arcserve®

eBook

NO SE PIERDA EN SUPOSICIONES: SUPOSICIONES:

cómo proteger los datos de Microsoft Office 365

arcserve®

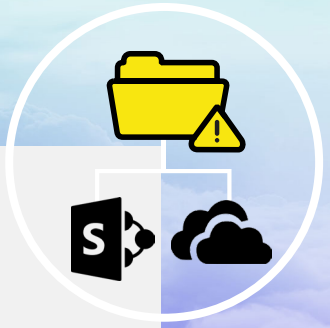
eBook

UN 56 PORCIENTO DE LAS EMPRESAS UTILIZAN MICROSOFT OFFICE 365, Y SU ORGANIZACIÓN ES UNA DE ELLAS.

Office 365 permite a sus empleados trabajar desde donde quieran y cuando quieran, y su organización depende de la solución para la comunicación por correo electrónico, la colaboración en equipo y la retención de documentos.

Aunque Microsoft administra la infraestructura de una manera excelente, hay mucha gente que, erróneamente, piensa que también se encargan de los datos de los usuarios tal y como ellos esperan. Para comprobar si su empresa está en situación de riesgo debido a deficiencias de seguridad de las que podría no ser consciente y saber cómo tomar el control de sus datos de Office 365, siga leyendo.

SITUACIÓN 01



Su equipo de ingeniería almacena archivos esenciales para el desarrollo en OneDrive para la Empresa y SharePoint Online, y usted necesita acceder a los archivos de un proyecto realizado hace varios años. El problema es que uno de sus compañeros eliminó la carpeta del equipo sin querer y, con ella, todos los documentos que usted necesita para la próxima versión del producto. A la desesperada, rápidamente va a la papelera de reciclaje para recuperar los archivos eliminados, pero resulta que los documentos tampoco están en ella.

Suposición:

Los elementos de la papelera de reciclaje de Office 365 solo se conservan durante 90 días, pero la papelera se puede vaciar en cualquier momento y los datos serían totalmente irrecuperables.

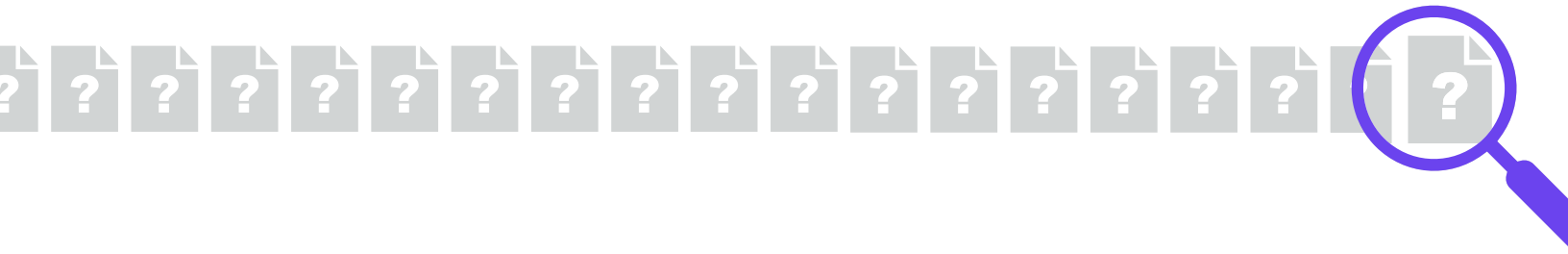
Realidad:

Los elementos de la papelera de reciclaje de Office 365 solo se conservan durante 90 días, pero la papelera se puede vaciar en cualquier momento y los datos serían totalmente irrecuperables.

Además, incluso en algunos casos en los que los datos pueden recuperarse, la recuperación en un momento determinado está fuera del alcance de los servicios prestados por Microsoft, por lo que no le quedaría otra opción que recuperar la versión más reciente disponible en la papelera de reciclaje con todas las modificaciones que podrían no servirle. Además, las políticas de retención son distintas para cada aplicación de la plataforma de nube, lo que hace que el proceso de recuperación de elementos eliminados resulte todavía más difícil.

Resultado:

Cientos de horas (¡y de dinero!) perdidos buscando documentos irrecuperables y teniendo que trabajar de nuevo en los archivos perdidos.



SITUACIÓN 02

Recibe un mensaje de correo electrónico urgente del vicepresidente de recursos humanos. En él se le pide que verifique información personal para que puedan reembolsársele los pagos de atención sanitaria que usted ha abonado. El mensaje de correo electrónico incluye un vínculo para confirmar su número de cuenta y de ruta, así como otra información personal. En cuanto pulsa el botón de envío, pone en tela de juicio esta solicitud, dado que no recuerda que el departamento de recursos humanos haya emitido una orden corporativa por la que deba hacerlo. Inmediatamente vuelve a abrir el mensaje, con el fin de confirmar su autenticidad, y se da cuenta de que la dirección del remitente corresponde a una cuenta de phishing y que ha sido objeto de un delito de suplantación de identidad.

Suposición:

Las aplicaciones de Office 365 están protegidas de las amenazas informáticas externas.

Realidad:

Controlar los datos de Office 365 es responsabilidad suya, y también debe proteger su correo electrónico de Exchange Online del ransomware, el malware y los hackers.

Sin contar con una solución de protección de datos externa, no tendrá la posibilidad de acceder a una copia independiente de sus datos si un empleado sigue por error las indicaciones de un mensaje de correo.

Resultado:

Los ataques de seguridad y las vulneraciones de datos externos pueden causar estragos en una organización, tener unas repercusiones financieras gravísimas en sus resultados y provocar daños irreparables en la reputación de su marca. Además, si los datos internos y de clientes se ven afectados, podría tener que hacer frente a cuantiosas sanciones relacionadas con el cumplimiento y la privacidad de los datos.

SITUACIÓN 03

Uno de sus empleados abandonó la empresa hace un año y se eliminó su cuenta para ahorrar en los costes de las licencias de los usuarios inactivos. Ahora, este empleado ha adoptado medidas legales contra su organización y usted debe presentar información relacionada con el pleito.

Suposición:

Office 365 incluye una medida de retención por juicio integrada, así que todo está bajo control.

Realidad:

Muchas organizaciones optan por eliminar usuarios antiguos para evitar la carga financiera que supone tener que pagar el precio de las licencias de usuarios que han finalizado su contrato con la empresa o que han optado por renunciar a su puesto de trabajo. Esta práctica puede generar ciertos problemas cuando surgen disputas legales, dado que eliminar un usuario también conlleva la eliminación de su sitio de SharePoint y su cuenta de OneDrive. Aunque Microsoft optó por incluir la medida de retención por juicio para reducir el riesgo de pérdida de datos, no puede usarse como protección de datos externa para hacer frente a requisitos y normativas de cumplimiento.

Resultado:

Las medidas legales pueden ser devastadoras, si tenemos en cuenta los costes legales y las consecuencias o sanciones que podría tener que afrontar si no puede presentar la información necesaria. Nunca sabe cuándo va a tener que facilitar mensajes de correo u otra documentación, así que estar preparado es la única forma de mantener su organización a salvo.

arcserve®

eBook

PROTEJA LOS DATOS DE OFFICE 365 CON ARCSERVE

Microsoft ofrece el backup dentro de un modelo de responsabilidad compartida. Esto significa que ellos se responsabilizan de la seguridad física de sus centros de datos y de los fallos de software en su infraestructura, pero es responsabilidad del usuario proteger sus datos de errores humanos, amenazas para la seguridad tanto internas como externas y problemas de programación.

Proteja Office 365 con Arcserve Unified Data Protection (UDP) y benefíciese de la serie de prestaciones de protección de datos más completa disponible para Office 365, entre las que se incluyen:

- Compatibilidad total con los servicios esenciales de Office 365: Exchange Online, SharePoint Online y OneDrive para la Empresa.
- Recuperación granular y backup a un momento dado.
- Deduplicación y compresión con potente cifrado AES.
- Compatibilidad flexible con soluciones de almacenamiento y opciones de licencia que se ajustan a las necesidades de su negocio.
- Interfaz de gestión optimizada y unificada para conformar una solución de disaster recovery y backup integrada.

Tome el control de sus datos de Office 365 con Arcserve. Proteja lo que no tiene precio.