

Seis costosas brechas de protección de datos en Microsoft 365 y cómo cerrarlas



Si su empresa utiliza Microsoft 365, puede esperar acceso confiable a sus aplicaciones con una alta disponibilidad. Microsoft tiene una gran reputación de disponibilidad de sus sistemas, pero no es responsable de mantener seguros los datos de los clientes, ya que no ofrece verdaderas capacidades de copia de seguridad y recuperación. De hecho, es Microsoft quien recomienda que los usuarios hagan regularmente copias de seguridad de contenido y datos mediante apps o servicios tercerizados.

Sin embargo, muchas empresas aún creen que Microsoft ofrece una protección de datos completa y retención de datos a largo plazo para Microsoft 365, pero no es exactamente así. Aunque Microsoft 365 ofrece una variedad de funciones, no cuenta con una protección total contra problemas comunes y graves de pérdida de datos; que pueden incluir eliminaciones accidentales, pérdida de datos por amenazas internas y externas, brechas en directivas de retención y más. Esto representa un vacío en la protección de datos que puede llevarlo a tener sorpresas desagradables. Aunque Microsoft ofrece algunas funciones para restaurar datos de Microsoft 365 que se hayan perdido, destruido o dañado; puede que no sea suficiente para que la mayoría de las empresas protejan totalmente sus apps críticas.

1. Eliminación de datos por accidente

Riesgo para los datos

Los empleados eliminan regularmente perfiles de usuarios de Microsoft 365, correos electrónicos y archivos adjuntos de Exchange Online, archivos de OneDrive para Empresas o contenido de Teams y SharePoint Online. Estas eliminaciones pueden ser accidentales o intencionales; y luego querer

revertirlas. En cualquier caso, pueden causar una pérdida de datos importantes del cliente.

Punto débil de Microsoft

Este tipo de eliminaciones cotidianas de recursos se replican de forma rutinaria por toda la red. Cuanto más antiguos sean los recursos, más definitiva será la eliminación y más difícil la recuperación. Las eliminaciones recientes de recursos no tan antiguos son ligeramente menos problemáticas, ya que los archivos y correos electrónicos no eliminados permanentemente pueden recuperarse durante un breve período de la papelera de reciclaje o de la carpeta de elementos recuperables.

2. Problemas de directivas de retención

Riesgo para los datos

Si las prioridades han cambiado o no son correctas en Microsoft 365, la directiva de la retención de los datos podría eliminarse de forma permanente. Este riesgo solo puede mitigarse parcialmente mediante revisión y actualización regular de las directivas de retención.

Punto débil de Microsoft

La responsabilidad de gestionar las directivas de retención recae en usted; pero, si por algún motivo se produce una eliminación permanente debido a que las políticas de retención actuales sean obsoletas, Microsoft no puede recuperar el recurso eliminado o caducado.

3. Problemas de seguridad interna

Riesgo para los datos

Sus datos y recursos de Microsoft 365 deben estar protegidos contra alteraciones maliciosas o destrucción

de datos por parte de empleados, exempleados, contratistas o partners descontentos.

Punto débil de Microsoft

Con la excepción de eliminaciones muy recientes de recursos relativamente nuevos, Microsoft no protege contra la destrucción o alteración interna de datos de Microsoft 365.

4. Migración desde Microsoft Office in situ

Riesgo para los datos

Si usted migra un paquete de apps tradicionales de Microsoft instaladas localmente a servicios Microsoft 365 en la nube, este esfuerzo generalmente consiste en la transición de una solución de protección de datos heredada a una nueva con capacidad para la nube. Por lo general, estas dos soluciones de copia de seguridad son incompatibles, por lo que es imposible restaurar datos anteriores en el nuevo entorno.

Punto débil de Microsoft

Microsoft no ofrece ninguna solución para los problemas de pérdida de datos durante la migración de Office a Microsoft 365. Pocas soluciones de protección de datos tercerizados integran la funcionalidad de copia de seguridad para Office y Microsoft 365. Lamentablemente, lo normal es que hagan una cosa o la otra, pero no ambas.

5. Problemas legales y de cumplimiento

Riesgo para los datos

Los requisitos de cumplimiento de regulaciones y problemas legales pueden disparar los costos por pérdidas de datos no protegidos como los ya descritos. La pérdida irrecuperable de datos de Microsoft 365 puede exponer a su empresa a

multas por regulaciones administrativas o específicas de su industria, sanciones legales, caídas de facturación y del precio de acciones, pérdida de confianza del cliente y daños a la marca de la empresa.

Punto débil de Microsoft

Ante todas las pérdidas de datos asociadas es poco lo que Microsoft puede hacer para proteger a las organizaciones que utilizan Microsoft 365 contra diversos riesgos legales y regulatorios. Por ejemplo, tras un ataque de ransomware, es posible que una empresa que almacene los datos personales de sus clientes europeos en SharePoint Online no pueda satisfacer las solicitudes de una copia de los datos, incurriendo así en una violación del RGPD.

Proteja sus datos de Microsoft 365

Si utiliza Microsoft OneNote, Teams, OneDrive o SharePoint, debe complementar la rudimentaria protección de datos de Microsoft con copias de seguridad tercerizada. Dicha solución agrega copias de seguridad rápidas, recuperación confiable en un momento dado, restauración flexible y funcionalidad de búsqueda.

Aunque Microsoft garantiza la resiliencia de su infraestructura, la protección de los datos de los clientes de su empresa es, en última instancia, responsabilidad suya.

Esto significa que necesita una solución de copia de seguridad para ayudar a prevenir el tiempo de inactividad, la pérdida irrecuperable de datos y mantener operativa su empresa.

Si desea más información, contáctenos:
Incopyme informática y comunicaciones, SL
info@incopyme.com
917 37 86 95