¿Son seguros los despachos de abogados?

FERNANDO J. BIURRUN

Abogado. Fundador de Law&Trends

Las noticias de los *Papeles de Panamá* no paran de dar nuevos nombres de famosos y no tan famosos. La filtración de documentos secretos del despacho de abogados panameño Mossak Fonseca, con la que se ha dado a conocer millones de informaciones que han descubierto a miles de personas en todo el mundo que ocultaban su patrimonio en sociedades situadas en paraísos fiscales, ha abierto una nueva crisis en la sociedad.

Tal vez muchos de los nombres que hay detrás de estas informaciones no lleguen a sorprendernos, pero las provenientes del despacho panameño han abierto la caja de pandora de miles de inversores que creían vivir en anonimato, con sus patrimonios protegidos y, en muchos casos, protegidos de las diferentes haciendas nacionales.

Con independencia de la legalidad o no de los negocios que allí se desarrollaban y de si los afectados tributaban en sus países o no -cuestiones con las que las diferentes administraciones tributarias se están frotando las manos en estos momentos y la prensa llenando ríos de tinta física o digital-, una pregunta subyace en todo esto: ¿son seguros los despachos de abogados?

Una de las obligaciones que tienen los abogados respecto de sus clientes es garantizar la confidencialidad de las informaciones que éstos transmiten y que, bajo el secreto profesional, los abogados debemos guardar y garantizar.

En la era de la tecnología, las informaciones de los clientes conviven entre servidores, discos duros y demás soportes de almacenamiento junto con el resto de soportes físicos (archivos, carpetas...). Sorprende saber que el mayor robo de datos no es de alta tecnología sino física (datos de EEUU) y, pese al impacto del caso de los *Papeles de Panamá,* los soportes físicos que se alojan en los propios despachos pueden resultar los más vulnerables.

Esta es una de las razones por las que en la última ABA *Techshow,* la reunión de tecnología más importante de los despachos de EEUU, se recomendaba acudir a los servicios en la nube, donde las empresas especializadas en ofrecer este tipo de servidores, garantizan altos niveles de seguridad. De un lado, por la protección que establecen en sus sistemas, de otro, porque desaparece la vulnerabilidad de un servidor en un armario en la oficina.

Protocolos de acceso

A todo esto, habría que añadir la existencia y el cumplimiento de protocolos de accesos a las diferentes informaciones de los clientes por los miembros del despacho (y no miembros), el control y registro de copiado de datos, y los sistemas preventivos.

Si a esta vulnerabilidad, añadimos otro dato proveniente de los EEUU que nos dice que sólo el 42% de las comunicaciones que realizan los despachos de abogados son comunicaciones cifradas, datos que para los expertos son alarmantes teniendo en cuenta el número de aplicaciones disponibles para facilitar una comunicación segura. Según se desprende del *Primer Informe sobre la necesidad legal de cifrar información y datos personales,* elaborado por la consultora Sophos y el despacho Abanlex, el cifrado de datos en la comunicación de los abogados con sus clientes es obligatorio. Ahora, solo nos falta conocer el grado de cumplimiento de esta obligación en nuestro país.

> Los ´Papeles de Panamá´ deberían abrir una revisión de la seguridad de la información existente en nuestros despachos

Está claro que los *Papeles de Panamá* deberían abrir una revisión de la seguridad de la información existente en nuestros despachos. La confianza es uno de los valores más importantes que los despachos transmiten a sus clientes y, por ende, esta no solo se limita a la comunicación y a la empatía con el cliente y a guardar el secreto profesional. La confianza acaba de dar un paso más, garantizar que la información depositada en los despachos es segura y que nunca va a salir de su espacio físico o virtual, por *hackers,* ladrones o exempleados vengativos.

Seguramente, muchos creamos que lo que ha pasado en Panamá no nos va a pasar, pero vivimos en una era donde ya no es suficiente tener una puerta blindada, una alarma, una caja fuerte... Ahora tenemos puertas virtuales que nos hacen más vulnerables, el router, la conexión wifi, los password, los dispositivos móviles y portátiles (olvidados o perdidos)...

Seguramente no tengamos los miles de clientes con millones escondidos en sus patrimonios, pero basta con que uno nos haya confiado una información sensible y transcendente, deseosa por competidores, medios o, simplemente, deseada por *justicieros,* para que podamos ser objeto de un ataque a nuestros sistemas.

La ciberseguridad, una cuestión estratégica y una prioridad

MARÍA GONZÁLEZ

Asociada senior de IT, Risk & Compliance de ECIJA

ECIJA

El pasado domingo saltaba a la palestra el último escándalo. Mediante la publicación de un gran volumen de información de uno de los más importantes despachos de abogados en la creación de sociedades "offshore" (Mossack Fonseca), se ponía al descubierto no sólo información que permite conocer con detalle el funcionamiento del mundo "offshore" sino que, además, pone de manifiesto un problema de seguridad de la información y ciberseguridad.

Los "Papeles de Panamá", como se ha denominado el caso, supone una filtración de un gran volumen de documentos en formato digital, que incluyen todo tipo de documentos, incluidos mensajes de email. Se habla de 11,5 millones de documentos y un volumen total de 2.6 TB de información, lo que supone que esta filtración pueda estar incluso, a nivel cuantitativo, por encima de otras filtraciones como Wikileaks (2010) y Snowden en 2013.

A diferencia de estas, donde las filtraciones tuvieron su origen en el interior de las organizaciones, parece que en el caso de los "Papeles de Panamá" el origen puede derivar de un ataque externo (hacker) sobre los sistemas de información del despacho, según parecen desprender las investigaciones e inspecciones forenses que han encargado a terceros especialistas.

Pero... **¿Están los despachos de abogados preparados ante problemas de Ciberseguridad?** Sean filtraciones internas o ataques externos, es esencial que los despachos de abogados implanten medidas de seguridad que permitan la protección de la información que tratan y custodian (que en muchos casos tendrá un carácter especialmente sensible), medidas que han de ser de carácter preventivo y reactivo; y que deben permitir minorar, por un lado, el riesgo de fuga o filtración de información y, por otro, permitir la detección y reacción a tiempo ante un ataque, minorando los daños que éste pueda producir.

En cuanto a las medidas de seguridad de carácter preventivo que pueden ser implantadas por los despachos, en línea con los sistemas de gestión de seguridad de la información y continuidad de negocio (alineados con estándares como ISO 27001y ISO 22301), pasan por cuestiones esenciales como:

- Sistemas de respaldo y recuperación de información. Puede parecer una cuestión básica, pero la realización de copias de seguridad de la información, así como la implantación de sistemas que permitan recuperar información en caso de pérdida o desastre es una cuestión clave.
- Sistemas de control de acceso. Deben ser implantados por los despachos tanto sistemas de control de acceso físico a las instalaciones y archivos, como sistemas de control de acceso lógico a la información. Segregar los permisos de acceso en base a las necesidades derivadas de las funciones desempeñadas partiendo del principio de "mínimo conocimiento". En el caso de acceso a sistemas o información especialmente sensibles, implantar sistemas de acceso con doble factor de autenticación o incluso utilizando otros sistemas como los biométricos, pueden reforzar la seguridad requerida.
- Sistemas de monitorización de la red empresarial. Sistemas antivirus, antimalware, firewalls, análisis del tráfico de datos, sistemas de prevención de fugas de información (DLP), permitirán la detección de cualquier incidencia, vulneración o fallo que pueda suponer un riesgo para la seguridad del despacho, adoptar acciones que permitan frenar el ataque y minorar los daños que puedan ocasionarse, así como desarrollar e implantar las medidas adecuadas que permitan corregir la vulnerabilidad.
- La protección del papel. Aunque cada vez es menor el uso de papel en los despachos de abogados, es esencial llevar a cabo políticas en relación a la protección de los datos e informaciones tratados en papel: uso de impresoras, la custodia de expedientes, la seguridad de acceso a los archivos, etc.
- Cumplimiento normativo. La actividad del sector de la abogacía está sometida a múltiples normas que tienen exigencias concretas de seguridad y protección de los datos e informaciones como: la normativa de protección de datos, normativa de prevención del blanqueo de capitales, así como entre otras, normas de carácter sectorial que dependiendo de la actividad concreta del despacho pueden ser también de aplicación como: normativa financiera y aseguradora, estándares como PCI-DSS, etc...
- Concienciación, concienciación, concienciación. Los riesgos en ciberseguridad y seguridad de la información derivan mayoritariamente de errores o falta de conocimiento de los usuarios de los sistemas, por ello es de suma importancia concienciar y formar a todos los compañeros del despacho.

> Los ´Papeles de Panamá´, como se ha denominado el caso, supone una filtración de un gran volumen de documentos en formato digital

> En materia de seguridad de la información ha de tenerse en cuenta además la importancia de la mejora continua

Mejora continua

En materia de seguridad de la información ha de tenerse en cuenta además la importancia de la mejora continua. Debe llevarse a cabo, no sólo el análisis y auditoría periódica exigida legalmente, sino además un análisis exhaustivo (incluso forense) de las vulnerabilidades y ataques detectadas, desarrollando e implantando de medidas correctivas que impidan que pueda producirse un evento similar en el futuro.

La ciberseguridad y la seguridad de la información en general, debe convertirse en una **prioridad y cuestión estratégica,** al igual que en otros sectores, también en los despachos de en los despachos de abogados. Las quiebras de seguridad y la vulneración de la protección de la información sensible y confidencial de los despachos, acarrean riesgos y daños de carácter legal, económico y sobre todo reputacional, que han de ser evitados.