Dropsuite

Hoja de ventas

¿Su entorno de Microsoft 365 está realmente protegido?

Proteja más que su contenido. Asegure el acceso con Dropsuite Entra Backup.

Confía en su MSP para proteger su negocio, y así lo hace. Pero la mayoría no se da cuenta de que uno de los mayores riesgos en el entorno de la nube actual no son los archivos perdidos: es el acceso perdido.

Microsoft Entra ID (antes Azure AD) controla quién puede iniciar sesión, a qué puede acceder y qué aplicaciones o dispositivos son considerados confiables. Si estos ajustes de acceso se modifican, se eliminan o se ven comprometidos, incluso accidentalmente, puede paralizar sus operaciones.

¿Por qué es importante esto?

Las personas cometen errores

El error humano representa el 60 % de las brechas de datos.[1] Un solo clic equivocado de un miembro de su equipo puede bloquear usuarios, eliminar configuraciones clave o exponer su entorno a riesgos.

Los ciberataques apuntan a los sistemas de identidad

En un informe reciente, las credenciales robadas (22 %) y las vulnerabilidades explotadas (20 %) fueron los principales puntos de entrada.[1] Entra ID suele ser la primera víctima. Una vez dentro, los atacantes pueden desactivar políticas, eludir la autenticación multifactor (MFA) y tomar el control de aplicaciones sin ser detectados.

Microsoft no respalda esto completamente

Microsoft no ofrece recuperación total de las políticas o permisos eliminados en Entra ID. Sin una copia de seguridad, restaurar el acceso puede llevar horas o, en algunos casos, ser imposible.

Este nivel de interrupción importa: El 46 % de las pequeñas empresas sufrieron un ciberataque, y casi 1 de cada 5 tuvo que cerrar o declararse en quiebra.[2] Para las pequeñas empresas, incluso unas pocas horas de inactividad pueden ser devastadoras, porque solo una hora puede costar hasta 100 000 dólares en pérdidas de productividad, ingresos y gastos de recuperación.[3]

¿Qué puede salir mal sin Entra Backup?

> *"Las eliminaciones accidentales y errores de configuración ocurrirán en su inquilino. Para minimizar el impacto de estos eventos no deseados, debe prepararse para que sucedan."*[4]
>
> **- Microsoft**

Cuando los sistemas de identidad no están protegidos, las interrupciones son rápidas y severas:

- Una política de acceso condicional eliminada bloquea a su fuerza laboral remota.
- Un cambio accidental en las reglas de cumplimiento de dispositivos impide que los portátiles se conecten.
- Un atacante desactiva la aplicación de MFA, y nadie se da cuenta hasta que ya es demasiado tarde.
- No tiene registro de qué administrador hizo los cambios, lo que dificulta las investigaciones.

Sin una copia de seguridad, solucionar estos problemas puede llevar horas, interrumpir las operaciones y erosionar la confianza de los clientes.

Proteja el sistema que protege todo lo demás

Su MSP ya realiza copias de seguridad de correos electrónicos y archivos. Pero Entra Backup añade una capa vital para proteger las reglas de acceso y políticas de seguridad que mantienen su negocio en marcha. Con Entra Backup, su MSP puede ayudarle a:

- **Recupérese rápidamente** después de un error o ataque
- **Evite tiempos de inactividad** causados por pérdida de acceso o errores de configuración
- **Proteja a su personal, dispositivos y aplicaciones** contra el uso no autorizado
- **Mantenga la conformidad** conservando un registro completo de los cambios en identidad y acceso

No espere a que se pierda el acceso

Hable con su MSP sobre Dropsuite Entra Backup, porque proteger sus datos también significa proteger el acceso.

1. Verizon, *Data Breach Investigations Report*, 2025.
2. Mastercard, *ciberseguridad para pequeñas empresas*, 2025.
3. ITIC, *informe sobre tiempos de inactividad de servidores y aplicaciones*, 2022.
4. Microsoft, *prácticas recomendadas en recuperabilidad*, 2024.