backupify
A Kaseya COMPANY

LOS 5 PRINCIPALES

Puntos ciegos de las copias de seguridad

en Microsoft 365

Los 5 principales puntos ciegos de las copias de seguridad en Microsoft 365

Los rápidos avances tecnológicos en los últimos años han transformado la forma en que las organizaciones realizan negocios, lo que permite a sus empleados trabajar de forma remota. Las empresas modernas dependen cada vez más de las aplicaciones de software como servicio (Software-as-a-Service, SaaS) para navegar por estos cambios. Hoy en día, las aplicaciones SaaS son herramientas esenciales para las empresas de todo el mundo. Estas soluciones basadas en la nube proporcionan escalabilidad, flexibilidad y rentabilidad, lo que permite a las empresas optimizar las operaciones, mejorar la colaboración e impulsar la productividad. Entre las numerosas ofertas SaaS disponibles en el mercado, Microsoft 365 se destaca como líder en el panorama empresarial.

Microsoft 365 incluye un conjunto de potentes herramientas para la administración profesional de correo electrónico, el almacenamiento en la nube y el uso compartido de archivos, diseñadas para admitir una variedad de funciones empresariales. Estas herramientas se integran de manera fluida y ofrecen una plataforma cohesiva que fomenta la colaboración y la comunicación dentro de las organizaciones. A pesar de los numerosos beneficios que Microsoft 365 ofrece a empresas de todos los tamaños, permanece la pregunta: ¿Confiar únicamente en la protección nativa del proveedor de servicios en la nube es suficiente para proteger sus datos?

Este documento técnico examina las posibles brechas de seguridad en la protección nativa de Microsoft. Identifica los riesgos y puntos ciegos clave dentro de Microsoft 365 para ayudarlo a proteger mejor sus datos y sus cargas de trabajo. Siga leyendo para obtener más información sobre estos riesgos y cómo fortalecer la estrategia de protección de datos de Microsoft 365.

Comprender la protección nativa de Microsoft

Aunque Microsoft proporciona funciones nativas de protección de datos, hay brechas significativas que se deben abordar para garantizar que los datos de su organización estén completamente protegidos.

Los mecanismos de protección de datos de Microsoft

Exchange Online Protection (EOP) es el servicio de filtrado de correo electrónico basado en la nube de Microsoft, diseñado para ayudar a proteger a las organizaciones contra spam, malware y otras amenazas de correo electrónico. Forma parte del conjunto de aplicaciones de Microsoft 365 y proporciona una capa de seguridad para correos electrónicos entrantes y salientes. El EOP utiliza técnicas de filtrado avanzadas para interceptar y evitar que los correos electrónicos no deseados lleguen a las bandejas de entrada de los usuarios. Incluye múltiples módulos antimalware para detectar y bloquear virus y otros software maliciosos en archivos adjuntos y enlaces de correo electrónico.

Las licencias Premium de Microsoft, como E5, incluyen a Microsoft Defender for Office 365, una solución de seguridad integral diseñada para proteger a los usuarios de Microsoft 365 de una amplia gama de amenazas cibernéticas. Proporciona capacidades avanzadas de protección, detección y respuesta ante amenazas para herramientas de colaboración y correo electrónico dentro del conjunto de aplicaciones de Office 365, incluidos SharePoint Online, OneDrive y Microsoft Teams.

Microsoft ofrece soporte de autenticación multifactor (MFA) para usuarios de Microsoft 365 y Office 365. Esta función fortalece la seguridad de la cuenta al requerir varias verificaciones para acceder a los servicios de Office 365. Esta capa adicional de seguridad ayuda a evitar el acceso no autorizado a la cuenta, incluso si la contraseña de un usuario se ve comprometida.

Opciones nativas de copia de seguridad y recuperación

Se espera que Microsoft 365 Backup esté disponible para uso general a mediados de 2024. Esta solución está diseñada para proteger a las empresas contra ataques de ransomware al proporcionar protección inmutable de la copia de seguridad y permitir la recuperación de datos en cuestión de horas. Los usuarios pueden realizar copias de seguridad y restauración de autoservicio dentro del Centro de Administración de Microsoft o a través de un socio de proveedor de software independiente (ISV) de confianza.

Microsoft 365 guarda automáticamente múltiples versiones de documentos almacenados en SharePoint Online y OneDrive for Business, permitiendo a los usuarios restaurar versiones anteriores si es necesario. Ayuda a las organizaciones a protegerse contra la pérdida de datos debido a la eliminación accidental, corrupción, virus o malware. Además, el Historial de versiones permite el seguimiento y la gestión de cambios en los archivos, lo que facilita la recuperación de versiones anteriores si se han realizado cambios no deseados a un archivo.

Los elementos eliminados en SharePoint y OneDrive son trasladados a la papelera de reciclaje, donde los usuarios o administradores pueden restaurarlos dentro de un período determinado (el valor predeterminado es 93 días).

Cuando los usuarios eliminan accidentalmente correos electrónicos en Exchange Online, primero se trasladan a la carpeta Elementos eliminados y luego a la carpeta Elementos recuperables si se eliminan nuevamente. El período de retención predeterminado para los elementos de la carpeta Elementos eliminados es de 14 días. Una vez finalizado el período recuperable, dentro de los 30 días, los administradores aún pueden encontrar y recuperar elementos eliminados a través del Centro de administración de Exchange. Los administradores pueden configurar políticas de retención para retener correos electrónicos durante un período específico.

Según IBM, en 2023, las organizaciones tardaron en promedio 207 días en identificar datos comprometidos, mucho después de que el período de retención de 30 días había finalizado.

Redundancia y disponibilidad de datos

La redundancia de datos y la disponibilidad en Microsoft 365 son elementos fundamentales diseñados para garantizar un acceso fluido a la información y a los servicios ininterrumpidos. Microsoft 365 logra la redundancia de datos al replicar datos de usuarios en múltiples centros de datos dispersos geográficamente. Este enfoque multicapa significa que, si un centro de datos experimenta una interrupción o falla, otro puede tomar el control de inmediato, minimizar el tiempo de inactividad y garantizar el acceso continuo a los servicios.

Si bien Microsoft replica datos para garantizar el acceso continuo a los datos, es importante tener en cuenta que una réplica no es una copia de seguridad. Las réplicas pretenden ser una copia exacta de los datos que se mantienen sincronizadas con el original, lo que proporciona una duplicación casi en tiempo real. Esto garantiza una alta disponibilidad y un tiempo de inactividad mínimo en caso de una falla primaria del sistema. Sin embargo, la replicación no protege contra errores lógicos o corrupción, los que podrían transferirse a la réplica.

Limitaciones de la protección nativa

La protección nativa de Microsoft dentro de sus servicios en la nube ofrece características de seguridad básicas diseñadas para proteger los datos de los usuarios. Sin embargo, si bien la protección nativa de Microsoft forma una base sólida, se centra principalmente en la seguridad “de” la infraestructura de la nube en lugar de los datos administrados “en” la nube por los usuarios. Esto significa que, si bien Microsoft protege el hardware y software subyacentes, los usuarios (usted) deben tomar medidas adicionales para proteger sus datos de eliminaciones accidentales, amenazas internas y ataques cibernéticos avanzados.

El modelo de responsabilidad compartida

A medida que las empresas dependen cada vez más de servicios en la nube como Microsoft 365, comprender el modelo de responsabilidad compartida se vuelve crucial para una gestión y seguridad de datos efectivas. Este modelo delinea las obligaciones de seguridad entre el proveedor de servicios en la nube (CSP) y el cliente, asegurando que ambas partes desempeñen un papel en el mantenimiento de un entorno de nube seguro.

En un modelo de responsabilidad compartida, como con una solución SaaS como Microsoft 365, el CSP (Microsoft) es responsable de la disponibilidad de las aplicaciones y la infraestructura subyacente. Por el contrario, el cliente (usted) es responsable de los datos de la aplicación, la administración y la gestión de usuarios. Este modelo dicta que Microsoft garantiza la integridad del centro de datos, cubriendo la seguridad, la infraestructura y las operaciones para mantener la disponibilidad y el rendimiento de los servicios de Microsoft 365. Por otro lado, los clientes son responsables a nivel operativo y contractual de la integridad de su inquilino, la seguridad de las credenciales de usuario y la protección de sus datos de Microsoft 365.

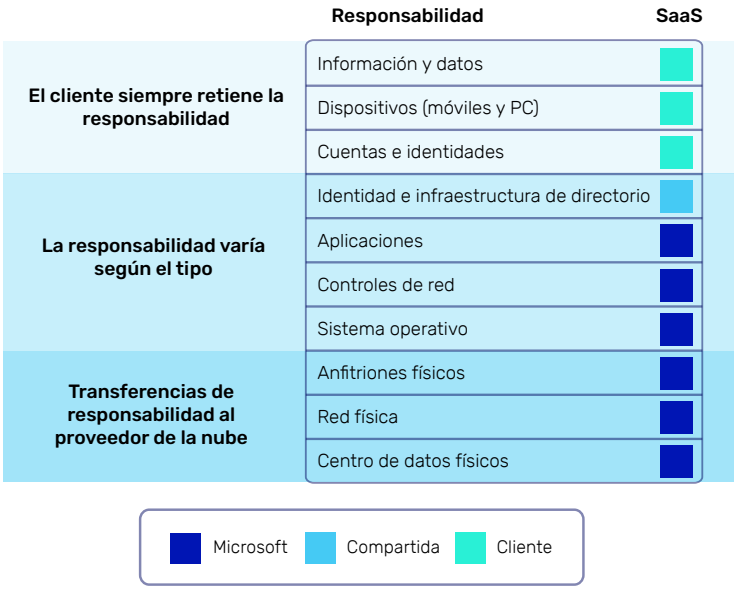


Figure 1: Responsabilidad compartida en la nube
Fuente: *Microsoft*

Reglas de retención y sus restricciones

Las políticas de retención y las etiquetas de retención en Microsoft 365 son herramientas esenciales para gestionar los ciclos de vida de los datos y garantizar el cumplimiento de los requisitos normativos y las políticas internas. Las empresas pueden aplicar etiquetas y políticas de retención a sitios, correos electrónicos, documentos y otros contenidos para garantizar que se conserven durante un período específico. Estas características permiten a las organizaciones controlar cuánto tiempo se retiene el contenido, lo que ayuda a proteger la información confidencial y facilita la gestión eficiente de los datos.

Los administradores pueden aplicar reglas de retención a ubicaciones específicas como buzones de Exchange, sitios de SharePoint, cuentas de OneDrive y canales de Microsoft Teams.

Se pueden configurar reglas de retención para retener datos durante un período específico o indefinidamente, según las necesidades de su organización. Por ejemplo, una regla de retención podría conservar correos electrónicos durante siete años para cumplir con las regulaciones de la industria. Después de que vence el período de retención, los datos se eliminan o archivan automáticamente.

Aunque los parámetros de retención nativa de Microsoft ayudan a las organizaciones a conservar sus datos para el cumplimiento normativo, no funcionan como una solución de copia de seguridad. Muchas empresas creen erróneamente que las políticas de retención y las etiquetas de retención de Microsoft pueden utilizarse para respaldar datos críticos. Este concepto erróneo es peligroso y puede poner en peligro la seguridad de los datos de una empresa. Además, estas funciones no se aplican a todos los datos dentro de las aplicaciones de Microsoft 365.

Las políticas de retención y las retenciones legales solo están disponibles en los planes Microsoft Enterprise E3 y E5. Según el plan Microsoft 365 con el que cuente su organización, a cada usuario se le asigna una cierta cantidad de capacidad de almacenamiento. Cuando se retienen los datos, se agregan a la cuota de almacenamiento. Si elimina datos para ahorrar espacio de almacenamiento o permanecer dentro del límite de almacenamiento asignado, estos datos no se pueden recuperar.

Umbrales de datos importantes que debe conocer

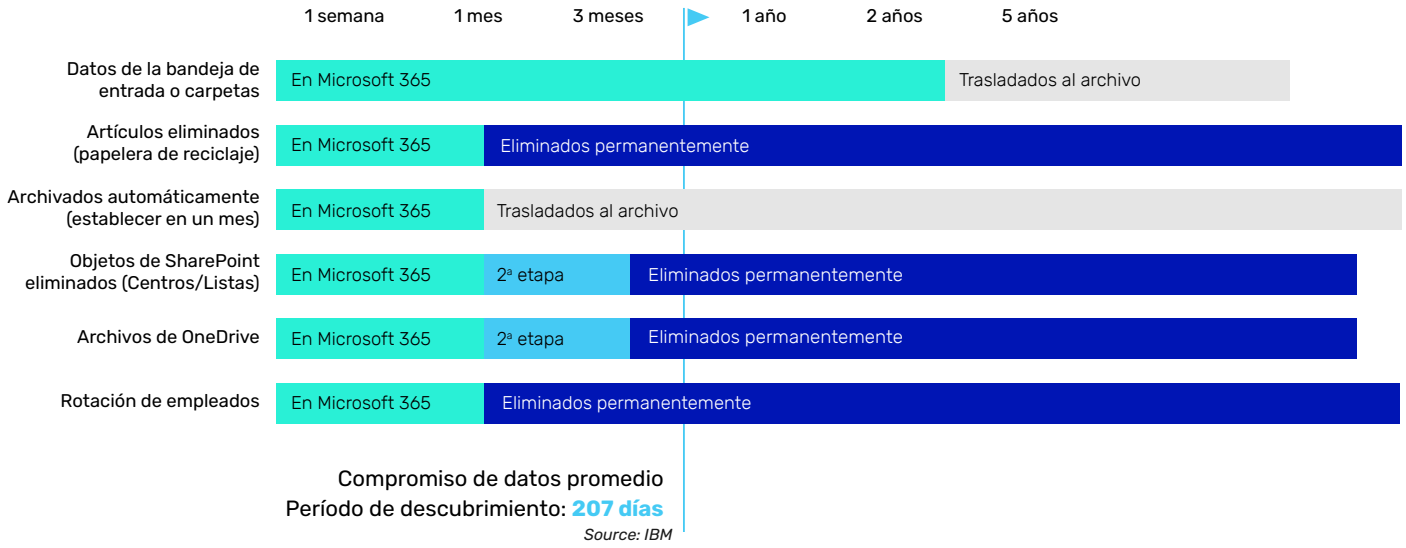


Figure 2: Creación de una estrategia de seguridad de datos eficaz

Tipos de pérdida de datos no cubiertos

Aunque Microsoft proporciona varias funciones nativas de seguridad y prevención de pérdida de datos, como Exchange Online Protection, Microsoft Defender para Office 365, Autenticación multifactor de Office 365, políticas de retención y otras, almacenar datos confidenciales en la nube aún puede ser una preocupación para algunas organizaciones debido a posibles vulnerabilidades. Microsoft 365 no cubre de manera integral las amenazas maliciosas de información privilegiada, las eliminaciones accidentales, la corrupción de datos debido a problemas de configuración o sincronización o ataques de ransomware, lo que deja los datos confidenciales de su organización vulnerables a la pérdida o corrupción.

Riesgos clave y cinco puntos ciegos principales en Microsoft 365

Muchas empresas hoy en día confían sus datos a los proveedores de servicios en la nube, creyendo que las protecciones nativas son suficientes para salvaguardar su valiosa información. Sin embargo, confiar únicamente en estas medidas de seguridad incorporadas puede ser riesgoso. Si bien los proveedores de nube, como Microsoft, ofrecen características de seguridad esenciales, no cubren todas las vulnerabilidades. Estos son los cinco principales puntos ciegos de las copias de seguridad en Microsoft 365 a los que debe estar atento para proteger sus cargas de trabajo críticas de manera efectiva.

1

ERROR HUMANO

Las acciones humanas, ya sean accidentales o intencionales, desempeñan un papel importante en la pérdida de datos dentro de los entornos SaaS. Algunos de los errores más comunes son:

Eliminaciones y sobreescrituras accidentales

Las eliminaciones y sobreescrituras accidentales pueden ocurrir cuando los empleados eliminan por error archivos críticos o reemplazan datos existentes con versiones incorrectas.

Corrupción involuntaria de datos

La corrupción involuntaria de datos es otra preocupación, en la que los archivos pueden volverse inutilizables debido a cambios involuntarios o un manejo inadecuado. Estos errores pueden interrumpir los flujos de trabajo y provocar pérdidas significativas de datos si no se abordan de inmediato. De acuerdo con el Informe de investigación de violaciones de datos 2024 de Verizon, el, 68 % de las violaciones estuvieron vinculadas a factores humanos no intencionales, como personas que caen víctimas de ataques de ingeniería social o que cometen errores.

2

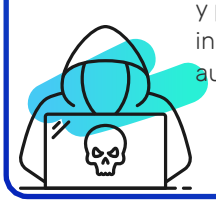
ACTIVIDADES MALICIOSAS

Microsoft 365 no está exento de actividades maliciosas.

Amenazas internas

Las amenazas internas representan un riesgo sustancial; empleados descontentos o aquellos con motivos ulteriores podrían eliminar deliberadamente o filtrar información confidencial. El informe de Verizon también descubrió que los actores internos fueron responsables del 35 % de las violaciones.

Microsoft sigue el "modelo de responsabilidad compartida", con los clientes como el "Controlador" de sus datos y Microsoft como el "Procesador". Microsoft es responsable de modificar los datos y de manejar los cambios en las configuraciones, ajustes y políticas a pedido. Esto significa que procesarán incluso solicitudes maliciosas o accidentales si están autenticadas con credenciales válidas.



Ataques cibernéticos externos

Los ciberataques externos, incluidos el phishing y el malware, también pueden comprometer la seguridad de los datos. A menudo, los atacantes apuntan a las cuentas de Microsoft 365 para obtener acceso no autorizado a información comercial confidencial, lo que puede provocar filtraciones de datos y pérdidas financieras. Si bien los ataques de ransomware pueden no apuntar específicamente a los datos de Microsoft 365, pueden alcanzar a su organización al afectar otras aplicaciones como Exchange Online y SharePoint Online.

La firma de ciberseguridad Obsidian informó acerca de un ataque de ransomware exitoso en SharePoint Online que se aprovechó de una cuenta de administrador SaaS de Microsoft Global, lo que resultó en el robo de cientos de archivos.

3 CUMPLIMIENTO Y RIESGOS LEGALES

Los riesgos legales y de cumplimiento son fundamentales para las organizaciones que manejan información confidencial.

Limitaciones de la política de retención y requisitos reglamentarios

Es posible que las políticas de retención nativas de Microsoft 365 no cumplan con todos los requisitos normativos, especialmente para industrias con estrictas reglas de conservación de datos. Las empresas deben asegurarse de que puedan mantener los datos durante los períodos requeridos para cumplir con las regulaciones y evitar sanciones.

Si bien las políticas de retención y las etiquetas de retención ayudan a preservar los datos durante un período determinado, no sustituyen a las copias de seguridad. Las políticas de retención de Microsoft 365 están diseñadas para cumplir con los requisitos normativos y de cumplimiento, pero es posible que no ofrezcan el mismo nivel de protección y recuperación de datos que las soluciones de copia de seguridad dedicadas. Las soluciones de copia de seguridad de terceros brindan a los usuarios un mayor control sobre la duplicación y distribución de datos, mejorando su disponibilidad e integridad. Además, a menudo implican el almacenamiento de las copias de los datos en múltiples ubicaciones, lo que refuerza la seguridad y la redundancia.

Retenciones legales y desafíos de eDiscovery

Las retenciones legales y los desafíos de eDiscovery surgen cuando las organizaciones necesitan preservar datos para litigios o investigaciones. Estos a menudo requieren herramientas avanzadas más allá de las capacidades nativas de Microsoft para gestionar y recuperar la información requerida de manera eficiente.

Microsoft 365 incluye la funcionalidad de retención para litigios nativa para eDiscovery, pero no está destinada a restaurar datos perdidos. El uso de la retención para litigios para todos sus datos puede ser riesgoso durante una solicitud de eDiscovery, ya que todo se vuelve recuperable, lo que aumenta la responsabilidad de ciberseguridad. Además, no almacena datos en una ubicación física secundaria ni permite la restauración del correo electrónico o de cuentas de manera directa. Si bien la recuperación manual es posible, no hay opción de restauración directa. Una retención para litigio tampoco es un método efectivo para la recuperación ante ransomware.

Por el contrario, las soluciones de copia de seguridad SaaS de terceros ofrecen copias de seguridad independientes de los servidores de Microsoft, lo que garantiza una restauración de datos rápida y eficiente.

4 INTEGRACIONES DE TERCEROS

La integración de aplicaciones de terceros con Microsoft 365 mejora la funcionalidad, pero introduce riesgos adicionales.

Riesgos asociados con aplicaciones de terceros conectadas

Las aplicaciones de terceros pueden agregar conveniencia y aumentar la eficiencia. Sin embargo, se debe tener cuidado al integrar aplicaciones y extensiones de terceros. Muchas aplicaciones de terceros pueden ser útiles, pero no necesariamente confiables. Cuando otorga permiso a dichas aplicaciones para acceder y administrar los datos de su organización, pueden cifrar archivos o robar o exponer información confidencial.

Pérdida de datos a través de conexiones API

Las interfaces de programación de aplicaciones (API) que conectan aplicaciones pueden exponer inadvertidamente los datos a vulnerabilidades, conduciendo a un acceso no autorizado o a la pérdida de datos. Garantizar que las integraciones de terceros cumplan con las mejores prácticas de seguridad es crucial para mantener la integridad de los datos.

5 INTERRUPCIONES DEL SERVICIO Y TIEMPO DE INACTIVIDAD

A pesar de la confiabilidad de la infraestructura de Microsoft, aún pueden ocurrir interrupciones del servicio y tiempo de inactividad.

Interrupciones del servicio de Microsoft

En enero de 2024, Microsoft Teams, una popular aplicación de colaboración en equipo, experimentó una interrupción generalizada que afectó a miles de usuarios. Dichas interrupciones pueden detener las operaciones comerciales, afectando la productividad y la comunicación. Las interrupciones prolongadas del servicio de Microsoft 365 podrían provocar inaccesibilidad o pérdida de datos si no se ha realizado una copia de seguridad externa. Su empresa debe contar con planes de contingencia para gestionar y mitigar el impacto de las interrupciones inesperadas del servicio, garantizando la continuidad durante las operaciones críticas.

Inquietudes sobre la continuidad del negocio

Microsoft 365 proporciona una base sólida para la productividad y la colaboración, pero no está exento de riesgos. Los errores humanos, las fallas de software, las amenazas internas, las estafas de phishing y los ataques de ransomware representan una amenaza constante para su entorno de Microsoft 365, lo que podría provocar una posible pérdida de datos o interrumpir las operaciones comerciales. Según el informe Cost of a Data Breach de IBM de 2023, más del 80 % de las violaciones involucraron datos almacenados en entornos en la nube.

Mitigación de los puntos ciegos del respaldo

Para proteger sus datos en Microsoft 365 de manera efectiva, se deben adoptar estrategias integrales que vayan más allá de confiar en las funciones de seguridad nativas de Microsoft.

Estrategias integrales de respaldo

La implementación de soluciones confiables de copias de seguridad de terceros es crucial, ya que proporcionan opciones de recuperación de datos extendidas y protegen contra eliminaciones accidentales, errores programáticos y actividades maliciosas. Las soluciones de copia de seguridad de proveedores reconocidos como Datto SaaS Protection también ofrecen funciones avanzadas como opciones de recuperación granular y copias de seguridad automatizadas, lo que garantiza la integridad y disponibilidad de los datos.

Mejores prácticas de protección de datos

Las auditorías periódicas y la capacitación especializada de los empleados son vitales para fortalecer la seguridad general y la resiliencia de su entorno de Microsoft 365. Realizar auditorías de seguridad frecuentes ayuda a identificar y abordar las vulnerabilidades, garantizando el cumplimiento de las mejores prácticas y los requisitos normativos. Las auditorías deben cubrir controles de acceso, integraciones de terceros y políticas de gestión de datos.

Igualmente importante es construir una cultura de concientización acerca de la seguridad a través de programas continuos de capacitación para empleados. Educar al personal sobre cómo reconocer los intentos de suplantación de identidad, el manejo seguro de datos y la comprensión de la importancia de las medidas de seguridad les permite actuar como una primera línea de defensa contra posibles amenazas.

Política y gobernanza

Crear políticas sólidas de gobernanza de datos es esencial para proteger los datos en Microsoft 365 y cumplir con los estándares regulatorios. Esto incluye establecer pautas claras sobre la clasificación de datos, los controles de acceso y las políticas de retención. Una gobernanza eficaz de los datos lo ayuda a mantener la integridad de los datos, mitigar los riesgos asociados con las filtraciones de datos y cumplir con las regulaciones de la industria.

También es importante que alinee sus estrategias de respaldo con estas políticas de gobernanza y requisitos de cumplimiento. Las opciones de copia de seguridad nativas de Microsoft 365 a menudo no cumplen con los estrictos estándares normativos, como GDPR o HIPAA, que exigen períodos de retención específicos para los datos y la capacidad de restaurar datos desde momentos particulares en el tiempo. La implementación de soluciones integrales de copias de seguridad de terceros garantiza que su organización pueda cumplir con estos requisitos al permitirle retener datos durante períodos más prolongados y proporcionar un medio confiable para recuperar datos durante auditorías o investigaciones legales.

Evaluación de las soluciones de copia de seguridad de terceros

Las soluciones de copia de seguridad de terceros proporcionan políticas de retención más amplias, lo que permite la recuperación de datos más antiguos y la protección contra la pérdida de datos prolongada. También actúan como una red de seguridad, llenando las brechas que dejan las protecciones nativas y brindando la tranquilidad de que los datos comerciales críticos son seguros y recuperables en cualquier escenario. Estos son algunos criterios a considerar al evaluar soluciones de copia de seguridad de terceros para Microsoft 365.

Compatibilidad con Microsoft 365

Un factor crítico al seleccionar una solución de copia de seguridad es garantizar que una integración fluida con Microsoft 365. La solución debe admitir todas las aplicaciones principales, lo que incluye OneDrive, SharePoint, Exchange y Teams. Esta compatibilidad garantiza que todos los datos dentro del entorno cuenten con un respaldo adecuado y se puedan restaurar cuando sea necesario.

Características de seguridad

La seguridad es primordial al respaldar datos. Busque soluciones que ofrezcan métodos de cifrado sólidos tanto en tránsito como en reposo, protegiendo los datos del acceso no autorizado. Su solución de copia de seguridad debe incluir controles de acceso, lo que permite a los administradores definir quién puede acceder y administrar las copias de seguridad. Las opciones granulares de recuperación también son esenciales, al permitir la restauración de archivos o correos electrónicos específicos sin tener que realizar una recuperación completa. Otra característica importante son las copias de seguridad automatizadas, que garantizan una protección de datos consistente sin necesidad de intervención manual.

Facilidad de uso e implementación

Considere una solución de copia de seguridad que sea fácil de implementar y fácil de usar. Esto es esencial para mantener la productividad y evitar el tiempo de inactividad durante la fase de configuración. Una interfaz intuitiva reduce la curva de aprendizaje, lo que permite a sus equipos aprovechar todas las capacidades de la solución de copia de seguridad sin necesidad de extensos períodos de incorporación o capacitación.

Reputación y apoyo del proveedor

Es importante considerar la reputación del proveedor de las soluciones de copia de seguridad antes de cerrar el acuerdo. Asegúrese de buscar proveedores que tengan un historial sólido de protección de datos y reseñas positivas de parte de clientes satisfechos. Cuando se trata de protección y recuperación de datos, cada segundo importa. Por lo tanto, es fundamental brindar una asistencia confiable al cliente. Su proveedor de copias de seguridad debe ofrecer asistencia con la configuración, la resolución de problemas y los procesos de recuperación.

Otro factor crítico es la flexibilidad y la escalabilidad. A medida que su negocio se expande, sus requisitos de protección de datos también cambian. Busque un proveedor de copias de seguridad que ofrezca flexibilidad y escalabilidad, permitiendo que el sistema de copias de seguridad se amplíe de manera fluida a medida que aumenten los requisitos de datos de su organización. Esta adaptabilidad garantiza que su solución de respaldo siga siendo eficaz y se mantenga relevante con el tiempo.

Experimente la protección de datos de Microsoft 365 sin esfuerzo con Datto SaaS Protection

Dadas las posibles brechas de seguridad en Google Workspace, implementar una solución de copia de seguridad de terceros de vanguardia es una ventaja para las empresas que buscan fortalecer la seguridad general y la resiliencia de sus cargas de trabajo de misión crítica.

Datto SaaS Protection es una solución de copia de seguridad para Microsoft 365 para "configurar y olvidarse", ahorrándole tiempo, esfuerzo y dinero. Además de las opciones de recuperación granular y restauración a un momento determinado, nuestra solución también proporciona copias de seguridad automatizadas tres veces al día, lo que garantiza que sus datos críticos en todas sus aplicaciones clave estén actualizados y cuenten con una copia de seguridad constante. También tiene la opción de ejecutar copias de seguridad bajo demanda en cualquier momento.

Datto SaaS Protection es increíblemente fácil de usar. En solo cinco minutos, puede configurar y comenzar a proteger sus datos de Microsoft 365.

Datto SaaS Protection hace que recuperar datos perdidos sea rápido y fácil, no en semanas o días, sino a unos pocos clics de distancia.

Además, nuestro enfoque de seguridad multicapa ofrece una protección integral contra el ransomware y otras amenazas y permite una recuperación eficiente cuando sea necesario.

¿Está listo para tomar el control total de sus datos? **Vea la demostración interactiva** para descubrir cómo Datto SaaS Protection puede transformar la forma en que administra y protege sus datos de Microsoft 365.

REALIZAR UN RECORRIDO POR LOS PRODUCTOS

backupify
A Kaseya COMPANY

Oficina central corporativa
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131
partners@datto.com
www.datto.com
888.294.6312

Oficinas globales
EE. UU.: 888.294.6312
Canadá: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapur: +65-31586291

Julio de 2024