Galvanize

¿Qué es la resiliencia operativa?

Tabla de contenidos

Más que la mera continuidad del negocio...

Durante la Segunda Guerra Mundial, el gobierno británico acuñó el eslogan "Mantengan la calma y sigan adelante" para motivar la perseverancia frente al desafío.

El espíritu de ese dicho sigue siendo relevante en los negocios modernos y podemos sintetizarlo como resiliencia operativa.

La resiliencia operativa es la capacidad de una organización para resistir una disrupción repentina y recuperarse. Antes, ese concepto era sinónimo de continuidad del negocio o recuperación de desastres. Pero gracias a la digitalización de los negocios, la resiliencia operativa se convirtió en algo más profundo: una mezcla de continuidad del negocio, gestión de riesgos de proveedores, ciberseguridad y más.

Este libro electrónico analiza cómo pueden enfocar la resiliencia operativa los profesionales de aseguramiento de riesgos. ¿Qué es lo que las juntas directivas y los reguladores desean saber al respecto? ¿A qué parte de la empresa "corresponde" la resiliencia operativa? ¿Qué recursos de supervisión y prueba se necesitan para cuantificarla?

A medida que los negocios avanzan hacia un terreno con mayores riesgos, operaciones digitales, interdependencia y supervisión, es cada vez más importante comprender las respuestas a estas preguntas.

¿Qué es la resiliencia operativa?

Una descripción útil de la resiliencia operativa proviene del Banco de Inglaterra.[1]

En 2019, publicó un documento que definía la resiliencia operativa como la capacidad de seguir prestando "importantes servicios de negocios". El documento establece que las empresas deben "considerar la cadena de actividades que componen un servicio de negocios, desde que se asume la obligación hasta que se cumple con el servicio, y determinar qué parte de la cadena es crítica para el cumplimiento".

En otras palabras, la resiliencia operativa es la capacidad de una organización de seguir prestando servicios a los clientes a pesar de una disrupción repentina. Para ello, la organización debe tener una idea clara de cuáles son sus servicios críticos y las circunstancias en las que podría ser incapaz de cumplirlos. Luego, la organización puede desarrollar e implementar planes de mitigación para reducir el riesgo de incumplimiento.

En el pasado, esos planes de mitigación incluían medidas como guardar reservas de inventario o materias primas, crear centros de datos redundantes, mantener efectivo suficiente para cubrir las necesidades de liquidez o capacitar personal de otros departamentos para realizar las tareas claves.

Todos ellos siguen siendo importantes para garantizar la resiliencia operativa. Pero gracias a los avances de la tecnología y la transformación digital de los procesos de negocios, la forma en la que usted gestiona su propio negocio mientras cumple con los servicios cambió drásticamente, al igual que el alcance de lo que realmente implica la resiliencia operativa.

RIESGO DE LA DEPENDENCIA DE TERCEROS

En la actualidad, las organizaciones dependen mucho más de terceros para ejecutar sus funciones críticas: nómina, correo electrónico, facturación, estudios analíticos de datos, marketing por correo electrónico, ciberseguridad, gestión de las relaciones con los clientes y muchas otras tareas ahora pueden —y suelen— tercerizarse.

Entonces, usted puede aumentar las reservas de liquidez frente a una amenaza de recesión, comprar materias primas antes de una escasez o capacitar personal de otros departamentos antes de una pandemia. Pero:

+ ¿Cómo "impulsa" una función de nómina tercerizada?
+ ¿Cómo capacita al personal clave para seguir trabajando cuando su proveedor de almacenamiento de datos está inhabilitado?
+ ¿Por qué pagar por un servicio de respaldo de comunicación en la nube si el ahorro de dinero fue el objetivo del uso del servicio primario en la nube?

[1] **Banco de Inglaterra,** *2019, Building operational resilience: Impact tolerances for important business services (Creación de resiliencia operativa: tolerancia al impacto para servicios importantes de negocios)*

La transformación digital de los procesos de negocios aumentó los riesgos en torno a la resiliencia operativa. Si la ejecución de sus propios procesos de negocios depende del uso de tecnología o servicios proporcionados por terceros, gran parte de la resiliencia operativa se transforma en ciberseguridad y gestión de riesgos de proveedores.

Este es el desafío de la resiliencia operativa que enfrentan las organizaciones en la actualidad: una mezcla indefinida de riesgos de ciberseguridad, gestión de proveedores y continuidad del negocio. Cualquier falla en esa "cadena de actividades" puede causar enorme disrupción e impacto sobre los objetivos de negocios, como demuestra el siguiente estudio de caso.

ESTUDIO DE CASO

Virtual Care Provider

Virtual Care Provider Inc. (VCPI) es una empresa de TI que presta servicios de almacenamiento de datos, correo electrónico, facturación y otras funciones administrativas y de soporte a más de 110 residencias de ancianos en todo EE. UU.

En 2019, VCPI fue víctima de cibersecuestro de datos. Los hackers exigían USD 14 millones y VCPI no los tenía. En consecuencia, VCPI estuvo paralizada durante semanas; y también sus clientes, las residencias de ancianos. Algunas no podían acceder a los registros de los pacientes, otras no podían usar el sistema de correo electrónico, otras más no podían procesar su facturación para reembolso gubernamental. Peor aún, se puso en riesgo la vida de los pacientes al congelar o no permitir acceder a las historias clínicas electrónicas y los datos de administración de medicamentos vitales.

Una investigación del ataque reveló que los hackers también aprovecharon programas maliciosos que se habían infiltrado en VCPI en 2018. Obviamente, un sólido plan de resiliencia con incorporación de estrategias y prácticas de ciberseguridad hubiese ayudado en esta crisis.

¿Qué dicen los reguladores?

No sorprende que los reguladores bancarios fueran los primeros en considerar la resiliencia operativa como una preocupación importante.

Después de los devastadores efectos de la crisis financiera global de 2008, los reguladores bancarios no solo quieren que las empresas financieras tengan liquidez suficiente para cubrir pérdidas sorpresivas; quieren que sigan trabajando pase lo que pase, de modo que se mantenga la estabilidad del sistema financiero.

Las empresas financieras están más expuestas a las amenazas de ciberseguridad que otras compañías,[2] y dependen de un sinnúmero de proveedores de tecnología y otros socios comerciales para el funcionamiento de sus operaciones. Por eso, casi inevitablemente, como los reguladores bancarios prestaron más atención a la resiliencia operativa, este concepto viró hacia cuestiones de ciberseguridad y gestión de riesgos de proveedores.

Por ejemplo, en 2017, el Consejo de Estabilidad Financiera mencionó por primera vez la dependencia de los bancos de los proveedores de tecnología como un posible riesgo operativo.[3] Los reguladores bancarios de EE. UU. quieren ampliar sus revisiones normativas para incluir directamente el examen de los socios tecnológicos de los bancos.[4]

El Banco de Inglaterra está revisando su marco normativo para convertir la resiliencia operativa de los bancos en la base de la estabilidad del sistema financiero. El Comité de Supervisión Bancaria de Basilea tiene un grupo de trabajo sobre resiliencia operativa que, según se espera, publicará en breve un documento en el que propondrá nuevas medidas para la resiliencia operativa.[5]

La Autoridad Monetaria de Singapur (MAS, por sus siglas en inglés) es un buen ejemplo de la forma en que los reguladores están enfocando este asunto.
En 2019, publicó dos documentos de discusión que proponían reformas a las Directrices de Gestión de Riesgo Tecnológico de la agencia y sus Directrices de Gestión de Continuidad del Negocio.[6] En conjunto, estas reformas tienen por objeto la mejora de la resiliencia operativa de las empresas financieras; MAS incluso lo manifiesta en su solicitud de comentarios. (El aspecto revelador es que MAS dividió la resiliencia operativa en sus componentes de riesgo tecnológico y continuidad del negocio).

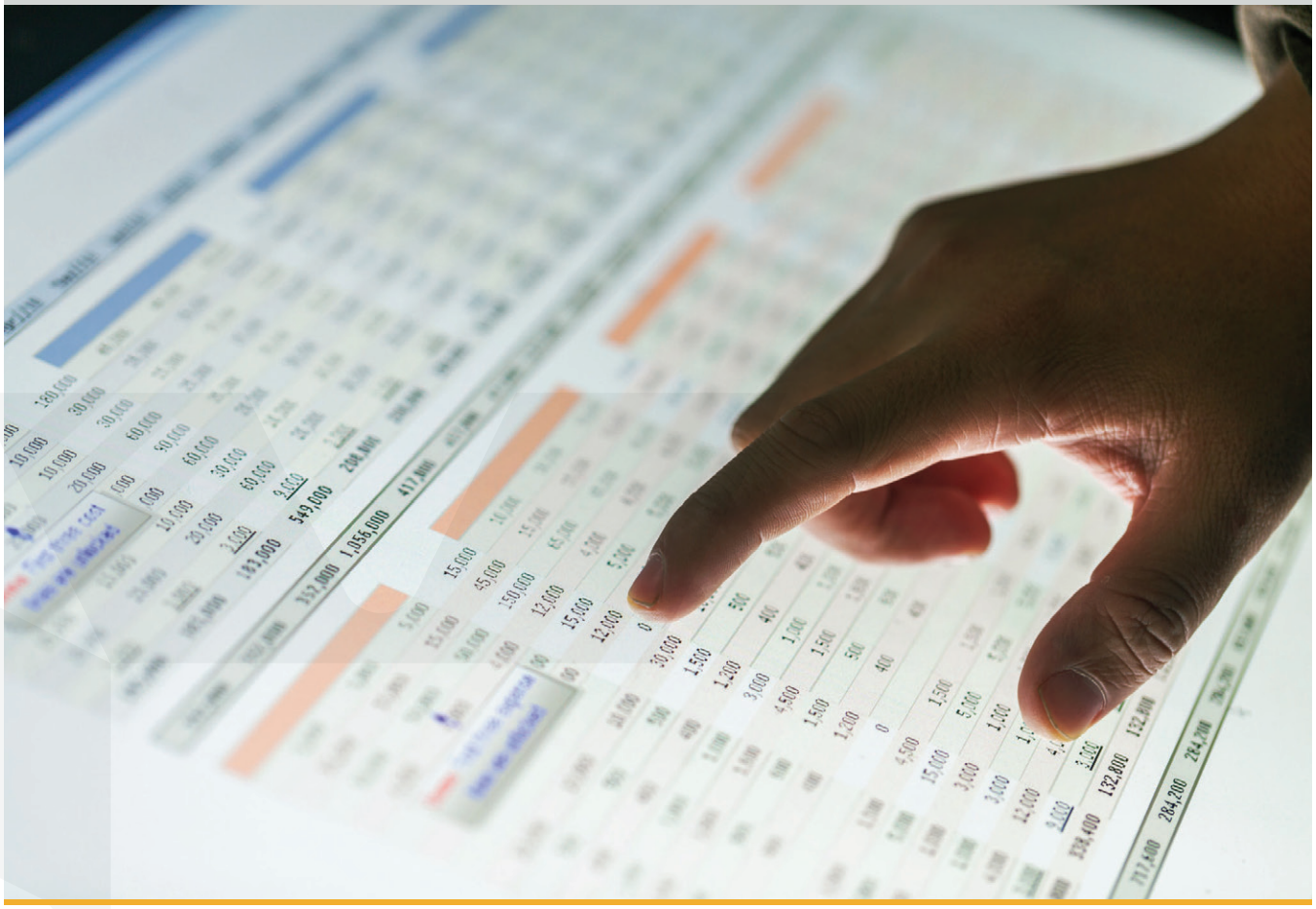
[2] **Markets Insider,** *2019, Cyber attacks are 300 times as likely to hit financial firms than other companies (Los ciberataques son 300 veces más probables en las empresas financieras que en otras compañías)*

[3] **Consejo de Estabilidad Financiera,** *2019, Third-party dependencies in cloud services (Dependencias de terceros en servicios en la nube)*

[4] **The Wall Street Journal,** *2019, Federal Reserve steps up scrutiny of tech firms that serve banks (La Reserva Federal intensifica el examen de empresas tecnológicas que sirven a los bancos)*

[5] **BIS,** *2020, Basel committee meets to review vulnerabilities and emerging risks, advance supervisory initiatives and promote Basel III implementation (El Comité de Basilea se reúne para revisar vulnerabilidades y riesgos emergentes, avanzar en las iniciativas de supervisión y promover la implementación de Basilea III)*

[6] **Autoridad Monetaria de Singapur,** *2019, MAS consults on proposed enhancements to technology risk and business continuity management guidelines (MAS consulta sobre las mejoras propuestas a las directrices de gestión de riesgo tecnológico y de continuidad del negocio).*



SIGNIFICADO DE TODA ESTA ACTIVIDAD REGULADORA PARA LA RESILIENCIA OPERATIVA

Si bien el sector bancario ha estado muy centrado en la resiliencia operativa, los reguladores de otras industrias prestarán atención al asunto con el tiempo.

De hecho, los contratistas de las fuerzas armadas de EE. UU. ya deben cumplir las normas de NIST 800-171, un marco que rige la ciberseguridad entre contratistas y terceros. Y también el Departamento de Seguridad Nacional estadounidense se apoya fuertemente en industrias de infraestructura crítica (banca, telecomunicaciones y servicios públicos) para aumentar su resiliencia.[7]

Piense en el ejemplo de la residencia de ancianos. Las residencias de ancianos ya están muy reguladas y representan un sector importante para los funcionarios públicos: los ancianos familiares de los contribuyentes que esperan una atención fiable y eficaz. A medida que crezca la cantidad de industrias vulnerables a disrupciones repentinas y los consumidores se enojen (o incluso estén en peligro), los reguladores comenzarán a preguntar sobre las amenazas a la resiliencia operativa.

En última instancia, la resiliencia operativa dejará de ser solo un tema de cumplimiento normativo. Comenzó así en el sector bancario, al igual que muchos otros aspectos de la gestión de riesgos. Pero dado que las operaciones de las organizaciones se integran cada vez más con las de los proveedores y clientes, la capacidad de resistir perturbaciones se convierte en un motor estratégico crucial, más allá de lo que digan los reguladores.

[7] **Departamento de Seguridad Nacional de EE. UU.,** *2019, A guide to critical infrastructure security and resilience (Una guía para la seguridad y la resiliencia de la infraestructura crítica)*

Evaluación de la resiliencia operativa

La evaluación de la resiliencia operativa incluye muchos conceptos que los equipos de auditoría ya conocen, aplicados de formas nuevas.

Algunos de los más importantes son:

+ **Criticidad.** Define los servicios empresariales más importantes de una organización. Por ejemplo, la falla repentina de una función de nómina tercerizada no inhabilita su capacidad de seguir operando, pero quizás la falla de los sistemas de correo electrónico, almacenamiento de datos o transporte, sí.
+ **Mapeo.** Un equipo de auditoría puede mapear e identificar todas las conexiones de la organización con sus proveedores y clientes —físicas, legales y tecnológicas— para comprender cómo puede fallar la prestación de servicios empresariales.
+ **Tolerancia al impacto.** Es la máxima disrupción que la organización puede resistir (incluida la máxima duración de la disrupción) sin dejar de cumplir con las operaciones de negocios importantes.
+ **Pruebas.** Los equipos de auditoría deben analizar qué tan bien queda una organización dentro de su tolerancia al impacto: en qué medida puede continuar operando incluso durante una disrupción. Incluye pruebas de cómo afecta la disrupción a los clientes de la organización o a otros participantes del mercado.
+ **Monitoreo.** Es necesario monitorear los sistemas y los activos críticos del negocio. (En este nuevo mundo en el que los proveedores basados en la nube proporcionan sistemas para los procesos de negocios críticos para los objetivos de la organización, esto puede incluir el monitoreo del desempeño y la ciberseguridad de los proveedores).
+ **Reportes.** Cuando se produce una disrupción, los altos ejecutivos necesitan comprender la naturaleza de la amenaza y responder rápidamente para mantener el funcionamiento de las operaciones.

Ninguno de estos pasos debería resultar nuevo, aunque algunos elevan los conceptos de la auditoría tradicional a nuevos niveles de sofisticación.

Por ejemplo, la tolerancia al impacto es similar a la tolerancia al riesgo, pero no es idéntica. La tolerancia al riesgo pregunta: "¿Qué grado de riesgo residual de que suceda un evento adverso estamos dispuestos a aceptar?" y normalmente la junta o la alta gerencia lo decide. La tolerancia al impacto pregunta: "¿Qué grado de disrupción podemos manejar una vez que el evento adverso haya sucedido?" y los clientes, reguladores o socios de negocios deberían ser tenidos en cuenta en la respuesta.

Las pruebas son otro ejemplo. Una aerolínea puede probar los procesos de continuidad del negocio para ver con qué rapidez puede restablecer un sistema de procesamiento de pasajes que dejó de funcionar. Sin embargo, una prueba de resiliencia operativa intentaría medir si la cantidad de pasajeros que pierden vuelos en el aeropuerto central de la aerolínea justifica que la aerolínea cuente con un sistema secundario para conmutar en caso de falla.

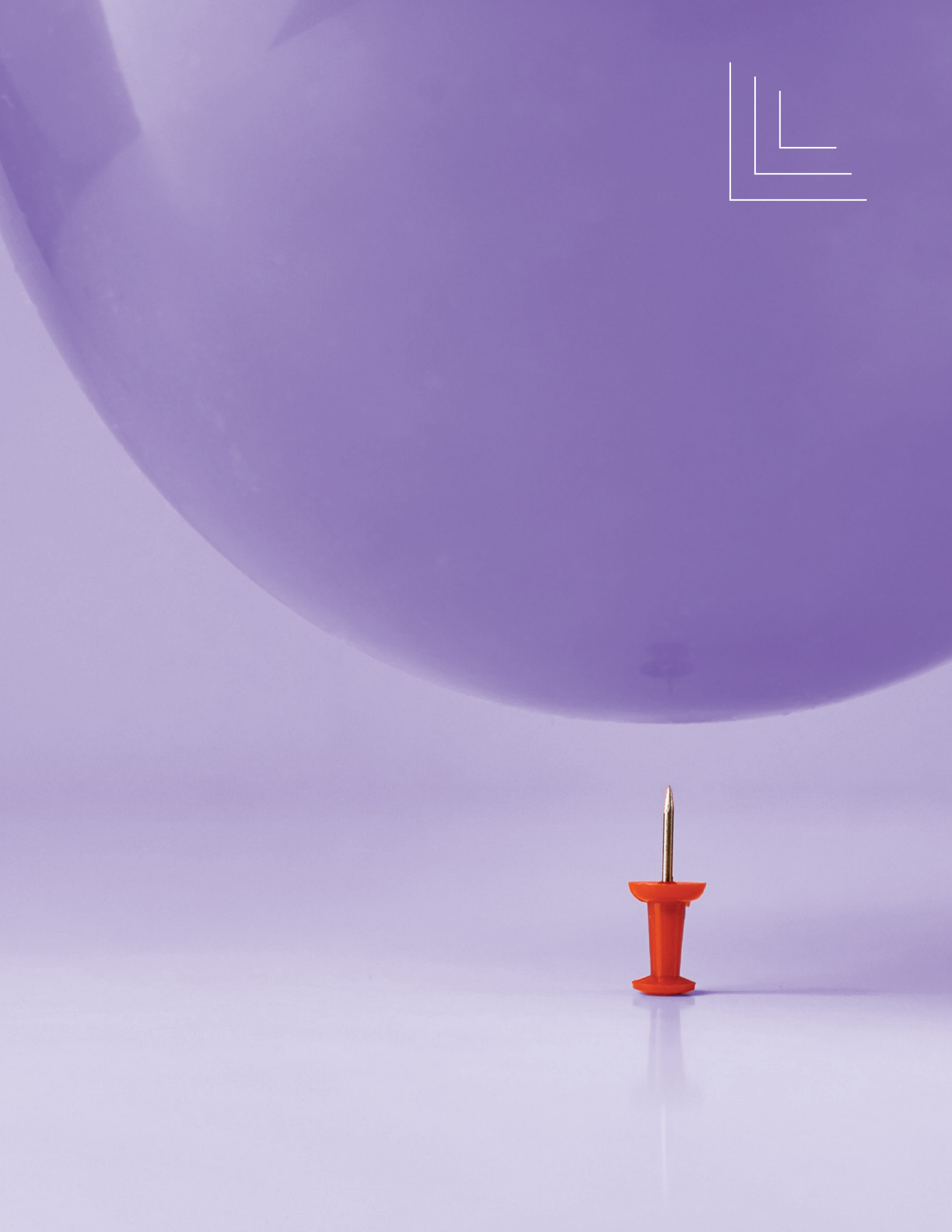
Todos estos matices ponen de manifiesto un punto clave. La gestión del riesgo operativo solo busca mantener las amenazas a las operaciones en un nivel de riesgo aceptablemente bajo. La resiliencia operativa intenta evaluar y documentar la capacidad de la organización para seguir operando si el riesgo adverso se concreta.

Esa es la diferencia entre estos dos conceptos relacionados pero distintos. Para llevar todo esto a la práctica, los equipos de auditoría deben confiar en la tecnología. Son demasiadas piezas en movimiento para poder manejarlas a mano.

El mapeo de todas las conexiones entre proveedores y clientes requiere coordinar varios departamentos. Lo mismo sucede con las pruebas de tolerancia al impacto y la documentación de los resultados. Ante todo, el desarrollo de la resiliencia operativa es un desafío interdisciplinario que implica comunicación entre muchas ubicaciones y funciones de negocios.

Una tecnología especializada es esencial para el logro de estos objetivos. Proporciona un único origen de información y una comprensión unificada de los riesgos y las tácticas de mitigación.

La resiliencia operativa intenta evaluar y documentar la capacidad de la organización para seguir operando si el riesgo adverso se concreta.



¿A quién le corresponde la resiliencia operativa?

Una de las preguntas más difíciles de responder puede ser cómo gobernar la resiliencia operativa y qué roles juegan las diferentes funciones de aseguramiento y gestión de los riesgos.

¿Es responsabilidad de la auditoría interna? No, a pesar de que la resiliencia operativa no funciona bien sin la participación de la auditoría.

¿Es responsabilidad del departamento de cumplimiento? En realidad, no. (Aunque para las empresas financieras y otras sumamente reguladas, el cumplimiento juega un rol importante si existen obligaciones normativas de certificación de la resiliencia).

¿Corresponde a los ejecutivos de operaciones en la primera línea de defensa? En cierta medida, sí, pero no es razonable esperar que la mayoría de los ejecutivos de la primera línea de defensa monitoreen todas las amenazas a la resiliencia ni sepan cuál es el impacto aceptable a la tolerancia.

Muchos opinan que la resiliencia operativa no le corresponde a ninguna función individual; en cambio, sostienen que es necesario asignar la supervisión a varios altos ejecutivos. El trabajo colectivo les permitiría comprender cuál es la resiliencia de la organización frente a las diferentes amenazas y asegurar que la resiliencia esté a la altura de las normas dictadas por la junta directiva o los reguladores, clientes, socios de negocios u otras partes interesadas.

Según otro punto de vista, un jefe de riesgos asumiría la responsabilidad de la resiliencia operativa, incluidas las obligaciones de cumplimiento normativo en torno a los riesgos de liquidez, disponibilidad de datos, ciberseguridad de los proveedores y otros temas de gestión de riesgos de terceros. Esta forma de enfocar la resiliencia operativa está muy orientada a los servicios financieros, en los que muchas empresas ya tienen jefes de riesgos o responsables de gestión del riesgo operativo. (Posiblemente no sea fácil de aplicar en otros sectores).

Lo que está claro es que:

+ La junta directiva deberá asegurar que la resiliencia operativa reciba la atención que merece, y asignar responsabilidades a los ejecutivos de la manera más adecuada para la organización.
+ La auditoría interna tendrá un rol de apoyo crucial, ya que evalúa la resiliencia operativa, recomienda cambios de políticas, procesos o controles cuando son necesarios y documenta el progreso de esas medidas correctivas.
+ La tecnología para coordinar todas las actividades de evaluación, prueba, monitoreo, documentación y generación de reportes será vital. El uso eficaz de la tecnología para medir la resiliencia operativa es clave para mejorarla.

¿QUÉ SE VUELVE IMPORTANTE PARA LA AUDITORÍA?

Los equipos de auditoría y de gestión de riesgo ayudan a sus organizaciones a comprender y desarrollar la resiliencia operativa, por eso, las herramientas y técnicas que usen deben estar listas y a la altura de este nuevo tipo de desafío.

Colaboración. Dado que los equipos de auditoría asocian los servicios empresariales importantes de la organización a personas, terceros o sistemas informáticos claves que hacen que esos servicios sean posibles, necesitan comunicarse con una gran variedad de personas en toda la organización. Lo mismo se cumple para las tareas subsiguientes como definir la tolerancia al impacto, probar los escenarios de disrupción e implementar las correcciones. Las herramientas de colaboración que favorezcan esas conversaciones y documenten las decisiones o los datos serán cruciales.

Evaluaciones de riesgos de proveedores. Una gran parte de la resiliencia operativa se basará en comprender los riesgos que presentan los proveedores mediante evaluaciones rigurosas de esos riesgos. Por ejemplo, es posible que los equipos de auditoría deseen desarrollar cuestionarios de evaluación de riesgos basados en marcos fiables de gestión de riesgos y luego trabajar con unidades operativas para asegurarse de que esas evaluaciones se completen con rapidez y eficiencia.

Pruebas. Probar los efectos de la disrupción en su propio negocio y otros es una tarea más compleja que las pruebas habituales de procesos de negocios. Posiblemente, los equipos de auditoría deban desarrollar nuevos tipos de pruebas y necesiten documentar cuidadosamente los resultados para poder reportarlos a los reguladores y otros que deseen ver de qué forma la organización asegura su resiliencia. (Aquí es donde un repositorio único de datos se vuelve esencial).

Monitoreo. El monitoreo también será más complejo. La resiliencia operativa puede incluir diferentes tipos de monitoreo al mismo tiempo: cualquier cosa desde el análisis de vulnerabilidad de la ciberseguridad frente a sus proveedores de primer nivel, o fuentes externas de datos sobre disponibilidad de materias primas claves, hasta los cambiantes requisitos de liquidez de los reguladores en medio de una crisis financiera. Toda esa información deberá utilizarse en las medidas de los riesgos operativos claves de la organización.

Gestión de asuntos. A medida que las organizaciones comiencen a abordar la resiliencia operativa, es probable que encuentren gran cantidad de debilidades, preguntas no respondidas u otros temas que necesiten atención. Por eso, la labor de auditoría avalada por el tiempo de desarrollar un plan de acción y monitorear el progreso (incluidas las alertas de notificación cuando vence el plazo de la entrada y los procedimientos de escalamiento si las unidades de negocios no responden dentro de los plazos definidos) será tan importante como lo ha sido siempre, aunque la naturaleza de las debilidades y las medidas correctivas sean nuevas para la organización.

Conclusión

Recuerde que en la introducción dijimos que las organizaciones deben comprender la "cadena de actividades" que les permite realizar negocios.

Eso siempre fue así, pero la tecnología digital permitió que las organizaciones se "encadenen" con más fuerza que nunca a sus proveedores, clientes y otros participantes en cualquier sector del mercado que ocupen.

Esos lazos estrechos pueden aumentar enormemente la eficiencia, pero también los riesgos. La resiliencia operativa intenta asegurar que la cadena no deje a todos paralizados cuando se produzca una disrupción.

Los equipos de auditoría y gestión de riesgos serán fundamentales para ayudar a las organizaciones a lograr la capacidad de mantener la calma y seguir adelante. Nada es nuevo —evaluación del riesgo, pruebas, documentación, corrección— pero la ejecución de estos pasos será más sofisticada. Los jefes de auditoría necesitarán una tecnología eficaz que les permita participar activamente para reforzar la resiliencia de la organización frente a las disrupciones que acechan a la vuelta de la esquina.

Los equipos de auditoría y gestión de riesgos serán fundamentales para ayudar a las organizaciones a mantener la calma y seguir adelante.

Si desea una evaluación de cómo su organización puede integrar la tecnología de Galvanize para lograr sus metas de continuidad de negocios y asegurar la resiliencia operativa, llame al 1 604 646 4254, envíe un correo electrónico a info@wegalvanize.com, o visite nuestro sitio web wegalvanize.com.

Galvanize

ACERCA DEL AUTOR

Matt Kelly

Director ejecutivo de Radical Compliance

Matt Kelly es un analista y consultor independiente del sector del cumplimiento que estudia y escribe sobre temas de cumplimiento corporativo, gobernanza y gestión de riesgos.

Tiene un blog, RadicalCompliance.com, en el que comparte sus ideas sobre asuntos de negocios y da charlas con frecuencia sobre temas de cumplimiento, gobernanza y riesgo.

En 2018, ganó un premio Reader's Choice de JD Supra como uno de los diez mejores autores sobre cumplimiento corporativo. Antes de iniciar Radical Compliance, Matt fue editor de Compliance Week, entre 2006 y 2015.

ACERCA DE GALVANIZE

Galvanize ofrece soluciones de software como prestación de servicios (SaaS) de gobernanza empresarial que ayuda tanto a gobiernos como a las empresas más grandes del mundo a cuantificar los riesgos, erradicar los fraudes y optimizar el desempeño.

wegalvanize.com

Nuestra familia integrada de productos, incluyendo nuestra solución basada en la nube para gobernanza, gestión de riesgo y cumplimiento (GRC) y los productos insignia para análisis de datos, se utilizan en todos los niveles de la empresa para ayudar a maximizar las oportunidades de crecimiento mediante la identificación y mitigación de los riesgos, la protección de los beneficios y la aceleración del desempeño.