WHITEPAPER

RGPD y Microsoft 365: Controles técnicos

Guía de implementación de controles técnicos para cumplimiento RGPD en entornos Microsoft 365.

Kwadrant Systems — Marzo 2026

El RGPD exige medidas técnicas y organizativas para proteger datos personales. Microsoft 365 ofrece las herramientas, pero la responsabilidad de configurarlas correctamente es de la organización. Este documento detalla los controles técnicos que se deben implementar.

1. Modelo de responsabilidad compartida

Microsoft es responsable de la seguridad de la infraestructura cloud (centros de datos, red, hardware). El cliente es responsable de la seguridad de sus datos, identidades, dispositivos y configuración de servicios.

Responsabilidad	Microsoft	Cliente
Infraestructura física	Sí	No
Red y conectividad	Sí	Parcial
Sistema operativo host	Sí	No
Identidad y acceso	Herramientas	Configuración
Datos y clasificación	Herramientas	Configuración
Dispositivos de usuario	No	Sí
Configuración de servicios	No	Sí

2. Controles técnicos obligatorios

2.1 Control de acceso (Art. 32.1.b)

Implementar medidas que garanticen que solo personas autorizadas acceden a datos personales.

- ✓ MFA obligatorio para todos los usuarios
- ✓ Acceso condicional por ubicación, dispositivo y riesgo
- ✓ Privilegios mínimos: cada usuario accede solo a lo que necesita
- ✓ Revisiones periódicas de accesos (Access Reviews)
- ✓ Bloqueo automático de cuentas tras intentos fallidos

2.2 Cifrado (Art. 32.1.a)

Los datos personales deben estar cifrados en tránsito y en reposo.

- ✓ TLS 1.2+ para datos en tránsito (por defecto en M365)
- ✓ BitLocker en dispositivos Windows con Intune
- ✓ FileVault en dispositivos macOS con Intune
- ✓ Cifrado de mensajes con OME cuando sea necesario
- ✓ Etiquetas de sensibilidad con cifrado automático

2.3 Prevención de fuga (Art. 5.1.f)

Medidas para evitar que datos personales salgan sin autorización.

- ✓ Políticas DLP en Exchange, Teams y SharePoint
- ✓ Reglas de detección de datos sensibles (DNI, tarjetas, IBAN)
- ✓ Bloqueo de reenvío automático a dominios externos
- ✓ Restricción de descarga en dispositivos no gestionados
- ✓ Control de Shadow IT con Defender for Cloud Apps

2.4 Registro de actividad (Art. 30)

Mantener registros de quién accede a datos personales y qué hace con ellos.

- ✓ Auditoría unificada activada en Purview
- ✓ Registro de accesos a buzones de correo
- ✓ Registro de accesos a sitios de SharePoint
- ✓ Alertas de actividad sospechosa configuradas
- ✓ Retención de logs mínimo 1 año

2.5 Derecho de supresión (Art. 17)

Capacidad técnica para localizar y eliminar datos personales a petición del interesado.

- ✓ Content Search en Purview para localizar datos
- ✓ eDiscovery para búsquedas avanzadas y exportación
- ✓ Políticas de retención para eliminación automática
- ✓ Procedimiento documentado de respuesta a solicitudes

3. Documentación para auditorías

Los controles técnicos deben estar documentados y ser demostrables. Kwadrant entrega:

- • Informe de configuración con capturas de cada control implementado
- • Registro de actividades de tratamiento (Art. 30) adaptado
- • Evaluación de impacto (DPIA) cuando el tratamiento lo requiera
- • Plan de respuesta a brechas con plantillas de notificación a la AEPD
- • Acta de pruebas de recuperación de backup

Contacto: kwadrant.es — Evaluación de cumplimiento RGPD gratuita