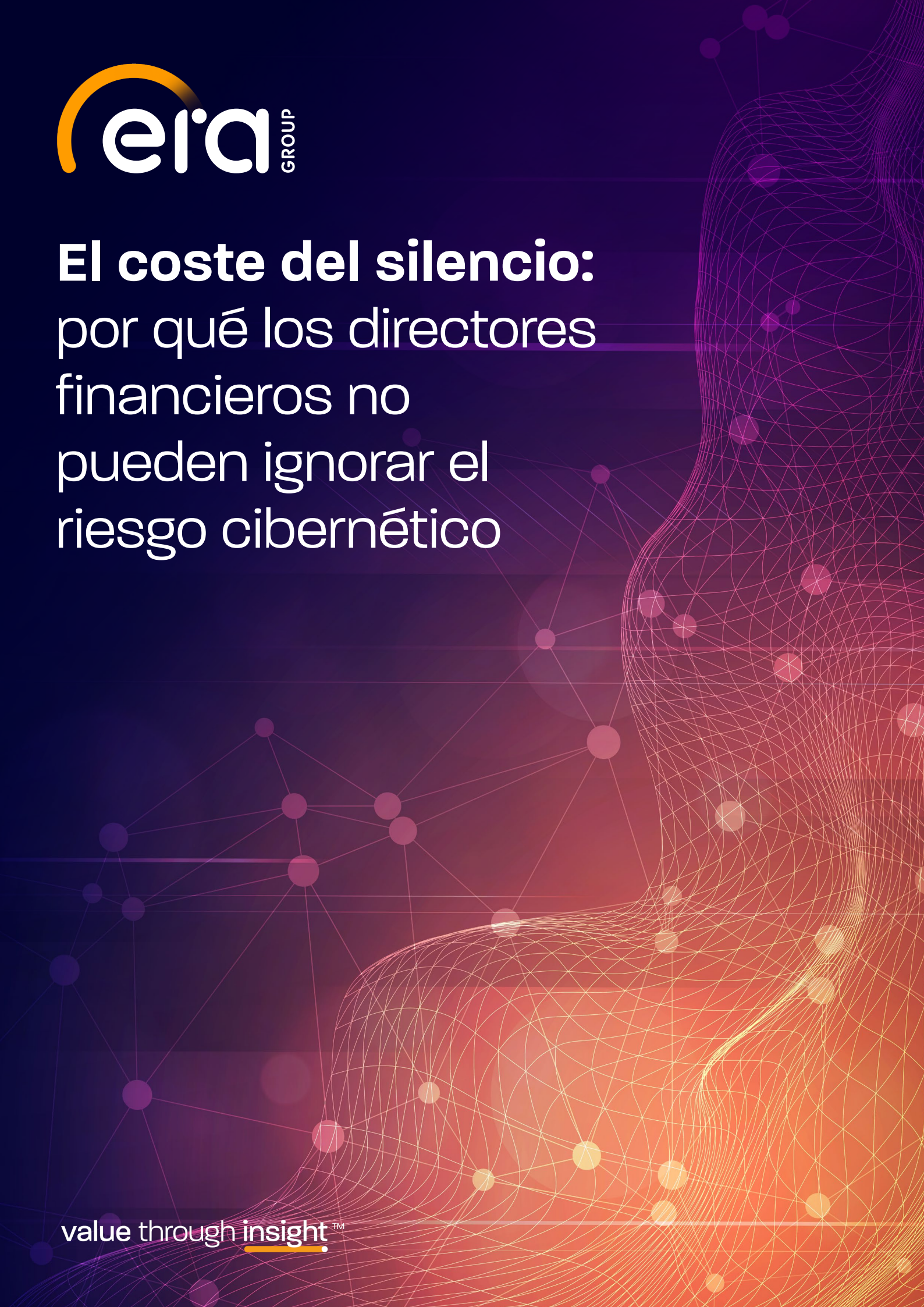
El coste del silencio: por qué los directores financieros no pueden ignorar el riesgo cibernético



value through insight™

EL RIESGO CIBERNÉTICO HA RECORRIDO UN LARGO CAMINO DESDE LA SALA DE SERVIDORES

Ahora afecta a los aspectos que más preocupan a los directores financieros: el flujo de caja, la confianza de los clientes, la continuidad del negocio, el cumplimiento normativo, el valor empresarial y la capacidad de la organización para seguir operando cuando algo sale mal.

Por eso, la antigua separación entre riesgo tecnológico y riesgo empresarial ya no funciona. Un incidente cibernético grave puede paralizar las operaciones comerciales, retrasar la producción, exponer datos sensibles, involucrar a los directivos en procesos legales y regulatorios, interrumpir la actividad de los proveedores y dañar la confianza de los clientes. También puede generar costes repentinos y no planificados precisamente en el momento en que la empresa tiene menos control.

El verdadero peligro no es únicamente el ataque en sí. También lo es la falsa sensación de seguridad que lo rodea. La creencia de que la cobertura de seguros existente es suficiente. De que el plan de continuidad sigue reflejando la realidad. De que los proveedores están preparados. De que la organización podría recuperarse dentro de los mismos plazos que calculó hace un año.

Paul Gravatt, especialista en riesgos y seguros de ERA Group, describe el riesgo cibernético como una de las mayores amenazas globales desde la perspectiva del riesgo y los seguros. Ya no se trata de individuos aislados que provocan interrupciones desde un ordenador. Cada vez más, la ciberdelincuencia está organizada, tiene motivaciones políticas y utiliza métodos muy sofisticados.

Esto cambia la conversación. El riesgo cibernético no es únicamente un problema técnico. Es una exposición financiera. Y el coste de gestionarlo mal rara vez aparece ordenadamente en una sola partida presupuestaria.

La oportunidad dentro del riesgo

La última Encuesta sobre Brechas de Ciberseguridad del Reino Unido pone de manifiesto la magnitud del problema. En 2025/26, el 43 % de las empresas declaró haber sufrido una brecha o un ataque cibernético, mientras que el phishing afectó por sí solo al 38 %. En total, la encuesta estima que aproximadamente 612.000 empresas británicas identificaron al menos una brecha o un ataque durante el año.

Este es el preocupante contexto. Sin embargo, no se trata únicamente de una historia sobre una amenaza creciente. También es una cuestión de oportunidad y momento.

Paul considera que, aunque la gravedad y la visibilidad de los ciberataques han aumentado, muchas organizaciones también están mejorando su capacidad de resistencia. En algunas partes del mercado, las primas de los seguros cibernéticos han estado disminuyendo, lo que ofrece a las empresas una oportunidad real para evaluar si ahora es más factible que antes contar con una cobertura más sólida, límites más altos o una protección más amplia.

Para los directores financieros, esto no significa contratar una póliza cibernética de forma aislada o simplemente añadir otra partida de costes. Significa analizar el coste total del riesgo de la organización y plantear una pregunta mejor: ¿podrían utilizarse los ahorros obtenidos en otras áreas de seguros, costes de proveedores o gastos operativos para financiar una mayor resiliencia cibernética?

Cuando se habla de riesgo cibernético, muchas personas piensan inmediatamente en ataques de ransomware: sistemas bloqueados, pantallas congeladas, operaciones paralizadas y una petición de rescate sobre la mesa. Por supuesto, eso ocurre. Sin embargo, los costes más dolorosos suelen aparecer en otros lugares.

Aparecen cuando no se pueden emitir facturas, procesar pedidos ni atender a los clientes. Se manifiestan cuando las líneas de producción se detienen, no se puede reponer el inventario, es necesario contratar proveedores de emergencia a precios elevados y los equipos directivos pierden días enteros gestionando cuestiones legales, regulatorias y de comunicación. Incluso después de restablecer los sistemas, el daño reputacional puede seguir generando consecuencias.

Aquí es donde la conversación debe ir más allá de la ciberseguridad y adentrarse en la continuidad del negocio.

Paul señala que las alteraciones más amplias de las cadenas de suministro han cambiado las perspectivas de recuperación. Sustituir equipos, obtener materiales de construcción o reponer existencias puede llevar ahora más tiempo del que muchas empresas presuponen. Un plan de recuperación que parecía razonable hace un año podría estar ya desactualizado. Los seguros de interrupción de actividad deben evaluarse frente a esta realidad, especialmente en lo relativo a los periodos de indemnización y al tiempo real durante el cual una empresa podría necesitar apoyo.

Una empresa puede tener cobertura, pero ¿es suficiente? Puede tener un plan de recuperación, pero ¿sigue siendo válido? Puede haber calculado el tiempo de inactividad, pero ¿ha tenido en cuenta la situación actual de la cadena de suministro? Puede asumir que los equipos de sustitución llegarán en cuestión de semanas, pero ¿qué ocurriría si tardaran meses?

El coste del silencio suele esconderse en estas suposiciones.

El riesgo cibernético no permanece aislado

Azunna Anyanwu, consultor de ERA Group en Estados Unidos, aporta otra perspectiva importante. Para los directores financieros, el coste del riesgo cibernético no es únicamente financiero. El impacto económico suele ser el resultado visible de fallos producidos en otros ámbitos: la reputación, las operaciones o el cumplimiento normativo.

Esto es importante porque el daño no termina una vez que se ha contenido el problema técnico.

El riesgo reputacional es una de las áreas más difíciles de valorar correctamente y una de las más fáciles de subestimar. Una brecha puede dañar la marca de la organización, su imagen pública, la confianza de las partes interesadas y la fidelidad de los clientes. Estos efectos pueden convertirse posteriormente en consecuencias financieras muy reales, como la pérdida de ingresos, una menor retención de clientes, unos costes de adquisición más elevados y una reducción del valor empresarial.

Esta amenaza se ha intensificado a medida que los grupos de ransomware utilizan cada vez más los datos robados como herramienta de presión. La amenaza no siempre es «páguenos o sus sistemas permanecerán bloqueados». También puede convertirse en «páguenos o publicaremos la información que hemos encontrado». Azunna lo describe como una «caza de la vergüenza pública», en la que la exposición de información sensible se convierte en la principal táctica de presión, en lugar de limitarse únicamente a la interrupción operativa.

El riesgo operativo puede ser menos visible, pero igualmente perjudicial. Puede tratarse de un proceso que falla, un sistema que deja de estar disponible, una cuenta de correo electrónico comprometida o un problema de un socio que repentinamente se convierte en un problema propio. El fraude por correo electrónico empresarial —Business Email Compromise— y los pagos enviados por error a proveedores son buenos ejemplos, porque no siempre parecen situaciones dramáticas desde el exterior. Se realiza un pago al destinatario equivocado, falla un proceso del proveedor, el dinero sale de la empresa y el impacto es dolorosamente real.

La cuestión de la cadena de suministro también es importante. Una empresa no necesita ser el objetivo directo para sufrir el coste de un incidente cibernético. Si un proveedor clave, un socio logístico, un proveedor tecnológico o un proceso externalizado se ve comprometido, la interrupción puede afectar rápidamente a los ingresos, la prestación de servicios, la productividad de los empleados y los compromisos adquiridos con los clientes.

Después llega el cumplimiento normativo. Los incidentes cibernéticos pueden desencadenar obligaciones legales, investigaciones regulatorias, compromisos contractuales y requisitos específicos del sector. Los incumplimientos en estas áreas pueden generar responsabilidades no previstas, gastos legales, costes de acuerdos y, en los sectores regulados, la pérdida de futuras oportunidades comerciales.

Para las organizaciones estadounidenses, este aspecto de gobernanza es cada vez más difícil de ignorar. Las empresas cotizadas están sujetas a las normas de divulgación de información sobre ciberseguridad de la SEC, que exigen que los incidentes cibernéticos materiales se comuniquen mediante el formulario 8-K en un plazo de cuatro días hábiles desde que se determina su materialidad. También deben realizarse declaraciones anuales sobre la gestión, la estrategia y la gobernanza del riesgo cibernético.

La exposición financiera también es considerable. El Centro de Denuncias de Delitos en Internet del FBI recibió 859.532 denuncias en 2024, con pérdidas declaradas superiores a los 16.600 millones de dólares.

Las preguntas que los directores financieros deberían plantearse ahora

La conversación adecuada sobre el riesgo cibernético no empieza por el software. Comienza con la exposición.

Un director financiero no necesita conocer todos los detalles técnicos del entorno cibernético, pero sí debe comprender qué consecuencias financieras, operativas y comerciales tendría un incidente grave para la empresa.

¿Qué ocurriría si los sistemas no estuvieran disponibles durante una semana? ¿Qué fuentes de ingresos se detendrían primero? ¿Se podrían seguir emitiendo facturas? ¿Podría seguir procesándose la nómina? ¿Qué proveedores se volverían inmediatamente críticos? ¿Respondería el seguro de la forma que la empresa espera? ¿Son suficientemente largos los periodos de indemnización? ¿Son realistas los límites de la cobertura cibernética? ¿Está la organización expuesta a través de un tercero? ¿Ha comprobado alguien las suposiciones en las que se basa el plan de recuperación?

Estas preguntas no pretenden generar alarma, sino proporcionar visibilidad.

La visibilidad ofrece opciones a los directores financieros. Les permite cuestionar las coberturas, revisar a los proveedores, mejorar los planes de continuidad, reforzar la protección contractual y decidir dónde es realmente necesario invertir. También les permite analizar el conjunto de la estructura de costes e identificar dónde podrían obtenerse ahorros para financiar una mayor resiliencia, sin limitarse a añadir más costes a la empresa.

Cómo puede ayudar ERA Group

ERA Group ayuda a las organizaciones a analizar el riesgo cibernético desde una perspectiva comercial.

No sustituimos a los equipos internos de TI, a los responsables de seguridad de la información ni a los especialistas técnicos en ciberseguridad. Ese no es nuestro papel. Nuestro trabajo complementa el suyo, ayudando a los directores financieros y a los equipos directivos a comprender las implicaciones financieras, operativas, aseguradoras y relacionadas con los proveedores que tiene el riesgo cibernético.

Esto puede incluir la revisión de los seguros cibernéticos y del coste total del riesgo, la comparación con el mercado, la evaluación de límites y exclusiones, y el análisis de si los ahorros obtenidos en otras líneas de seguros podrían utilizarse para reforzar la protección cibernética.

También puede implicar analizar conjuntamente la cobertura por interrupción de actividad y la planificación de la continuidad, en lugar de tratarlas como ejercicios separados. Si los plazos de recuperación han cambiado debido a las presiones sobre la cadena de suministro, la disponibilidad de equipos, la dependencia de proveedores o la complejidad operativa, el programa de seguros debe reflejarlo.

En el ámbito tecnológico, ERA puede ayudar a las organizaciones a comprender en qué se está gastando en servicios en la nube y TI, si la facturación está estructurada de forma eficiente y dónde podrían optimizarse los costes sin comprometer la resiliencia.

La revisión de proveedores y contratos es otra parte fundamental de este análisis. El riesgo cibernético se transmite con frecuencia a través de terceros, por lo que es importante entender qué proveedores son críticos, qué responsabilidades se establecen en los contratos, si los niveles de servicio están claramente definidos y si los aumentos de costes o los acuerdos de transferencia de riesgos son razonables.

El objetivo no es asustar a las empresas para que gasten más. Es ayudarlas a gastar mejor.

ERA ayuda a sus clientes a encontrar valor en toda su estructura de costes para que puedan reforzar su resiliencia sin tratar el riesgo cibernético como otro coste inevitable.

Hablemos

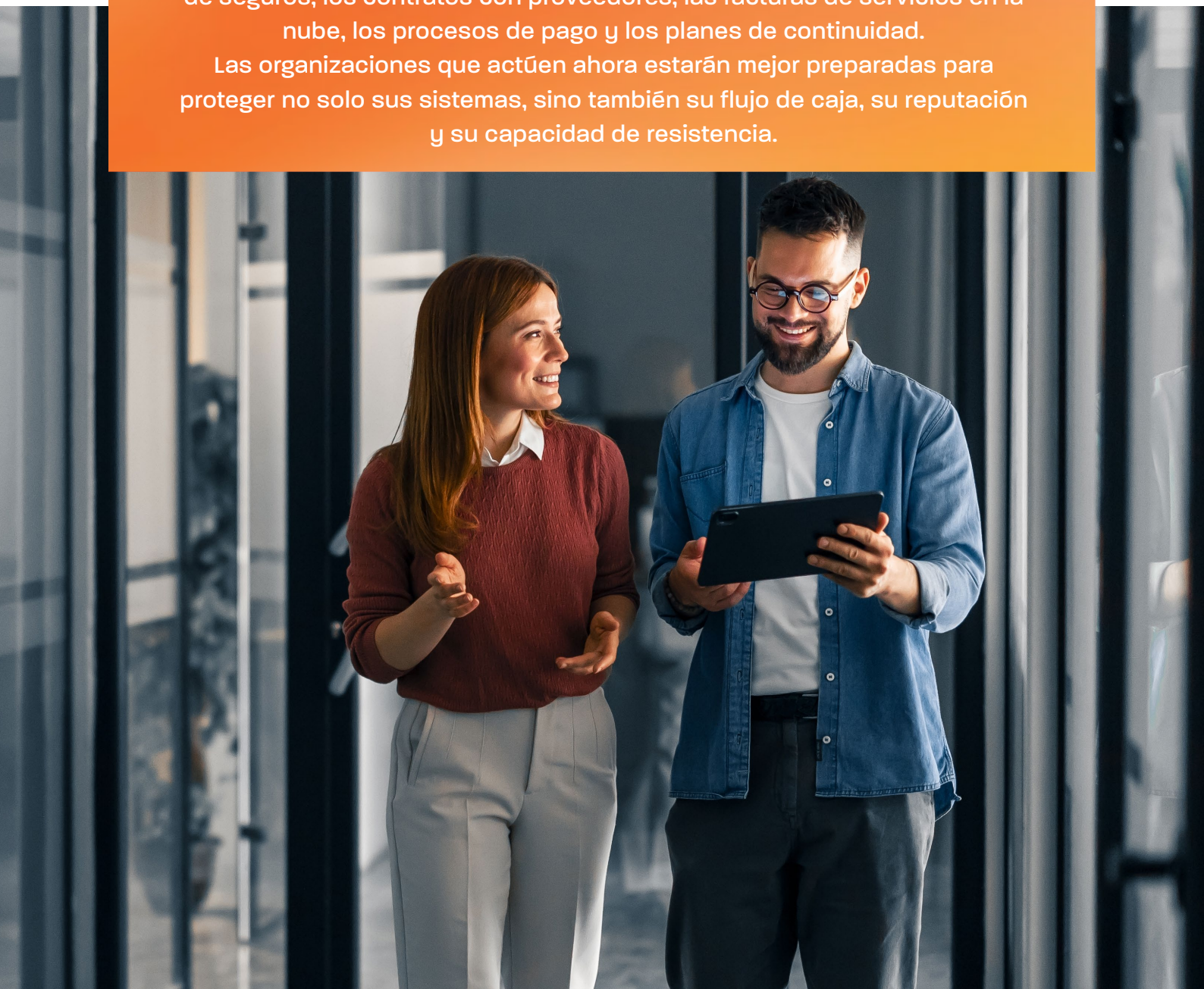
El riesgo cibernético no va a desaparecer. Es cada vez más sofisticado, está más conectado con las cadenas de suministro y es más visible para los reguladores, las aseguradoras, los clientes y los inversores.

Para los directores financieros, el peligro no consiste únicamente en que ocurra algo. El mayor riesgo es descubrir demasiado tarde que la empresa no comprendía el coste de lo que podría ocurrir.

La cobertura era demasiado limitada. El periodo de indemnización era demasiado corto. La exposición a través de los proveedores era mayor de lo esperado. El entorno en la nube era más complejo de lo que nadie había imaginado.

El coste del silencio ya se encuentra en los registros de riesgos, las pólizas de seguros, los contratos con proveedores, las facturas de servicios en la nube, los procesos de pago y los planes de continuidad.

Las organizaciones que actúen ahora estarán mejor preparadas para proteger no solo sus sistemas, sino también su flujo de caja, su reputación y su capacidad de resistencia.



Want to know more?
eragroup.com

value through insight™