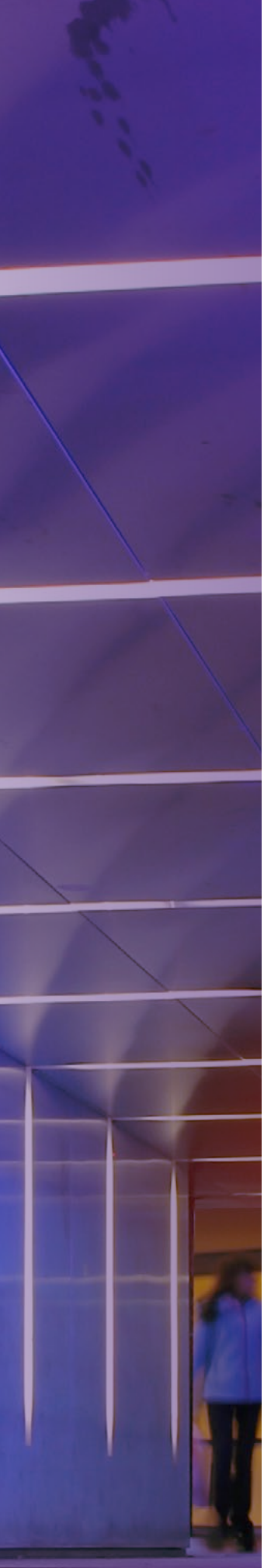
Velocidad, escala y confianza

Servicios de respuesta rápida *'on demand'* de KPMG

kpmg.com



Introducción

Actualmente las empresas globales manejan volúmenes abrumadores de información física y electrónica que podrían ser objeto de análisis en un procedimiento regulatorio o estar en riesgo de sufrir una filtración cibernética. El volumen cada vez mayor de datos, la presencia de nuevas fuentes de datos, las numerosas formas de comunicación, las tecnologías en rápida evolución y un panorama regulatorio cambiante presentan desafíos únicos en materia de identificación de evidencia ("eDiscovery") y seguridad cibernética.

Desde 2013, el riesgo cibernético se ha triplicado y continúa intensificándose. Globalmente, las empresas se enfrentan a un mayor escrutinio regulatorio sobre la privacidad de los datos, la gestión de datos y la integridad en los informes financieros. Además, existe un aumento continuo en los litigios en todo el mundo. Esto hace esencial que las empresas estén preparadas de forma adecuada para responder ante las solicitudes de divulgación de sus datos electrónicos. A medida que todos los sectores e industrias del mundo se vuelven cada vez más digitales, también lo hace la velocidad con la que el ciberdelito afecta a todos a nivel mundial. Una gestión eficaz de la seguridad de los datos y de la identificación de evidencia es clave para ayudar a minimizar los riesgos de datos.

Las noticias están llenas de artículos sobre empresas involucradas en incidentes de fraude y mala conducta que de repente se enfrentan a investigaciones regulatorias que requieren esfuerzos de identificación de evidencias a gran escala. También, cada vez más se conocen casos de empresas que son víctimas de ataques cibernéticos de gran magnitud, que les cuestan millones en pagos de rescate, que paralizan su infraestructura y destruyen la confianza. El COVID-19 y el aumento de empleados que trabajan de forma remota sin protocolos de seguridad sólidos, o que utilizan dispositivos de almacenamiento de datos no autorizados por sus organizaciones, ha impulsado tanto los ataques cibernéticos como los protocolos de gestión e identificación de datos poco eficaces.

La dura verdad del entorno actual es que todos deben ser conscientes de su seguridad.

Desde las multinacionales globales hasta las empresas sin fines de lucro más pequeñas, todas las organizaciones pueden verse afectadas por el fraude, el incumplimiento normativo y el delito cibernético, sin importar su tamaño.

¿Sabías?

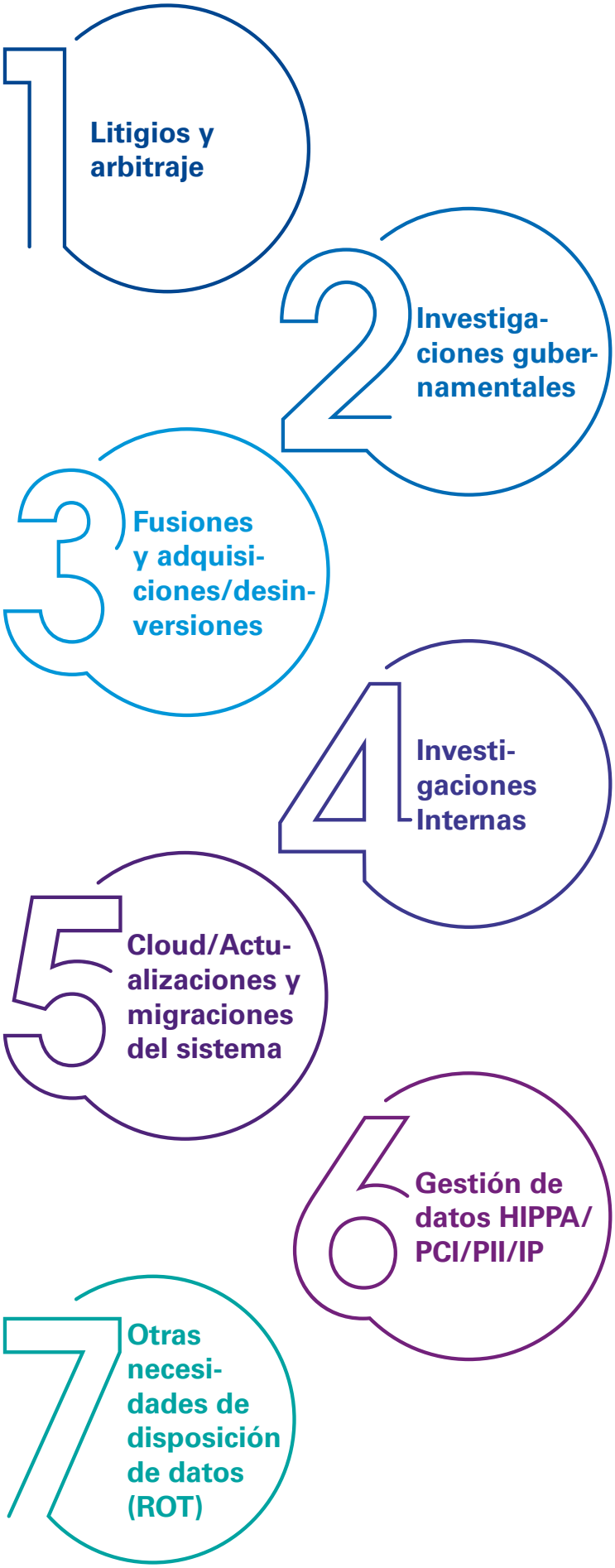
74% de los CEO encuestados en la Encuesta CEO Outlook Pulse de 2021 de KPMG, indica que la velocidad de la digitalización se ha acelerado en cuestión de meses.

La mayoría señala el asombroso progreso logrado en la digitalización de sus operaciones, modelos comerciales y flujos de ingresos durante la pandemia. El 49% de los CEO están asimismo invirtiendo fuertemente en nuevas tecnologías y planean gastar más en tecnologías digitales en comparación con el año pasado.

Estos escenarios se dan cada vez más en todo el mundo:

- Una empresa ha sido notificada por un regulador respecto a una investigación por presuntas violaciones a la ley o a las regulaciones en mercados extranjeros.
- Un CEO recibe una llamada de su director de seguridad de la información diciendo que se detectó un acceso no autorizado a los sistemas financieros de su empresa, los cuales almacenan los datos de millones de clientes, y pone en riesgo la integridad de las finanzas de su empresa.
- Una corporación recibe una denuncia a través de su línea directa alegando un fraude a gran escala, informes financieros/gestión de ganancias u otras acusaciones graves. En consecuencia, será necesario revisar millones de datos de forma exhaustiva para investigar dicha denuncia.
- Una empresa nacional global está involucrada en un litigio, lo que requiere la identificación, recopilación y producción de grandes cantidades de datos que deben revisarse y corregirse antes de la detección de evidencias.

Ahora todo puede ponerse en duda: las auditorías, el cumplimiento normativo, y los estados contables.

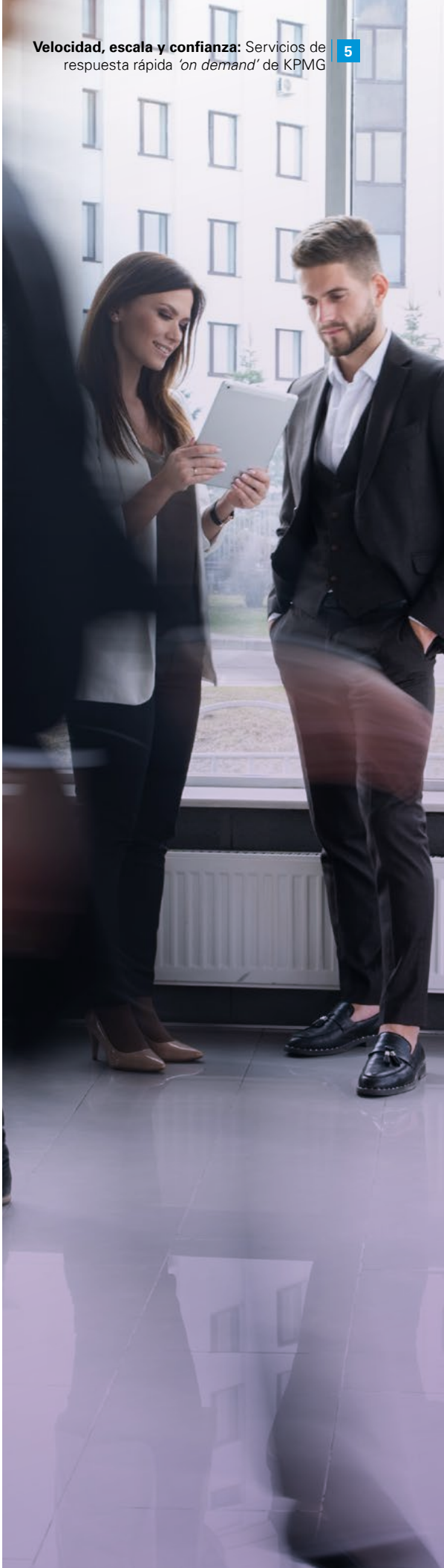


Servicios de respuesta rápida 'on demand' de KPMG

Cuando necesitamos actuar con celeridad

Cuando existen denuncias de fraude, solicitudes de datos por parte de un regulador o alguna filtración cibernética, ser capaz de responder con rapidez es fundamental y, a menudo, algo complejo, especialmente si los incidentes se informan en las operaciones extranjeras de una empresa. Tener recursos con la combinación adecuada de habilidades, fluidez en el idioma local, conocimiento de las costumbres locales, y la capacidad de desplegarse en cuestión de horas es una tarea difícil para cualquier organización.

Para ayudar a mejorar el tiempo de respuesta, la eficiencia, y los costos, muchas organizaciones están estableciendo de manera proactiva relaciones de colaboración con KPMG, permitiéndonos disponer de un contrato marco, y responder lo antes posible según sea necesario. Las firmas de KPMG en todo el mundo cuentan con 6000 profesionales forenses y cibernéticos en más de 100 países que están listos para brindar ayuda. KPMG puede ayudarlo a usted y a su asesor externo a responder con rapidez y escala a estas necesidades, con análisis forenses e investigaciones detalladas.



¿Qué podemos hacer para ayudar?

El modelo de servicios de respuesta rápida -*on demand*- de KPMG es personalizado y aborda colectivamente muchos de los servicios forenses y cibernéticos de KPMG en un solo paquete. Nuestro servicio de respuesta rápida ayuda a reducir los riesgos, y puede alertar a los clientes con relación a amenazas. También se centra en el desarrollo a largo plazo de una capacidad de respuesta cibernética, al mismo tiempo que proporciona un acceso rápido a los conocimientos y profesionales de KPMG.

KPMG quiere ser el proveedor preferido de su organización en lo que respecta a servicios forenses digitales y de respuesta a incidentes, y/o actuar como una extensión de su equipo interno añadiendo capacidades de investigaciones forenses, análisis de malware u otros trabajos altamente especializados.

A través de un contrato de respuesta rápida '*on demand*' con KPMG, su organización puede beneficiarse de nuestro conocimiento sobre su cultura, operaciones, y relaciones con proveedores, entre otros. Este enfoque también puede ayudar a minimizar los desafíos inherentes a la contratación de diversos proveedores de servicios para realizar investigaciones pequeñas o en múltiples jurisdicciones.

> "Los clientes que se incorporaron a los servicios de respuesta rápida '*on demand*' de KPMG antes de un incidente descubrieron que podían responder a ellos en cuestión de minutos en lugar de días."

David Nides
Director, Respuesta Cibernética de KPMG en EE.UU.

Alternativas de contratación:

1. Sobre una base de retención. Por ejemplo, mediante la compra anticipada de una cantidad de horas.
2. Sobre una base de tiempo y materiales. Podemos responder de inmediato cuando necesite ayuda, sin costo anticipado antes de un incidente.

Incorporación por adelantado: la clave para una respuesta rápida a incidentes

Cuando se produce un incidente de ciberseguridad, un fraude, un requerimiento de un regulador, o un litigio, debe actuar con rapidez para identificar y proteger los datos.

Para prepararse y garantizar que nuestro equipo pueda responder rápidamente, comenzaremos con un proceso de incorporación personalizado (por ejemplo, una reunión de dos a tres horas), sin ningún costo para usted.

KPMG hará lo siguiente:

— Se reunirá con las partes interesadas clave que forman parte del proceso de eDiscovery y/o del equipo de respuesta a incidentes cibernéticos.

— Revisará su documentación (incluidas las evaluaciones de preparación para litigios, los planes de respuesta a incidentes, el programa de gestión de riesgos de fraude y los procedimientos de gestión de crisis).

— Logrará entendimiento sobre su red, sistemas e infraestructura de aplicaciones y herramientas de seguridad para comprender dónde y cómo se administran, almacenan y preservan sus datos.

En caso de que ocurra un incidente en su entorno, nuestro conocimiento preexistente de su negocio e infraestructura ayudará a nuestros analistas a comenzar el proceso de respuesta a incidentes sin necesidad antecedentes extensos ni discusiones exploratorias.

Ejecución sencilla y eficaz

Cómo puede ayudar KPMG

1. Respuesta a incidentes

Si ocurre un incidente (como un ataque cibernético, una consulta regulatoria, una acusación de fraude o la presentación de un litigio), las organizaciones deben actuar con rapidez.

En momentos de crisis, las organizaciones pueden contar con los profesionales de KPMG a nivel mundial, con gran experiencia en todos los sectores y jurisdicciones. Todos ellos han sido capacitados de manera constante en nuestras metodologías globales y pueden identificar rápidamente riesgos clave y desarrollar acciones correctivas apropiadas.

Para ayudar a mitigar los riesgos iniciales, comenzaremos proporcionando un plan de acción para identificar qué tareas deben realizarse, y en qué momento. Podemos ayudar con una porción de la investigación como complemento de su propio equipo de investigaciones internas, o bien, podemos realizar toda la investigación de forma independiente bajo la dirección de la gerencia o el abogado de la compañía.

2. Investigación

Llevaremos a cabo análisis forenses e investigaciones detalladas para ayudar a determinar qué sucedió, cómo sucedió y, si corresponde, quién estuvo involucrado. En casos de investigaciones de fraude y cumplimiento normativo, utilizamos herramientas de eDiscovery patentadas y con licencia para llevar a cabo recopilaciones y conservación de datos específicos y con solidez forense, lo que ayuda a nuestros clientes a reducir la cantidad de datos no relevantes.

3. eDiscovery

Para respaldar la investigación, el litigio o la anticipación de un litigio, utilizamos nuestra amplia gama de tecnologías licenciadas y desarrolladas internamente para ayudar a garantizar que brindamos las capacidades adecuadas para cada caso. En casos de investigaciones forenses y cumplimiento normativo, aplicamos inteligencia artificial y aprendizaje activo para identificar documentos de interés en una fracción del tiempo, en comparación con una revisión lineal. A través de una combinación de principios, podemos centrarnos en ayudar a reducir los costos e impulsar un proceso bien posicionado, desde la recopilación hasta la revisión y la producción, mejorando constantemente la calidad, la eficiencia y la productividad, y brindando transparencia a lo largo de la investigación.

Todos los pasos anteriores son clave para implementar una estrategia de ciclo de vida de eDiscovery efectiva y ayudar a garantizar que los datos se muevan a través de las etapas de identificación, conservación, recopilación, procesamiento y análisis de manera precisa y eficiente.

4. Reconstruir la confianza

Cuando nuestros clientes inspiran confianza, crean una plataforma para el crecimiento responsable, la innovación audaz y los avances sostenibles en rendimiento y eficiencia.

— Los profesionales de KPMG tienen habilidades profundas en riesgo y regulación, soluciones digitales avanzadas y una experiencia en cambios sustentada en un enfoque poderoso y global. Podemos ayudarlo a generar confianza con todos los que tienen interés en su negocio, desde clientes, empleados y proveedores, hasta reguladores, accionistas y las comunidades en las que opera.

— Abordamos el riesgo haciendo un cambio positivo desde el cumplimiento pasivo a una generación activa de valor. La confianza multiplica los beneficios.

— Además, KPMG puede ayudarlo a proporcionar un experto neutral designado por el tribunal — La necesidad de una voz neutral es común cuando se presentan problemas técnicos. Los profesionales de KPMG tienen experiencia explicando incluso los desafíos técnicos más complejos, y desarrollando procedimientos objetivos para ayudar a reducir la confusión. Nuestro equipo comprende el proceso legal, y la necesidad de una voz imparcial.

¿Sabías?

Las empresas a menudo consideran los enormes costos tangibles de un ataque cibernético: pérdida de ingresos mientras los sistemas están inactivos, el costo de la reparación, y la compensación o litigio del cliente. Pero los costos intangibles, aunque más difíciles de medir, pueden tener consecuencias a largo plazo aún mayores, por ejemplo, el daño a su reputación y la erosión de la confianza de las partes interesadas.

Profesionales expertos a escala

— KPMG brinda acceso a robustas capacidades cibernéticas y forenses en todo el mundo. Nuestro equipo global altamente colaborativo está formado por profesionales de la materia en varios idiomas que residen en más de 100 países, y estamos comprometidos a cumplir con procesos consistentes que pueden ser aceptados por los organismos reguladores locales.

— Nuestro enfoque basado en datos incluye acceso a extensas bases de datos globales, análisis de inteligencia, y recursos capacitados. Brindamos conocimientos líderes en el mercado, y soluciones habilitadas con inteligencia artificial (IA), para ayudarlo a desafiar la norma y obtener mejores resultados.

— KPMG ha compartido metodologías globales y modelos optimizados de gestión de proyectos que se centran en los riesgos, y simplifican las complejidades para nuestros clientes. Hemos invertido mucho en procesos automatizados, lo que nos permite ayudar a impulsar la consistencia, aumentar la calidad y reducir los costos del cliente.

— Aprovechando la tecnología, hemos desarrollado conocimientos especializados para identificar y analizar sistemas corporativos para evaluar cómo los empleados se comunican, mantienen correspondencia, y mantienen registros comerciales. También brindamos servicios de remediación, ayudando a las empresas a aislar los datos que deben conservarse o eliminarse.

— Tenemos una gran experiencia con una variedad de entornos y sistemas de TI, lo que nos permite brindar un enfoque holístico para las colecciones forenses.

— Combinado con nuestra capacidad global, KPMG también tiene conocimiento local y presencia en casi todos los mercados en los que hace negocios. Por lo tanto, entendemos los riesgos y las ramificaciones que pueden cambiar de un país a otro.

— Podemos ayudarlo a generar confianza con todos los que tienen interés en su negocio, desde clientes, empleados y proveedores, hasta reguladores, accionistas y las comunidades en las que opera.

Velocidad

Nuestro enfoque permite una mayor velocidad y precisión.

KPMG ayuda a acelerar los esfuerzos de investigación y remediación a través del uso significativo de IP y herramientas propietarias.

— Herramientas propias para contener e investigar incidentes a gran escala en las principales plataformas en la nube.

— Flujos de trabajo patentados para tratar la identificación de datos confidenciales estructurados o no estructurados y la revisión de documentos. Esto ayuda en el proceso de notificación obligatoria (normativa, legal).

— Cambio a la nube, particularmente a la luz de los crecientes requisitos regulatorios sobre el transporte transfronterizo de datos.

USD$1m

El costo promedio a nivel mundial para remediar un ataque de ransomware[1]

21%

El 21% de los ataques se realizan por correo electrónico o phishing[2]

29%

El 29% de los ataques son a través de acceso remoto[3]

[1] Informe de reclamos de seguros cibernéticos del primer semestre de 2020, Coalition inc. 2020.

[2-3] Informe técnico de Sophos, mayo de 2020.

¿Por qué KPMG?

Décadas de experiencia en el manejo de infracciones cibernéticas, respuesta regulatoria e investigaciones de fraude/ delitos financieros.

Hemos trabajado en algunas de las investigaciones de informes financieros de más alto perfil; investigaciones reglamentarias sobre denuncias de mala conducta; *ransomware*, APT y ataques internos; y litigios.

Tenemos una experiencia significativa trabajando con todas las partes interesadas involucradas: asesores externos, asesores generales, auditoría interna, cumplimiento, aplicación de la ley, reguladores, seguros de fidelidad, seguros cibernéticos y el negocio más amplio en todos los aspectos de la respuesta a incidentes.

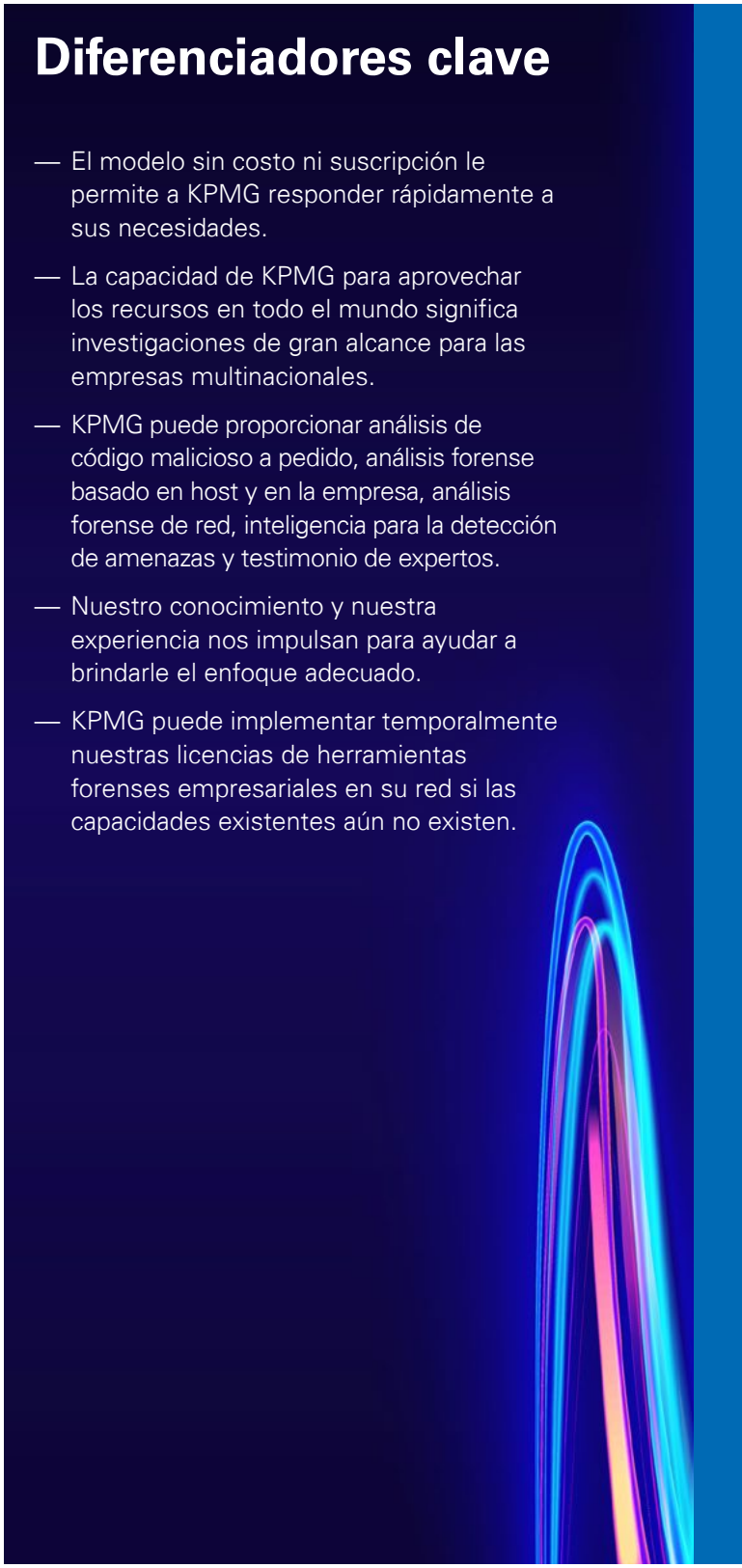
Global y local
Combinado con las capacidades globales de las firmas de KPMG, los profesionales de KPMG tienen conocimiento local, capacidades y presencia en casi todos los mercados en los que hace negocios. Esta profunda experiencia local le permite a KPMG comprender los riesgos y las ramificaciones que varían de un país a otro. Aprovechamos una estructura de gobierno de participación consistente a nivel mundial y le asignamos un único punto de contacto para ayudar a garantizar una entrega consistente en todo el mundo.

Independiente y neutral del proveedor
Estamos totalmente impulsados por nuestra experiencia. Puede confiar en nuestro juicio y asesoramiento libres de prejuicios.

Estamos en las listas de compañías de seguros cibernéticos
Estamos preaprobados como proveedor preferido en muchas de las principales listas de compañías de seguros cibernéticos. Esto puede ayudar a agilizar sus reclamos de seguros cibernéticos.

Diferenciadores clave

- El modelo sin costo ni suscripción le permite a KPMG responder rápidamente a sus necesidades.
- La capacidad de KPMG para aprovechar los recursos en todo el mundo significa investigaciones de gran alcance para las empresas multinacionales.
- KPMG puede proporcionar análisis de código malicioso a pedido, análisis forense basado en host y en la empresa, análisis forense de red, inteligencia para la detección de amenazas y testimonio de expertos.
- Nuestro conocimiento y nuestra experiencia nos impulsan para ayudar a brindarle el enfoque adecuado.
- KPMG puede implementar temporalmente nuestras licencias de herramientas forenses empresariales en su red si las capacidades existentes aún no existen.



"KPMG adopta un enfoque integral de los incidentes cibernéticos a través de su práctica cibernética integrada. Los servicios de preparación para incidentes incluyen ciberestrategia y planificación, configuración y monitoreo de seguridad, pruebas de controles de seguridad, y simulaciones comerciales y técnicas. La respuesta a incidentes de KPMG incluye análisis forense digital, seguimiento de casos e incidentes, análisis de datos y análisis de registros de origen, remediación y mejora empresarial."

IDC MarketScape: Servicios de preparación para incidentes en todo el mundo Evaluación de proveedores de 2021, doc n° US46741420, noviembre de 2021

¿Sabías?

KPMG se posiciona en la categoría de Líderes en el **IDC MarketScape 2021** para servicios de preparación para incidentes en todo el mundo.

Casos de estudio

Proveedor mundial de seguros

El desafío

Una investigación de seguridad cibernética provocada por una notificación del FBI al proveedor de seguros con respecto a la fuga de datos.

Lo que hicimos

KPMG montó una operación 24/7 que comenzó escaneando la red del cliente en busca de servidores externos, realizando evaluaciones de vulnerabilidad de sistemas clave y revisando los registros de red disponibles en busca de signos de actividades sospechosas. Más detalles de fuentes externas permitieron a KPMG centrar su investigación e identificar los sistemas comprometidos. Además de identificar los hosts comprometidos derivados de una explotación de VNC, KPMG pudo identificar otras debilidades de seguridad dentro del entorno del cliente, y otros dispositivos potencialmente comprometidos que no estaban relacionadas con el incidente que se estaba investigando.

El resultado

La organización tenía una postura de seguridad general significativamente mejorada.

Las pruebas conservadas por KPMG se proporcionaron al gobierno a través de los canales legales adecuados.

El sospechoso responsable de la filtración de datos fue arrestado poco después, y luego sentenciado a varios años de prisión. Se le ordenó pagar casi USD 3 millones en restitución al cliente.

Compañía global farmacéutica

El desafío

Una empresa global farmacéutica, de dispositivos médicos y de mercados de consumo de Fortune 50 contrató a KPMG para proporcionar servicios de contabilidad forense e investigación de respuesta rápida '*on demand*' fuera de los EE. UU.

Lo que hicimos

KPMG llevó a cabo una multitud de investigaciones en todo el mundo que van desde denuncias de irregularidades en informes financieros (reconocimiento de ganancias y fraude contable complejo), soborno y corrupción, y preocupaciones sobre conflictos de intereses. KPMG también ayudó a la empresa con inteligencia corporativa y servicios de diligencia debida centrados en antisoborno y corrupción para los grupos legales y de cumplimiento de la empresa. En algunos casos, se solicitó a KPMG que trabajara bajo la dirección de un abogado externo y una auditoría interna, mientras que, en otros casos, ayudamos a proporcionar recursos en el país para aumentar los recursos internos del cliente que conducen las investigaciones.

El resultado

Nuestra asistencia en investigaciones de campo ha ayudado a la empresa a mejorar sus protocolos de respuesta a incidentes, mejorar su tiempo de respuesta para investigar denuncias de fraude y mala conducta, y reducir el tiempo que lleva completar las investigaciones. Como parte de nuestro trabajo, también brindamos información sobre los factores de riesgo de fraude, remediación, recomendaciones y otras oportunidades de mejora para los procesos y controles de la empresa para ayudar a prevenir, detectar y responder al fraude y la mala conducta.

Casos de estudio

Retail en México

El desafío

Una empresa minorista mexicana identificó un pago de nómina a una cuenta no registrada en su maestro de empleados. Se descubrió que la cuenta pertenecía a un empleado de TI.

Lo que hicimos

KPMG llevó a cabo la recopilación y el análisis forenses de las comunicaciones electrónicas del empleado de TI y los registros clave del sistema. Al mismo tiempo, recopilamos y procesamos un año de datos de nómina de más de 20 000 empleados para identificar desviaciones. Como se confirmaron las desviaciones, nuestro análisis condujo a la identificación de un programa no autorizado en el sistema ERP que permitía el descuento automático de una cierta cantidad de la nómina de todos los empleados. El monto desviado se aplicó automáticamente a una cuenta bancaria. Además, este programa fue diseñado para sobrescribir los archivos de pago de nómina, superando los controles de seguridad. También se identificó que el empleado de TI otorgó acceso remoto al sistema ERP a varios terceros.

El resultado

Como resultado de nuestro trabajo, la empresa implementó controles más sólidos sobre el proceso de pago de nómina, realizó una revisión profunda de los programas desconocidos que se ejecutaban en el sistema ERP, mejoró su proceso de monitoreo de acceso remoto e inició acciones legales contra el empleado involucrado.

Compañía farmacéutica

El desafío

Debido a una denuncia interna, la empresa nos solicitó investigar la posible pérdida de propiedad intelectual producto de la salida de un empleado del área comercial.

Lo que hicimos

Nuestro análisis incluyó la recopilación y el análisis forense de la información de los dispositivos asignados a dicho empleado, así como de su correo electrónico corporativo. El análisis también se centró en identificar las actividades realizadas en la computadora durante la semana anterior a la salida del empleado.

El resultado

Como resultado de nuestro análisis, la empresa identificó actividades indicativas de una posible fuga de información de la empresa: conexión de discos duros externos, presencia de herramientas anti-forense para la eliminación segura de información y envío de información a cuentas personales, entre otras.

A partir de estos resultados, la empresa implementó medidas adicionales de control sobre sus activos tecnológicos para evitar fugas de información, y contactó a sus asesores legales para una posible denuncia ante las autoridades.

Contactos

Luis Preciado
Socio líder de Risk Advisory Solutions
de KPMG en México y América Central
luispreciado@kpmg.com.mx

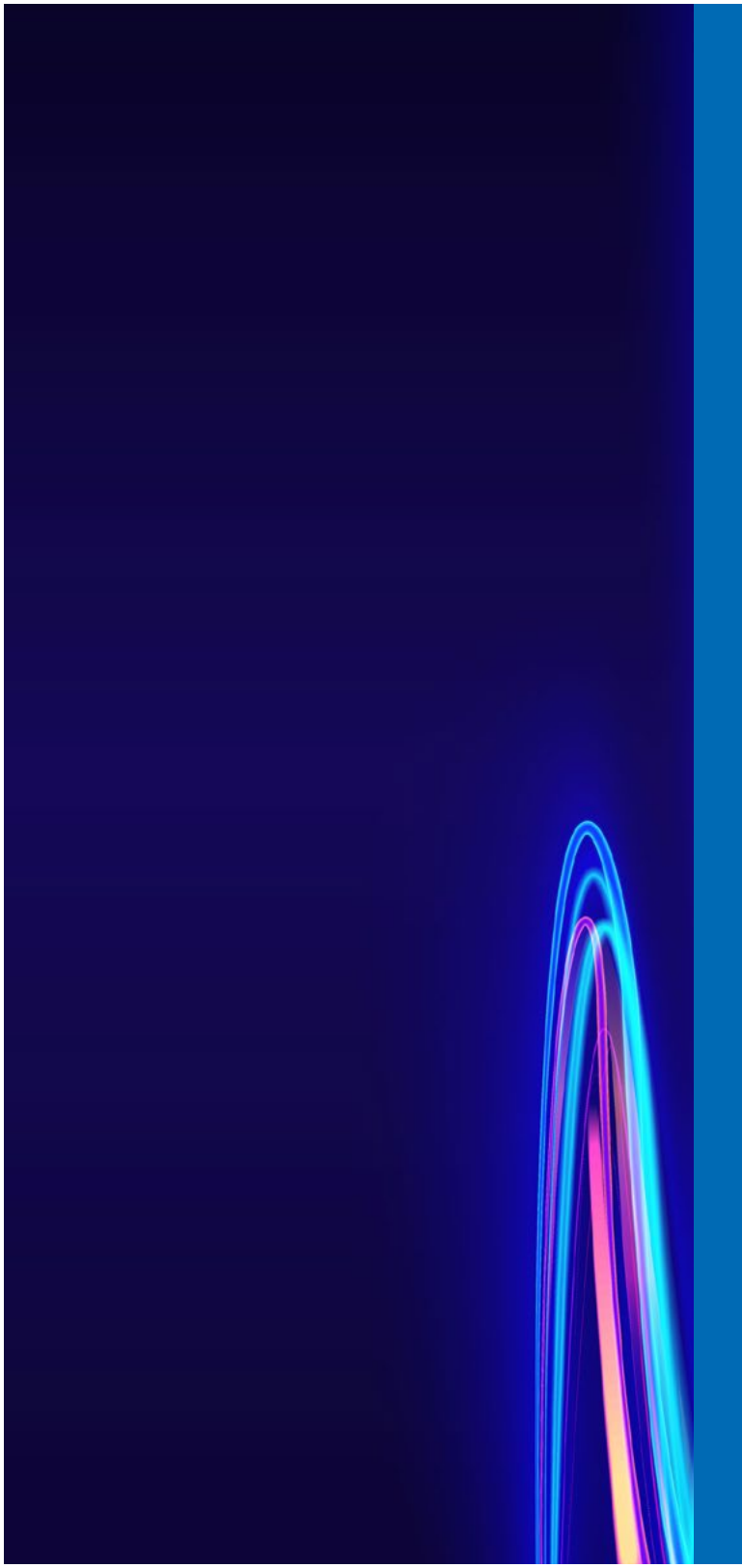
David Nides
Director, Ciberseguridad
de KPMG en Estados Unidos
dnides@kpmg.com

Ivan Velez-Leon
Socio de Forensic Services
de KPMG en Estados Unidos
ievelez@kpmg.com

Ana Lopez Espinar
Socia Líder de Forensic Services de KPMG en
Argentina y Co-lider de KPMG en América del Sur
ablopez@kpmg.com.ar

Emerson Melo
Socio líder de Forensic & Litigation de
KPMG en Brasil y Co-lider de
KPMG en América del Sur
emersonmelo@kpmg.com.br

** Todos los servicios profesionales son proporcionados por las firmas miembro registradas y autorizadas por KPMG International.*



Ser digital
transforma los negocios.

#KPMGTransforma

Descargue nuestra APP