

# Microsoft 365 Security Check

MÁS VISIBILIDAD  
MÁS CONTROL  
UN NEGOCIO  
MÁS SEGURO

Análisis, hallazgos y plan de acción  
para un entorno más seguro



Cliente  
**Nombre de la empresa**



Fecha del informe  
**22 de septiembre de 2026**



Referencia  
**M365-SC-2026-001**

## APLICACIONES ANALIZADAS



Outlook



Teams



Word



Excel



PowerPoint



OneDrive



SharePoint



Entra ID



Microsoft 365

Convertimos la información  
en decisiones que protegen  
tu negocio.

## ÍNDICE

# Contenido del informe

Una visión completa de la seguridad de tu entorno Microsoft 365, con hallazgos, análisis y un plan de acción claro y priorizado.

|    |                                                                                          |         |
|----|------------------------------------------------------------------------------------------|---------|
| 01 | <b>Resumen ejecutivo</b><br>Principales conclusiones, nivel de riesgo y recomendaciones  | Pág. 03 |
| 02 | <b>Alcance del análisis</b><br>Entorno evaluado, áreas incluidas y fuentes de evidencia  | Pág. 04 |
| 03 | <b>Postura de seguridad</b><br>Resultado global y puntuación por áreas                   | Pág. 05 |
| 04 | <b>Hallazgos principales</b><br>Riesgos críticos, altos, medios y bajos                  | Pág. 06 |
| 05 | <b>Análisis por áreas</b><br>Resultados detallados de cada área evaluada                 | Pág. 07 |
| 06 | <b>Plan de acción prioritario</b><br>Qué corregir, prioridad, esfuerzo y recomendaciones | Pág. 11 |
| 07 | <b>Anexo técnico</b><br>Detalle de controles, evidencias y metodología                   | Pág. 12 |

## MICROSOFT 365 SECURITY CHECK

### FICHA DEL ANÁLISIS



Cliente  
**Empresa Ejemplo, S.L.**



Tenant analizado  
**empresa.onmicrosoft.com**



Fecha del análisis  
**15 – 22 de septiembre de 2026**



Tipo de análisis  
**Business**



Áreas evaluadas  
**7**



Controles ejecutados  
**48**



Estado  
**Finalizado**



### Cómo leer este informe

Este informe presenta los resultados del análisis de seguridad de tu entorno Microsoft 365, realizado por OLATIC.

Los hallazgos se clasifican según su nivel de riesgo y prioridad de actuación. Cuando no existe evidencia suficiente para evaluar un control, se identifica como "No evaluado" y nunca se considera automáticamente seguro.

El objetivo de este informe es proporcionarte una visión clara y accionable para mejorar la seguridad de tu organización.

**"La seguridad no es un destino,  
es un proceso continuo."**

Información  
para decisiones  
**más seguras.**

MICROSOFT 365  
SECURITY CHECK

## 01. RESUMEN EJECUTIVO

# Una visión clara de tu seguridad en Microsoft 365

Hemos analizado tu entorno de Microsoft 365 para identificar riesgos, configuraciones mejorables y oportunidades de mejora. A continuación se presenta un resumen de los resultados más relevantes.



Más visibilidad.  
Más control.  
Un entorno más seguro.

Convertimos la información en decisiones que protegen tu negocio.

## Security Score global



Nivel de riesgo

**Medio**

Tu entorno presenta una base sólida, pero existen riesgos relevantes que deben ser priorizados.

## Hallazgos por severidad

3

**Críticos**

Requieren atención inmediata

7

**Altos**

Deben abordarse a corto plazo

14

**Medios**

Se recomienda su revisión y mejora

9

**Bajos**

Buenas prácticas y ajustes menores



1.248

Identidades analizadas



687

Aplicaciones revisadas



516

Permisos analizados



320

Dispositivos evaluados



48

Controles ejecutados

## Principales conclusiones

1

### Superficie de identidad expuesta

Se han detectado cuentas con privilegios elevados y métodos de autenticación mejorables.

2

### Aplicaciones con permisos excesivos

Existen aplicaciones y service principals con permisos amplios y sin propietario.

3

### Protección del correo y colaboración

Configuraciones de seguridad mejorables en Exchange Online, SharePoint y OneDrive.

4

### Cumplimiento y configuración general

Se han identificado desviaciones respecto a buenas prácticas de Microsoft y controles recomendados.

## Acciones prioritarias

Estas son las acciones que recomendamos abordar en primer lugar:

**Crítico**

### Revisar cuentas con privilegios globales

Reducir el número de cuentas con rol Global Administrator.

**Crítico**

### Aplicaciones sin propietario

Revisar y asignar propietario o eliminar aplicaciones no utilizadas.

**Alto**

### Mejorar la protección del correo

Revisar políticas anti-phishing, anti-spam y reglas de reenvío.

**Alto**

### Revisar permisos de aplicaciones

Reducir permisos innecesarios en aplicaciones y service principals.

**Medio**

### Reforzar la autenticación multifactor (MFA)

Extender MFA a todos los usuarios y revisar métodos de autenticación.

02. ALCANCE DEL ANÁLISIS

# Qué hemos **analizado** y cómo lo hemos hecho

Este informe se basa en el análisis de la configuración de tu entorno Microsoft 365, utilizando herramientas de análisis y mejores prácticas de seguridad reconocidas.



## Objetivo

Identificar riesgos, evaluar la postura de seguridad y proporcionar recomendaciones prácticas y priorizadas para mejorar la protección de tu organización.

## Áreas incluidas en el análisis

|  |                                                                                       |   |
|--|---------------------------------------------------------------------------------------|---|
|  | <b>Identidades y accesos</b><br>Usuarios, grupos, roles y métodos de autenticación.   | > |
|  | <b>Privilegios</b><br>Roles con privilegios elevados y accesos administrativos.       | > |
|  | <b>Aplicaciones y permisos</b><br>Aplicaciones empresariales y service principals.    | > |
|  | <b>Exchange Online</b><br>Correo, antispam, anti-phishing y reglas.                   | > |
|  | <b>SharePoint, OneDrive y Teams</b><br>Colaboración, compartición y acceso externo.   | > |
|  | <b>Dispositivos y acceso</b><br>Estado de dispositivos y políticas de acceso.         | > |
|  | <b>Configuración general</b><br>Políticas de seguridad, cumplimiento y configuración. | > |

## Metodología

- 1 Recopilación de datos**  
Conexión segura a tu tenant de Microsoft 365 y extracción de configuración y evidencias.
- 2 Análisis y evaluación**  
Revisión de controles de seguridad, comparación con mejores prácticas (Microsoft, CIS, NIST).
- 3 Clasificación de hallazgos**  
Identificación y priorización según nivel de riesgo, impacto y probabilidad.
- 4 Elaboración del informe**  
Presentación de resultados, conclusiones y recomendaciones prácticas.

## Información del entorno analizado

|  |                             |                                                                                 |
|--|-----------------------------|---------------------------------------------------------------------------------|
|  | <b>Tenant</b>               | empresa.onmicrosoft.com                                                         |
|  | <b>Número de usuarios</b>   | 1.248                                                                           |
|  | <b>Periodo de análisis</b>  | 15 – 22 de septiembre de 2026                                                   |
|  | <b>Tipo de análisis</b>     | Business                                                                        |
|  | <b>Fuentes de evidencia</b> | Microsoft Graph API, configuración del tenant, registros y políticas aplicables |



## Limitaciones

Este análisis se basa en la información accesible mediante permisos de lectura y en las fuentes disponibles en el momento de la evaluación.

- No se incluyen análisis de dispositivos locales.
- No se ha realizado testing de ingeniería social.
- La ausencia de datos no implica que el control sea seguro.
- Algunos hallazgos pueden requerir validación adicional en el entorno.



## Resultados fiables

Utilizamos fuentes oficiales y metodologías reconocidas para garantizar la precisión de los resultados.

## 03. POSTURA DE SEGURIDAD

# Resultado global y por áreas

Tu organización presenta una buena base de seguridad, con áreas clave bien configuradas, pero también riesgos relevantes que deben ser abordados para mejorar la postura general.

## Security Score



Nivel de riesgo

**Medio**

La configuración actual reduce significativamente el riesgo, pero se han identificado áreas críticas de mejora que requieren atención prioritaria.



## En resumen

Tienes una base sólida, pero existen riesgos que podrían ser aprovechados por amenazas actuales. Abordar las recomendaciones de este informe te permitirá mejorar tu nivel de seguridad y reducir la superficie de exposición.



La seguridad no es un destino, es un proceso continuo de mejora.

OLATIC

## Puntuación por áreas

Resultado obtenido en cada área analizada sobre 100 puntos.

● ≥ 80 (Bueno) | ● 50 – 79 (Mejorable) | ● < 50 (Crítico)

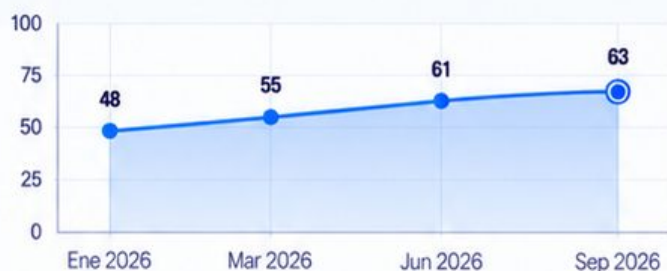
Identidades  
y accesos**58**

Privilegios

**42**Aplicaciones  
y permisos**51**Exchange  
Online**78**SharePoint  
OneDrive y Teams**66**Dispositivos  
y acceso**71**Configuración  
general**85**

## Evolución del Security Score

Comparativa con análisis anteriores (si aplica).



## Principales insights

- 1 Mejora la gestión de cuentas con privilegios elevados.
- 2 Revisa las aplicaciones con permisos amplios o sin propietario.
- 3 Refuerza la protección del correo frente a phishing y spam.
- 4 Mantén una monitorización continua de cambios y actividad inusual.

04. HALLAZGOS PRINCIPALES

# Riesgos que requieren tu atención

Se han identificado 34 hallazgos relevantes en tu entorno Microsoft 365, de los cuales 10 son críticos o de alta severidad. A continuación, se muestran los principales riesgos y su impacto.



## 10 hallazgos críticos o altos

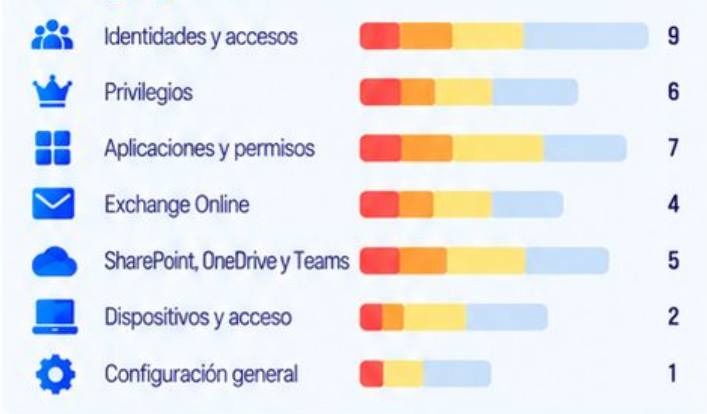
Requieren atención en el corto plazo para reducir la exposición a amenazas y mejorar la seguridad del entorno.

La mayoría de los riesgos están relacionados con identidades, permisos y configuraciones de seguridad.

### Hallazgos por severidad



### Hallazgos por área



### Top 5 hallazgos más relevantes

| # | Hallazgo                                                | Severidad | Área                         | Impacto                                           | Recomendación                                         |
|---|---------------------------------------------------------|-----------|------------------------------|---------------------------------------------------|-------------------------------------------------------|
| 1 | Cuentas con privilegios de administrador global sin MFA | Crítico   | Identities and access        | Alto riesgo de compromiso total del tenant.       | Habilitar MFA y revisar necesidad de privilegios.     |
| 2 | Aplicaciones con permisos excesivos                     | Crítico   | Applications and permissions | Acceso amplio a datos de la organización.         | Revisar permisos y eliminar accesos innecesarios.     |
| 3 | Cuentas inactivas con privilegios                       | Alto      | Privileges                   | Posible uso no autorizado en caso de compromiso.  | Revisar y deshabilitar cuentas inactivas.             |
| 4 | Políticas de correo anti-phishing no optimizadas        | Alto      | Exchange Online              | Mayor riesgo de phishing y suplantación.          | Revisar y reforzar políticas de seguridad del correo. |
| 5 | Aplicaciones sin propietario                            | Medio     | Applications and permissions | Riesgo de permisos no controlados y uso indebido. | Asignar propietario o eliminar aplicaciones.          |



### Conclusión

Los hallazgos identificados representan oportunidades claras de mejora en la seguridad de tu entorno Microsoft 365. Abordar en primer lugar los riesgos críticos y altos permitirá reducir significativamente la exposición y mejorar la resiliencia de la organización.

“La seguridad se construye con acciones, no con intenciones.”

05. ANÁLISIS POR ÁREAS

# Detalle de resultados por cada área de evaluación

A continuación se muestran los resultados obtenidos en cada área analizada, con su puntuación, principales hallazgos y recomendaciones.



Cada área, una oportunidad de mejora

El análisis por áreas permite identificar con precisión dónde se concentran los riesgos y qué acciones aportarán un mayor impacto en la seguridad global de tu entorno.

| Área                                                                                                                                                                 | Puntuación                                                                                            | Estado                                                                                                      | Principales hallazgos                                                                                                                                                                                        | Recomendaciones clave                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Identidades y accesos</b><br>Usuarios, grupos, roles y autenticación             |  <b>58</b><br>/100   | <ul style="list-style-type: none"><li>2 Críticos</li><li>3 Altos</li><li>5 Medios</li><li>2 Bajos</li></ul> | <ul style="list-style-type: none"><li>Cuentas con privilegios globales sin MFA.</li><li>Cuentas inactivas con permisos elevados.</li><li>Políticas de contraseñas mejorables.</li></ul>                      | <ul style="list-style-type: none"><li>Habilitar MFA en todas las cuentas privilegiadas.</li><li>Revisar y deshabilitar cuentas inactivas.</li><li>Aplicar políticas de acceso condicional por riesgo.</li></ul>             |
|  <b>Privilegios</b><br>Roles y accesos administrativos                               |  <b>42</b><br>/100  | <ul style="list-style-type: none"><li>3 Críticos</li><li>2 Altos</li><li>1 Medio</li><li>0 Bajos</li></ul>  | <ul style="list-style-type: none"><li>Exceso de cuentas con rol Global Administrator.</li><li>Falta de revisión periódica de privilegios.</li><li>Roles innecesarios asignados.</li></ul>                    | <ul style="list-style-type: none"><li>Reducir el número de cuentas con privilegios globales.</li><li>Implementar revisiones periódicas de roles.</li><li>Aplicar el principio de mínimo privilegio.</li></ul>               |
|  <b>Aplicaciones y permisos</b><br>Aplicaciones empresariales y service principals |  <b>51</b><br>/100 | <ul style="list-style-type: none"><li>2 Críticos</li><li>3 Altos</li><li>4 Medios</li><li>1 Bajo</li></ul>  | <ul style="list-style-type: none"><li>Aplicaciones sin propietario.</li><li>Permisos excesivos en service principals.</li><li>Consentimientos de tenant amplio sin justificación.</li></ul>                  | <ul style="list-style-type: none"><li>Revisar permisos y eliminar accesos innecesarios.</li><li>Asignar propietario a todas las aplicaciones.</li><li>Monitorizar nuevos consentimientos de alto impacto.</li></ul>         |
|  <b>Exchange Online</b><br>Correo, antispam y reglas                               |  <b>78</b><br>/100 | <ul style="list-style-type: none"><li>0 Críticos</li><li>1 Alto</li><li>3 Medios</li><li>1 Bajo</li></ul>   | <ul style="list-style-type: none"><li>Reglas de reenvío externas sin control.</li><li>Falta de protección avanzada en algunos buzones.</li><li>Configuración antispam mejorable.</li></ul>                   | <ul style="list-style-type: none"><li>Revisar reglas de reenvío y acceso externo.</li><li>Habilitar protección avanzada (Safe Links, Safe Attachments).</li><li>Revisar y ajustar políticas antispam.</li></ul>             |
|  <b>SharePoint, OneDrive y Teams</b><br>Colaboración y acceso externo              |  <b>66</b><br>/100 | <ul style="list-style-type: none"><li>1 Crítico</li><li>2 Altos</li><li>4 Medios</li><li>2 Bajos</li></ul>  | <ul style="list-style-type: none"><li>Sitios con acceso externo amplio.</li><li>Compartición de archivos sin caducidad.</li><li>Falta de etiquetas de sensibilidad en algunos contenidos.</li></ul>          | <ul style="list-style-type: none"><li>Revisar accesos externos y aplicar restricciones.</li><li>Definir caducidad en enlaces compartidos.</li><li>Implementar etiquetas de sensibilidad y DLP.</li></ul>                    |
|  <b>Dispositivos y acceso</b><br>Estado de dispositivos y políticas de acceso      |  <b>71</b><br>/100 | <ul style="list-style-type: none"><li>1 Crítico</li><li>2 Altos</li><li>3 Medios</li><li>1 Bajo</li></ul>   | <ul style="list-style-type: none"><li>Dispositivos sin cumplimiento de políticas.</li><li>Equipos sin cifrado.</li><li>Acceso desde ubicaciones inusuales sin restricciones.</li></ul>                       | <ul style="list-style-type: none"><li>Aplicar políticas de cumplimiento de dispositivos.</li><li>Habilitar cifrado en todos los equipos.</li><li>Revisar y ajustar políticas de acceso condicional.</li></ul>               |
|  <b>Configuración general</b><br>Políticas, cumplimiento y seguridad del tenant    |  <b>85</b><br>/100 | <ul style="list-style-type: none"><li>0 Críticos</li><li>1 Alto</li><li>2 Medios</li><li>1 Bajo</li></ul>   | <ul style="list-style-type: none"><li>Algunas políticas de seguridad no activadas.</li><li>Configuración de auditoría mejorable.</li><li>Oportunidades de alineación con recomendaciones CIS/NIST.</li></ul> | <ul style="list-style-type: none"><li>Activar políticas recomendadas de Microsoft.</li><li>Revisar configuración de auditoría y retención de logs.</li><li>Avanzar en la adopción de buenas prácticas (CIS/NIST).</li></ul> |



## Conclusión del análisis por áreas

El análisis muestra una base sólida en la mayoría de áreas, con oportunidades de mejora significativas en identidades, privilegios y aplicaciones. Abordar estas áreas permitirá reducir el riesgo global y mejorar la resiliencia de la organización.

“La mejora continua en seguridad empieza por conocer tu situación actual.”

06. PLAN DE ACCIÓN PRIORITARIO

# De los hallazgos a la acción

Estas son las recomendaciones prioritarias para reducir el riesgo en tu entorno Microsoft 365. Se han seleccionado en base a su impacto en la seguridad, la probabilidad de ocurrencia y el esfuerzo de implementación.



## Resultados medibles

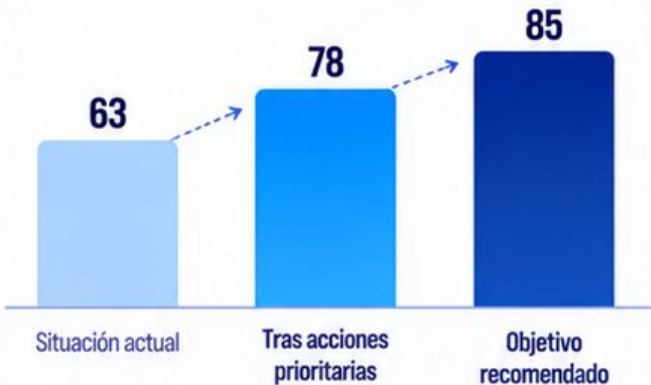
La aplicación de estas acciones te permitirá mejorar tu Security Score, reducir la exposición a amenazas y avanzar hacia un entorno más seguro y resiliente.

### Acciones prioritarias

| # | Acción recomendada                                            | Área                                                                                                             | Prioridad      | Impacto esperado                            | Esfuerzo     | Plazo                    |
|---|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|----------------|---------------------------------------------|--------------|--------------------------|
| 1 | Habilitar MFA en todas las cuentas privilegiadas              |  Identidades y accesos          | <b>Crítico</b> | Reduce el riesgo de compromiso del tenant   | <b>Bajo</b>  | Inmediato (0-30 días)    |
| 2 | Revisar y eliminar aplicaciones sin propietario               |  Aplicaciones y permisos       | <b>Crítico</b> | Evita accesos no controlados a datos        | <b>Medio</b> | Corto plazo (0-60 días)  |
| 3 | Revisar permisos excesivos en aplicaciones                    |  Aplicaciones y permisos      | <b>Alto</b>    | Reduce la superficie de exposición          | <b>Medio</b> | Corto plazo (0-60 días)  |
| 4 | Reforzar la protección del correo (anti-phishing y anti-spam) |  Exchange Online              | <b>Alto</b>    | Disminuye el riesgo de suplantación         | <b>Medio</b> | Corto plazo (0-60 días)  |
| 5 | Revisar políticas de compartición en SharePoint y OneDrive    |  SharePoint, OneDrive y Teams | <b>Medio</b>   | Evita fugas de información no intencionadas | <b>Bajo</b>  | Medio plazo (60-90 días) |

### Impacto en el Security Score

La implementación de estas acciones puede incrementar significativamente tu puntuación de seguridad.



### Próximos pasos

- 1 Validar y priorizar las acciones con tu equipo.
- 2 Definir responsables y planificación.
- 3 Ejecutar las acciones y realizar seguimiento.
- 4 Reevaluar la postura de seguridad tras la implementación.



### Pequeñas acciones. Grandes resultados.

La seguridad es un proceso continuo. Cada mejora cuenta.

## 07. CONCLUSIONES Y PRÓXIMOS PASOS

# Una base sólida para seguir avanzando

El análisis muestra que tu organización cuenta con una buena base de seguridad en Microsoft 365, pero existen áreas de mejora que requieren atención prioritaria. La implementación de las acciones recomendadas permitirá reducir el riesgo, mejorar la resiliencia y avanzar hacia un entorno más seguro y preparado.

“La seguridad no se alcanza con un único proyecto, sino con una mejora continua y una estrategia bien definida.

OLATIC



## Reducir el riesgo

Abordar los hallazgos críticos y altos para disminuir la exposición a amenazas.



## Mejorar la postura

Implementar las recomendaciones para aumentar el Security Score y la resiliencia.



## Protección continua

Establecer procesos de monitorización y revisión periódica de la configuración.



## Acompañamiento

Contar con un partner especializado para implementar las mejoras y resolver dudas.

### Resumen de indicadores clave

Situación actual y objetivo tras la implementación de las acciones.



### Próximos pasos recomendados

- 1 Revisar y validar el informe con los equipos implicados.
- 2 Priorizar las acciones según impacto y esfuerzo.
- 3 Definir un plan de implementación y responsables.
- 4 Ejecutar las acciones y realizar seguimiento.
- 5 Programar una nueva evaluación para medir la evolución.



#### Reevaluación recomendada

Se recomienda realizar una nueva evaluación en un plazo de 3 a 6 meses para medir el progreso y detectar nuevas oportunidades de mejora.

— OLATIC

Transformamos la tecnología  
en un negocio más seguro.

Personas  
Tecnología  
Confianza

08. ANEXO TÉCNICO

# Detalle de controles y evidencias

A continuación, se muestra el detalle de los controles evaluados, con su resultado, nivel de riesgo y evidencia obtenida. Este anexo proporciona una visión completa de la configuración analizada en tu entorno Microsoft 365.

TECNOLOGÍA  
SEGURIDAD  
TU NEGOCIO  
MÁS FUERTE



## Controles ejecutados

48

- 31 Correctos
- 10 Con incidencias
- 7 No aplicables

Cada control incluye la evidencia obtenida y, en su caso, recomendaciones específicas para su remediación.

|                                    |                         |                                           |                              |                                              |                                 |                                    |
|------------------------------------|-------------------------|-------------------------------------------|------------------------------|----------------------------------------------|---------------------------------|------------------------------------|
| <br>Identities and access<br>8 / 8 | <br>Privileges<br>6 / 7 | <br>Applications and permissions<br>7 / 9 | <br>Exchange Online<br>6 / 6 | <br>SharePoint, OneDrive and Teams<br>8 / 10 | <br>Devices and access<br>4 / 5 | <br>General configuration<br>6 / 6 |
|------------------------------------|-------------------------|-------------------------------------------|------------------------------|----------------------------------------------|---------------------------------|------------------------------------|

### Ejemplo de controles evaluados

| ID    | Control                                      | Área          | Resultado  | Riesgo | Evidencia                                       |
|-------|----------------------------------------------|---------------|------------|--------|-------------------------------------------------|
| ID-01 | MFA habilitado para administradores globales | Identidades   | Correcto   | Bajo   | Captura de configuración en Entra ID >          |
| ID-05 | Cuentas inactivas (> 90 días)                | Identidades   | Incidencia | Alto   | Listado de cuentas inactivas (12) >             |
| PR-02 | Roles innecesarios asignados                 | Privilegios   | Incidencia | Alto   | Export de roles en Entra ID >                   |
| AP-03 | Aplicaciones sin propietario                 | Aplicaciones  | Incidencia | Alto   | Listado de aplicaciones (678 sin propietario) > |
| EX-01 | Políticas anti-phishing                      | Exchange      | Correcto   | Bajo   | Captura de políticas EOP >                      |
| SH-04 | Compartición externa en SharePoint           | SharePoint    | Parcial    | Medio  | Captura de configuración de compartición >      |
| DV-02 | Dispositivos sin cifrado                     | Dispositivos  | Incidencia | Alto   | Informe de cumplimiento (Intune) >              |
| CF-01 | Auditoría unificada habilitada               | Configuración | Correcto   | Bajo   | Captura de configuración de auditoría >         |



## Sobre la evidencia

Toda la evidencia incluida en este informe ha sido obtenida de forma automatizada a través de Microsoft Graph y las APIs de Microsoft 365. Las capturas y listados se incluyen como soporte de los resultados y pueden ser ampliados bajo solicitud.



## Evidencias completas

Puedes solicitar el detalle completo de todas las evidencias y exportaciones generadas durante el análisis.



Solicitar evidencias

## 09. BUENAS PRÁCTICAS

# Recomendaciones para un entorno más seguro

Además de las acciones específicas derivadas de los hallazgos, te recomendamos aplicar estas buenas prácticas para mejorar la seguridad de tu entorno Microsoft 365 y reducir el riesgo de futuras incidencias.

“

La prevención y la mejora continua son la mejor defensa frente a las amenazas actuales y futuras.

OLATIC

1



## Refuerza la identidad

Habilita MFA en todas las cuentas, aplica políticas de acceso condicional y revisa periódicamente los permisos y roles asignados.

2



## Minimiza privilegios

Aplica el principio de mínimo privilegio, elimina cuentas y roles innecesarios y revisa los accesos con privilegios elevados.

3



## Controla las aplicaciones

Revisa las aplicaciones con permisos en tu tenant, elimina las que no sean necesarias y controla los consentimientos de alto impacto.

4



## Protege el correo

Implementa políticas anti-phishing y anti-spam, habilita Safe Links y Safe Attachments y forma a los usuarios en buenas prácticas.

5



## Protege la información

Clasifica la información, aplica etiquetas de sensibilidad y revisa los permisos de acceso a SharePoint, OneDrive y Teams.

6



## Gestiona los dispositivos

Asegura que todos los dispositivos estén enrolados y cumplan las políticas de seguridad (Intune), con cifrado y configuración segura.

7



## Mantén la configuración

Revisa y aplica las recomendaciones de seguridad de Microsoft, mantén la auditoría habilitada y monitoriza los cambios relevantes.

8



## Monitoriza y revisa

Establece revisiones periódicas del Security Score, analiza los nuevos hallazgos y adapta las políticas a la evolución de tu organización.



## Beneficios esperados

La aplicación de estas recomendaciones te permitirá:



Menor exposición a amenazas



Mayor resiliencia del negocio



Cumplimiento normativo



Entorno más seguro y productivo



## Siguiente revisión

Te recomendamos realizar una nueva evaluación en un plazo de 3 a 6 meses para medir el progreso de las acciones implementadas, identificar nuevos hallazgos y seguir mejorando la postura de seguridad de tu entorno Microsoft 365.

## 10. CIERRE Y VALOR PARA TU ORGANIZACIÓN

# Más seguridad hoy para un mejor mañana

Este análisis te proporciona una visión clara de la situación actual de tu entorno Microsoft 365, identifica los principales riesgos y te ofrece un plan de acción realista para mejorar tu postura de seguridad, reducir la exposición a amenazas y aumentar la resiliencia de tu organización.

“

La seguridad no es un destino, es un proceso continuo. Evaluar, mejorar y adaptarse es clave para afrontar los retos de hoy y del futuro.

OLATIC

## Principales beneficios



### Menor riesgo

Reducción de la probabilidad de incidentes y de su impacto en el negocio.



### Mayor resiliencia

Una organización más preparada para detectar, responder y recuperarse ante amenazas.



### Cumplimiento normativo

Alineación con buenas prácticas (CIS, NIST) y requisitos regulatorios.



### Más confianza

Protección de la información, los usuarios y la reputación de tu organización.

— OLATIC

## Personas Tecnología Confianza

Acompañamos a tu organización en el camino hacia un entorno digital más seguro.



PREVENIR



DETECTAR



MEJORAR

## Próximos pasos

1

Revisar el informe con tu equipo



2

Priorizar las acciones



3

Definir un plan de implementación



4

Realizar seguimiento y nueva evaluación



### ¿Hablamos?

Estamos a tu disposición para resolver cualquier duda y ayudarte a implementar las mejores recomendaciones.

— OLATIC

## La seguridad de hoy impulsa el mañana.

Contáctanos



info@olatic.es



944 362 257



www.olatic.es

Hablemos de tu seguridad

