IRON MOUNTAIN®

GUÍA DE LAS MEJORES PRÁCTICAS DE SECTOR SANITARIO

SOLO ERES TAN FUERTE COMO TU ESLABON MÁS DÉBIL

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

INTRODUCCIÓN

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.

En ningún otro sector esto es tan tangible como en el sector sanitario, donde los ciberataques cada vez son más sofisticados y están poniendo en peligro los datos confidenciales de los pacientes. Mientras tanto, las vulnerabilidades se multiplican a medida que los registros médicos se trasladan a plataformas digitales, prolifera la telemedicina y los dispositivos médicos del Internet de las cosas (IoT) son cada vez más comunes. La capacidad de atender a los pacientes de forma remota y efectiva, manteniendo sus datos seguros y de acuerdo a la normativa, nunca ha sido más crítico que ahora.

¿SABÍAS QUE?

En mayo de 2021, un ataque de ransomware **paralizó los sistemas informáticos** del servicio de salud irlandés, dejando a la mayoría de los hospitales del país sin acceso a los ordenadores durante más de una semana[1].

En 2020, un ataque ransomware dirigido a un hospital europeo tuvo graves consecuencias para los pacientes[2].

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 ponen en peligro a los proveedores de atención sanitaria al arriesgar vidas y causar pérdidas económicas, por no hablar de los daños a su reputación si hay pérdida de información médica confidencial. En un momento de digitalización tan rápida las organizaciones sanitarias tienen mucho que perder, más que la mayoría.

Un estudio reciente de IBM estima en **9,23 millones de dólares** el coste medio por incidente de una brecha de datos en el sector sanitario, más que en cualquier otra industria[3].

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. El hospital de Nueva Zelanda se enfrenta a la segunda semana de interrupciones después de un gran ataque cibernético.
2. 10 días después del ataque de ransomware, el sistema de salud irlandés sigue luchando.
3. Informe 'Data Breach Report' de IBM, 2021.
4. Encuesta a 11.000 empleados en 10 países, realizada en septiembre de 2021 por One Poll.

CAPÍTULOS:

SOLUCIONES RÁPIDAS

1

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**?

¡CLICK EN LOS ICONOS PARA DESCUBRIR MÁS!

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 sanitarias establecieron respuestas de emergencia a la pandemia mundial del Covid, pero ahora han cambiado a estrategias a largo plazo basadas en el consultas virtuales y trabajo híbrido. 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.

Dado que los proveedores de atención médica aceleran el proceso de digitalización de los registros de los pacientes, es fundamental garantizar una **cadena de custodia** completa en todos los procesos de recolección, transporte, digitalización y disposición.

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, que es una preocupación importante en la atención médica. Asegúrese de que sus **flujos de trabajo están construidos para gestionar el riesgo**. Utiliza nuevas tecnologías impulsadas por la inteligencia artificial y el aprendizaje automático de forma que el personal pueda brindar una mejor atención al paciente y trabajar a través de listas de espera inducidas por la pandemia.

¿Qué es la resiliencia 'by design'?

La resiliencia 'by desing' - 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.

CREAR UNA CULTURA DE CONSCIENCIA DEL RIESGO

2

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 de pacientes 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 el auge de las consultas virtuales y los registros digitales de los hospitales estandarizándose, se están creando volúmenes de datos cada vez mayores. Esto requiere que se **reconsidere 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.

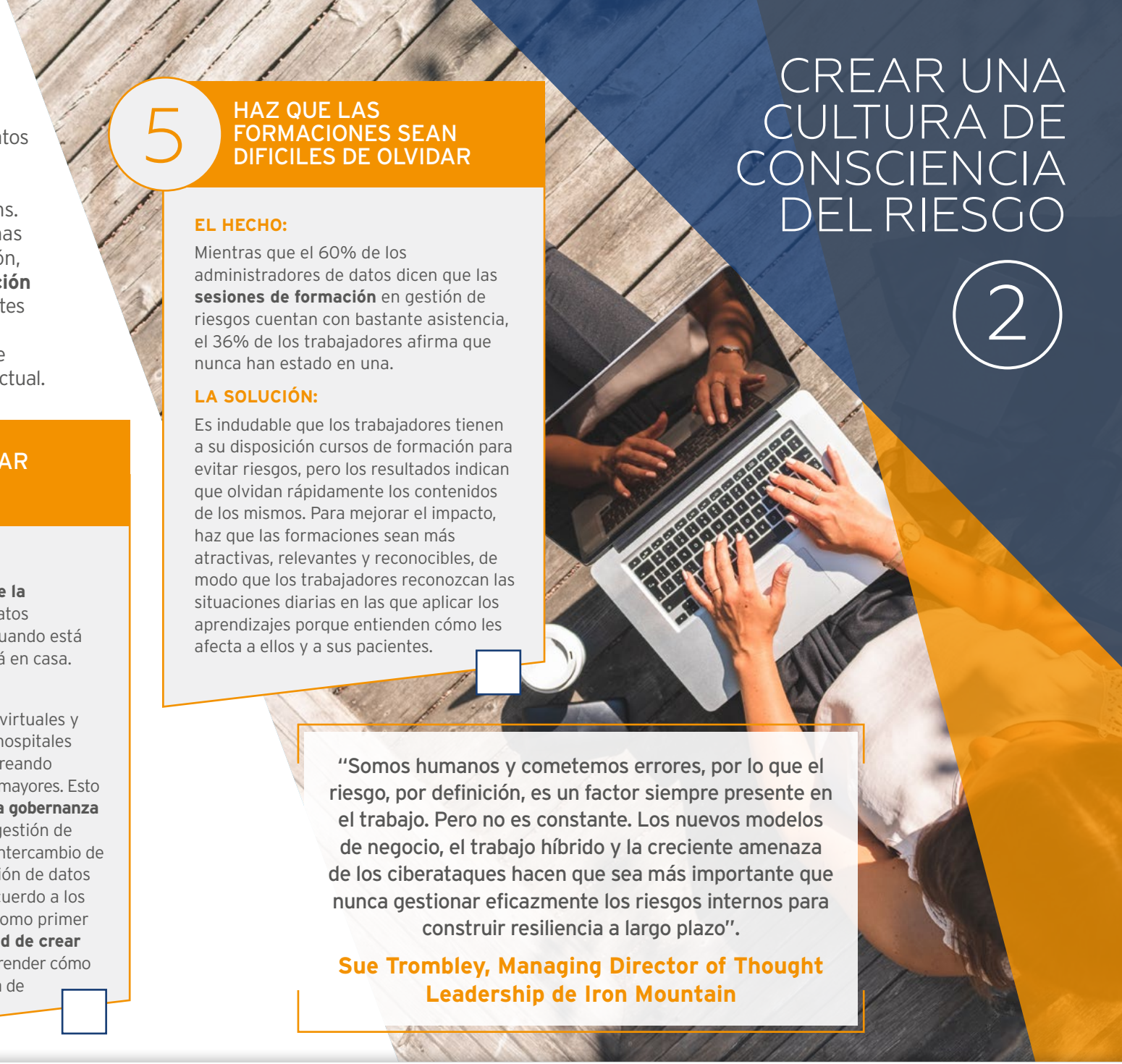
5 HAZ QUE LAS FORMACIONES SEAN DIFICILES DE OLVIDAR

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:

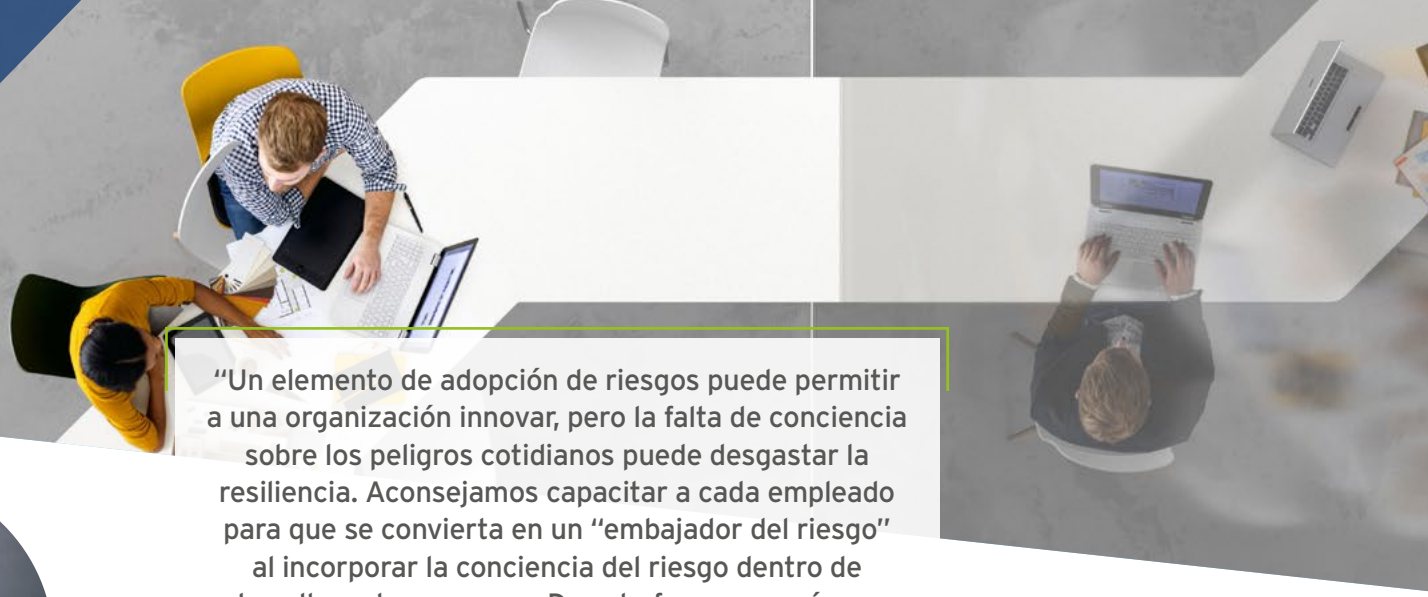
Es indudable que los trabajadores tienen a su disposición cursos de formación para evitar riesgos, pero los resultados indican que olvidan rápidamente los contenidos de los mismos. Para mejorar el impacto, haz que las formaciones sean más atractivas, relevantes y reconocibles, de modo que los trabajadores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



> "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**

INTEGRA TU ESTRATEGIA CON "RESILIENCIA BY DESIGN"

3



"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 empressa. 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

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

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 clínicos como administrativos.

A medida que los proveedores de atención médica trabajan para digitalizar rápidamente sus operaciones, es importante recordar que los riesgos por cambios inesperados 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 que cualquier organización sanitaria prospere a largo plazo. Soluciones que, por ejemplo, permiten el acceso seguro a la información desde cualquier lugar, agilizan los flujos de trabajo para archivar y digitalizar archivos y ayudan a administrar de manera efectiva todo el ciclo de vida de los datos y los de los pacientes, independientemente de su formato o tipo. Soluciones que permiten proteger y mejorar la accesibilidad de tu información, al mismo tiempo que mejoran la toma de decisiones clínicas y mejoran la atención al paciente.

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/healthcare-services

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.

900 22 23 24 | IRONMOUNTAIN.ES

IRON MOUNTAIN®