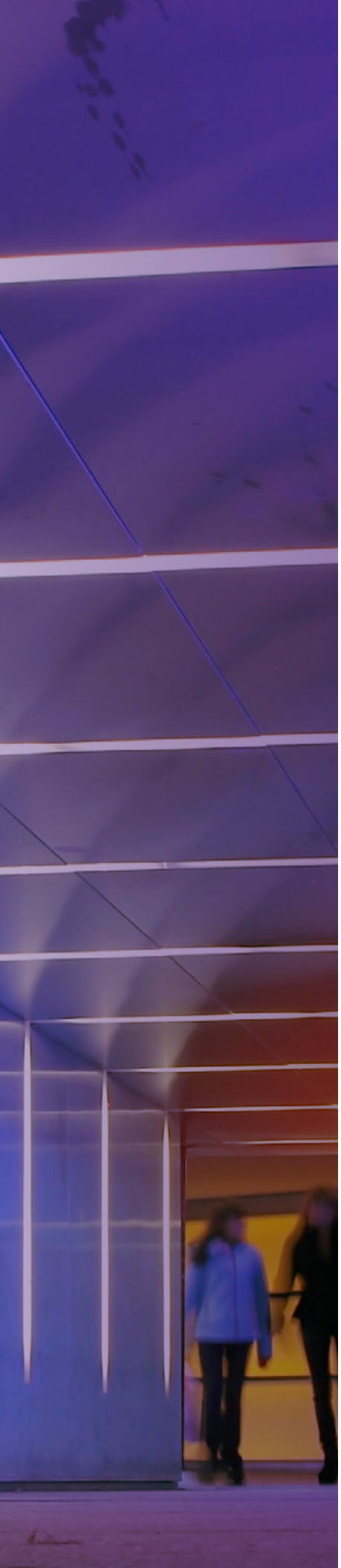
KPMG

Velocidad, escala y confianza

On-Call Services
Servicios bajo solicitud

kpmg.com



Introducción

Las empresas globales de hoy en día gestionan volúmenes abrumadores de información física y electrónica que puede estar sujeta a procesos robustos de recopilación de evidencia, conocidos como *discovery,*[1] en un procedimiento regulatorio o en riesgo de un incidente cibernético. El constante crecimiento del volumen de datos, la existencia de nuevas fuentes de estos, las diversas formas de comunicación, las tecnologías en rápida evolución y un panorama regulatorio cambiante presentan desafíos únicos de descubrimiento electrónico de evidencia (*eDiscovery*) y seguridad cibernética.

El riesgo cibernético se ha triplicado desde 2013 y se está intensificando. Las compañías se enfrentan a un mayor escrutinio regulatorio global sobre la gestión y privacidad de los datos y la integridad en informes financieros. También existe un crecimiento continuo en los litigios en todo el mundo. Esto vuelve esencial que las empresas estén adecuadamente preparadas para responder a las solicitudes de revelación de sus datos electrónicos. A medida que todos los sectores e industrias del mundo se vuelven más digitales, también lo hace la velocidad con la que el cibercrimen afecta todo y a todos en el ámbito global. La efectividad de la seguridad de datos y la gestión de procesos y procedimientos de descubrimiento electrónico de *discovery* resultan clave para ayudar a minimizar los riesgos relacionados con la información.

Las noticias están repletas de artículos sobre empresas involucradas en incidentes de fraude y conductas impropias, que de pronto se enfrentan a investigaciones regulatorias que requieren esfuerzos de descubrimiento de pruebas a gran escala. También se sabe cada vez más acerca de compañías víctimas de ataques cibernéticos a gran escala recientes, que les cuestan millones de dólares en pagos de rescate, y que, en consecuencia, paralizan su infraestructura y destruyen la confianza. La pandemia de COVID-19 y el consiguiente aumento de colaboradores trabajando a distancia, en ocasiones sin protección de ciberseguridad suficiente, o que utilizan dispositivos de almacenamiento de datos no aprobados, han impulsado tanto los ciberataques como protocolos de gestión e identificación de datos poco efectivos.

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

Sin importar su tamaño, tanto las multinacionales globales como las empresas sin fines de lucro más pequeñas pueden ser afectadas por el fraude, el incumplimiento regulatorio y el cibercrimen.

¿Sabía usted que…?

74% de las personas a cargo de la Dirección General participantes en *KPMG 2021 CEO Outlook Pulse Survey*[2] afirman que la velocidad de la digitalización en sus organizaciones se ha acelerado en cuestión de meses.

La mayoría señala el asombroso progreso que ha logrado en la digitalización de sus operaciones, modelos de negocio y flujos de ingresos durante la pandemia. 49% reconoce estar invirtiendo de manera relevante en nuevas tecnologías, y planea destinar más recursos en tecnologías digitales en comparación con el año anterior.

1 En un proceso legal, el término *discovery* corresponde al intercambio de información entre las partes antes de un juicio, que permite a cada cual conocer la evidencia que será presentada.

2 *KPMG 2021 CEO Outlook Pulse Survey,* KPMG International, 2021.

Con cada vez mayor frecuencia se observan los siguientes escenarios en todo el mundo:

- Una empresa es notificada por un regulador sobre una investigación en torno a denuncias por violaciones de leyes o regulaciones en mercados extranjeros
- La Dirección General recibe una llamada de la Dirección de Seguridad de la Información (CISO, por sus siglas en inglés) indicando que se detectó un acceso no autorizado a los sistemas financieros de la empresa: la "joya de la corona" que almacena millones de datos de clientes y que pone en riesgo la integridad de las finanzas de la organización
- Una corporación es alertada por un denunciante mediante su línea directa para ese propósito, alegando un fraude a gran escala, informes financieros o de gestión de resultados fraudulentos u otras acusaciones graves. En ese momento, se deben analizar con urgencia cantidades exorbitantes de datos para investigar la queja
- Una empresa nacional con presencia global está involucrada en un litigio, lo que requiere la identificación, preservación y producción de grandes cantidades de datos que deben revisarse y redactarse antes del proceso de descubrimiento (discovery)

Ahora todo puede ser cuestionable: auditoría, cumplimiento regulatorio e informes financieros

1. **Litigios y arbitraje**
2. **Investigaciones gubernamentales**
3. **Fusiones y adquisiciones o desinversiones**
4. **Investigaciones internas**
5. **Actualizaciones y migraciones de sistemas a la nube**
6. **Gestión de datos HIPPA, PCI, PII, IP[3]**
7. **Otras necesidades de disposición de datos como requerimientos de eliminación de información redundante u obsoleta (ROT)[4]**

3 HIPPA: Health Insurance Portability and Accountability Act: establece responsabilidades para entidades del sector salud en EE.UU. en relación con la privacidad de la información de salud de los pacientes. PCI DSS: Payment Card Industry Data Security Standard, parámetro de seguridad de la información que se aplica a todas las entidades que almacenan, procesan o transmiten datos de los titulares de tarjetas. PII: información de identificación personal (datos personales o datos personales sensibles). IP: propiedad intelectual, por sus siglas en inglés.

4 Redundant, Obsolete and Trivial (ROT).

KPMG On-Call Services Servicios bajo solicitud

Cuando necesita reaccionar rápidamente

Una respuesta inmediata y ágil ante denuncias de fraude, solicitudes de datos por parte de reguladores y posibles incidentes cibernéticos es crítica y a menudo resulta compleja, en especial si los incidentes suceden en las operaciones de la empresa en el extranjero. Contar con los recursos y el conjunto de habilidades adecuados, la fluidez en el idioma del país en cuestión, el conocimiento de sus prácticas locales y la capacidad para desplegar recursos en unas cuantas horas es una tarea difícil para cualquier organización.

Para ayudar a mejorar el tiempo de respuesta, favorecer la eficiencia y reducir costos, muchas compañías están estableciendo, de manera proactiva, relaciones de colaboración con KPMG mediante un contrato prestablecido con la finalidad de responder lo antes posible con base en las necesidades de la empresa. La red de firmas de KPMG en el mundo cuenta con 6,000 especialistas forenses y de ciberseguridad en más de 100 países, preparados para apoyarle. KPMG puede ayudarle a usted y a su consejero independiente a responder, rápidamente y en la escala requerida, a estas necesidades, utilizando análisis forenses y llevando a cabo investigaciones detalladas.

¿Qué podemos hacer para ayudarle?

Los servicios bajo solicitud (On Call Services) es un modelo de respuesta personalizado que, en su conjunto, incluye muchos de los servicios forenses y en materia de ciberseguridad que ofrece KPMG en un solo paquete. Este ayuda a reducir los riesgos y puede informarle de manera proactiva de las amenazas. También se centra en el desarrollo a largo plazo de una capacidad de respuesta cibernética, al tiempo que proporciona un acceso rápido al conocimiento y experiencia de KPMG y sus especialistas.

KPMG se propone ser la clara elección para su empresa en servicios forenses digitales y de respuesta a incidentes, ya sea como su proveedor de confianza, o actuar como una extensión de su equipo interno, aumentando sus capacidades con investigaciones forenses, el análisis de *malware* u otras labores altamente especializadas.

Mediante un acuerdo de servicios bajo solicitud (*on-call agreement*), su empresa puede beneficiarse de nuestro conocimiento sobre su cultura, operaciones, relaciones con proveedores, entre otros temas. Nuestro enfoque puede ayudarle a minimizar los desafíos inherentes al uso de múltiples proveedores de servicios cuando se realizan investigaciones ya sea a baja escala o en múltiples jurisdicciones.

> “Los clientes que optaron por KPMG On-Call Services antes de un incidente descubrieron que era posible responder a estos en cuestión de minutos en lugar de días”.

David Nides
Socio de Respuesta Cibernética de KPMG en EE.UU.

Le ofrecemos dos posibles formas de colaboración

1. Con una base de retención (por ejemplo, mediante la compra anticipada de cierta cantidad de horas)
2. Con base en el tiempo y los materiales que se requieran. No implica costo alguno implementar este acuerdo en previsión de un incidente, y esto nos permite responder de inmediato cuando necesite ayuda

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

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

Para preparar y ayudar a cercionarse de que nuestro equipo pueda responder rápidamente, comenzamos un proceso de incorporación personalizado (por ejemplo, una reunión de dos a tres horas) sin costo alguno para su empresa.

KPMG:

— Se reunirá con las partes interesadas clave que integran el proceso de *eDiscovery* o con el 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 manejo de crisis)

— Obtendrá un entendimiento de su red, sistema e infraestructura de aplicaciones y herramientas de seguridad para comprender dónde y cómo se administran, almacenan y preservan los datos

En caso de que ocurra un incidente en su entorno, el conocimiento prexistente que tengamos de su negocio e infraestructura puede ayudar a nuestros especialistas a comenzar el proceso de respuesta a incidentes sin necesidad de analizar antecedentes extensos ni incurrir en discusiones exploratorias.

Ejecución sencilla y eficaz

¿Cómo puede ayudar KPMG?

1. Respuesta a incidentes

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

En momentos de crisis, los especialistas de KPMG a nivel mundial están a disposición; cuentan con amplia experiencia en los diversos sectores y jurisdicciones, y se han capacitado continuamente en metodologías globales, lo que les habilita para identificar rápidamente riesgos clave y desarrollar acciones correctivas apropiadas.

Para ayudarle a mitigar los riesgos iniciales, comenzamos proporcionando un plan de acción para identificar qué tareas deben realizarse y cuándo. De esta manera podemos apoyarle ya sea con una porción de la investigación como un complemento al equipo de investigaciones internas de la empresa, o realizarla en su totalidad, de forma independiente, bajo la dirección de la Administración o de los asesores legales.

2. Investigación

Llevamos a cabo análisis forenses e investigaciones detalladas para ayudar a determinar qué sucedió, cómo sucedió y, en su caso, quién o quiénes estuvieron involucrados. Nuestras herramientas y propiedad intelectual pueden acelerar estos esfuerzos. Por ejemplo, en caso de un ataque cibernético, automatizamos las tareas comunes de clasificación forense de manera oportuna y consistente mediante el uso de KPMG Digital Responder. En casos de investigaciones de fraude y cumplimiento regulatorio, utilizamos herramientas propias de *eDiscovery* con licencia para llevar a cabo recopilaciones y conservación de datos específicos, con solidez forense, lo que ayuda a nuestros clientes a reducir la cantidad de datos no relevantes. A lo largo del proceso de *eDiscovery*, utilizamos la herramienta de trazabilidad de evidencia de KPMG para documentar y mantener una cadena de custodia de todos los datos que adquirimos y recibimos.

3. Descubrimiento electrónico, *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 en cada ocasión. En aquellos casos de investigaciones forenses y cumplimiento regulatorio, ayudamos a monitorear los datos y aplicamos inteligencia artificial y aprendizaje activo para identificar documentos de interés en una fracción del tiempo, en comparación con una revisión lineal tradicional. Mediante una combinación de principios, podemos centrarnos en ayudar a reducir los costos e impulsar un proceso bien posicionado, desde la preservación 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 para ayudar a garantizar que los datos transitan, de manera precisa y eficiente, las etapas de identificación, conservación, preservación, procesamiento y análisis.

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 las habilidades necesarias en temas de riesgo y regulación, soluciones digitales avanzadas, así como experiencia sólida en procesos de cambio con un enfoque eficaz y global. Podemos ayudarle a generar la confianza de quienes tienen interés en su negocio, desde clientes, empleados y proveedores, hasta reguladores, accionistas y las comunidades en las que opera
- Nuestro enfoque en el riesgo ofrece un cambio positivo para pasar del cumplimiento pasivo a la generación activa de valor. La confianza es un multiplicador de beneficios
- Además, KPMG puede ayudarle poniendo a su disposición un especialista neutral designado por las autoridades competentes. La necesidad de una voz neutral es común ante temas técnicos. Nuestros profesionales tienen experiencia explicando, incluso, los desafíos técnicos más complejos y desarrollando procedimientos objetivos para ayudar a reducir el desconcierto. Nuestro equipo entiende el proceso legal y la necesidad de una voz verdaderamente imparcial y libre de cualquier sesgo

¿Sabía usted que…?

Los negocios a menudo consideran los enormes costos tangibles de un ataque cibernético: pérdida de ingresos mientras los sistemas están inactivos, el costo de la remediación y la compensación o litigio del cliente; sin embargo, 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.

Experimentados especialistas a escala

— KPMG brinda acceso a amplias capacidades forenses y en ciberseguridad en todo el mundo. Nuestro equipo global altamente colaborativo está formado por profesionales multilingües especialistas en la materia, que residen en más de 100 países. Estamos comprometidos con el cumplimiento de procesos consistentes que puedan ser aceptados por los organismos reguladores locales

— Nuestro enfoque basado en datos incluye acceso a extensas bases globales, inteligencia analítica y personal capacitado. Brindamos conocimientos líderes en el mercado y soluciones habilitadas con inteligencia artificial (IA) para ayudar 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 la complejidad para nuestros clientes. Hemos invertido sustancialmente en procesos automatizados, lo que nos permite ayudar a impulsar la consistencia, aumentar la calidad y reducir costos

— Aprovechando la tecnología, hemos desarrollado conocimientos especializados para identificar y analizar sistemas corporativos para evaluar cómo los colaboradores se comunican, mantienen correspondencia y registros comerciales. También brindamos servicios de asistencia para la eliminación de información obsoleta, redundante o trivial (*defensible deletion*), ayudando a las empresas a identificar los datos que deben conservarse, extraerse o eliminarse

— Contamos con una gran experiencia en una variedad de entornos y sistemas de tecnologías de la información (TI), lo que nos permite brindar un enfoque holístico para las preservaciones forenses

— Combinado con nuestra capacidad global, KPMG cuenta con 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 darse de un país a otro

— Podemos ayudarle a generar la confianza de sus grupos de interés, desde clientes, empleados y proveedores, hasta reguladores, accionistas y las comunidades donde 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 propiedad intelectual y herramientas propias

— KPMG Digital Responder[5] (patente pendiente) automatiza las tareas comunes de clasificación forense de manera oportuna y consistente. Esto permite a las organizaciones responder a los incidentes cibernéticos ayudándoles a aumentar la eficacia y eficiencia de la respuesta

— Contamos con herramientas propias para contener e investigar incidentes a gran escala en las principales plataformas en la nube

— Hemos diseñado flujos de trabajo propios para la identificación de datos confidenciales estructurados o no estructurados y la revisión de documentos. Lo anterior ayuda en el proceso de notificación obligatoria (regulatoria, legal)

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

Confianza

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

— KPMG concentra grandes habilidades en riesgo y regulación, soluciones digitales avanzadas y experiencia de cambio bien establecida en un poderoso alcance global

— Nuestro enfoque en el riesgo ofrece un cambio positivo para pasar del cumplimiento pasivo a la generación activa de valor. La confianza es un multiplicador de beneficios

— Podemos ayudarle a generar la confianza de sus grupos de interés, desde clientes, empleados y proveedores, hasta reguladores, accionistas y las comunidades donde opera

USD 1,000,000

es el costo promedio a nivel mundial para remediar un ataque de *ransomware*[1]

21%

de los ataques se realizan por correo electrónico o *phishing*[2]

29%

de los ataques son mediante acceso remoto[3]

1 *H1 2020 Cyber insurance Claims Report,* Coalition inc., 2020.

2-3 Sophos *Whitepaper*, mayo de 2020.

5 Patente en trámite.

¿Por qué KPMG?

Décadas de experiencia en el manejo de incidentes cibernéticos, respuesta regulatoria e investigaciones de fraude y delitos financieros

Hemos trabajado en algunas de las investigaciones de informes financieros del más alto perfil; investigaciones regulatorias sobre denuncias de conducta indebida; *ransomware*, amenaza persistente avanzada (APT, por sus siglas en inglés), ataques desde el interior, así como litigios.

Contamos con experiencia relevante trabajando con todas las partes interesadas involucradas: consejeros independientes, abogados generales, Auditoría Interna, cumplimiento, aplicación legal, reguladores, seguros de fidelidad, seguros cibernéticos y la cobertura más amplia en todos los aspectos de la respuesta a incidentes.

Global y local
Combinado con las capacidades globales de las firmas de KPMG, nuestros especialistas cuentan con conocimiento local, capacidades y presencia en casi todos los mercados en los que hacemos negocios. Esta amplia 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 las vinculaciones consistente a nivel mundial y le asignamos un único punto de contacto para ayudar a garantizar una entrega de la misma calidad en todo el mundo.

Independiente y neutral
Somos impulsados completamente por nuestra experiencia. Puede confiar en nuestro juicio y asesoría libre de sesgos.

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

Diferenciadores clave

- El modelo sin costo ni suscripción le permite a KPMG responder rápidamente a sus necesidades
- Un proceso de integración ágil y eficiente implica que KPMG también invierte en la relación
- KPMG conforma una red global de firmas miembro de reconocida trayectoria
- La capacidad de KPMG para aprovechar los recursos en todo el mundo se traduce en investigaciones de gran alcance para empresas multinacionales
- KPMG puede proporcionar análisis de código malicioso (*malware*) a solicitud, así como análisis forense en dispositivos individuales o en toda la organización, y *network forensics* (análisis forense de red), inteligencia de amenazas y testimonio de expertos
- Nuestro conocimiento y experiencia nos impulsan a brindarle el enfoque adecuado
- KPMG puede implementar temporalmente licencias de herramientas forenses empresariales en su red, si carece de las capacidades requeridas

"KPMG adopta un enfoque integral de los incidentes cibernéticos gracias a su práctica de ciberseguridad integrada. Los servicios de preparación para incidentes incluyen el desarrollo de elementos estratégicos y planificación, configuración y monitoreo de seguridad, pruebas de controles de seguridad, así como simulaciones tanto de negocios como técnicas. La respuesta a incidentes de KPMG incluye análisis forense digital, seguimiento de casos e incidentes, análisis de datos y de fuentes de bitácoras, recuperación ante desastres, remediación y mejora empresarial".

***IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment,* Documento US46741420, noviembre de 2021.**

¿Sabía usted que…?

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

Casos de estudio

Proveedor mundial de seguros

Desafíos

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

Lo que hicimos

KPMG montó una operación 24/7 que comenzó escaneando la red del cliente en busca de servidores conectados directamente a internet, realizando evaluaciones de vulnerabilidad de sistemas clave y revisando las bitácoras de red disponibles en busca de actividad sospechosa. Detalles obtenidos a partir de fuentes externas de información ayudaron a centrar la investigación e identificar los sistemas en entredicho. Además de identificar los *hosts* comprometidos derivados de un aprovechamiento de una vulnerabilidad en su VNC (*virtual network computing*), KPMG pudo identificar otras debilidades de seguridad en el entorno del cliente, así como equipos adicionales potencialmente comprometidos que no estaban relacionados con el incidente investigado.

El resultado

La organización mejoró de forma significativa su postura en materia de ciberseguridad.

Las evidencias preservadas por KPMG se proporcionaron al gobierno mediante los canales legales adecuados.

El sospechoso de la filtración de datos fue arrestado poco después y luego sentenciado a varios años de prisión, y se le ordenó pagar al cliente casi USD 3,000,000 en restitución.

Compañía global de ciencias de la vida

Desafíos

Una empresa global farmacéutica de dispositivos médicos y de mercados de consumo, perteneciente al segmento *Fortune* 50, contrató a KPMG para proporcionar servicios de contabilidad forense e investigación bajo solicitud fuera de Estados Unidos.

Lo que hicimos

KPMG llevó a cabo una multitud de investigaciones en todo el mundo partiendo desde denuncias en materia de reportes financieros —como gestión de ganancias, fraude contable complejo y saturación del canal de ventas (*channel stuffing*)—, soborno y corrupción, hasta preocupaciones sobre conflictos de intereses. KPMG también ayudó a la empresa con servicios de inteligencia corporativa y debida diligencia, centrados en temas antisoborno y anticorrupción, para los equipos legales y de cumplimiento. En algunos casos, se solicitó a KPMG que trabajara bajo la dirección de un consejero legal externo y de Auditoría Interna, mientras que, en otros, la Firma asignó personal en el país correspondiente para aumentar los recursos internos del cliente dedicados a las investigaciones.

El resultado

Nuestro apoyo en investigaciones bajo solicitud ha ayudado a la empresa a mejorar sus protocolos de respuesta a incidentes, acortando el tiempo para investigar denuncias de fraude y conductas impropias, y reduciendo el tiempo para completar las investigaciones. Como parte de nuestro trabajo, también brindamos información sobre los factores de riesgo de fraude, un análisis de causa raíz, remediación, recomendaciones y la identificación de otras oportunidades de mejora para los procesos y controles que ayuden a prevenir, detectar y responder al fraude y la conducta indebida.

Casos de estudio

Sector minorista en México

Desafíos

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

Lo que hicimos

KPMG llevó a cabo la preservación y el análisis forense de las comunicaciones electrónicas del empleado de TI y los registros clave del sistema. Al mismo tiempo, se recopiló y procesó un año de datos de nómina de más de 20,000 empleados para identificar desviaciones. Como se confirmaron las desviaciones, el análisis condujo a la identificación de un programa no autorizado en el sistema ERP (*enterprise resource planning*) 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, vulnerando 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 los hallazgos, se ayudó a la empresa a implementar controles más sólidos sobre el proceso de pago de nómina mediante una revisión profunda de los programas desconocidos que se ejecutan en el sistema ERP, mejorando el proceso de monitoreo de acceso remoto. Asimismo, se iniciaron acciones legales contra el empleado responsable.

Compañía farmacéutica

Desafíos

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

Lo que hicimos

Nuestro análisis incluyó la preservación 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 su salida.

El resultado

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

A partir de estos resultados, la empresa pudo implementar medidas adicionales de control sobre sus activos tecnológicos para evitar fugas de información e inició una denuncia ante las autoridades.

Contactos

Amanda Rigby
Líder de Forensic para Américas
Socia de Asesoría
KPMG en EE.UU.
amandarigby@kpmg.com

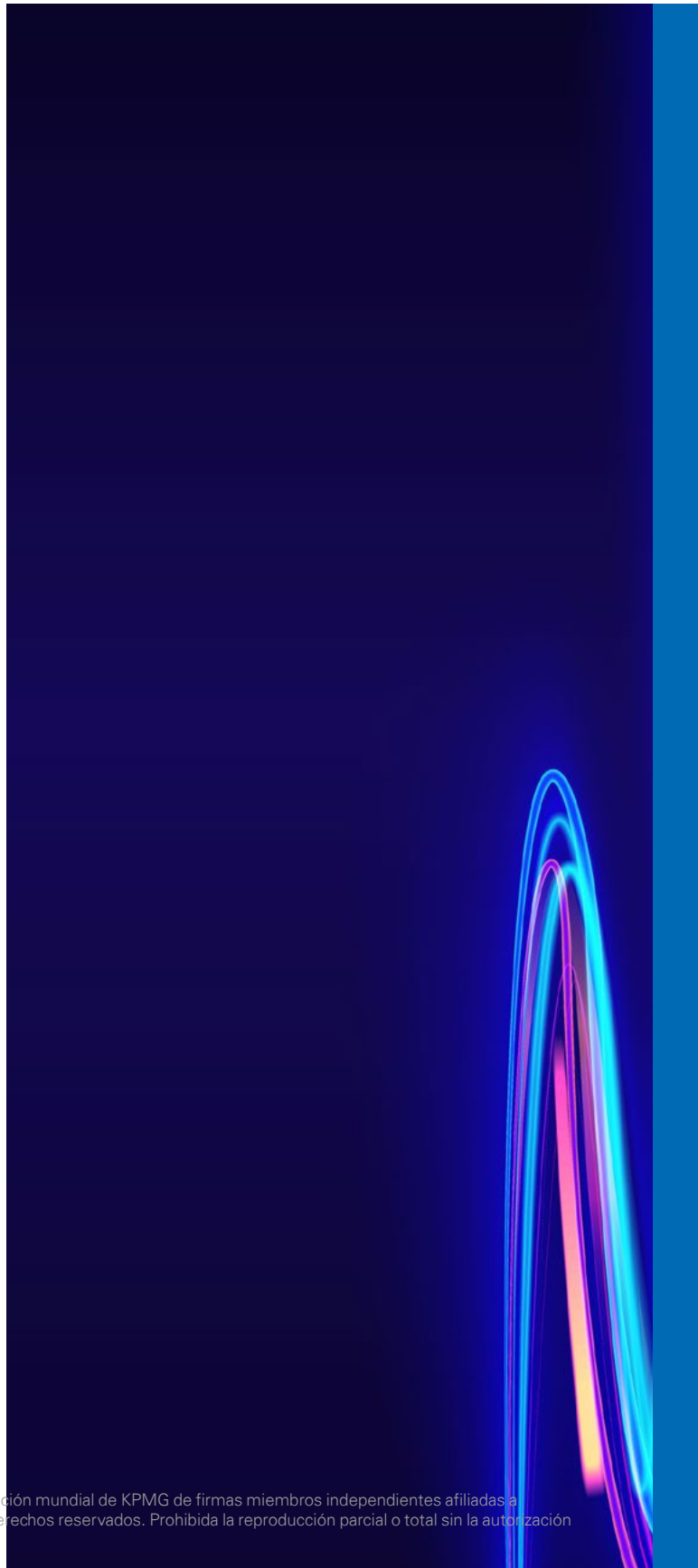
Luis Preciado
Socio Líder de Risk Advisory Solutions
KPMG en México
Líder de Forensic para México y Centroamérica
luispreciado@kpmg.com.mx

David Nides
Socio de Respuesta Cibernética
KPMG en EE.UU.
dnides@kpmg.com

Iván Vélez-León
Director General de Forensic
KPMG en EE.UU.
ievelez@kpmg.com

Ana López Espinar
Socia de Forensic
KPMG en Argentina
ablopez@kpmg.com.ar

Emerson Melo
Socio de Forensic
KPMG en Brasil
emersonmelo@kpmg.com.br



*Todos los servicios son provistos por firmas miembros de KPMG International registradas y con licencia de KPMG

kpmg.com.mx
800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX