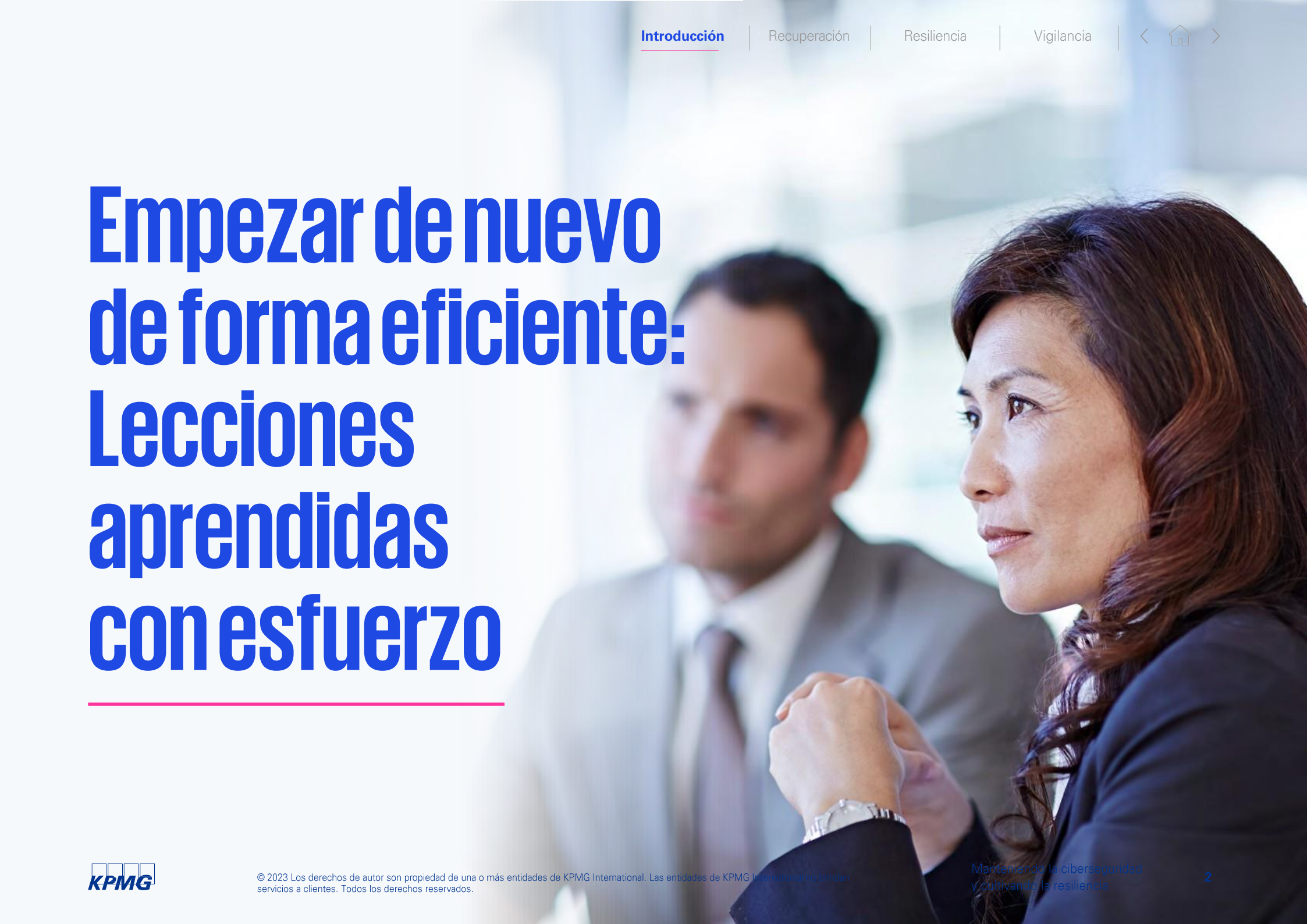
KPMG

Manteniendo la ciberseguridad y cultivando la resiliencia

Cómo recuperarse de un ciberataque, reconstruirse de forma eficaz y evitar la complacencia

KPMG
noviembre 2023

Empezar de nuevo de forma eficiente: Lecciones aprendidas con esfuerzo



En un panorama en constante cambio, los métodos de defensa ya no son rivales para los delincuentes sofisticados, que se benefician cada vez más de los ataques cibernéticos y obligan a los países a invertir millones en ciberseguridad.

Al explorar nuevas tecnologías y rutas de ataque y, al mismo tiempo, aprovechar herramientas antiguas, los delincuentes están utilizando la Inteligencia Artificial (IA) a su favor. Según el estudio KPMG 2023 CEO Outlook, el 82% de los directores ejecutivos están de acuerdo en que la Inteligencia Artificial generativa (*genAI*) es un arma de doble filo que ayudará a detectar ciberataques pero que podría usarse como herramienta para crear estafas y estrategias para los delincuentes. [1]

La solución es trabajar en la reducción de daños. Si bien la prevención sigue siendo una prioridad para evitar ataques, los líderes reconocen que este tipo de estafas tendrán éxito independientemente de cuánto se invierta en seguridad, lo que puede resultar en el robo de propiedad intelectual y datos sensibles, e incluso la extorsión. En el mismo estudio, el 74% de los directores ejecutivos afirmaron que el cibercrimen y la inseguridad en el entorno digital son factores que afectarán la prosperidad. Detectar rápidamente los problemas, responder a los ataques y recuperarse después del hecho será lo más importante para minimizar daños y desarrollar resiliencia.

La complacencia es uno de los mayores enemigos de la resiliencia. Algún tiempo después de que ocurre un ataque, es común que los malos hábitos regresen lentamente a medida que la atención se centra en cuestiones operativas más urgentes. No es de extrañar que cuando se baja la guardia puedan producirse nuevos ataques. Y no se sorprenda si los clientes y *las partes interesadas* muestran menos simpatía cuando su empresa vuelva a ser víctima de un ciberataque.

Por este motivo, es importante cultivar la ciberresiliencia, manteniendo las capacidades operativas empresariales y la confianza de los clientes, al tiempo que se protege contra futuros ataques.

Según el informe de KPMG Global Tech 2023, el 71% *de* las empresas dicen que se han vuelto más proactivas, integrando confianza, seguridad, privacidad y resiliencia en la implementación de nuevas tecnologías. Los organismos reguladores de todo el mundo están enfocándose cada vez más en la resiliencia cibernética, ya sea a través de la Ley de Resiliencia Operacional Digital de la Unión Europea (DORA) y la nueva Directiva de Sistemas de Información y Redes, o las recientes regulaciones cibernéticas de la Comisión de Bolsa y Valores de Estados Unidos (SEC).

Las organizaciones están bajo presión para ser más transparentes sobre su capacidad para responder a violaciones de seguridad antes, durante y después de un incidente. En algunas industrias críticas, como las de servicios financieros, los reguladores exigen la restauración del servicio dentro de un período de tiempo específico, mientras que otras industrias pueden requerir que se centre la atención en proteger a los clientes del daño causado por los ataques.

En julio de 2023, la SEC creó una regla que exige que las empresas divulguen sobre la gestión de riesgos, la estrategia, la gobernanza y los incidentes de ciberseguridad.

El objetivo después de una brecha de seguridad no es sólo reconstruir la empresa, sino hacerla más fuerte que antes, más resistente a los ataques, segura y resiliente.

En este estudio, compartimos lecciones aprendidas con esfuerzo con el objetivo de ayudar a las organizaciones a enfrentar con confianza y proactivamente las amenazas cibernéticas, recuperarse de un incidente y regresar aún más fuertes.

La seguridad se reconoce como una oportunidad

El 74% de los directores ejecutivos reconocen la delincuencia y la ciberseguridad como factores que afectarán la prosperidad.

El 71% de las empresas confirma la necesidad de ser más proactivos a la hora de integrar la confianza, la seguridad, la privacidad y la resiliencia en el *despliegue* de nuevas tecnologías.

El 82% de los directores ejecutivos reconoce que *genAI* es un arma de doble filo que ayudará a detectar intrusiones cibernéticas pero también brindará a los delincuentes nuevas formas de llevar a cabo ataques.

1 KPMG 2023 CEO Outlook, KPMG International, 2023.
2 Ibid.
3 KPMG Global Tech report 2023, KPMG International, 2023.
4 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216; 34-97989; File No. S7-09-22, (September 5, 2023).

Pasos clave para recuperarse de un ciberataque y evitar la complacencia

En el calor del momento:

Recupérese

1. **Defina la gravedad del problema:** priorice su negocio.
2. **Enfóquese en lo que importa:** hacerlo puede sorprenderlo.
3. **Sea claro sobre las responsabilidades de cada persona,** y colabore en el éxito de las tareas.
4. **Comunique** con firmeza, claridad y coherencia a quien sea necesario.
5. **Deténgase a reflexionar,** incluso en los peores momentos.
6. **Sea adaptable:** no existe un manual para todo.
7. **Sepa cuándo terminó la crisis:** avance rápidamente, pero sea cauteloso.

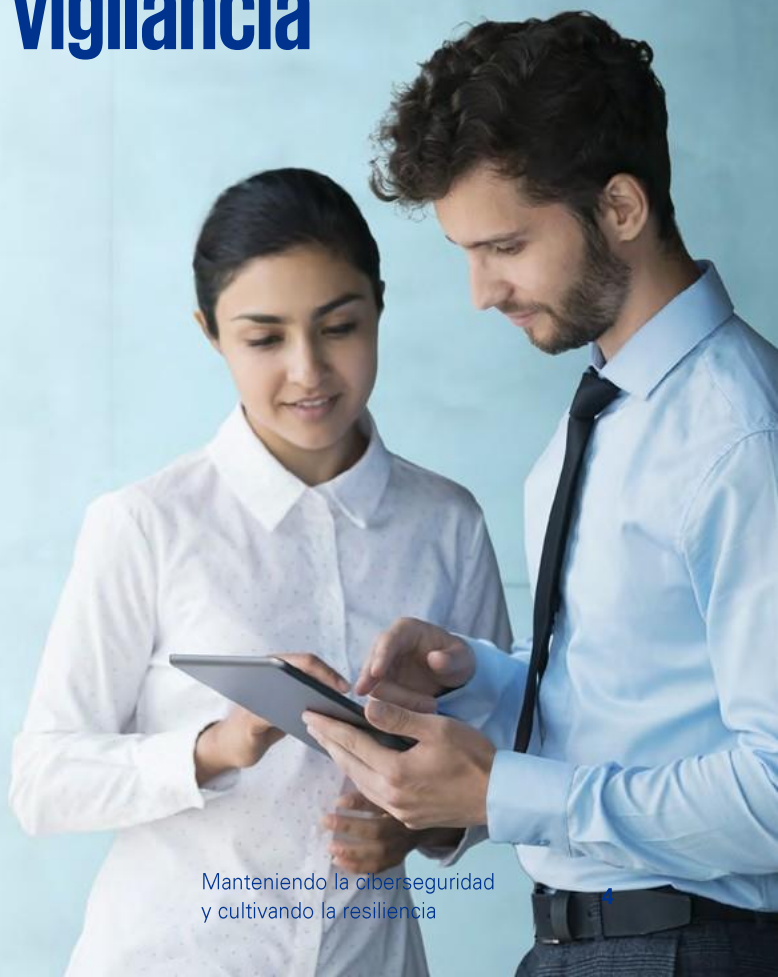
Cuando lo peor haya pasado:

Sea resiliente

1. **Sea honesto acerca de lo que sucedió** y aprenda de ello.
2. **Desarrolle resiliencia** y siga mejorando.
3. **Haga limpieza:** de datos y aplicaciones.
4. **La tarea es de toda la empresa,** y no la función de un solo equipo.
5. **Comprenda la cadena de suministro** y su papel en la construcción de resiliencia.
6. **Retenga el talento** para acceder rápidamente a las habilidades que necesita.
7. **El mundo cambia,** no asuma que los desafíos de hoy serán los mismos que los de mañana.

Pero, sobre todo:

Mantenga la vigilancia



En el calor del momento: Recupérese

01 Define la gravedad del problema: priorice su negocio

Existe el riesgo de que los altos ejecutivos subestimen el alcance del impacto de una violación de seguridad, tratándola como una cuestión principalmente técnica. Hablar a los ejecutivos con antelación puede ayudar a explicar la gravedad de la situación, aclarar lo que podría suceder en los próximos días y presentar un panorama realista, con un cronograma y una medida de la incertidumbre. Los consultores externos pueden aportar *conocimientos esenciales* a partir de sus propias experiencias. Una vez que el CEO y el CFO reconocen que aspectos fundamentales de sus operaciones están amenazados (por ejemplo, es posible que no puedan pagar a sus empleados y proveedores o incluso comunicarse con los clientes), tienden a adoptar un enfoque más participativo en su papel de liderazgo para abordar la situación y el problema.

02 Enfóquese en lo que importa: hacerlo puede sorprenderlo

En el clima tenso que sigue a un ciberataque, es natural querer arreglar todo rápidamente; sin embargo, es necesario resistir este impulso. Al contrario, los líderes deben definir qué procesos y sistemas son más importantes y deben recuperarse como prioridad.

Por ejemplo, en una industria que depende en gran medida de recursos, como la construcción, la capacidad de pagar a los trabajadores subcontratados es esencial para garantizar que sigan asistiendo a trabajar. Por otro lado, los médicos y profesionales sanitarios de un hospital necesitan acceso a los datos de los pacientes y al equipo funcional.

Un fabricante a escala global, por otro lado, necesita centrar su atención en las instalaciones que generan la mayor parte de las ganancias y mantener la liquidez. En otros sectores, las cuestiones de seguridad pueden ser la preocupación principal. La reconstrucción de la infraestructura técnica debe diseñarse considerando estas variables.

> **"Una empresa que sufrió un ataque no tenía un registro de empleados, por lo que no podía pagar a su personal, comprometiendo a la empresa en su conjunto. Una vez que se dieron cuenta de esto, se concentraron en recuperar y restaurar los detalles de la nómina mediante *copias de seguridad*."**

Jason Haward-Grau
Líder global de servicios de recuperación cibernética en KPMG International y líder de KPMG en EE. UU.

03 Sea claro sobre las responsabilidades de cada persona, y colabore en el éxito de las tareas

En medio del estrés causado por un ciberataque, algunos altos ejecutivos pueden tener dificultades para delegar responsabilidades y es probable que intenten tomar el control directo de la situación. Los CEO están acostumbrados a tomar las decisiones, pero en estos casos deben ceder espacio para que el CISO y el CIO puedan resolver los problemas.

El papel del director ejecutivo es dictar la estrategia general de recuperación y garantizar que se centre en las necesidades de la empresa. En su papel como representantes de la organización, los directores ejecutivos son esenciales para comunicarse con *las partes interesadas*, y mantener la confianza de los clientes, reguladores, *accionistas* y ciudadanos en la viabilidad de la empresa.

El apoyo al CEO normalmente debería ser realizado por el COO, responsable de la recuperación técnica (incluida la gestión de proveedores de TI), mientras que otros líderes empresariales asumen la misión de comprender y mitigar el impacto en el negocio.

Durante una redada, es posible que se vea obligado a imponer altas exigencias a personas clave, lo que genera largas jornadas de trabajo y riesgo de *agotamiento*. Por ello, es fundamental que haya sustitutos disponibles y un plan de rotación para que todos puedan descansar y regresar renovados. Esto incluye contar con el apoyo de terceros y proveedores contratados bajo acuerdos de nivel de servicio definido (SLA), que reflejan prioridades de recuperación previamente definidas.

> **"Asegúrese de comprender cómo interactúan los distintos equipos. Aclarar los puntos de contacto entre el equipo de respuesta a incidentes, el equipo de crisis, el equipo de continuidad, el equipo de recuperación ante desastres y el equipo de comunicaciones. Crear planes y estructuras para que cada equipo comprenda sus funciones y las lleve a cabo de manera competente."**

Campbell Logie-Smith
Líder de Práctica *de Servicios de Resiliencia Empresarial* en KPMG en Australia

04 Comunique con firmeza, claridad y coherencia a quien sea necesario.

Primero, decida si es necesario o no revelar el incidente y, de ser así, qué información necesita compartir. Es posible que se le exija legalmente que comparta cierta información.

Si *las partes interesadas* se ven afectadas de alguna manera, explique que los servicios pueden verse afectados temporalmente y consulte con asesores externos sobre las obligaciones legales. Internamente, garantice la colaboración y el intercambio de información entre el equipo de gestión de crisis (compuesto por ejecutivos, recursos humanos, comunicaciones y asuntos legales) y el equipo de tecnología que lidera la investigación y la respuesta al ataque.

Esté atento a los requisitos contractuales y legislativos sobre cómo comportarse en casos de violaciones de seguridad: varían según el grado del problema, pero normalmente dan a la organización un plazo para revelar lo sucedido y el impacto en las operaciones críticas. La conversación con los organismos reguladores puede ayudarle a comprender cuánto necesitan saber y cuándo necesitan la información. Tenga cuidado de no dar demasiada información demasiado pronto; al mismo tiempo, tenga cuidado de no omitir información. Informar de manera responsable y oportuna.

> **"En mi experiencia, es importante que todos sepan que tienes un plan: comunicarte de manera equilibrada para que la gente entienda lo que está pasando y no empiece a crear sus propias teorías. Si dejas que otras personas definan la narrativa, perderás el control de la situación."**

Dani Michaux
Líder en seguridad cibernética en la región de Europa, Medio Oriente y África y socio en KPMG Irlanda

05 Detente a reflexionar, incluso en los peores momentos

Puede parecer que el mundo se va a acabar si no toma medidas inmediatas, pero es mucho más probable que tome mejores decisiones si actúa con cautela y espera hasta que la situación se aclare. Descubrir la verdadera gravedad del incidente es clave para la recuperación, lo que puede demandar su tiempo. Desarrolle un espacio estratégico y evite ahogarse en detalles. En una situación estresante, los líderes deben acostumbrarse a sentirse "cómodos estando incómodos" y estar preparados para vivir con la incertidumbre que acompaña a una violación de la seguridad.

Evite hacer suposiciones que no estén respaldadas por evidencia. Al pedir a los técnicos y otros expertos que realicen una investigación, que puede durar hasta 24 horas, el liderazgo debería obtener una imagen más clara del problema y su impacto en las operaciones.

Por ejemplo, si simplemente apaga su sistema durante un ataque, no podrá descubrir las intenciones del atacante, ni siquiera rastrear sus acciones. Esto es especialmente importante en el caso del espionaje, donde el adversario generalmente tiene una estrategia a largo plazo más sofisticada. En un ataque rápido, como *el ransomware* , el delincuente suele utilizar estrategias más agresivas para extorsionar lo máximo posible.

Los detalles sutiles determinan cuándo es necesario aislar, contener y erradicar a un atacante y cuándo es mejor monitorear y comprender mejor sus actividades. Se recomienda buscar asesoramiento de expertos para determinar cómo afrontar la amenaza, lo que, en algunos casos, puede incluso implicar cierto compromiso con el grupo atacante para comprender sus intenciones. No existe una manera única y perfecta de abordar las amenazas y cada sector puede tener necesidades radicalmente diferentes que dictan cómo abordar la situación. En servicios como la asistencia sanitaria, por ejemplo, la interrupción del servicio tiene consecuencias mucho más graves que la seguridad de los datos.

> **"Cuando se enfrenta a una amenaza, es necesario rastrear a los atacantes para saber dónde están, qué tocaron, qué robaron y realizar un análisis completo del sistema para asegurarse de que no hayan implementado *puertas traseras* que podrían facilitar una nueva intrusión."**

Matt Dri
Socio, Cyber Response y Forensic Technology en KPMG Australia

06 Sea adaptable: no existe un manual para todo

Los simulacros y ejercicios de simulación son útiles para desarrollar la confianza y la memoria muscular, pero nada puede prepararlo completamente para un ciberataque. Esté abierto a adaptarse según la situación, posiblemente desviándose significativamente de la respuesta practicada. Acepte que habrá prioridades contradictorias y esté preparado para afrontar la incertidumbre. A menudo, las organizaciones están demasiado ocupadas "apagando incendios" y no pueden tener una imagen completa de los acontecimientos. Los expertos externos con experiencia en responder a ciberataques y reconstruir empresas afectadas pueden identificar más fácilmente los pros y los contras de los diferentes caminos posibles hacia la recuperación, brindando asesoramiento sobre la viabilidad, la complejidad y los plazos de las acciones a tomar.

Entienda cuáles son los "procesos mínimos viables" y monitoréelos, así como las adaptaciones realizadas, para tener mayores posibilidades de restaurar la actividad.

07 Sepa cuándo terminó la crisis: avance rápidamente, pero sea cauteloso

Establezca métricas para monitorear la restauración del negocio y utilícelas para identificar qué tan rápido es posible reanudar las actividades normales de la empresa, incluida la disponibilidad de sistemas y servicios, atención al cliente y soporte de prensa. Los informes simples y confiables ayudan a mantener a los altos ejecutivos actualizados sobre el progreso de la situación.

A medida que se supera la crisis, el área forense completa gran parte de su trabajo y mitiga riesgos. Pero prepárese para permanecer hipervigilante por un tiempo para evitar una segunda ola de ataques a través de nuevos vectores que pueden haber pasado desapercibidos inicialmente.

Intente avanzar rápidamente, pero tenga cuidado de deshacerse de todos los posibles *exploits* que permitirían a los atacantes regresar. La atención se centra ahora en la recuperación y en las formas de hacer que la empresa sea más segura y resiliente.

Cuando lo peor haya pasado: Sea resiliente

01 Sea honesto acerca de lo que sucedió y aprenda de ello.

Una revisión integral posterior al incidente (PIR) debe determinar cómo ocurrió el ataque y la causa raíz del problema (por ejemplo, falta de autenticación multifactor o falta de conciencia *sobre phishing*). Evalúe honestamente cómo la organización manejó el problema y cómo responder mejor en caso de una nueva crisis. El PIR no sirve para culpar a las áreas o individuos, sino para reflexionar y mejorar.

Un PIR bien administrado es independiente, desafiante y analiza todos los aspectos de las lecciones aprendidas de seguridad técnica y empresarial. Esté preparado para enfrentar problemas relacionados con la gestión de riesgos, la gestión de crisis, la participación de los proveedores, la comunicación, las habilidades y la cultura de la empresa y, por supuesto, la ciberseguridad. Ninguna organización puede manejar perfectamente una crisis importante, pero todos estos aspectos se pueden mejorar.

02 Desarrolle resiliencia y siga mejorando

En un intento por volverse más resilientes, las empresas pueden embarcarse en programas a gran escala que, debido a problemas de infraestructura, pueden llevar años, tiempo durante el cual pueden ocurrir nuevos incidentes.

Por supuesto, estas mejoras son necesarias, pero consideremos qué medidas se pueden tomar rápidamente para generar resiliencia en el corto plazo. La pregunta: "¿Cómo podría responder mejor la organización si fuera atacada el próximo mes?" probablemente traerá algunas victorias rápidas.

Por ejemplo: ¿hay alguna forma de pagar más rápidamente a proveedores y empleados durante una crisis? ¿Es posible mantener la liquidez? ¿Cómo mejorar las habilidades comunicativas? ¿Y cómo movilizar respuestas más rápidamente ante un nuevo ataque?

03 Haga limpieza de datos y aplicaciones

Un incidente cibernético importante puede tener un resultado sorprendente (y positivo): dirigir la atención de la empresa hacia la necesidad de mantener sistemas y aplicaciones heredados específicos. Esto puede conllevar una necesaria limpieza del área TI, deshaciéndose de sistemas irrelevantes.

Es posible que su organización también esté acumulando una gran cantidad de datos innecesarios y esta es una oportunidad para eliminar estos archivos. Los servidores de datos, que pueden tener décadas de antigüedad, contienen cantidades significativas de información no estructurada que son blancos fáciles para los delincuentes que logran vulnerar las defensas de una empresa. Al almacenar solo lo que necesita, puede reducir significativamente la amenaza.

04 La tarea es de toda la empresa, y no la función de un solo equipo

La digitalización ha desdibujado las líneas entre funciones operativas, ciberseguridad, seguridad y ética. Las barreras entre TI, tecnología operativa y seguridad de los productos comenzaron a colapsar. Ahora todo está conectado y las organizaciones deben adoptar una visión amplia de la resiliencia en lugar de centrarse sólo en una dimensión simplificada del problema.

Un simple portátil desprotegido puede ser vector de los más variados tipos de ataques, desde el robo de datos hasta el fraude y la *piratería informática* de sistemas importantes. La ciberresiliencia requiere un enfoque que abarque toda la empresa para fomentar los comportamientos correctos de todos los equipos, centrándose en lo que realmente importa a la organización, ya sean datos, servicios o infraestructura.

> **"Hoy en día, un ciberataque suele ser el resultado de *inicios de sesión de usuarios comprometidos* en lugares que no forman parte de su función empresarial. En muchos casos, estos también pueden pertenecer a otras organizaciones o proveedores de confianza dentro de su cadena de suministro. Pero, a través de esta infracción aparentemente inofensiva, los delincuentes obtienen acceso a toda su organización, lo que incluso provoca el cierre de instalaciones, fugas prolongadas de información e incluso daños ambientales."**

Dani Michaux
Líder en seguridad cibernética en la región de Europa, Medio Oriente y África y socio de KPMG Irlanda

05 Comprenda la cadena de suministro y su papel en la creación de resiliencia

Las complejidades de las cadenas de suministro modernas y el crecimiento del fenómeno "todo como servicio" (XaaS) han dejado a las organizaciones dependientes de un número cada vez mayor de empresas subcontratadas. Es importante comprender las capacidades de estos equipos para hacer frente a las violaciones de seguridad y dónde puede existir el peligro de un ciberataque. Uno de los desafíos radica en el hecho de que los contratos basados en servicios, con pequeños márgenes de ganancia, dan como resultado que los proveedores tengan menos recursos para desarrollar habilidades en ciberseguridad.

Sea claro acerca de las responsabilidades y obligaciones de sus proveedores cuando se trata de una violación de la ciberseguridad. Incorpore esto en los contratos siempre que sea posible y tenga en cuenta que los proveedores intentarán minimizar sus posibles responsabilidades. Debido al alto costo financiero que puede surgir de un incidente cibernético, puede ser necesario apoyo legal especializado para aclarar las obligaciones legales de cada parte involucrada.

Los reguladores serán despiadados con las organizaciones que citan fallas en la cadena de suministro como una razón para no cumplir con sus obligaciones para con los clientes. Esté preparado para que requieran mayor diligencia de su parte en el futuro.

> **"Existe una presión significativa para comprender la cadena de suministro de manera más efectiva e implementar una gobernanza para gestionarla mejor. Es necesario saber si las organizaciones con las que trabaja, especialmente sus proveedores de servicios de TI más críticos, pueden manejar un ciberataque y si le notificarán si ocurre un incidente."**
>
> **Jason Haward-Grau**
> Líder global de servicios de recuperación cibernética en KPMG International y líder en KPMG en EE. UU.

06 Retenga el talento para acceder rápidamente a las habilidades que necesita

La ciberseguridad es una disciplina altamente especializada y las habilidades de respuesta a incidentes son escasas y, a menudo, costosas en situaciones de emergencia. Cuando se produce una invasión, tener a mano un equipo preparado y experimentado puede marcar la diferencia en la rapidez y eficacia con la que se aborda el problema. Al contratar especialistas en los procesos de respuesta y recuperación, usted garantiza una rápida movilización en caso de un incidente y puede construir una relación de confianza de antemano, en la que sus especialistas pueden ayudar a capacitar y preparar la respuesta de su empresa a los ataques.

07 El mundo cambia: no asumas que los desafíos de hoy serán los mismos que los de mañana

Un plan de defensa basado en patrones históricos de intrusiones cibernéticas puede no adaptarse a la forma en que los delincuentes evolucionan y cambian constantemente. Hace cinco años, DdoS (*denegación distribuida de servicio*), los ataques *smash and grab* y los *ransomwares* (como *WannaCry*) eran comunes, ya que el objetivo principal era la TI. Hoy en día, los ataques se han desplazado a la cadena de suministro y a la doble o triple extorsión, todo ello respaldado por un sofisticado sistema de "crimen como servicio". Los ataques se han vuelto "expertos en la nube" y cada vez más sofisticados y tienen como objetivo destruir *las copias de seguridad en línea*. También demuestran un interés creciente en la tecnología operativa y los sistemas de control industrial.

Mantenga sus planes de acción bajo revisión constante y asegúrese de que reflejen no solo las nuevas amenazas, sino también los cambios organizacionales y su dependencia de TI.

> **"Los delincuentes siguen mejorando sus técnicas, por lo que los planes también deben ser flexibles y evolucionar; de lo contrario, es posible que su equipo no pueda responder a las amenazas de manera eficaz."**
>
> **Matt Dri**
> Socio, Cyber Response y Forensic Technology
> KPMG en Australia

Pero, sobre todo: mantenga la vigilancia

Establecer resiliencia significa que si experimenta un nuevo ataque, estará mejor preparado para afrontarlo, lo que reduce el impacto potencial de los delincuentes. No puede controlar las amenazas externas, pero puede controlar su capacidad para responder a ellas y recuperarse de los ataques. Después de un hackeo o una violación de seguridad, no pierda la oportunidad de mejorar su resiliencia.

La tendencia es que las organizaciones se vuelvan complacientes con el tiempo, lo que resulta en una menor inversión en ciberseguridad y en una relajación respecto a las actitudes de prevención. El CISO (o, cada vez más, el "director de resiliencia") tiene la difícil función de recordar a las juntas directivas y a los altos ejecutivos lo que sucedió, lo que les está sucediendo a los demás y lo que podría volver a suceder.

Desde el punto de vista de los empleados, una cultura de ciberresiliencia implica instrucciones y ejercicios preparatorios para que todos sean conscientes de la amenaza y estén preparados para responder cuando sea necesario. Esto es más difícil de lo que parece, ya que la gravedad de un ciberataque nunca puede replicarse por completo en un ejercicio. Sin embargo, la práctica ayuda a comprender el problema y a desarrollar la "memoria muscular".

Quienes desempeñan un rol de liderazgo deben estar preparados para lidiar con prioridades conflictivas y una gran incertidumbre, lo que requiere que el enfoque regrese a lo que es verdaderamente crítico para la organización.

Deben poder tomar decisiones difíciles si son necesarias para proteger la organización.

> **"Existe una carrera constante entre usted y los ciberdelincuentes; están evolucionando e innovando más rápido que nosotros. Si mantiene las conversaciones adecuadas y se prepara con antelación, tendrá muchas más posibilidades de desarrollar la memoria muscular necesaria para el momento de necesidad."**

Jason Haward-Grey
Líder global de servicios de recuperación cibernética en KPMG International y líder de KPMG en EE. UU.

¿Cómo se conecta esto con lo que hacemos?

Incluso las organizaciones que cuentan con los mejores controles de ciberseguridad están en constante riesgo de sufrir ciberataques disruptivos . El Cyber Resilience Framework de KPMG está diseñado para ayudar a las organizaciones a protegerse, detectar amenazas y recuperarse de un ciberataque importante.

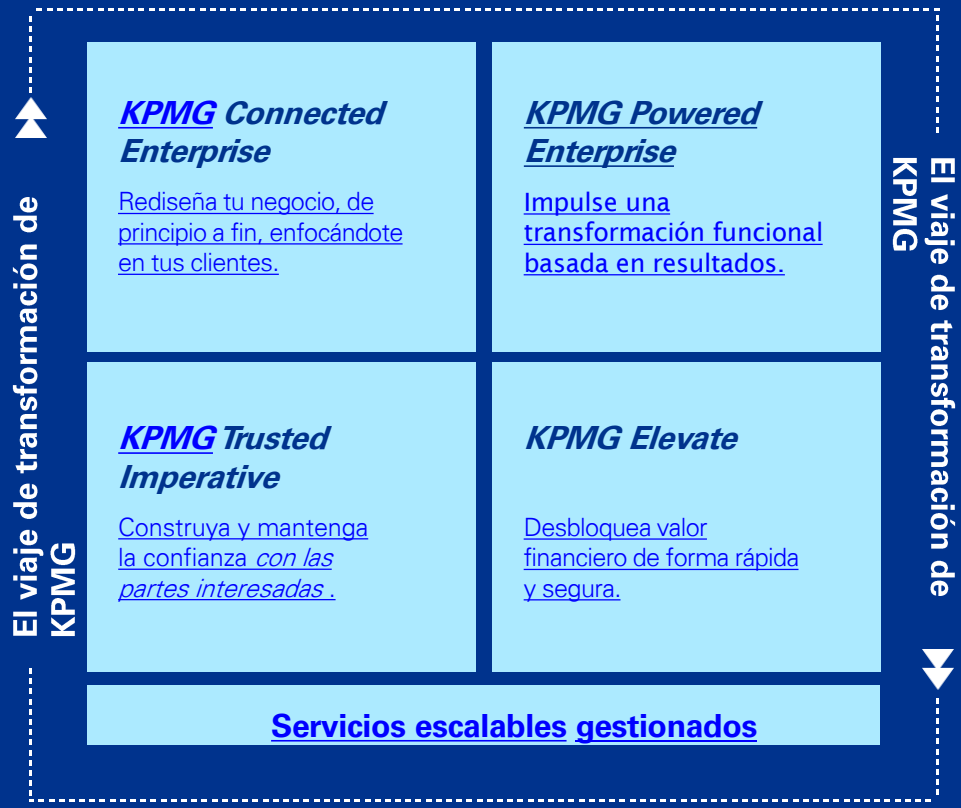
Nuestro marco cubre los estándares y regulaciones más importantes, además de complementarse con la experiencia de KPMG en el desarrollo de soluciones tecnológicas clave. Cada paso del marco de resiliencia cibernética de KPMG incorpora Recuperación, Resistencia y Resiliencia y garantiza que todos los empleados tengan un papel para garantizar que la organización permanezca segura.

Este marco beneficia a las organizaciones con un aumento de su resiliencia a través de ejercicios, pruebas y simulaciones. Además de ayudar a minimizar el impacto de un ciberataque en los servicios críticos de la empresa, y permitir una rápida recuperación de las operaciones más importantes, orienta y anima a las empresas a utilizar la inteligencia para responder rápidamente a las ciberamenazas sofisticadas.
Los profesionales de KPMG pueden ayudarle a evitar costosas interrupciones en su negocio y a mantenerse preparado para el futuro mediante el desarrollo de ciberresiliencia en toda su organización.

Obtenga más información en: kpmg.com/cybersecurity

Además, KPMG está ayudando a empresas globales de todos los sectores a adoptar una nueva era de oportunidades en la economía digital. Desde la estrategia hasta la implementación, los profesionales de KPMG pueden marcar la diferencia en su viaje hacia la transformación. Juntos, podemos transformar su modelo de negocio actual e impulsar su competitividad, crecimiento y valor. KPMG: Make the Difference .

Suite de transformación digital de KPMG



Hable con nuestro equipo

Leandro Augusto
Socio Líder de Seguridad Cibernética y Privacidad
de KPMG en Brasil y América del Sur
lantonio@kpmg.com.br

Thiago Labliuk Leme
Socio Director de Servicios Gestionados de
Riesgo y Seguridad de KPMG en Brasil
tleme@kpmg.com.br

Ciertos aspectos de algunos de los servicios descritos en este material no están autorizados para clientes de auditoría de KPMG y sus filiales o entidades relacionadas.

kpmg.com/ciberseguridad

Nombre de la publicación: Mantenga la vigilancia cibernética y
manténgase resiliente Número de publicación: 139036-G
Fecha de publicación: octubre de 2023