

Zero365

Backup & restauración de Microsoft 365 — Exchange, OneDrive, SharePoint, Teams & Entra ID

“Tus datos de Microsoft 365, tu storage.” — Recupera un buzón, un archivo o una identidad, sin vendor lock-in.

Servicio	Zero365 — Backup & restauración de Microsoft 365
Enfoque	Backup consciente de la carga de trabajo de Exchange, OneDrive, SharePoint, Teams y Entra ID en un storage que tú controlas
Versión	1.0
Fecha	Junio de 2026
Cobertura	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Proveedor	BackupSec

1. ¿Qué es Zero365?

Zero365 es un servicio de backup en la nube para Microsoft 365. Se conecta a tu tenant a través de Microsoft Graph y realiza el backup de Exchange Online, OneDrive, SharePoint Online, Microsoft Teams y Entra ID — cada uno con su propia semántica de restauración consciente de la carga de trabajo, no un volcado plano de archivos. Las copias cifradas se escriben en el storage que tú eliges y controlas (BYOS), y recuperas exactamente lo que necesitas — un mensaje, un archivo, un sitio o una identidad — desde una única consola. Zero365 es la capa de protección de Microsoft 365 de la familia BackupSec, junto con la monitorización de ZeroMON, la asesoría de ZeroTAM, el test de penetración de ZeroPEN y el storage inmutable de ZeroVault.

¿Por qué Zero365? La retención nativa de Microsoft no es un backup. Los elementos eliminados caducan, el ransomware cifra los archivos sincronizados y las identidades dadas de baja desaparecen. Zero365 mantiene una copia independiente y cifrada en un storage que tú controlas — recuperable elemento por elemento, mucho después de que expiren las propias papeleras de reciclaje de Microsoft.

La familia BackupSec

Zero365 funciona junto con el resto de la familia BackupSec:

Servicio	Función
ZeroMON	Monitorización & observabilidad de backup — visibilidad en tiempo real en todo tu parque Veeam
ZeroTAM	Asesoría experta, gestión de cuentas & soporte en crisis
ZeroPEN	Test de penetración de backups & prueba de recuperación — pone a prueba los backups como lo haría un atacante
Zero365	Backup & restauración de Microsoft 365 — Exchange, OneDrive, SharePoint, Teams, Entra ID (este documento)
ZeroVault	Cloud storage inmutable para Veeam — una última copia que no se puede eliminar ni cifrar

¿Para quién es?

- Equipos de IT y de mensajería responsables de la protección y recuperación de datos de Microsoft 365
- MSPs y proveedores de servicios que gestionan entornos multi-tenant de Microsoft 365
- Equipos de seguridad y riesgo que exigen una copia de backup independiente y cifrada
- Organizaciones con requisitos de residencia o soberanía de datos (bring your own storage)
- Equipos con obligaciones GDPR / KVKK / DORA / ISO 27001 para los datos de negocio

2. Catálogo de cobertura de cargas de trabajo

Cada carga de trabajo de Microsoft 365 se respalda con su propia semántica y su propia vía de restauración:

Carga de trabajo	Qué se protege	Restauración
Exchange Online	Correo, calendario, contactos y tareas de buzónes principales y compartidos — fidelidad MIME completa con sincronización delta.	Restauración a nivel de elemento o de buzón al buzón original o a uno alternativo; exportación EML/ZIP; vista previa antes de confirmar; no destructiva por defecto.
OneDrive	Jerarquía de la unidad, archivos, carpetas, historial de versiones y permisos / ACLs.	Restauración a un momento concreto y recuperación de ACL; modo <i>restaurar-solo-si-el-hash-difiere</i> para una recuperación quirúrgica frente a ransomware.
SharePoint Online	Bibliotecas de documentos y contenido estructurado basado en listas, incluidos los valores de columnas personalizadas.	Restauración que preserva los metadatos al sitio original o a uno alternativo; recuperación diferencial basada en hash.
Microsoft Teams	Canales estándar, privados y compartidos, además de chats 1:1 y de grupo.	Se restaura como paquetes de exportación estructurados (JSON con manifiestos); sin reproducción en vivo del canal — una limitación de la Graph API que declaramos con honestidad.
Entra ID	Usuarios, grupos, aplicaciones y service principals con pertenencia y propiedad.	Tres vías: recuperación por soft-delete (30 days), recreación completa del objeto o replay de propiedades vía PATCH; pertenencia a grupos solo de adición (add-only).

3. Despliegue & storage

Conexión	Microsoft Graph con autenticación moderna y un registro de aplicación — sin APIs heredadas.
Despliegue	Plataforma SaaS en contenedores con consola web; sin infraestructura de backup que tengas que gestionar tú mismo.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV o sistema de archivos local.
Cifrado	Payload cifrado escrito a través de Kopia; las claves de cifrado permanecen bajo tu control.
Programación	Backups programados y automatizados con sincronización incremental delta-first.
Alcance de cloud	Microsoft 365 comercial global y Entra ID. GCC, GCC High, DoD y 21Vianet no están dentro del alcance del lanzamiento.

Tus datos, tu storage. Los backups se escriben en cuentas de storage de tu propiedad — nunca en un repositorio con vendor lock-in. Como las claves de cifrado permanecen contigo, una copia de tus datos de Microsoft 365 nunca tiene que salir de tu jurisdicción.

4. Características principales

- Bring your own storage — S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Semántica de restauración consciente de la carga de trabajo por servicio
- Sincronización incremental delta-first
- Restauración a nivel de elemento y en bloque
- Vista previa antes de cada restauración
- Recuperación diferencial por hash frente a ransomware (OneDrive & SharePoint)
- Restauraciones no destructivas por defecto
- RBAC, SSO (SAML / OIDC) y MFA
- Registro de auditoría y exportación a SIEM
- Separación de funciones y acceso de restauración just-in-time

5. Qué obtienes

- 1 Un tenant de Microsoft 365 conectado con backups programados y conscientes de la carga de trabajo
- 2 Copias de backup cifradas en un storage de tu propiedad y bajo tu control (BYOS)
- 3 Un explorador de restauración para navegar, buscar, previsualizar y recuperar por carga de trabajo
- 4 Recuperación diferencial consciente de ransomware para OneDrive y SharePoint
- 5 Recuperación de identidad por tres vías para los objetos de Entra ID
- 6 Control de acceso, registro de auditoría y exportación a SIEM para la governance

6. Seguridad & cumplimiento

Marco	Cómo ayuda Zero365
GDPR	Una copia independiente y cifrada con un claro derecho a restaurar; los datos permanecen en un storage que tú controlas.
KVKK	Residencia de datos mediante bring-your-own-storage, con registro de accesos y separación de roles.
DORA	Resiliencia TIC — backups recuperables e independientes de los datos críticos de Microsoft 365.
ISO 27001	Control de acceso, cifrado y registro de auditoría alineados con los controles del Annex A.
SOC 2	Controles de seguridad, disponibilidad y confidencialidad en el backup y la restauración.

7. Siguiente paso

Inicia una prueba de Zero365. Conecta tu tenant, elige tu storage y observa cómo se ejecuta tu primer backup. Zero365 protege lo que la retención nativa de Microsoft no protege.
www.backupsec.com · info@backupsec.com · BackupSec