



GUÍA DE LAS MEJORES PRÁCTICAS
DEL SECTOR PÚBLICO

SOLO ERES TAN FUERTE COMO TU ESLABON MÁS DÉBIL

Cómo tener en cuenta el comportamiento
humano en la gestión interna de riesgos

INTRODUCCIÓN

CAPÍTULOS:

La inestabilidad de los últimos años ha obligado a las empresas a repensar sus estrategias de gestión del riesgo, adoptando un enfoque que garantice la resiliencia a largo plazo.

El sector público es un excelente ejemplo, donde la creciente presión por la accesibilidad digital y la conectividad interdepartamental están impulsando una transformación sin precedentes. Los crecientes volúmenes de datos, desde las solicitudes de desempleo hasta los registros de vacunación y los flujos de trabajo, recientemente automatizados, agudizados por la transición al trabajo flexible, suponen que los datos confidenciales que maneja el sector y las vulnerabilidades para este tipo de operaciones se están multiplicando.

¿SABÍAS QUE?

Según nuestro estudio¹, casi la mitad (46%) de los gestores de datos afirman haber experimentado un aumento de los riesgos en sus datos como consecuencia de la pandemia.

Pero, ¿cómo proteger tu negocio ante el aumento de ataques?

Un área clave, que a menudo no se tiene en cuenta, es el de las amenazas internas. Aunque en su mayoría no son intencionales, el comportamiento y los errores humanos

están costando dinero a las organizaciones, sin mencionar que causan daños a la reputación si hay una pérdida de información confidencial. En un momento de digitalización tan rápida para satisfacer las demandas internas y externas, las organizaciones del sector público tienen más que perder que la mayoría. Esto ha quedado demostrado durante la pandemia, que llevó a muchos departamentos a tener mayores cantidades de datos personales, atendidos por equipos no preparados para el trabajo remoto y, por lo tanto, expuestos a un mayor estrés y riesgo de errores en sus esfuerzos por ayudar a los ciudadanos de forma rápida.

Un estudio reciente de IBM revela que el coste medio por incidente de una brecha de datos en el sector público ha aumentado de **1,08 millones de dólares a 1,93 millones** (un aumento del 79%), durante el año pasado².

Por ello Iron Mountain ha encargado un estudio paneuropeo que identifica las potenciales áreas de riesgo vinculadas al factor humano que las compañías deben tener en cuenta. Algunos de los resultados del mismo son sorprendentes.

Sigue leyendo para descubrir más detalles al respecto y algunos consejos prácticos para gestionar el riesgo en equipos híbridos y crear una estrategia empresarial resiliente.

1. Encuesta a 11.000 empleados en 10 países, realizada en septiembre de 2021 por One Poll.
2. Informe 'Data Breach Report' de IBM, 2021.

Empecemos con algunas oportunidades que hemos identificado.

Estas son algunas de las sorprendentes conclusiones sobre cómo trabajamos en casa y en la oficina.

¿Con cuántas de estas situaciones **te identificas?**



Afortunadamente, estos problemas se pueden solucionar. Por ello cabría considerar:

- Compartir estas estadísticas para visibilizar el problema sin tener que “señalar con el dedo”
- Señalar la importancia de un cambio de comportamiento
- Destacar las herramientas, la formación y el apoyo disponibles
- Reiterar la diferencia entre un riesgo calculado y uno innecesario
- Actualizar las políticas para garantizar la máxima comprensión y responsabilidad de la gestión de riesgos

CREAR UNA CULTURA DE CONSCIENCIA DEL RIESGO

2

Aunque no podemos cambiar la naturaleza humana, sí podemos cambiar la forma en la que **gestionamos los riesgos**, mientras fomentamos la excelencia clínica, mediante la construcción de una cultura consciente del riesgo desde cero.

Estos son nuestros cinco consejos para construir resiliencia frente a los riesgos desde el inicio:

1 CAMBIA LA MENTALIDAD DE TU ORGANIZACIÓN

EL HECHO:

Uno de cada tres empleados (32%) afirma haber cometido un error "crítico" en el trabajo y el 14% ha asumido un riesgo que le costó dinero a su organización.

LA SOLUCIÓN:

Comienza por capacitar a cada empleado para que se convierta en un "embajador del riesgo", incorporando la conciencia del riesgo dentro de la cultura de empresa. Profundiza en una mentalidad que destaque que ésta es una responsabilidad fundamental de los empleados. Es una tarea de la mayoría, no de unos pocos.

MARCA LAS CASILLAS
QUE CORRESPONDAN
A TU PLAN

2

REMODELA TUS POLÍTICAS DE GESTIÓN DE LA INFORMACIÓN

EL HECHO:

La mitad (49%) de los empleados considera que **vale la pena correr riesgos** en el trabajo, a pesar de que el 25% haya sido víctima de estafas o phishing.

LA SOLUCIÓN:

Las organizaciones del sector público establecieron respuestas de emergencia a la pandemia mundial del Covid, pero ahora han cambiado a estrategias a largo plazo basadas en la automatización del flujo de trabajo, la conectividad móvil y el acceso digital a la información. Piensa en **políticas de administración de información bien articuladas** que se apliquen a los empleados de la oficina, los que adoptan un modelo híbrido o están en remoto, así como a proveedores y contratistas.

Igualmente importante es disponer de un **archivo digital y físico** para la información que tiene la obligación legal de almacenar a largo plazo, así como un programa sólido para deshacerse de los documentos físicos y el equipo de TI cuando ya no está en uso.

3

GENERA UNA CULTURA DE SOLIDARIDAD Y APOYO

EL HECHO:

El 51% de las personas han quedado **marcadas por un error** cometido en el trabajo.

LA SOLUCIÓN:

Está demostrado que los entornos de trabajo híbridos fomentan la productividad, pero ésta puede verse afectada por el estrés. Asegúrese de que sus **flujos de trabajo están contruidos para gestionar el riesgo**. Utiliza nuevas [tecnologías impulsadas por la inteligencia artificial y el aprendizaje automático](#) para ayudar a optimizar y mejorar tus procesos.

¿Qué es la resiliencia 'by design'?

La resiliencia 'by design' - o desde la base-, es la capacidad de la empresa para defenderse de ataques, y no debería plantearse nunca en el último momento. Debe incluirse en cada etapa de las políticas y procesos comerciales.

Integración tecnológica tras la pandemia

Más de la mitad (59%) de los administradores de datos consultados **compraron nuevo software** durante la pandemia y dos tercios (62%) **implementaron herramientas colaborativas** como Microsoft Teams. Todo ello requiere de la integración en los programas de administración del ciclo de vida de la información, incluido **el establecimiento de períodos de retención para datos no estructurados**, como chats y grabaciones de reuniones, así como un sistema centralizado de cumplimiento de normas y gestión de políticas adaptado al complejo entorno tecnológico actual.

4

HAZ EVOLUCIONAR TUS PROCESOS

EL HECHO:

El 36% es más **consciente de la necesidad de proteger** los datos relacionados con el trabajo cuando está en la oficina, que cuando está en casa.

LA SOLUCIÓN:

Con la creciente modernización empresarial, cada día se crean mayores volúmenes de datos, incluida la información confidencial y privada. Esto obliga a **replantearse la gobernanza de la información**: desde la gestión de derechos de acceso hasta el intercambio de información digital, la retención de datos y la destrucción segura de acuerdo a los requisitos legales vigentes. Como primer paso, **considera la posibilidad de crear un mapa de datos** para comprender cómo fluyen los datos dentro y fuera de tu organización.

5

HAZ QUE LAS FORMACIONES SEAN DIFÍCILES DE OLVIDAR

EL HECHO:

Mientras que el 60% de los administradores de datos dicen que las **sesiones de formación** en gestión de riesgos cuentan con bastante asistencia, el 36% de los trabajadores afirma que nunca han estado en una.

LA SOLUCIÓN:

Es indudable que los trabajadores tienen a su disposición cursos de formación para evitar riesgos, pero los resultados indican que olvidan rápidamente los contenidos de los mismos. Para mejorar el impacto, haz que las formaciones sean más atractivas, relevantes y reconocibles, de modo que los trabajadores reconozcan las situaciones diarias en las que aplicar los aprendizajes porque entienden cómo les afecta a ellos y a sus clientes.

“Somos humanos y cometemos errores, por lo que el riesgo, por definición, es un factor siempre presente en el trabajo. Pero no es constante. Los nuevos modelos de negocio, el trabajo híbrido y la creciente amenaza de los ciberataques hacen que sea más importante que nunca gestionar eficazmente los riesgos internos para construir resiliencia a largo plazo”.

Sue Trombley, Managing Director of Thought Leadership de Iron Mountain

CREAR UNA CULTURA DE CONSCIENCIA DEL RIESGO

2

INTEGRA TU ESTRATEGIA CON "RESILIENCIA BY DESIGN"

3



Según nuestro estudio, el **70%** de los data managers creen que todos los empleados son responsables de la gestión de riesgos.

"Un elemento de adopción de riesgos puede permitir a una organización innovar, pero la falta de conciencia sobre los peligros cotidianos puede desgastar la resiliencia. Aconsejamos capacitar a cada empleado para que se convierta en un "embajador del riesgo" al incorporar la conciencia del riesgo dentro de la cultura de empresa. De esta forma crearás un espacio seguro en el que las personas puedan innovar y las organizaciones prosperar".

Sue Trombley, Managing Director of Thought Leadership de Iron Mountain

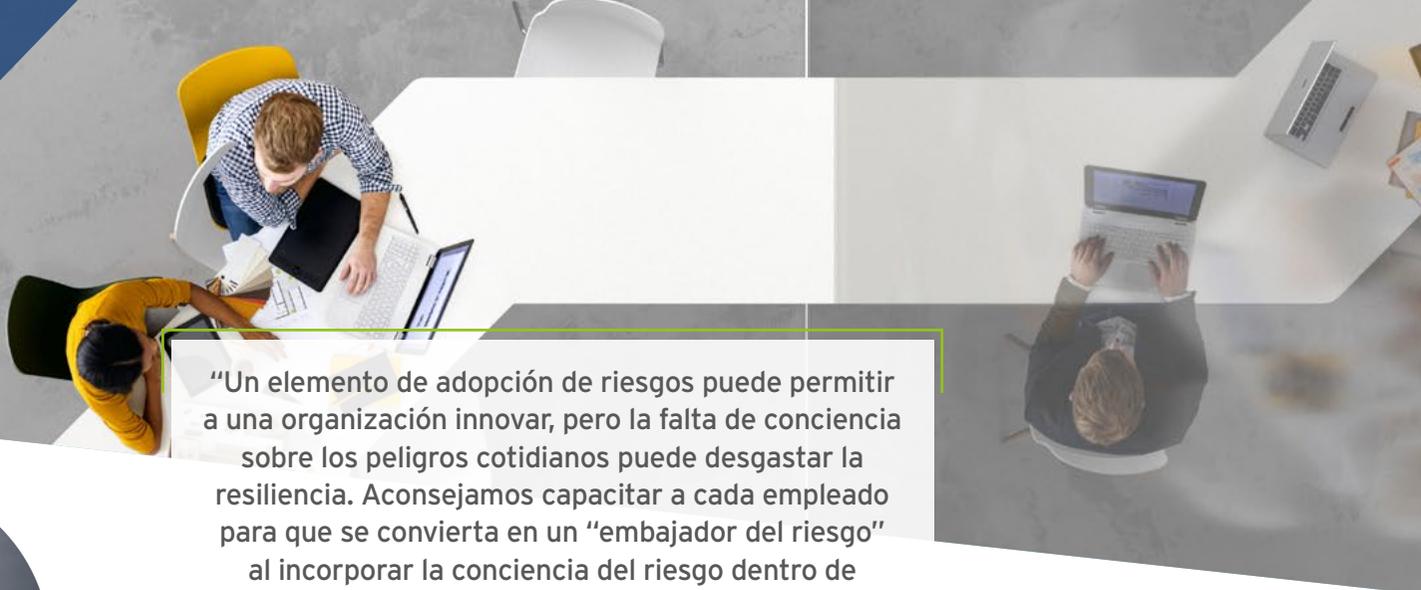
Para un impacto duradero, la resiliencia debe integrarse en cada etapa de tus procesos comerciales y reforzarse con acciones diarias de todos los empleados, tanto operacionales como administrativos.

A medida que el sector público trabaja para adoptar nuevas tecnologías como la IA y responder a las crecientes demandas de acceso móvil y conectividad entre departamentos, es importante recordar que los riesgos de sufrir ciberataques persistirán mientras sigamos recuperándonos de la crisis generada por el COVID-19.

Esto hace que **las soluciones de trabajo híbridas integradas con "resiliencia by design"** sean clave para el desempeño a largo plazo de las organizaciones del sector público.

Soluciones que, por ejemplo, permiten [el acceso seguro a la información](#) desde cualquier lugar, para empleados y ciudadanos, agilizan [los flujos de trabajo](#) para procesar reclamos por desempleo o beneficios y ayudan a administrar de manera efectiva todo el ciclo de vida de los datos. Soluciones que permiten desbloquear el potencial de la información y hacer que funcione de manera más eficiente e inteligente para la organización y para el público.

Para obtener ayuda para abordar los desafíos cambiantes de la gestión de la información de tu empresa y hablar sobre soluciones que te ayuden a impulsar la resiliencia en un mundo de trabajo híbrido, ponte en contacto con nuestro equipo o visita ironmountain.com/es/industries/public-sector.



ACERCA DE IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), fundada en 1951, es el líder mundial en servicios de almacenamiento y gestión de la información. Con la confianza de más de 225.000 organizaciones en todo el mundo, y con una red inmobiliaria de casi 8,6 millones de metros cuadrados en aproximadamente 1.450 instalaciones en 56 países, Iron Mountain almacena y protege miles de millones de activos valiosos, incluyendo información empresarial crítica, datos altamente sensibles y artefactos culturales e históricos. Proporcionamos soluciones que incluyen almacenamiento Seguro de registros, gestión de la información, transformación digital, destrucción segura, así como centros de datos, servicios en la nube y almacenamiento y logística de arte, Iron Mountain ayuda a los clientes a reducir los costes y los riesgos, a cumplir con la normativa, a recuperarse de los desastres y a permitir una forma de trabajo más digital. Visita www.ironmountain.es para obtener más información.

© 2021 Iron Mountain Incorporated. Todos los derechos reservados. Iron Mountain y el diseño de la montaña son marcas registradas de Iron Mountain Incorporated en los Estados Unidos y otros países. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.

900 22 23 24 | IRONMOUNTAIN.ES

