te salga rentable.

El problema que veo es que cuando sea obligado disponer de este servicio para las empresas, esas empresas se van a ver en la necesidad de tener esas figuras y cumplir con esos reglamentos. Por tanto, esto es un caldo de cultivo para muchos oportunistas que van a vender humo o servicios no verdaderamente eficientes. Estos oportunistas están viendo un mercado y quieren apuntarse al carro de esta demanda a esos profesionales. Las PYME deben tener mucho cuidado con saber a quién delegan ese servicio, porque va a haber mucha guerra de mercado y pueden no hacértelo bien pero cobrártelo igual; luego, si pagas, tienes que exigir que realmente se te de ese servicio. Hay que buscar el equilibrio. Si las PYME no tienen alguien que les asesore bien para que realmente conozcan a quien van a contratar, ese es el problema que les veo yo. Otro inconveniente va a ser encontrar a la persona idónea para delegar ese servicio, no por temas de implementación. Una asesoría no puede cobrar lo mismo a una grande empresa que a una PYME. De hecho, es bastante fácil proteger a una PYME y le puede salir bastante barato. Las PYME son las empresas más atacadas."

PREGUNTA: Si tuviera que aconsejar a una empresa sobre qué medidas tomar en su empresa acerca de las TIC, ¿qué le recomendaría? ¿Podría hacerme un decálogo de medidas básicas que toda empresa debería tener en sus sistemas?

"Como medidas básicas de prevención y monitorización:

- *Saber y comprender que no estamos seguros.*
- *Conocer los riesgos, amenazas y vulnerabilidades de nuestro sistema IT.*
- *Formar y concienciar a nuestros empleados.*
- *Gestionar los riesgos del uso de redes sociales, foros y comunicaciones.*
- *Tener una política de seguridad, un plan de reacción y un plan de contingencias al día.*
- *Establecer una buena política de salvaguardas.*
- *Disponer de un responsable de seguridad, interno o externo, que supervise y controle la seguridad.*
- *Instalar soluciones de seguridad multipropósito y actualizarlas.*
- *Tener los equipos, sistemas operativos y aplicaciones actualizadas.*
- *Control de los usuarios que realizan teletrabajo (trabajo a distancia).*
- *BYOD (Bring Your Own Device) o BYOT (Bring Your Own Technology), tenerlo en cuenta.*
- *Canalizar las comunicaciones exteriores a un mínimo de puntos para controlarlo mejor (cortafuegos y IDS/IPS).*
- *Controles continuos de los privilegios de las cuentas de usuarios y recursos.*
- *Autenticación y gestión de las identidades de los usuarios.*
- *Bastionado de los equipos (hardening) para fortalecer la seguridad.*
- *Conocer y clasificar nuestros activos, así como los potenciales enemigos.*
- *Aplicar diferentes círculos de seguridad en aquellos activos más valiosos.*
- *Si se ha producido un incidente o se sospecha, actuar de forma profesional.*
- *Vigilancia constante y esperar lo inesperado.*
- *Equipo preparado o empresa forensics para dar respuesta a lo sucedido.*

Y, con respecto al protocolo de acción, hay que tener en cuenta:

- *Estudio y análisis del caso donde debería estar presente no solo el alto cargo de la empresa sino también el representante legal, responsable de informática, investigador del caso, testigos y víctimas.*
- *Nombrar una persona encargada del caso (coordinador), quien tomará notas de todas las personas relacionadas con el incidente, mantendrá el control de la situación y permanecerá en la escena evitando la manipulación hasta que sea revelado por un investigador. No se trata de nombrar una persona a quien "echarle el muerto" si las cosas van mal.*

- *Comprobar si los hechos pueden ser constitutivos de delito y, de ser así, ponerlo en conocimiento de las autoridades. También se puede realizar ante las FFCCSE.*
- *Adquisición de las evidencias ante fedatario público priorizando aquellas evidencias volátiles y realizado por un experto. En la medida que sea posible, estas evidencias deberán ser clonadas para su análisis y custodiadas o los originales puestos a disposición notarial / judicial. Salvo necesidad imperiosa, nunca debe alterarse la evidencia y, de ser inevitable, las alteraciones deberán estar documentadas y motivadas.*
- *Análisis de las evidencias (copias u originales sino es factible aquella) realizado también por un experto, preferentemente ajeno a la empresa para mantener al máximo la integridad y objetividad de sus conclusiones.*
- *Correlación de información necesaria para poner en contexto el resultado de los análisis como pudiera ser las sincronías horarias de equipos y servidores, topología de la red, protocolos de comunicaciones y almacenamiento de información, registros de historiales, copias de seguridad, roles de usuarios, etc.*
- *Redactar el informe pericial del compromiso y actuar en consecuencia. Si es un hecho delictivo presentar el informe conjuntamente con el escrito de denuncia.*
- *Mantener el máximo de discreción con el incidente y las diligencias a efectuar y medidas cautelares solicitadas, si es necesario solicitar el secreto de las actuaciones."*

PREGUNTA: Por último, ¿cuáles son los retos a los que cree que tendrán que enfrentarse las empresas en un futuro próximo en relación a las TIC y el *compliance*?

"Si extrapolamos un poco a lo que ha pasado otras veces, que al principio va haber mucha reacción, animadversión con todas las modificaciones, habrán empresas que lo sigan, otras serán reacias a implementarlo, pero poco a poco todo se va a ir encausando, de hecho, muchas de estas medidas ya están premeditadas desde hace tiempo y se están siguiendo. Las sociedades occidentales o más bien latinas, acabarán llegando a una situación parecida, igual no llegamos a ese nivel, pero sí acercando cada vez más. Se irán asumiendo. Evidentemente, el reglamento sufrirá modificaciones, de vez en cuando aparecerá jurisprudencia, habrán interpretaciones del reglamento y esperemos que sean con sentido común. Es decir, que se apliquen en su justa medida, que no sean tan receptiva como semánticamente nos da a leer si leemos realmente el reglamento. Entonces, se tendrán que adecuar, que llegar a un equilibrio.

Las empresas en principio lo que tendrán que ver que esto que parece ser algo nuevo dejará de ser algo excepcional y tendría que ser algo normal. Cada vez más hay digamos una protección a la información, a seguridad, y tienen que ser conscientes que si no implementan, puede ir contra el propio negocio. Evidentemente, si empiezan a haber sanciones a otras empresas, puedes pensar que "me puede tocar a mí", si me toca a mí puedes pensar por qué no lo he implementado y entonces lo implementarán

para no volver a caer en la situación. Si realmente se cumple, se llegarán a implementar y las empresas empezarán a tener consciencia y a hacer cumplimiento normativo. Si realmente no se aplica y no hay sanciones importantes y solamente afecta a bastantes empresas, las pequeñas empresas dirán "esto no va para mí" y tardaremos muchos años a que todas las empresas empiecen a tener consciencia. Solución: claro, tampoco se trata de que las primeras sancionadas lo sean cuantiosamente porque las hundes.

En advertimiento tampoco soy muy partidario, es como cuando meten en una carretera unos radares y las primeras multas solamente te llegan a tu casa y te avisan con una carta diciendo que la próxima vez el mes que viene ya será esta multa. También puede ser un toque de atención, dejar un plazo. Sí que eso conlleva una situación, que es que reinventamos un reglamento y tiene que haber alguien que supervise que realmente ese reglamento se está cumpliendo. Puede pasar que no haya esa supervisión metódica o que solamente sea a raíz de incidentes. Si se produce el incidente se comprueba si realmente se estaba haciendo, o si hay una denuncia de si la empresa no está cumpliendo con el reglamento, entonces los inspectores que van a supervisar esa denuncia. O también pueden haber inspecciones periódicas, comprobando en esa empresa aleatoriamente si se está llevando a cabo. Eso es según como lo implementen pueden hacer que sean más rápido o más eficiente la implementación.

Yo recuerdo cuando se descentralizó en policía nacional los ordenadores, en las comisarias habían máquinas de escribir, entonces se cambiaron las máquinas por ordenadores. Muchas comisarias dejaron un tiempo las maquinas y los ordenadores y así un comisario podía hacer la denuncia con la máquina o con el ordenador. Después de dos o tres meses, en toda España tuvieron que desechar el sistema informático porque no se implementó. En cambio, en Cataluña se instalaron los ordenadores y quitaron las máquinas, obligando a utilizar los ordenadores, sin alternativa. Aquí siguió funcionando el sistema informático. Antes de implementarlo, se hizo una estrategia: formamos a los usuarios en nuestras dependencias y no pusimos el sistema informático hasta que estuvieran los funcionarios formados. Los primeros 15 días de implementación mandamos gente nuestra las 24 horas con las usuarios por si alguno se estancaba ayudarles in situ, y luego les dejamos solos.

Hay que hacer un cambio disruptivo total pero ayudando, dando formación, concienciación y apoyo en la implementación. Si nosotros queremos implementar algo nuevo en las empresas, tenemos que hacer eso: formar, concienciar y cuando lo implementemos, no darles alternativas a que no lo hagas pero tener gente ayudándoles a implementarlo. No lo van a hacer así, con lo cual, la gente seguirá manteniéndose hasta ahora. Entonces el mensaje es que si quieres implementar algo tienes que hacer una estrategia de implementación para que esto funcione; si no se hace, la probabilidad de fracaso es muy alto."

ANEXO III

ENTREVISTA III: JOSÉ RAMÓN AGUSTINA SANLLEHI

PREGUNTA: ¿Cuál es su perfil profesional y a qué se dedica actualmente?

"Soy abogado penalista y profesor de universidad. Trabajo en la UIC como director de Derecho Penal y en el despacho Molins & Silva como abogado consultor, donde llevamos temas de compliance y defensa procesal de personas físicas y jurídicas."

PREGUNTA: Sobre la Circular 8/2015, ¿considera una buena redefinición normativa que el acceso irregular a un contenido protegido con la finalidad de no pagar el precio exigible de esa obra quede fuera del derecho penal? ¿Se podría decir que se ha encontrado ya un equilibrio entre los intereses de las grandes corporaciones productoras de contenido audiovisual y los derechos civiles de los internautas?

"Tuvimos un "Laboratorio de Piratería" en febrero y hubo una discusión. Hubo gente de la empresa del mundo audiovisual, que les importaban los derechos contra la propiedad intelectual, pero también del mundo de las asociaciones internautas. Allí se veía un poco que el factor cultural influye mucho, es decir, hay una falta de percepción social de que hay personas que necesitan vivir de ello porque es el fruto de su trabajo, y luego sucede que los creadores o autores muchas veces ceden sus derechos a empresas que explotan sus obras, que son los que realmente ganan dinero.

El problema que hay con los derechos contra la propiedad intelectual es que hay una lucha constante. ¿Cómo llegar a un punto medio? Se buscan nuevas formas de consumo en streaming que de alguna manera permitan no un consumo pirata sino más asequible y en los cuales no haya que pagar unos precios tan elevados, todo ello para, de alguna manera, hacer frente a la situación de piratería. Esto tiene el peligro que, por ejemplo, en la creación literaria, si se sabe que es un libro que va a ser pirateado y que no va a obtener beneficios porque no se va a vender suficientemente, eso tiene el riesgo que la gente que realmente vale y tiene talento para escribir ya no lo siga haciendo."

PREGUNTA: Es sabido por una gran cantidad de estudios que las empresas son potenciales víctimas de ciberdelitos, teniendo especial relevancia los daños, en términos económicos, que le supone a la empresa. Así, ¿cuáles son los delitos relativos a las nuevas tecnologías que más padecen las empresas?

"Por un lado, los ciberataques. Por ejemplo, un ataque de denegación de servicio, el cual es un bombardeo constante a una central y una página web y eso bloquea y colapsa la página. El phishing, es decir, cuando en las interacciones de la empresa alguien clica un link que lo lleva a una página web falsa

para hacer una transacción económica que en el fondo es un fraude. Otros podrían ser los delitos contra la propiedad intelectual, esto es, ataques a bienes inmateriales de la empresa, como pueden ser obras de arte, obras del mundo audiovisual, a las cuales se hacen es un plagio y se hace que gane menos dinero aquella empresa. Después, también puede haber delitos de descubrimiento y revelación de secretos, donde una empresa sufre una fuga de información, a veces porque se te mete el hacker y se te lleva información que pone a conocimiento del público o a veces puede ser porque haya un trabajador que es despedido de la empresa y se lleva información confidencial propiedad de la empresa con la que monta otra empresa en la competencia."

PREGUNTA: En una empresa, las amenazas internas resultan ser la infracción más relevante en términos cuantitativos y estratégicos. Entonces, ¿qué puede hacer la empresa para prevenir tales infracciones? ¿Es suficiente con haber implementado un modelo de organización y gestión, sobretodo en aquello relativo a una cultura ética y de cumplimiento?

"Se tendrán que adquirir una políticas TIC dentro de la empresa sobre cómo tienen que usarlas. En el caso de las políticas BYOD, sabemos que cuando usas un instrumento tuyo o una herramienta de trabajo proporcionada por la empresa podemos generar que haya un ataque informático, porque podemos generar una fuga de información. Ahí, hay estrategias de protección de los activos de la empresa que están basados en el impedimento, son barreras. Por ejemplo, hay empresas que impiden el uso del pendrive o enviar archivos adjuntos por el correo electrónico corporativo. Esto es una primera dificultad.

Si uno quiere revelar información o llevársela al final lo conseguirá, pero de alguna manera el mundo digital lo que te permite es dejar rastro de todo. Si yo imprimo un documento, quedará registrado que he imprimido ese documento. Entonces, si los trabajadores son conscientes de que todo lo que hagan en el contexto de la empresa va a quedar registrado, de alguna manera lo disuadirá. Como la prevención situacional del delito: si tienes una consciencia elevada del delito porque puedes ser descubierto, disuadiré mucho al potencial infractor. Es una de las cosas más importantes.

En España, hay muchas empresas que no se preguntan más, dependerá mucho de la empresa, del tipo de información que tengan. Por ejemplo, hay despachos de abogados que no tienen mucha sensibilidad sobre la información, con lo cual podría un periodista robarte información para hacer una exclusiva, como en algunos casos ya ha sucedido. Entonces, hay que ver como cada empresa identifica los bienes más sensibles y cómo protegerlos."

PREGUNTA: En relación al modo de implementación de políticas de uso, prevención y control de las TIC en la empresa, ¿cuál es la capacidad técnica real de la empresa en la

detección e identificación de la infracción? ¿Qué métodos se implementan? (e. g. identificación del usuario, revisiones periódicas de cumplimiento, control de fugas de información, etc.)

"Esto dependerá de cada empresa. Yo hace unos años hice un protocolo para medir la capacidad de respuesta del departamento de IT ante un incidente. Pasamos un protocolo para ver si el departamento de IT estaba entrenado para resolver los incidentes (e. g. me han hackeado la página web de la empresa y quiero descubrir quién ha sido). Se les hacían una serie de preguntas para ver si tenían los mecanismos adecuados en un tiempo razonable, breve, y podían detectar quién había sido. Entonces, esto todavía falta mucho por hacer y dependerá del tipo de empresa pero sí que es muy importante hacer un test de capacidad de respuesta porque hay que partir de pautas."

PREGUNTA: Actualmente, a las empresas constantemente se les exige la acreditación de un buen gobierno corporativo con la obligación de cumplir con regulaciones, a menudo pensadas para las grandes corporaciones. Entonces, ¿cuál es el lugar ocupado por las PYME en el mundo del *compliance*? ¿Cómo pueden implementar un modelo de tales características con sus limitados recursos?

"Es un gran problema. Mucho presupuesto no tienen porque al final ellos lo que buscan es cumplir. A ver, sabemos que tener un MPD no es obligatorio, pero estamos hablando que no sirve únicamente para evitar la responsabilidad penal de la empresa sino que estamos intentando fomentar que las empresas tengan mecanismos para protegerse de ataques externos, no porque sean responsables sino porque son víctimas. Esto a veces se confunde. Una cosa es que la empresa tenga modelos de prevención de delitos para no ser ella responsable y otra es tener modelos de prevención de delitos para no ser ella objeto de un ataque y víctima. Ahora lo único que se está discutiendo es que con el primer sentido te olvidas del segundo, puesto que muchas veces tener un mapa de riesgos en la empresa no sólo le sirve para acreditar que no entre nadie vía artículo 31 bis y no ser sancionable penalmente, sino que tú puedes ser capaz de detectar los riesgos, curarte en salud y protegerte contra esos riesgos como víctima, no como responsable.

Entonces, en el caso de las PYME pueden escoger un despacho de abogados que le ofrezca a un precio más razonable hacer un MPD un poco de modelo y poco más, porque a lo mejor no pueden aspirar a tener un sistema muy bien montado, etc. Ahora bien, también es verdad que aun así el mundo de las Big Four, de las grandes empresas, según qué despacho de abogados te puede hacer un MPD que sea "una patata", que te haga un documento escrito muy bien hecho que luego no sirva para nada en la práctica. Todo esto se irá viendo conforme haya más procesamientos de personas jurídicas, se irá viendo qué MPDs están bien hechos, cómo hay que hacerlo, cómo mejorarlo. No obstante, hay gente que piensa que es como un sello más y con eso ya está tranquilo."

PREGUNTA: Hoy en día, la seguridad de la información en una empresa es una cuestión a tener en cuenta y a la cual deberían destinarse gran parte de los recursos disponibles. ¿Es actualmente la seguridad de la información un ítem valorado y costeado por las empresas o predomina la falta de consciencia de la importancia que tienen los riesgos tecnológicos y del posible impacto de sus consecuencias?

"Yo creo que cada vez empieza a haber más consciencia de los riesgos que hay porque salen noticias de empresa, aunque también es verdad que hay muchas noticias o potenciales noticias silenciadas, porque tú si eres una empresa y tienes un ataque informático lo que menos te interesa es que salga en los medios. Por ejemplo, así sucede con las entidades bancarias. Una entidad bancaria tiene muchos ataques cada año y algunos acaban entrando pero no les interesa decirlo, puesto que entonces la gente no irá a esos bancos. Con lo cual, aquí estamos ante una, no sé si llamarlo así, cifra negra, porque muchas veces aquí el problema de la empresa es que no se pueden incoar procedimientos porque la pista se hace desde países donde no hay convenio de colaboración o de extradición u otro cualquiera y entonces es imposible seguir una investigación. En consecuencia, habría más empresas que se concienciarían si afloraran la cantidad de ataques que están habiendo, que son constantes."

PREGUNTA: En la sentencia de 26 de septiembre de 2007, el Tribunal Supremo declaró que era un elemento esencial para que la empresa pueda desarrollar una actividad de supervisión y control de los medios informáticos la existencia de una política empresarial clara, conocida por los trabajadores. Pero, ¿pueden los trabajadores alegar que sus derechos fundamentales se han lesionado, en este caso, la intimidad? ¿Cómo se ven afectados los derechos de los trabajadores en estos casos?

"Tengo mi tesis doctoral[2] *sobre ello, así que me remito a ella. Aquí lo que ha habido es una evolución prudencial muy importante que, en un principio, surgió en el ámbito de la jurisdicción laboral y luego en el ámbito del Tribunal Constitucional (TC), donde se ha ido flexibilizando sobre los requisitos para que el empresario pueda entrar en el correo del trabajador incluso sin un previo aviso individualizado. El TC viene a decir que si en el convenio colectivo de la empresa o incluso sectorial consta como infracción el hecho de que un trabajador utilice las herramientas del trabajo con fines particulares, fines privados indirectamente, eso ya justifica un control, esa es un poco la idea. Yo lo encuentro una salvajada, nos estamos un poco americanizando.*

Al final, viene a decir que las normas de la empresa las pone el empresario y si no te gustan te vas a otra empresa. Ha cambiado un poco la consecuencia, puesto que al principio había una cierta tolerancia o uso privado de las herramientas de trabajo donde no podía entrar el empresario y ahora

2 https://www.educacion.gob.es/teseo/mostrarRef.do?ref=480009

cada vez más se tiende a un mundo de transparencia, en el cual el trabajador a través del BYOD ya tiene sus maneras de comunicarse en su esfera privada, pero si está en la empresa y es una herramienta de trabajo, ésta es propiedad del empresario."

PREGUNTA: Si tuviera que dar orientaciones prácticas para el buen gobierno de las TIC a una empresa, ¿me podría relatar un decálogo de medidas preventivas o buenas prácticas que debería llevar a cabo la empresa y también su personal durante el día a día? ¿Qué me recomendaría como empresa?

"En primer lugar, que haya una normativa en la cual se diga al trabajador, ya sea en el momento de firmar el contrato o como después de una sesión informativa, lo que puede y no puede hacer con claridad. Por ejemplo, si en su ordenador de la empresa se pueden establecer mecanismos de filtrado para que no pierda el tiempo o para limitarlos en sus necesidades. Que sepan que como va a estar controlada de alguna manera su actividad va a tener una responsabilidad o una disuasión para utilizar esa herramienta con fines de dispersión o absentismo, con lo cual eso le va a llevar a ser más responsable. Eso puede reducir su confianza al no ser su esfera privada. Yo creo que cada vez más tenemos que entender que si estamos trabajando estamos en el trabajo; uno tiene su Smartphone y lo puede usar para lo que quiera pero el ordenador es una herramienta de trabajo. Yo creo que es importante ganar consciencia de esta realidad. Esto es para mí de las cosas más importantes."

PREGUNTA: Por último, ¿cuáles son los retos a los que cree que tendrán que enfrentarse las empresas en un futuro próximo en relación a las TIC y el *compliance*?

"Es complicado. Cada vez más estamos interconectados, y al estar interconectados todos los dispositivos y las personas, la vulnerabilidad de un ataque cada vez es mayor. Entonces, las empresas van a tener que establecer mecanismos de seguridad muy claros, porque con sólo una brecha de seguridad, al estar todo interconectado te pueden acceder a cualquier punto. Entonces, yo técnicamente no sé cómo explicar cómo habría que hacerlo pero, la idea sería establecer cortafuegos de unos dispositivos y otros, así como tener maneras de bloquear el acceso a hackers cuando entran en un sistema. Pero me da mucho miedo tal y como está avanzando la sociedad. Uno utiliza las mismas contraseñas o tiene toda la información compartimentada en las mismas redes, ahora se puede hackear un marcapasos, el calentador de un biberón y cualquier cosa que esté interconectada. Eso es muy peligroso."