Porque un backup externo con Microsoft 365?

Microsoft 365 no está diseñado como una solución de backup, sino como una plataforma de productividad con mecanismos básicos de retención.

El propio modelo de Microsoft establece una responsabilidad compartida, donde:

Microsoft garantiza la disponibilidad del servicio
Pero el cliente es responsable de la protección y recuperación de sus datos

Esto implica que situaciones como:
Borrados accidentales o intencionados
Ataques de ransomware
Errores de sincronización
Eliminación de usuarios

pueden derivar en pérdida definitiva de información si no existe un backup externo.

brontobyte cloud

Propuesta de valor de un backup especializado

Soluciones como **Veeam Backup for Microsoft 365** aportan:

Seguridad real del dato (copia independiente)
Recuperación granular y rápida
Flexibilidad total en retención
Visibilidad y control centralizado
Protección frente a ransomware y errores humanos
Soporte al cumplimiento normativo (ISO 27001, ENS, NIS2)

En este contexto, y teniendo en cuenta las limitaciones del enfoque nativo de Microsoft en cuanto a protección real del dato, resulta clave analizar de forma clara qué nivel de seguridad, recuperación y control estamos garantizando a la organización.

No se trata únicamente de disponer de mecanismos básicos de retención, sino de asegurar la continuidad del negocio ante cualquier escenario: desde un error humano hasta un incidente de ciberseguridad o una necesidad de cumplimiento normativo.

A continuación, se presenta una comparativa directa entre las capacidades incluidas en Microsoft 365 y una solución de backup especializada como Veeam Backup for Microsoft 365, con el objetivo de identificar las diferencias reales y facilitar una toma de decisión informada.

Además, es importante tener en cuenta que la implantación de una solución de backup externo no solo aporta tecnología, sino también un componente clave de servicio. Contar con un **partner certificado Gold de Veeam como Brontobyte Cloud** permite complementar la herramienta con un servicio gestionado, acompañamiento experto y soporte especializado, garantizando no solo que el backup existe, sino que está correctamente configurado, supervisado y preparado para responder cuando realmente sea necesario.

brontobyte cloud

Análisis de protección y recuperación de datos en Microsoft 365

Aspecto clave	Microsoft 365 (nativo)	Backup externo (ej. Veeam)
Modelo de protección	Basado en retención y reciclaje, no es un backup real	Backup completo independiente (copia separada)
Responsabilidad del dato	Modelo de responsabilidad compartida (el cliente es responsable del dato)	Control total por parte del cliente
Protección ante borrado accidental	Limitada (papelera 1ª y 2ª fase, con caducidad)	Restauración granular sin límite de versiones mientras exista backup
Protección ante borrado malicioso	Vulnerable (si un usuario o admin elimina datos, pueden perderse definitivamente tras retención)	Recuperación incluso tras ataques internos o sabotaje
Protección ante ransomware	Limitada (depende de detección y retención)	Copias inmutables y aisladas (air-gap lógico)
Histórico de versiones	Limitado y dependiente de configuración	Versionado completo y configurable
Retención a largo plazo	Compleja y dependiente de políticas (compliance, eDiscovery)	Retención flexible sin depender de licencias avanzadas
Granularidad de recuperación	Limitada (según servicio: Exchange, SharePoint, OneDrive...)	Recuperación granular: emails, archivos, Teams, sitios completos, etc.
Recuperación ante eliminación de cuenta/licencia	Riesgo alto: al eliminar licencia, los datos pueden perderse	Datos protegidos independientemente del estado de la licencia
Exportación de datos	Compleja (requiere herramientas adicionales o scripting)	Exportación sencilla (PST, archivos, etc.)
Independencia del proveedor	Total dependencia de Microsoft	Copia independiente fuera de Microsoft
Protección ante errores de sincronización	No protegidos (errores se replican automáticamente)	Permite volver a estados anteriores
Visibilidad y control	Limitado (herramientas dispersas: Purview, Compliance, etc.)	Consola centralizada y reporting avanzado
Cumplimiento normativo (ISO, ENS, NIS2)	Puede ser insuficiente sin configuración avanzada	Facilita cumplimiento (retención, trazabilidad, control)
Tiempo de recuperación (RTO)	Variable y no garantizado	Definido y optimizable
Coste	Incluido en licencia (pero limitado)	Coste adicional, pero con valor en seguridad y continuidad