CHECKLIST

Checklist: Seguridad en Microsoft 365

10 controles esenciales que toda empresa debería tener configurados.

Kwadrant Systems — Marzo 2026

Este documento lista los controles de seguridad fundamentales para un entorno Microsoft 365. Cada control incluye su descripción, por qué es importante y dónde se configura. Utilice las casillas para verificar el estado de su entorno.

1. Autenticación multifactor (MFA)

Activar MFA para todos los usuarios sin excepción. Es la medida más efectiva contra el robo de credenciales. Un atacante con tu contraseña no puede acceder sin el segundo factor.

> ***Dónde:*** *Entra ID → Seguridad → Autenticación multifactor*
>
> ***Requisito:*** *Security Defaults o Conditional Access (según licencia)*

■ Verificado en nuestro entorno

---

2. Acceso condicional

Definir políticas que controlen desde dónde y cómo se accede a los recursos corporativos. Bloquear accesos desde ubicaciones geográficas no habituales, dispositivos no gestionados o sesiones de alto riesgo.

> ***Dónde:*** *Entra ID → Protección → Acceso condicional*
>
> ***Requisito:*** *Entra ID P1 o superior*

■ Verificado en nuestro entorno

---

3. Protección anti-phishing

Configurar políticas avanzadas de anti-phishing en Defender for Office 365. Incluye protección contra suplantación de identidad (impersonation), safe links y safe attachments.

Dónde: *Security Portal → Políticas de amenazas → Anti-phishing*

Requisito: *Defender for Office 365 P1 o superior*

■ Verificado en nuestro entorno

---

4. Gestión de dispositivos

Inscribir los dispositivos corporativos en Intune. Aplicar políticas de compliance: cifrado obligatorio (BitLocker/FileVault), PIN de bloqueo, versión mínima de SO, antivirus activo.

Dónde: *Endpoint Manager → Dispositivos → Políticas de cumplimiento*

Requisito: *Intune (incluido en M365 Business Premium)*

■ Verificado en nuestro entorno

---

5. Prevención de fuga de datos (DLP)

Crear reglas que detecten y bloqueen el envío no autorizado de información sensible (números de tarjeta, DNIs, datos médicos) por correo, Teams o SharePoint.

Dónde: *Purview → Prevención de pérdida de datos → Políticas*

Requisito: *M365 E3/E5 o Purview add-on*

■ Verificado en nuestro entorno

---

6. Etiquetado de sensibilidad

Clasificar y etiquetar documentos y correos electrónicos según su nivel de confidencialidad. Las etiquetas pueden aplicar cifrado y restricciones de acceso automáticamente.

Dónde: *Purview → Information Protection → Etiquetas*

Requisito: *M365 E3/E5 o Azure Information Protection P1*

■ Verificado en nuestro entorno

---

7. Auditoría unificada

Activar el registro unificado de auditoría para rastrear qué hacen los usuarios y administradores: accesos a archivos, cambios de permisos, envío de correos, acciones administrativas.

Dónde: *Purview → Auditoría → Habilitar*

Requisito: *Incluido en todos los planes M365 (retención varía)*

■ Verificado en nuestro entorno

---

8. Alertas de actividad sospechosa

Configurar alertas automáticas para eventos críticos: inicios de sesión desde ubicaciones inusuales, envíos masivos de correo, elevación de privilegios, creación de reglas de reenvío.

Dónde: *Security Portal → Alertas → Políticas de alerta*

Requisito: *Incluido en M365 Business Premium y E3/E5*

■ Verificado en nuestro entorno

---

9. Backup independiente

Implementar backup de terceros para Exchange Online, OneDrive, SharePoint y Teams. Microsoft no ofrece backup granular con retención a largo plazo. La responsabilidad de los datos es del cliente.

Dónde: *Solución de terceros (Veeam, AvePoint, etc.)*

Requisito: *Licencia independiente del proveedor de backup*

■ Verificado en nuestro entorno

---

10. Revisión periódica de accesos

Programar revisiones trimestrales de quién tiene acceso a qué. Eliminar cuentas inactivas, revocar permisos innecesarios, revisar roles de administrador. Usar Access Reviews de Entra ID cuando la licencia lo permita.

> ***Dónde:*** *Entra ID → Gobernanza de identidades → Revisiones de acceso*
>
> ***Requisito:*** *Entra ID P2 para Access Reviews automatizadas*
>
> ■ Verificado en nuestro entorno

Siguiente paso

Si su entorno no cumple con 3 o más de estos controles, recomendamos un diagnóstico de seguridad. Kwadrant ofrece una evaluación inicial gratuita del entorno Microsoft 365.

Contacto: kwadrant.es — Diagnóstico gratuito sin compromiso