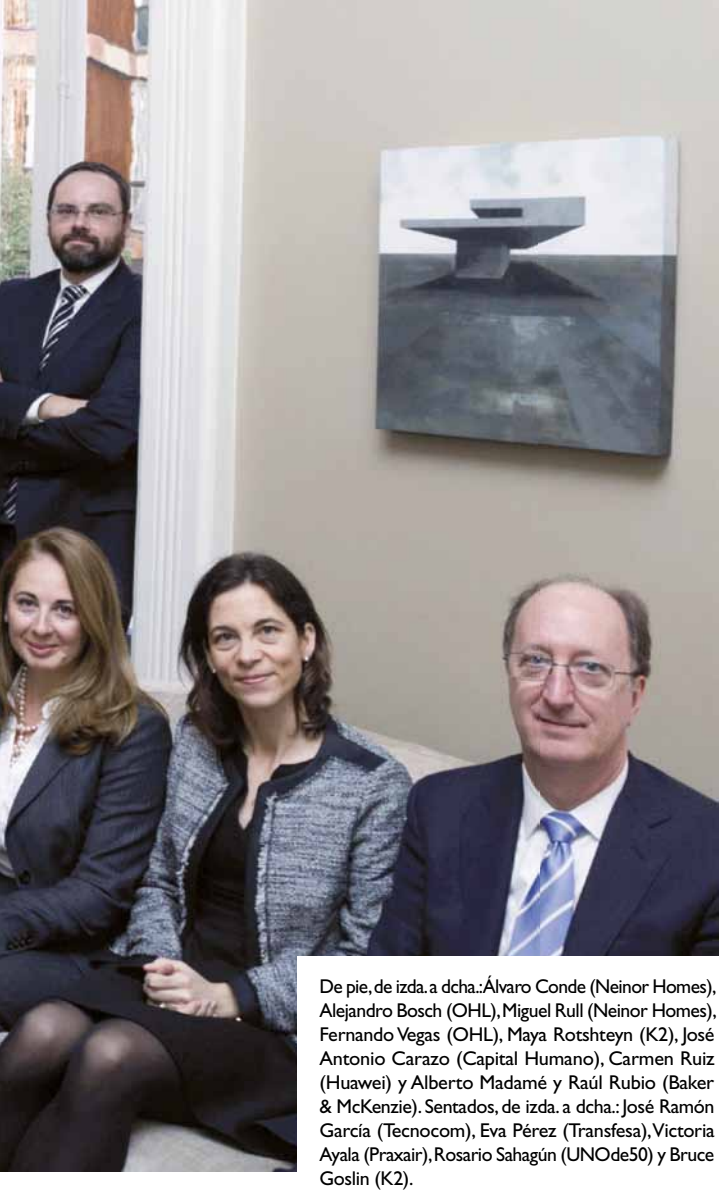
# Cumplimiento normativo, luces y sombras de la ciberseguridad

¿Están preparadas las empresas para asumir las nuevas exigencias en materia de cumplimiento normativo? ¿La regulación puede evitar los riesgos ciber? ¿Qué medidas hay que tomar para asegurar la continuidad del negocio y preservar la información sensible? ¿Es una cuestión jurídica o también cultural? Para analizar todas estas cuestiones, K2 Intelligence y Capital Humano, organizaron un desayuno de trabajo sobre "Cumplimiento normativo: Prevención de delitos internos, de terceros y consideraciones sobre la ciberseguridad". Estas son las principales conclusiones.

**Redacción de Capital Humano.**



De pie, de izda. a dcha.: Álvaro Conde (Neinor Homes), Alejandro Bosch (OHL), Miguel Rull (Neinor Homes), Fernando Vegas (OHL), Maya Rotshteyn (K2), José Antonio Carazo (Capital Humano), Carmen Ruiz (Huawei) y Alberto Madamé y Raúl Rubio (Baker & McKenzie). Sentados, de izda. a dcha.: José Ramón García (Tecnocom), Eva Pérez (Transfesa), Victoria Ayala (Praxair), Rosario Sahagún (UNOde50) y Bruce Goslin (K2).

## FICHA TÉCNICA

**Autor:** REDACCIÓN DE CAPITAL HUMANO.

**Título:** Cumplimiento normativo, luces y sombras de la ciberseguridad.

**Fuente:** Capital Humano, nº 309. Mayo, 2016.

**Resumen:** ¿Están preparadas las empresas para asumir las nuevas exigencias en materia de cumplimiento normativo? ¿Qué medidas hay que tomar para asegurar la continuidad del negocio y preservar la información sensible? Para analizar todas estas cuestiones, K2 Intelligence y Capital Humano organizaron un desayuno de trabajo sobre "Cumplimiento normativo: Prevención de delitos internos, de terceros y consideraciones sobre la ciberseguridad" para analizar estas y otras cuestiones. Los participantes señalaron la indefensión en la que se encuentran algunas empresas dado que es difícil prevenir los ataques y, en muchas ocasiones, es más urgente frenar los posibles daños que investigar quién los ha llevado a cabo. Los procedimientos internos y la tecnología son las medidas defensivas más eficaces.

**Descriptores:** Cumplimiento normativo / Ciberseguridad / Prevención de delitos

La globalización, la complejidad de las organizaciones, las crecientes exigencias de seguridad por parte del mercado de las autoridades y las nuevas tecnologías están dibujando un nuevo panorama en el que se desenvuelven las empresas. De un tiempo a esta parte las regulaciones nacionales y supranacionales han diseñado un marco de actuación nuevo y las exigencias de cumplimiento de la normativa han crecido. ¿Están preparadas las empresas para asumir estos nuevos desafíos? ¿La regulación puede evitar los ciberriesgos? ¿Qué medidas hay que tomar para asegurar la continuidad del negocio y preservar la información sensible?

Para analizar todas estas cuestiones, K2 Intelligence[1] y Capital Humano, organizaron un desayuno de trabajo en el que, bajo el enunciado "Cumplimiento normativo: Prevención de delitos internos, de terceros y consideraciones sobre la ciberseguridad", se reunió un grupo de directivos y abogados. Los participantes en el coloquio fueron: Alberto Madamé, Socio del Departamento Laboral y Compliance, y Raúl Rubio, Socio del Departamento de TIC, ambos de Baker & McKenzie; Carmen Ruiz, Legal Counsel de Huawei; Bruce Goslin, Executive Managing Director de K2 Intelligence; Miguel Rull, Compliance Officer, y Álvaro Conde, Internal Audit Director, ambos de Neinor Homes; Fernando Vegas, Director de Riesgos de Proyectos de Construcción de OHL; Victoria Ayala, Institutional Relations de Praxair; José Ramón García, Responsable de Seguridad Interna de Sistemas de Información de Tecnocom; Eva Pérez, Risk & Insurance Manager de Transfesa; y Rosario Sahagún, Legal Counsel de UNOde50. Moderó el debate José Antonio Carazo, Director de Capital Humano.

## UNA VISIÓN PANORÁMICA

Alberto Madamé, Socio del Departamento Laboral y Compliance de Baker & McKenzie, hizo un planteamiento general del tema al explicar que, desde el punto de vista laboral cuando se piensa en compliance y en ciberseguridad hay dos focos de interés principales. El primero, el más >

1 K2 Intelligence es una consultora en riesgos e investigaciones corporativas, creada en el 2009 por Jeremy M. Kroll y Jules B. Kroll, el reconocido fundador de la actual industria de las investigaciones corporativas. A lo largo de los últimos 40 años, Jeremy, Jules y sus equipos se han ganado una sólida reputación no sólo por la excelencia de sus investigaciones, análisis y asesoramiento, sino también por la independencia y el conocimiento que aportan a su trabajo. Con oficinas en Nueva York, Londres, Madrid, Tel Aviv, Ginebra y Los Ángeles, K2 Intelligence asesora a gobiernos, empresas e individuos en áreas como Asesoría a Consejos de Administración, Cumplimiento Normativo y Prevención de Blanqueo de Capitales, Monitorización de Integridad, Análisis y Visualización de Datos, e Investigaciones en Ciberseguridad y Ciberdefensa. www.k2intelligence.com

> polémico, sobre el derecho a la intimidad o privacidad vs. control empresarial. "Hay una colisión de derechos y, obviamente, se genera conflicto y hay que resolverlo. Aquí lo que dice la jurisprudencia es que básicamente la empresa puede establecer sistemas de control de las tecnologías de información y comunicación que se ponen a disposición de los trabajadores, pero siempre que se cumpla un doble criterio: que se haga llegar al trabajador una información suficiente como para eliminar la expectativa de privacidad que pueda tener sobre el uso de los medios de la empresa y que las medidas sean "proporcionadas, idóneas y necesarias", dijo.

Otro elemento que destacó fue lo que sucede cuando se intervienen equipos personales en un proceso de investigación porque hay un incumplimiento. Aquí también los dos elementos que destaca la jurisprudencia son muy importantes. Según Madamé, "donde pone el foco es en garantizar que la información que se obtiene no ha sido manipulada, por eso se habla de las cadenas de custodia. Un segundo nivel, para el que se contrata normalmente a expertos, es cómo garantizar que en el análisis de esa información has minimizado al máximo la intromisión en el posible contenido personal".

**"Cumplir con la reglamentación es relativamente sencillo, pero con eso no ganas dinero, sólo evitas que metan en la cárcel al Consejero Delegado"**

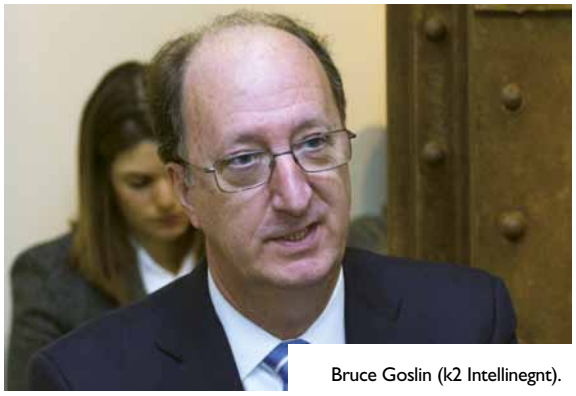
A su juicio, el segundo bloque se centra en cuándo se pueden sancionar incumplimientos vinculados al uso de tecnologías y la importancia de los códigos éticos. Comentó que "la conclusión a la que llegamos es que estamos en un área que está altamente desregulada desde el punto de vista laboral y, por tanto, presenta muchas aristas sobre hasta qué punto algo es un incumplimiento o no, si se puede sancionar o no. Sobre todo cuando intervienen elementos como el acceso remoto a los equipos o los comentarios sobre la empresa en Facebook, por ejemplo".

Raúl Rubio, Socio del Departamento TIC de la misma firma de abogados, aseguró que "los riesgos ahora no son los que eran. Estamos en un entorno en que los riesgos son muchísimo mayores, hay más ataques y las organizaciones se han complicado orgánicamente. También el uso que los empleados hacen de la tecnología es diferente. Venimos de un entorno en el que se trabajaba con un PC fijo y hoy tenemos portátiles y móviles que son como ordenadores y que tienen cámaras y dispositivos de grabación. Además, el empleado instala en su equipo personal herramientas corporativas, está la nube… Nos podemos aburrir poniendo ejemplos de cómo le hemos complicado la vida al Director de Sistemas de la empresa".

En su opinión, este contexto obliga a implantar medidas que mitiguen los riesgos y nos lleva a navegar en una situación de mayor incertidumbre. Para Rubio, "uno de los elementos clave es la necesidad de tener políticas de uso de los recursos informáticos y tecnológicos. Pero no todas son iguales ni se aplican de la misma manera según el contexto y la situación. Hay mayores amenazas porque los activos han cambiado y los intangibles son cada día más importantes. Se ha producido una revolución digital que ha alcanzado a todos los sectores".

Rubio continuó su argumentación haciendo referencia a que "ahora el activo a proteger es todavía más etéreo, más débil y más vulnerable. Esto puede asociarse con posibles comportamientos de empleados desleales que, en algunos casos, puedan tener una conciencia de ilegalidad limitada. Cuando despides a alguien no se le ocurre llevarse la mesa, pero sí grabar archivos en un disco o enviárselos a su correo personal sin conciencia de estar haciendo nada malo. El delito existe igualmente y posiblemente es más grave en el segundo caso por el valor que tiene lo que ese trabajador se está llevando. Sin embargo las medidas con las que cuenta la empresa son menores y generan una situación de mayor incertidumbre".

Para este profesional el tema no queda ahí. "Por si eso fuera poco ha irrumpido desde hace unos años la responsabilidad penal de las empresas. Ese trabajador que

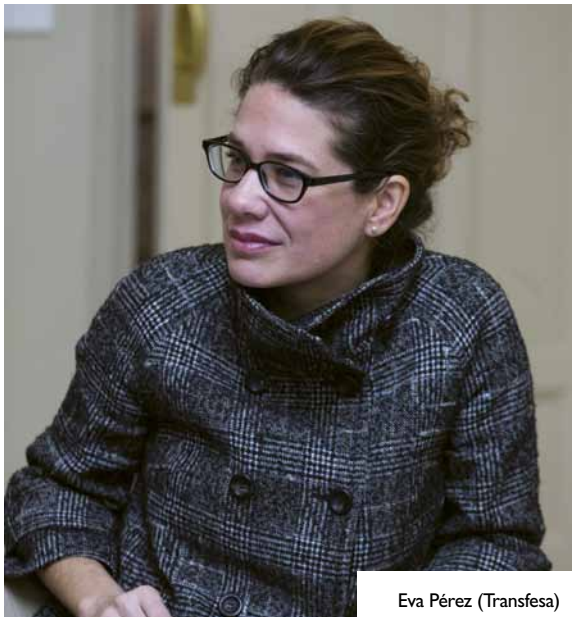


Bruce Goslin (k2 Intellinegnt).

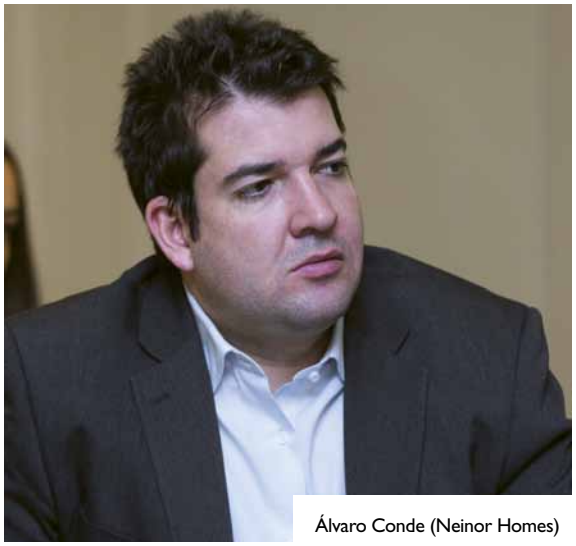
en un momento dado hace algo ilícito en un ámbito tecnológico, cuando lo hace en beneficio de la empresa, no solo se pone en riesgo a sí mismo sino también a su propia compañía. Si, además, le sumamos la existencia de posibles infracciones en materia de protección de datos, podemos ver fácilmente como el uso de la tecnología puede generar un ámbito de riesgo adicional en empresas no necesariamente tecnológicamente avanzadas", aseveró.

Raúl Rubio se preguntó en voz alta cuál puede ser la mejor manera de actuar frente a todos estos riesgos. Gestionar estas amenazas en grupos empresariales es tremendamente complicado, sin embargo no por ello se debe tirar la toalla. El mensaje es que hay mucho por hacer, pero que es factible. Hay que anticiparse a los hechos, hay que establecer procedimientos, medidas, sobre todo en la parte de la seguridad".

Rubio recordó que está a punto de aprobarse el Reglamento Europeo de Protección de Datos, que será de aplicación directa, sin necesidad de leyes nacionales, y que previsiblemente entrará en vigor en 2018, con un régimen sancionador muy duro que puede llegar al cuatro por ciento de la facturación mundial del grupo empresarial. "Francia pretende adelantarse. La autoridad de protección de datos francesa está promoviendo una reforma legislativa para adelantar la aplicación de este régimen sancionador antes del 2018. No sería descartable que en España ocurriera lo mismo", dijo y añadió que el Reglamento establece que va a ser necesario notificar a la autoridad los fallos de seguridad en un plazo de 72 horas, lo que hará necesario contar con un equipo de alerta temprana para prevenir esos riesgos y tratar de evitar las sanciones. "Las empresas que sepan entender esta complejidad y que sepan reaccionar van a estar infinitamente mejor posicionadas que el resto", puntualizó.



Eva Pérez (Transfesa)



Álvaro Conde (Neinor Homes)

## UNA RESPONSABILIDAD COMPARTIDA

Miguel Rull, Compliance Officer de Neinor Homes, aseguró que "nos movemos en un terreno muy pantanoso, porque en protección de datos los modelos de protección descansan sobre acciones tan discutiblemente efectivas como la formación o la comunicación interna, dado que el cumplimiento atañe a la actividad de todos y cada uno de los miembros de una organización". Rosario Sahagún, Legal Counsel de UNOde50, apuntó que "el compromiso debe venir de arriba, desde donde debe darse ejemplo, pero además debe extenderse a cada uno de los empleados y creo que en esto hay un componente de ética fundamental", y Alberto Madamé añadió que "las normas >

Fernando Vegas (OHL)

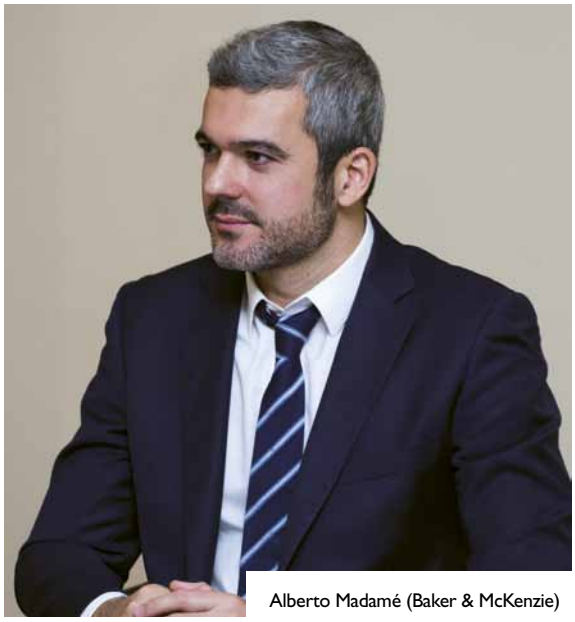
éticas tienen una gran ventaja, que llena las lagunas que una regulación detallada no cubre".

Según Carmen Ruiz, Legal Counsel de Huawei, las empresas no están suficientemente preparadas para enfrentarse con algo tan complejo como el cumplimiento del entorno en el que se desenvuelven y porque la tecnología avanza más rápido de lo que somos capaces de asumir. "Además, hay una inseguridad jurídica tremenda. Hay jueces que han declarado que no van a aplicar algunas directrices europeas por entender que van contra las disposiciones sobre privacidad e intimidad que recoge la Constitución. Por ejemplo, el derecho a la privacidad es importante pero no está pensado para la realidad de hoy en día que puedes pasar archivos en cuestión de minutos y cargarte un proyecto". A este respecto, Eva Pérez, Risk & Insurance Manager de Transfesa, comentó que "actuamos

Alejandro Bosch (OHL)

reactivamente no proactivamente. Yo creo que es mejor prevenir, aunque hay algunas cosas que es difícil regular".

Según Miguel Rull, "debemos establecer compromisos que vayan más allá de la propia relación laboral. Lo que marca la diferencia no es tener información en tus dispositivos privados sino el hacer un uso malicioso, o no, de esa información. Poner barreras al intercambio de información a estas alturas es tremendamente difícil y costoso, además de que puede comprometer la productividad". Álvaro Conde, Internal Audit Director en la misma compañía, aseguró que "hay una gran falta de concienciación. Estamos a años luz de los anglosajones. La conciencia de la empresa es la del negocio y el propio CEO de la empresa debe ser el que trasmita estos mensajes". Miguel Rull agregó: "es



Alberto Madamé (Baker & McKenzie)

el mundo ideal, pero es difícil crear valor en algunas de las acciones de compliance y el poder trasladar esta idea de cumplimiento al negocio genera mucha resistencia".

## INTERESES COMUNES

Para Raúl Rubio (Baker & McKenzie), la clave es cómo alinear el cumplimiento con los objetivos de negocio "porque al final hay una parte de la organización luchando contra la otra". En su opinión, "lo que es necesario es que para el vendedor sea tan importante la venta como que esa venta sea lícita. Eso en las empresas americanas es fundamental. Una venta no se contabiliza hasta que no se dan una serie de parámetros que implican una cierta

Rosario Sahagún (UNOde50)

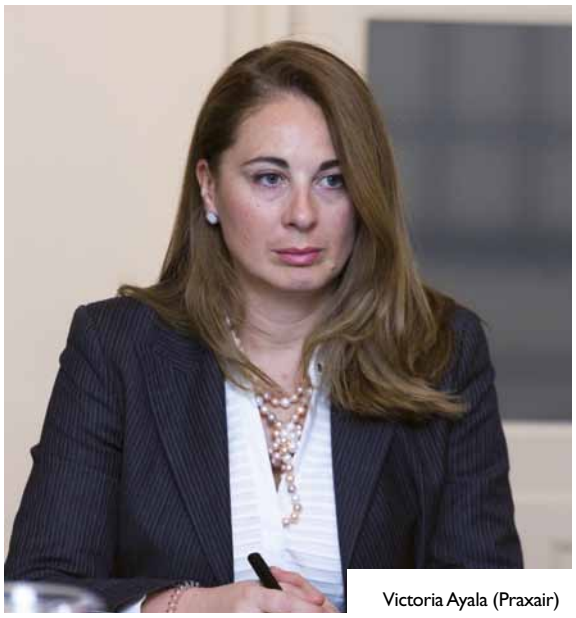
investigación por parte del Departamento Jurídico o de Auditoría Interna, que hacen un chequeo sobre si se ha cumplido con determinadas obligaciones. Obviamente eso puede generar tensiones pero lo que implica es que hay un compromiso por parte de la organización al más alto nivel con el cumplimiento normativo. Es una cultura en la que áreas que se suelen considerar de puro coste, como son las de cumplimiento normativo, dejan de serlo porque de ellos depende la continuidad del negocio.

Según José Ramón García, Responsable de Seguridad Interna de Sistemas de Información de Tecnocom, "las grandes compañías podrían tener ahora mismo mecanismos suficientes que permitan prevenir o monitorizar estas cuestiones, pero las pequeñas no tienen esa capacidad. Según las previsiones de la Unión Europea tenemos dos años para que las empresas adaptemos sus políticas y podamos establecer medidas de prevención, y de alerta temprana, en muchas ocasiones las compañías no saben que están siendo atacadas". A lo que Rosario Sahagún apuntó que "es lógico porque los recursos en una empresa pequeña son menores. En este sentido, debe aplicarse aquí el principio de la proporcionalidad, fundamental en la implantación e interpretación de las medidas de prevención".

García añadió que "en nuestro caso tenemos equipos de alerta temprana y tenemos medidas de seguridad, pero

Raúl Rubio (Baker & McKenzie)

la seguridad absoluta no existe. No puedes minimizar el riesgo 100 por ciento. Cuanto más grande sea la compañía, mayor capacidad tendrá para prevenir ataques, pero también está más expuesta".



Victoria Ayala (Praxair)

En este sentido, Carmen Ruiz advirtió que "es difícil cumplir con toda la normativa en una multinacional cuya matriz se encuentra en China, puesto que la legislación china es muy diferente, resultando difícil de adaptar los procesos corporativos, -que tratan de cumplir la legislación china a la legislación local"-, Por su parte, para Eva Pérez, "el papel de las estructuras locales es que han de enseñar a las internacionales, porque estamos en diferentes sitios, en cada uno se actúa de manera diferente y siempre debemos adaptar las políticas que vienen de fuera". >

Miguel Rull (Neinor Homes)

## VALORAR EL IMPACTO

Bruce Goslin, Executive Managing Director de K2 Intelligence, explicó que "en las multinacionales en las que nosotros trabajamos la aplicación del cumplimiento y normativas varía bastante según el país en el cual estés. La mayoría de los ataques tardan en detectarse una media de 208 días. Lo que nosotros estamos comprobando es que hay cierta incertidumbre legal porque las empresas no saben cómo actuar y las amenazas están creciendo de una manera tan veloz que la mayoría de las empresas sólo quieren parar los ataques y no perder más datos. Hay bancos que reciben entre 30.000 o 40.000 ataques al mes que les hacen perder datos. En esta situación lo más importante es parar los ataques.

Carmen Ruiz (Huawei)

Para José Ramón García, "es necesario un marco regulador del ciberespacio. Estamos acostumbrados a trasladar el entorno jurídico de lo físico al ciberespacio y eso ha quedado demostrado en muchas ocasiones que no funciona", mientras que Fernando Vegas considera que "el problema no es denunciar o no denunciar, el problema es que si tienes 30.000 ataques todos los meses, tendrías que tener un departamento solo para poner las denuncias. La cuestión no es sufrir un ataque sino el cuándo me entero de que lo he sufrido, si es que me entero. Además, no podemos estar 3 días decidiendo qué hacemos".

José Ramón Garcia (Tecnocom)

Con todo, y a su juicio, el alcance del problema también depende de la empresa. "Si hackean a Google, ellos pueden tener un gran problema, si nos hackean a nosotros, seguramente el impacto en el negocio será menor. En términos estrictamente éticos se debería denunciar siempre, aunque afecte poco al negocio. Pero el verdadero problema de los ataques es que me pueden hacer perder mucho dinero. Y si no he cumplido con mis obligaciones de cumplimiento, me pueden poner una multa que me puede hacer cerrar el negocio. Nos centramos mucho en la técnica pero hay muchos más aspectos", argumentó.

A esto Bruce Goslin apuntó que "uno de ellos, y posiblemente el más importante, es el factor humano. La mayoría de los ataques llegan a través de los empleados".

Por su parte, Alberto Madamé añadió que "tenemos una normativa muy centrada en el cumplimiento formal de obligaciones con una finalidad policial y sancionadora".

## NUEVAS DIMENSIONES

Miguel Rull se lamentó de que "aunque ha avanzado mucho la normativa de protección de datos yo, como titular de datos, me siento cada día más desprotegido. No parece que tanta normativa sirva para mejorar la seguridad de los datos de carácter personal. Todos nos entregamos a la causa de documentarlo todo perfectamente, pero mi pronóstico es que el único avance en este tipo de cosas va a ser a través del marketing. Las empresas tomarán conciencia de que es un valor que se puede vender, que puede ser un valor diferencial frente a la competencia y, gracias a ello, van a ofrecer un valor real al cliente".

Victoria Ayala, Institutional Relations de Praxair, coincidió con él: "Estoy de acuerdo con lo que dices. Nosotros que nos dedicamos al sector Salud y el manejo de todos estos datos es muy delicado, sabemos que hay mucha suspicacia por parte de la población". Y explicó que "para nosotros la ética y los valores son una cuestión cultural. En Praxair hay una doble preocupación de que todo lo que se haga se haga correctamente porque el cliente principal es la Administración Pública, pero también la preocupación es por la seguridad" en cada uno de los procedimientos.

Rull también señaló dos problemas a tener en cuenta: "Uno es de claridad de ideas, qué es lo que puedo y lo que no puedo hacer. Esto no está claro y la jurisprudencia está dando bandazos. En segundo lugar, fijar un límite que social y culturalmente sea aceptable, ahí también estamos en una situación de incertidumbre.". Eva Pérez coincidió en señalar "que la normativa está para cumplirla, pero hay que ir más allá. En cuanto a las responsabilidades de los directivos no sé cómo las van a interpretar los jueces, ni las consecuencias que va a tener esto a futuro. Tienes que hacer tu mapa de riesgos, que es un eximente penal, pero nadie te dice cómo".

Rull también apuntó que "los jueces deberán discernir cuándo un programa de Compliance es o no es eficiente, y las empresas siempre han sido una especie de zona gris en la que jueces y fiscales no han entrado en los procedimientos internos, los controles que se suelen establecer para prevenir responsabilidades penales son difíciles de diseñar y poco eficientes". A esto Álvaro Conde añadió que "muchas veces es imposible hacer un buen control".

Fernando Vegas aseguró que "esto del compliance es muy sencillo. Hay que dar cumplimiento a una normativa. Se crea un mapa de riesgos corporativo, que no tiene que ser muy complejo, y se persigue el cumplimiento. Esto es bastante fácil de hacer y con eso se exime absolutamente de responsabilidad a todo el equipo de gobierno de la empresa. Es decir, cumplir con la reglamentación es relativamente sencillo, pero con eso no ganas dinero, sólo evitas que metan en la cárcel al Consejero Delegado, lo cual está bastante bien. Pero, lo que más preocupa a las empresas, según una reciente encuesta de Allianz en 2015, es la pérdida de reputación. Nosotros, por ejemplo, estudiamos los posibles riesgos de cada proyecto".

Conde corroboró que "es preciso hacer un scoring de cada contrato para evitar asociarse a un socio malo, por ejemplo, que nos vaya a perjudicar económicamente o en nuestra reputación. Esto también debe formar parte de compliance". A lo que Fernando Vegas añadió que "el análisis de 'riesgos del proyecto' debe ser muy detallado y orientado a ser más productivos y sacar el máximo beneficio de cada proyecto". Para Eva Pérez, "lo óptimo sería que tuviéramos tan asimilados los temas éticos que no tuviéramos que dedicar más de un recurso a comprobar que efectivamente se han cumplido. Creo que es un tema de cultura y que en algún momento conseguiremos llegar a que eso esté asimilado".

Miguel Rull se mostró partidario de "empujar el compliance hacia el negocio, que esas tareas no estén centradas en un órgano 'policial' sino que cada proceso o procedimiento administrativo o contractual dentro del modelo de cumplimiento sea una responsabilidad compartida por parte de todos".

Carmen Ruiz también estuvo de acuerdo en señalar la cultura empresarial y la ética como "una tarea de todos". Por un lado está la responsabilidad del directivo, y por otro lado el mensaje de que al compliance se tiene que llegar desde arriba y hacerse capilar a toda la organización. Al mismo tiempo, tiene que haber departamentos, Como RR.HH. o Legal, que controlen y creen esa necesaria mentalización. Ahora se habla de tener cultura de compliance, pero la cultura se tiene o no se tiene y modificarla es un proceso complejo que no se alcanza automáticamente". Se ha trasladado a las empresas la necesidad de autocontrolarse y eso es muy difícil porque hay que crear una mentalidad de autocontrol". "Totalmente de acuerdo", dijo Alberto Madamé, "pero, además, compliance es mucho más que eso". ■