

Guía de Seguridad de las TIC CCN-STIC 885A

Guía de configuración segura para Office 365



MAYO 2024





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-177-0

Fecha de Edición: mayo de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

| | |
|--|-----------|
| 1. OFFICE 365 | 4 |
| 1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA | 4 |
| 1.2 DEFICIÓN DE LA SOLUCIÓN | 4 |
| 1.3 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL..... | 5 |
| 2. DESPLIEGUE DE OFFICE 365 | 7 |
| 2.1 ADMINISTRADOR – CONFIGURACION INICIAL..... | 7 |
| 2.2 USUARIO FINAL – PRIMEROS PASOS..... | 11 |
| 3. CONFIGURACIÓN DE OFFICE 365 | 13 |
| 3.1 MARCO OPERACIONAL..... | 13 |
| 3.1.1 CONTROL DE ACCESO | 13 |
| 3.1.1.1 IDENTIFICACIÓN..... | 13 |
| 3.1.1.2 REQUISITOS DE ACCESO | 27 |
| 3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS | 27 |
| 3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO | 36 |
| 3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS) | 36 |
| 3.1.1.6 MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN) | 42 |
| 3.1.2 EXPLOTACIÓN | 42 |
| 3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO..... | 42 |
| 3.1.2.2 GESTIÓN DE INCIDENTES | 44 |
| 3.1.2.3 REGISTRO DE LA ACTIVIDAD | 46 |
| 3.2 MEDIDAS DE PROTECCIÓN..... | 49 |
| 3.2.1 PROTECCIÓN DE LAS COMUNICACIONES..... | 49 |
| 3.2.2 MONITORIZACIÓN DEL SISTEMA..... | 49 |
| 3.2.3 PROTECCIÓN DE LA INFORMACIÓN | 55 |
| 3.2.3.1 CALIFICACIÓN DE LA INFORMACIÓN | 55 |
| 3.2.3.2 LIMPIEZA DE DOCUMENTOS..... | 84 |
| 3.2.3.3 COPIAS DE SEGURIDAD..... | 84 |
| 3.2.4 PROTECCIÓN DE LOS SERVICIOS | 85 |
| 3.2.4.1 PROTECCIÓN FRENTE A DENEGACIÓN DE SERVICIO | 85 |
| 4. OTRAS CONSIDERACIONES DE SEGURIDAD | 86 |
| 4.1 SERVICIOS Y COMPLEMENTOS..... | 86 |
| 5. CARACTERÍSTICAS DISPONIBLES POR LICENCIAMIENTO | 87 |
| 6. GLOSARIO Y ABREVIATURAS | 89 |
| 7. ANEXO A. CREAR UNA CUENTA DE USUARIO INDIVIDUAL | 91 |
| 8. ANEXO B. CREAR VARIAS CUENTAS DE USUARIO | 92 |
| 9. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD | 94 |

1. OFFICE 365

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración de Office 365 cumpliendo con los requisitos Esquema Nacional de Seguridad en su categoría ALTA.

En esta guía se abordarán los **servicios esenciales comunes** a todos los servicios de la solución informática Office 365 y debe consultarse juntamente con el resto de las guías específicas de cada servicio: Sharepoint Online [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online], Exchange Online [CCN-STIC-885C - Guía de configuración segura para Exchange Online] y Teams [CCN-STIC-885D - Guía de configuración segura para Microsoft Teams].

El escenario que se presenta en las guías es el de “sólo nube”, no contemplándose la hibridación de sistemas On-premises de la organización con entorno Cloud.

Para la confección de esta guía se han consultado las siguientes fuentes:

- Documentación oficial de Microsoft.
- CCN-STIC-884A - Guía de configuración segura para Azure.
- ENS Real Decreto BOE-A-2010-1330.
- ENS Real Decreto BOE-A-2022-7191.

1.2 DEFICIÓN DE LA SOLUCIÓN

Office 365 es un conjunto de aplicaciones y servicios basados en la nube alojados en servidores propiedad de Microsoft y disponibles desde dispositivos con conexión a Internet. Office 365 funciona sobre Entra ID.



Se trata de una solución de Microsoft que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint desde cualquier dispositivo que tenga acceso a internet.

Además de proporcionar herramientas adicionales de correo electrónico, mensajería instantánea, videoconferencias, pantallas compartidas, almacenamiento en la nube, calendarios, contactos, etc.

1.3 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL

PowerShell de Office 365 permite administrar la configuración de Office 365 desde la línea de comandos. Conectarse a PowerShell de Office 365 es un proceso sencillo que consiste en instalar el software necesario y conectarse a la organización de Office 365.

Hay tres versiones del módulo de PowerShell que puede usarse para conectarse a Office 365 y administrar cuentas de usuario, grupos y licencias:

- a) *Microsoft Azure Active Directory PowerShell para Graph* (los cmdlets incluyen Azure AD en su nombre).
- b) *Microsoft Azure Active Directory para Windows PowerShell* (los cmdlets incluyen MSOL en su nombre).
- c) *Microsoft Graph PowerShell* (los cmdlets incluyen MG en su nombre).

El día 30 de marzo del 2024, los módulos *Microsoft Azure Active Directory PowerShell para Graph* y *Módulo Microsoft Azure Active Directory para Windows PowerShell* fueron deprecados y sustituidos por *Microsoft Graph PowerShell*. Esto no significa que no se puedan utilizar, si no que al estar deprecados dejarán de recibir actualizaciones.

Conviene destacar que existen dos caminos para la ejecución de los comandos de PowerShell descritos en esta guía: Azure Cloud Shell, incluido en el propio portal de Entra ID; y ejecución remota de PowerShell, instalando los módulos necesarios en el equipo cliente del administrador. La seguridad para la conexión con *Microsoft Graph*, se hace desde:

- a) Autenticación inicial. Mediante un usuario, Token y Certificado digital con los derechos adecuados para la administración del servicio.
- b) Cifrado continuo de la comunicación. Una vez completada la autenticación inicial, el protocolo de comunicación remota de PowerShell cifra toda la comunicación con una clave simétrica AES256 por sesión.

Requerimientos previos

Usar una versión de 64 bits de Windows. Es necesario así mismo, usar la versión 7 o posterior de PowerShell. Más información sobre requerimientos previos de plataformas en: [Install the Microsoft Graph PowerShell SDK | Microsoft Learn](#)

Instalar módulo Microsoft Graph PowerShell

Estos pasos son necesarios una sola vez en el equipo, no cada vez que se conecta. Sin embargo, probablemente se necesitará instalar las versiones más recientes de software periódicamente.

- a) Instalar el Módulo *Microsoft Graph PowerShell* para Windows siguiendo estos pasos:
 1. Abrir un símbolo del sistema de Windows PowerShell con privilegios elevados (ejecute Windows PowerShell como administrador).

2. Ejecutar el comando:

```
Install-Module Microsoft.Graph -Scope CurrentUser
```

- b) Para actualizar una nueva versión del módulo ejecutar el comando anterior con el parámetro Force:

```
Update-Module Microsoft.Graph
```

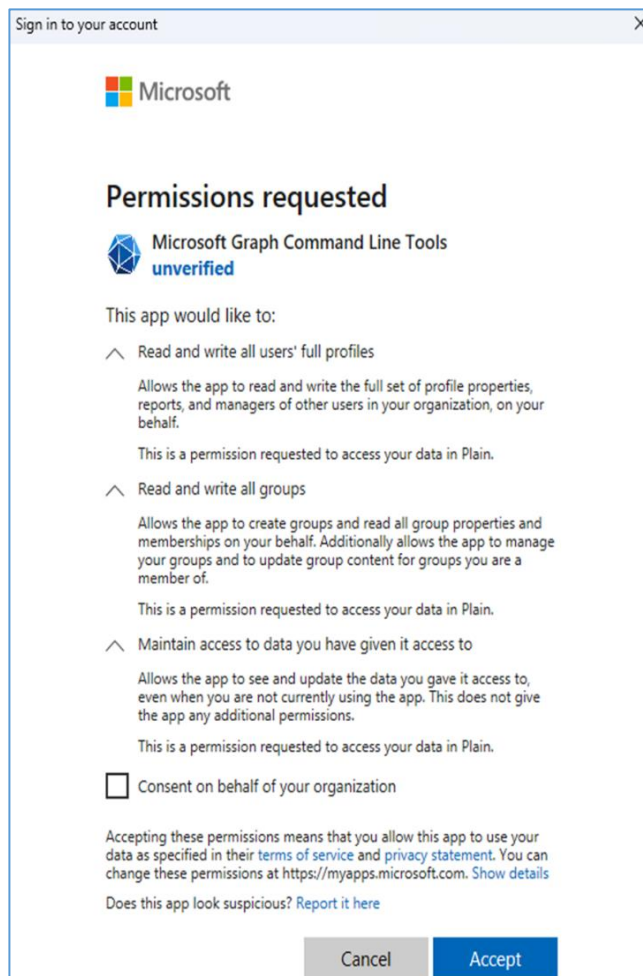
Nota: Se recomienda realizar actualizaciones mensuales.

- c) Conectarse a Microsoft Graph

Para conectarse a Microsoft Graph tenemos varios métodos, por usuario y contraseña, token, certificado, etc. El método más rápido es:

```
Connect-MgGraph -Scopes "User.Readwrite.All"
```

La etiqueta -Scope se refiere a los permisos que tendrá el usuario cuando haga login, en este ejemplo son de lectura y escritura de usuarios. Existen más métodos de login con este comando, para obtener más información, revisar el enlace [Connect-MgGraph](#).



Una vez ejecutado el comando anterior nos saldrá esta ventana, pidiendo permisos sobre el tenant, click en Aceptar.

2. DESPLIEGUE DE OFFICE 365

Esta guía hace referencia a la configuración de seguridad de Office 365. La información específica de cada servicio se encuentra en las siguientes guías: Sharepoint Online [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online], Exchange Online [CCN-STIC-885C - Guía de configuración segura para Exchange Online] y Teams [CCN-STIC-885D - Guía de configuración segura para Microsoft Teams].

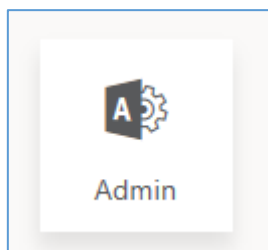
Office 365 se encuentra englobado en la categoría de servicio SaaS (Software as a Service). El CSP (Microsoft) es el encargado de ofrecer al cliente el software como un servicio.

2.1 ADMINISTRADOR – CONFIGURACION INICIAL

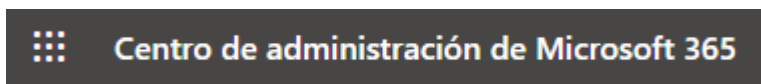
a) Acceder al portal de Office 365 con usuario administrador.

El usuario administrador podrá acceder al portal Office 365 a través de esta URL que el usuario final: portal.office365.com.

Al crear la suscripción de Office 365, Microsoft envía un correo con el usuario y una password temporal que deberá cambiarse en el primer login.

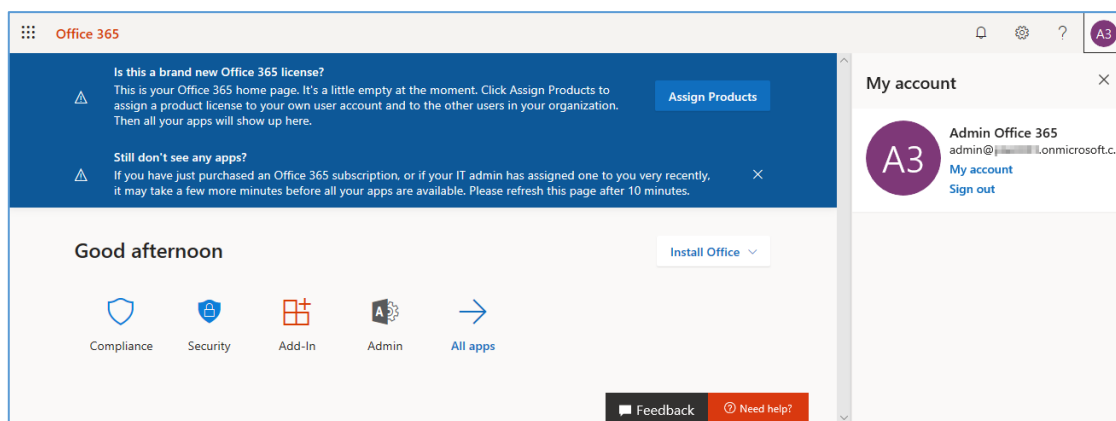


Además de las aplicaciones a las que tiene acceso según su licencia, cuenta con un icono de administración, para acceder al **Centro de Administración de Microsoft 365**.



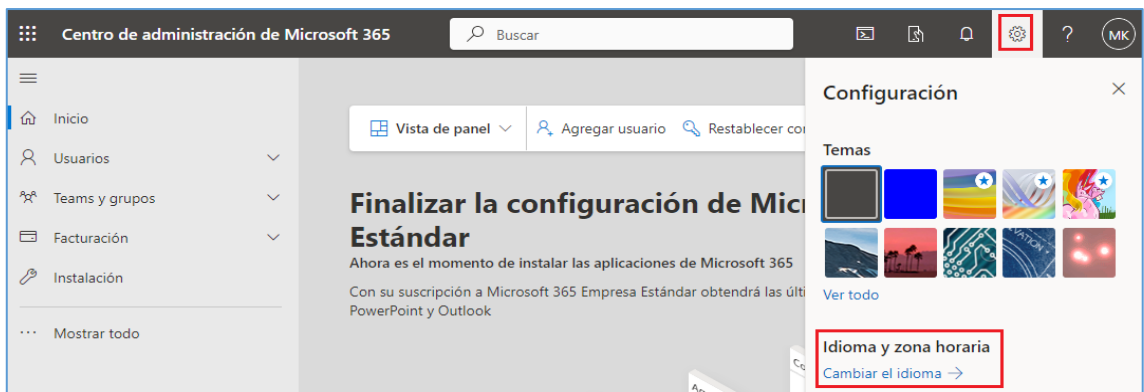
La primera vez que se accede al portal de Office 365 como administrador, puede aparecer un mensaje como el de la figura de abajo. Se muestra cuando aún no se han asignado licencias de productos a los usuarios de la organización.

La asignación de licencias a usuarios se realiza desde el Centro de administración de Microsoft 365.



b) Cambiar el idioma a español.

Se accede desde el icono de Configuración de la barra superior del portal.



Click en *Idioma y zona horaria*.



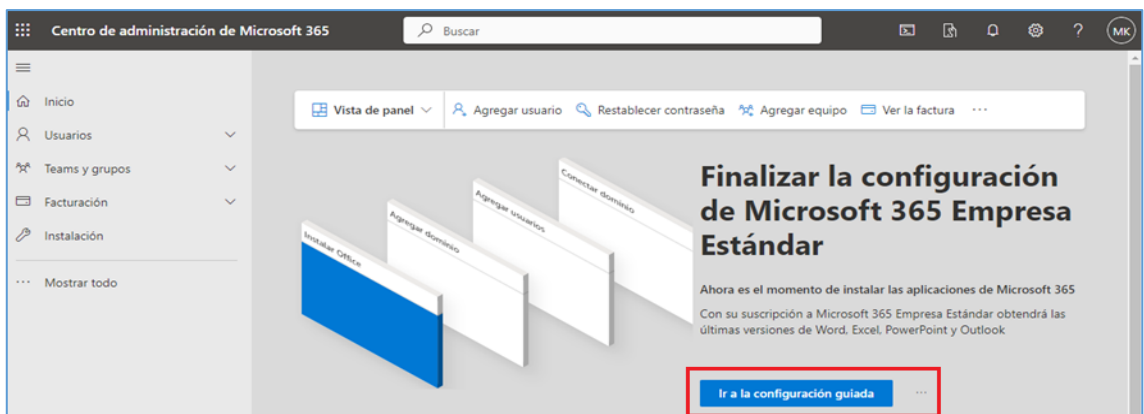
Click en Cambiar idioma para mostrar y seleccionamos el idioma.

c) Acceder al Centro de Administración de Microsoft 365.

Se accede a través del icono Admin del portal de Office 365 o bien mediante la url: admin.microsoft.com.

Si es la primera que se accede al panel aparecerá el siguiente mensaje indicando el terminar la configuración de 365. Es este ejemplo tenemos la licencia **M365 Empresa Estándar**.

Pulsar el botón “Ir a la configuración guiada”:



1. Instalar Microsoft 365

Una vez dentro de la configuración, dará la opción de instalar las aplicaciones del paquete office. En el caso de querer instalarlas, simplemente hacer click en el botón de descargar.



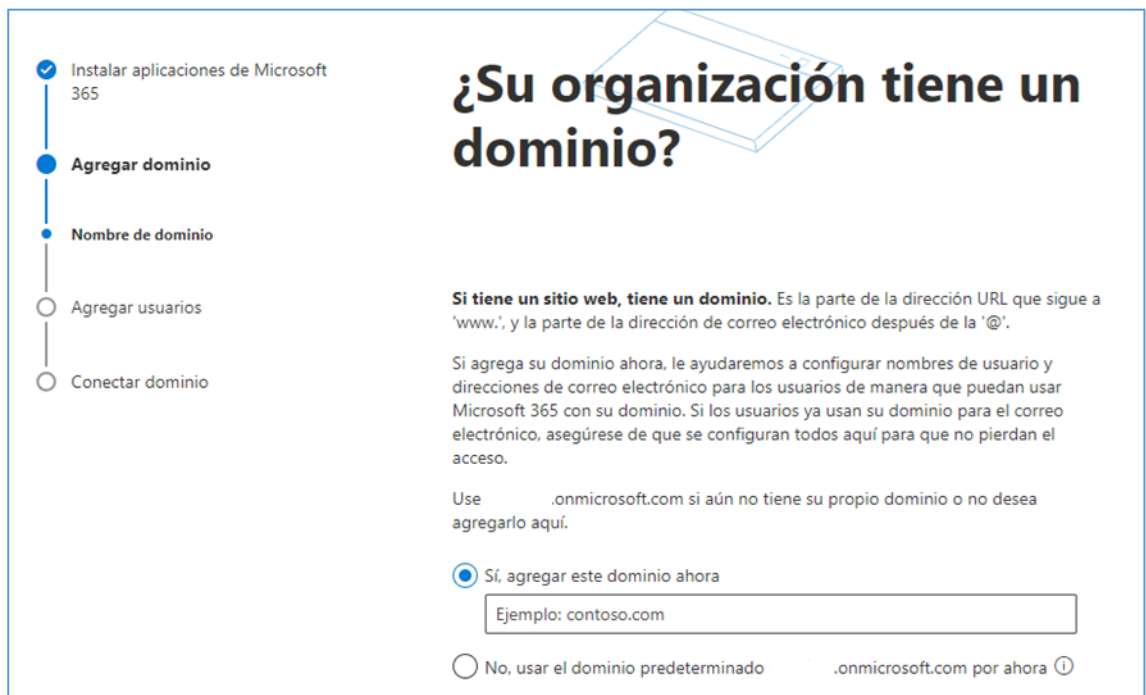
The screenshot shows the 'Instalar Microsoft 365' screen. On the left, a vertical progress bar has four steps: 'Instalar aplicaciones de Microsoft 365' (selected with a blue dot), 'Agregar dominio', 'Agregar usuarios', and 'Conectar dominio'. The main heading is 'Instalar Microsoft 365'. Below it, a paragraph explains that the user can download and install Microsoft 365 for their device, and that selecting an option will assign a license. A button labeled 'Aplicaciones de Microsoft 365' with a download icon and a list of applications (Word, Excel, PowerPoint, OneNote, Outlook) is visible.

En el caso de que querer omitir este paso, hacer click en “Continuar”.

Continuar

2. Configuración de un dominio personalizado

Se recomienda la personalización con un dominio propio de la organización.



The screenshot shows the '¿Su organización tiene un dominio?' screen. The progress bar on the left has five steps: 'Instalar aplicaciones de Microsoft 365' (checked), 'Agregar dominio' (selected with a blue dot), 'Nombre de dominio', 'Agregar usuarios', and 'Conectar dominio'. The main heading is '¿Su organización tiene un dominio?'. Below it, a paragraph explains that if the user has a website, they have a domain, and that adding a domain now will help configure user names and email addresses. A radio button is selected for 'Sí, agregar este dominio ahora', with a text input field containing 'Ejemplo: contoso.com'. Another radio button is for 'No, usar el dominio predeterminado .onmicrosoft.com por ahora'.

3. Agregar nuevos usuarios

Para la asignación de licencias a los usuarios que se especifiquen en este paso.



Instalar aplicaciones de Microsoft 365

Agregar dominio

Agregar usuarios

Conectar dominio

Agregar usuarios y asignar licencias

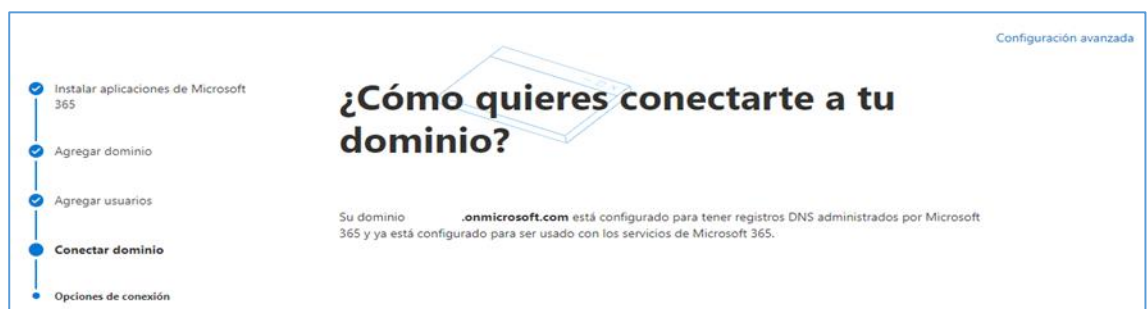
Total de licencias de Microsoft 365 Empresa: 25
 Licencias restantes: 24
 A los usuarios que agregue aquí se les asignará una licencia de Microsoft 365 Empresa. [Ver todos los usuarios](#)

Para reemplazar Plain255.onmicrosoft.com, retroceda y agregue su propio dominio. Agregue su dominio antes de agregar usuarios para no tener que configurar los dos veces.

| Nombre | Apellidos | Nombre de usuario |
|----------------------|----------------------|---|
| <input type="text"/> | <input type="text"/> | <input type="text"/> @255.onmicrosoft.com |
| <input type="text"/> | <input type="text"/> | <input type="text"/> @255.onmicrosoft.com |
| <input type="text"/> | <input type="text"/> | <input type="text"/> @255.onmicrosoft.com |
| <input type="text"/> | <input type="text"/> | <input type="text"/> @255.onmicrosoft.com |
| <input type="text"/> | <input type="text"/> | <input type="text"/> @255.onmicrosoft.com |

Envía las contraseñas de nuevos usuarios a mi dirección de correo electrónico.

4. Fin del proceso de instalación.



Configuración avanzada

Instalar aplicaciones de Microsoft 365

Agregar dominio

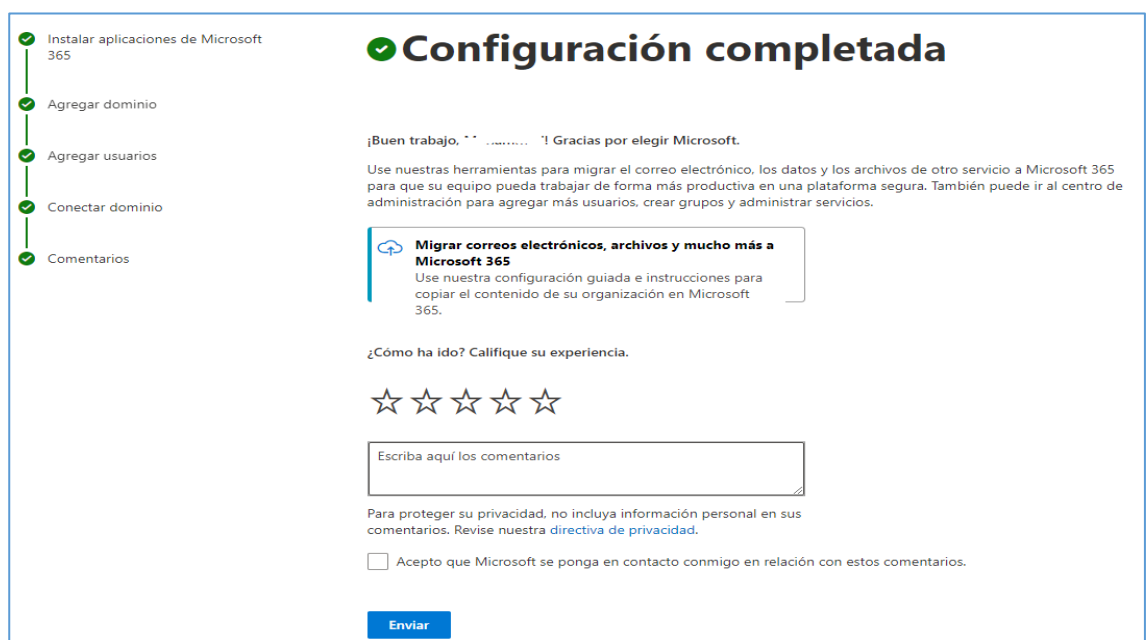
Agregar usuarios

Conectar dominio

Opciones de conexión

¿Cómo quieres conectarte a tu dominio?

Su dominio .onmicrosoft.com está configurado para tener registros DNS administrados por Microsoft 365 y ya está configurado para ser usado con los servicios de Microsoft 365.



Instalar aplicaciones de Microsoft 365

Agregar dominio

Agregar usuarios


Conectar dominio

Comentarios

Configuración completada

¡Buen trabajo, ** ! Gracias por elegir Microsoft.

Use nuestras herramientas para migrar el correo electrónico, los datos y los archivos de otro servicio a Microsoft 365 para que su equipo pueda trabajar de forma más productiva en una plataforma segura. También puede ir al centro de administración para agregar más usuarios, crear grupos y administrar servicios.

 **Migrar correos electrónicos, archivos y mucho más a Microsoft 365**
 Use nuestra configuración guiada e instrucciones para copiar el contenido de su organización en Microsoft 365.

¿Cómo ha ido? Califique su experiencia.

☆☆☆☆☆

Escriba aquí los comentarios

Para proteger su privacidad, no incluya información personal en sus comentarios. Revise nuestra [directiva de privacidad](#).

Acepto que Microsoft se ponga en contacto conmigo en relación con estos comentarios.

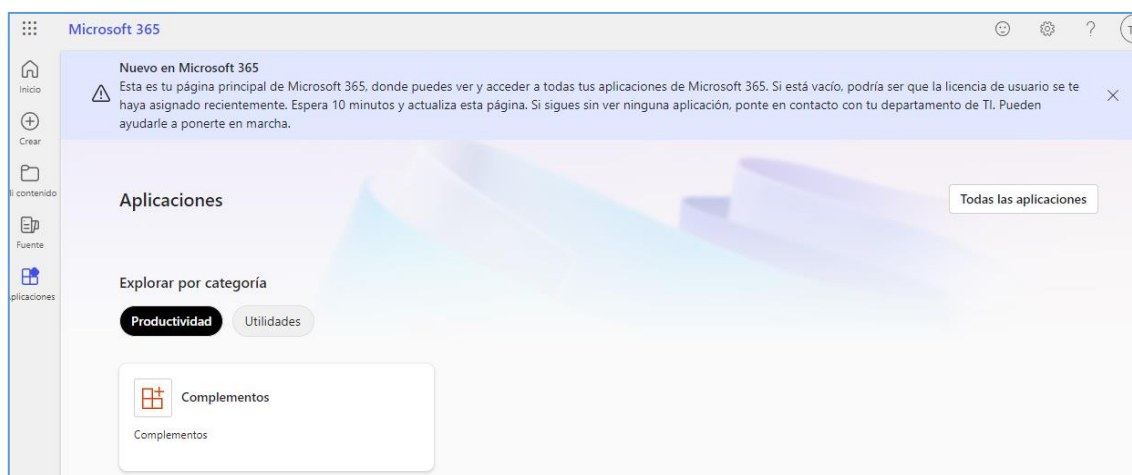
Enviar

Información más detallada de cómo añadir usuarios y licencias en el apartado [3.1.1 Control de acceso] de la presente guía.

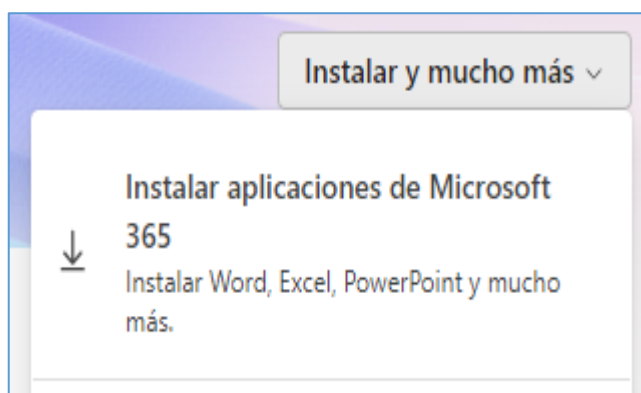
2.2 USUARIO FINAL – PRIMEROS PASOS

El usuario final podrá acceder al portal Office 365 a través de la url: portal.office365.com. Tras introducir las credenciales se muestra un panel con todas las aplicaciones a las que tiene acceso.

En algunas ocasiones, si la licencia de usuario no ha sido asignada correctamente, podría aparecer el siguiente mensaje de aviso:

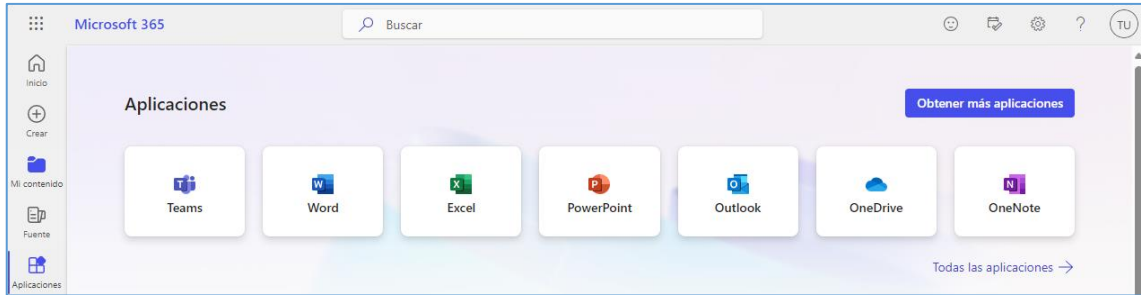


Desde el propio panel de Office 365 se permite instalar la versión de escritorio de las aplicaciones.

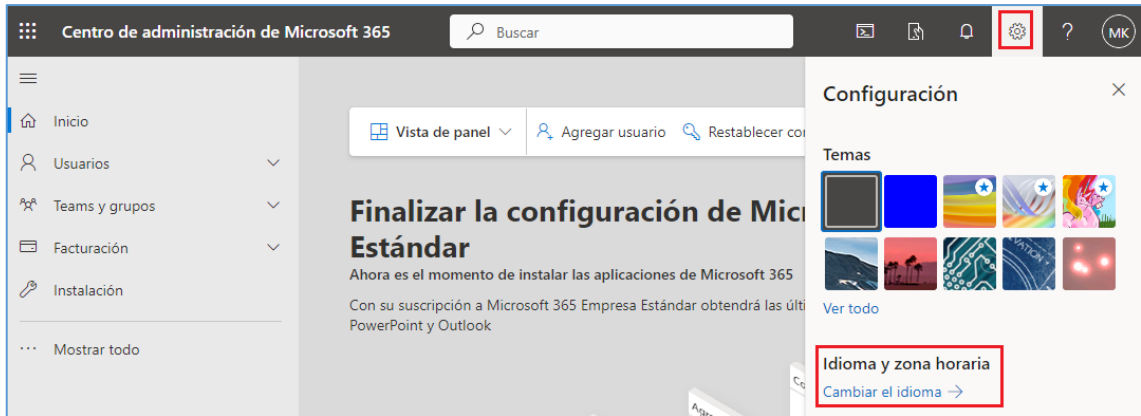


Nota: Para la configuración de seguridad de la versión de escritorio de las aplicaciones Office remitirse a la Guía CCN-STIC más actualizada (CCN-STIC-585 en el momento de edición de la presente guía).

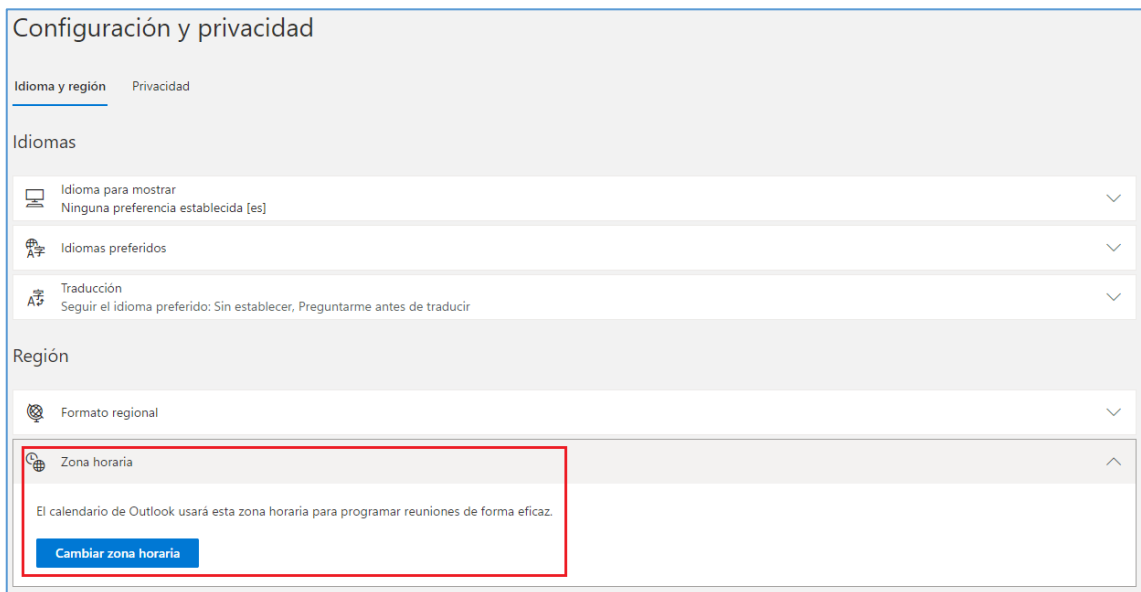
Una vez asignadas la licencia al usuario final, y tras logarse en el portal de Office 365, se mostrará una página de inicio con los iconos de todas las aplicaciones a las que se tiene acceso.



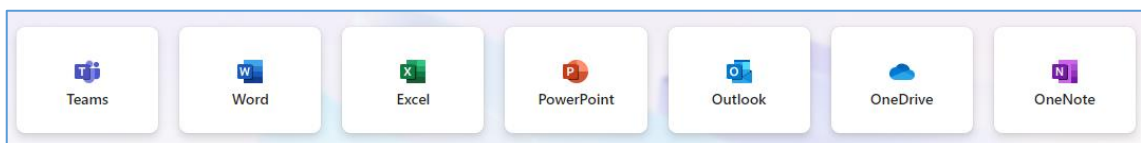
Es aconsejable establecer el idioma y la zona horaria.



Click en Idioma y región.



Es posible instalar las versiones de escritorio de las aplicaciones o acceder on-line, pulsando los iconos correspondientes.



3. CONFIGURACIÓN DE OFFICE 365

A continuación, se abordará la configuración de Office 365 centrándose en el cumplimiento de los requisitos del Esquema Nacional de Seguridad.

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

3.1.1.1 IDENTIFICACIÓN

Office 365 usa Microsoft Entra ID, una identidad de usuario basada en la nube y un servicio de autenticación que se incluye con la suscripción a Office 365, para administrar las identidades y la autenticación de Office 365. Para más información consultar [CCN-STIC-884A - Guía de configuración segura para Azure].

MODELOS DE GESTIÓN DE IDENTIDADES

En esta sección se abordarán los distintos modelos y mecanismos para la gestión de identidades en Office 365. Principalmente nos centraremos en dos: modelo identidad sólo nube (que será tomado como referencia en esta guía) y modelo de identidad híbrida.

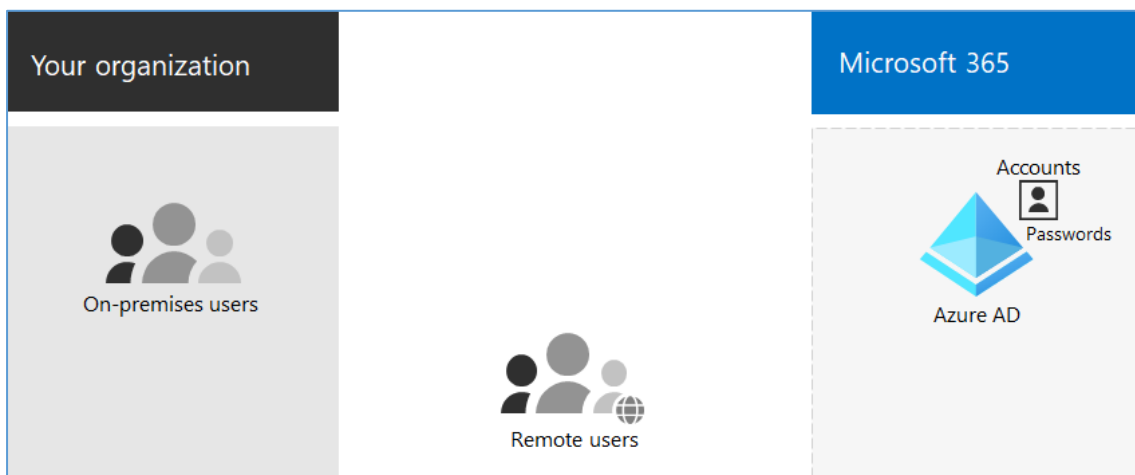
| | Identidad solo de nube | Identidad híbrida |
|---|--|---|
| Definición | La cuenta de usuario solo existe en el tenant de Entra ID para su suscripción a Microsoft 365. | La cuenta de usuario existe en AD DS y una copia también se encuentra en el tenant de Entra ID para su suscripción a Microsoft 365. La cuenta de usuario en Entra ID también puede incluir una versión hash de la contraseña de la cuenta de usuario. |
| Cómo autentica Microsoft 365 las credenciales de usuario | El tenant de Entra ID para su suscripción a Microsoft 365 realiza la autenticación con la cuenta de identidad de nube. | El tenant de Entra ID para su suscripción de Microsoft 365 administra el proceso de autenticación o redirige al usuario a otro proveedor de identidades. |
| Ideal para | Organizaciones que no tienen ni necesitan un AD DS local. | Organizaciones que usan AD DS u otro proveedor de identidades. |

| | | |
|------------------------|---|---|
| Mayor beneficio | Fácil de usar. No se necesitan servidores o herramientas de directorio adicionales. | Los usuarios pueden usar las mismas credenciales al obtener acceso a los recursos locales o basados en la nube. |
|------------------------|---|---|

Modelo identidad sólo nube

Una identidad de solo nube usa cuentas de usuario que solo existen en Entra ID. La identidad de nube suele usarse en organizaciones pequeñas que no tienen servidores locales o que no usan AD DS para administrar identidades locales.

Estos son los componentes básicos de la identidad solo de la nube.



Los usuarios locales y remotos (en línea) usan sus cuentas de usuario y contraseñas de Entra ID para acceder a los servicios en la nube de Office 365. Entra ID autentica las credenciales de usuario en función de sus cuentas de usuario y contraseñas almacenadas.

Administración

Como las cuentas de usuario se almacenan solo en Entra ID, se puede administrar las identidades de nube con herramientas como el Centro de administración de Microsoft 365 y Windows PowerShell.

Modelo identidad híbrido

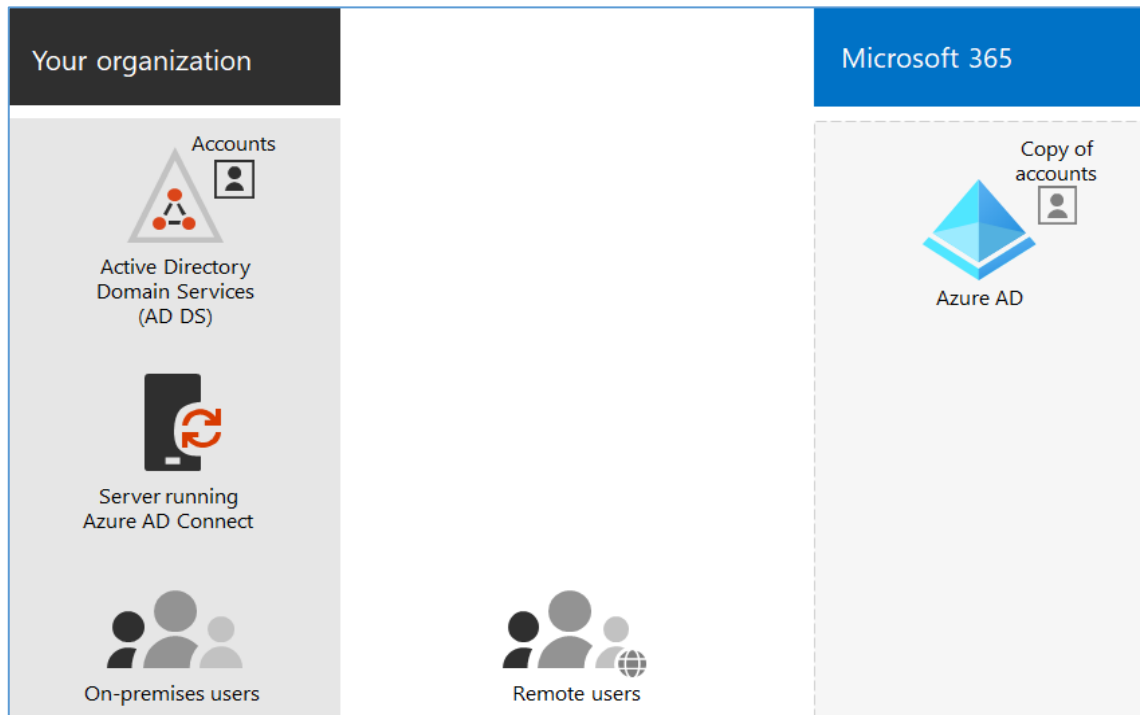
La identidad híbrida usa cuentas que se originan en un AD DS local y tienen una copia en el tenant de Entra ID de una suscripción a Microsoft 365. Sin embargo, la mayoría de los cambios solo fluyen en un sentido. Los cambios que realice en las cuentas de usuario de AD DS se sincronizan con su copia en Entra ID. Pero los cambios realizados en cuentas basadas en la nube en Entra ID, como nuevas cuentas de usuario, no se sincronizan con AD DS.

Microsoft Entra Connect proporciona la sincronización de cuentas en curso. Se ejecuta en un servidor local, comprueba los cambios en AD DS y reenvía dichos cambios a Entra ID. Microsoft Entra Connect permite filtrar las cuentas que se van a

sincronizar y si se debe sincronizar una versión hash de las contraseñas de usuario, conocidas como sincronización de hash de contraseña (PHS).

Al implementar la identidad híbrida, su AD DS local es el origen de autoridad para la información de la cuenta. Esto significa que las tareas de administración se realizan principalmente en el entorno local, que luego se sincronizan con Entra ID.

Estos son los componentes de la identidad híbrida.



El tenant de Entra ID tiene una copia de las cuentas de AD DS. En esta configuración, los usuarios locales y remotos que tienen acceso a los servicios en la nube de Microsoft 365 se autentican con Entra ID.

GESTIÓN DE IDENTIDADES EN EL MODELO SÓLO NUBE

Con la identidad solo de nube, todos los usuarios, grupos y contactos se almacenan en el tenant de Microsoft Entra ID de la suscripción a Office 365.

Tanto la creación de usuarios como de grupos puede realizarse desde:

- Centro de administración de Microsoft 365
- Microsoft Graph PowerShell

Centro de Administración de Microsoft 365

Se accede a través del icono Admin del portal de Office 365 o bien mediante la url: admin.microsoft.com.

Creación de usuarios

- a) Desde el menú [Usuarios\Usuarios activos] pulsar el icono “Agregar un usuario”, y rellenar el formulario.

 Agregar un usuario

- Información básica
- Licencias de producto
- Configuración opcional
- Finalizar

Configurar la información básica

Para empezar, rellene información básica sobre el usuario que va a agregar.

Nombre

Apellidos

Nombre para mostrar *

Nombre de usuario *

@

Dominios

@

.onmicrosoft.com

Crear una contraseña de manera automática

Requerir que este usuario cambie la contraseña cuando inicie sesión por primera vez

Enviar contraseña por correo electrónico al finalizar

Nota: más información sobre gestión de contraseñas en el apartado [3.1.1.5 Mecanismos de autenticación].

- b) Se asigna la licencia y se asocian las aplicaciones a las que tendrá acceso el usuario.

Asignar licencias de producto

Asigne las licencias que desea que tenga este usuario.

Seleccione la ubicación *

Licencias (1) *

Asignar una licencia de producto al usuario

Microsoft 365 Empresa Estándar
 19 de 25 licencias disponibles

Crear usuario sin licencia de producto (no se recomienda)
 Es posible que tengan acceso limitado o que no tengan acceso a Microsoft 365 hasta que asigne una licencia de producto.

Aplicaciones (37)

Mostrar aplicaciones para:

Seleccionar todo

Administración de dispositivos móviles para Office 365
 Microsoft 365 Empresa Estándar
 Esta aplicación se asigna a nivel de organización. No se puede asignar por usuario.

Aplicaciones de Microsoft 365 para negocios
 Microsoft 365 Empresa Estándar

Avatares para Teams
 Microsoft 365 Empresa Estándar

Avatares para Teams (adicional)
 Microsoft 365 Empresa Estándar

- c) En el caso de que el usuario requiera un rol especial, seleccionar uno desde el listado. Si el usuario no necesita ningún rol, dejar marcada la opción Usuario (*sin acceso al centro de administración*).

Configuración opcional

Puede elegir el rol que desea asignar a este usuario y rellenar la información de perfil adicional.

Roles (Usuario: sin acceso de administración) ^

Los roles de administrador ofrecen permiso a los usuarios para ver los datos y completar las tareas en los centros de administración. Asigne el rol menos permisivo para que los usuarios solo tengan el acceso que necesitan.

[Más información sobre roles de administración](#)

Usuario (sin acceso al centro de administración)

Acceso al centro de administración

Los lectores globales tienen acceso de solo lectura en los centros de administración, mientras que los administradores globales tienen acceso ilimitado para editar toda la configuración. Los usuarios que tienen asignados otros roles están más limitados en lo que pueden ver y hacer.

Administrador de Exchange i

Administrador de SharePoint i

Administrador de Teams i

Administrador de soporte técnico de servicio i

Administrador de usuarios i

- d) Añadimos información del usuario, si es necesario.

Información del perfil

^

Puesto

Departamento

Oficina

Teléfono de la oficina **Número de fax**

e) Una vez creado el usuario aparece el siguiente mensaje.

 **CCN-O365 agregado a los usuarios activos**

CCN-O365 aparecerá ahora en la lista de usuarios activos.

Detalles del usuario

Nombre para mostrar: CCN-O365

Nombre de usuario: CCN-O365@ .onmicrosoft.com

Contraseña: ***** [Mostrar](#)

Para comprobar que el usuario se ha creado correctamente revisar la lista de “usuarios activos”.

Usuarios activos


Acciones recomendadas (1) ▼

[Agregar un usuario](#)
[Plantillas de usuario](#)
[Agregar varios usuarios](#)

⋮





| <input type="checkbox"/> | Nombre para mostrar ↑ | | Nombre de usuario | Licencias |
|--------------------------|-----------------------|---|----------------------------|--------------------------------|
| <input type="checkbox"/> | CCN-O365 | ⋮ | CCN-O365@ .onmicrosoft.com | Microsoft 365 Empresa Estándar |

Operaciones básicas sobre usuarios

 Desde el menú [Usuarios\Usuarios activos] seleccionar el usuario y se pulsar sobre el icono “Más opciones”.


[Agregar un usuario](#)
[Autenticación multifactor](#)
[Actualizar](#)
[Eliminar usuario](#)
[Restablecer contraseña](#)

| <input type="checkbox"/> | Nombre para mostrar ↑ | | Nombre de usuario | Licencias |
|--------------------------|-----------------------|---|----------------------------|---------------|
| <input type="checkbox"/> | CCN-O365 | ⋮ | CCN-O365@ .onmicrosoft.com | Microsoft 365 |

-  Administrar licencias de producto
-  Administrar grupos
-  Eliminar usuario
-  Administrar nombre de usuario y correo electrónico

Administrar licencias

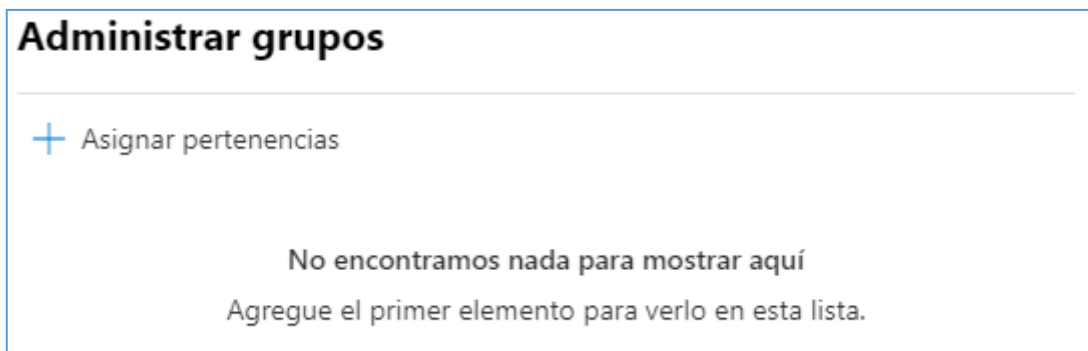
Desde el menú [Usuario\Usuarios activos] se despliega la lista de usuarios con las licencias asignadas. Seleccionar el usuario adecuado y pulsar sobre el nombre. En el panel de la derecha, pestaña “Licencias y Aplicaciones” configurar las opciones pertinentes.



The screenshot shows the user management interface for a user named CCN-O365. The user's profile is displayed with a blue circular icon containing the letters 'CC'. Below the icon is the text 'Cambiar foto'. To the right of the icon, the user's name 'CCN-O365' is shown in bold. Below the name are three action links: 'Restablecer contraseña', 'Bloquear inicio de sesión', and 'Eliminar usuario'. Below these links are five tabs: 'Cuenta', 'Dispositivos', 'Licencias y aplicaciones' (which is selected and underlined), 'Correo', and 'OneDrive'. Below the tabs is a section titled 'Seleccione la ubicación *' with a dropdown menu showing 'España'. Below this is a section titled 'Licencias (1)' with a blue arrow pointing up. Underneath, there is a single license entry: 'Microsoft 365 Empresa Estándar' with a blue checkmark icon to its left and the text '22 de 25 licencias disponibles' below it.

Asignar usuario a grupo

Desde el menú [Usuarios\Usuarios activos] pulsando sobre el icono “Más opciones” del usuario.



The screenshot shows the 'Administrar grupos' section of the user management interface. At the top, the title 'Administrar grupos' is displayed in bold. Below the title is a blue plus sign icon followed by the text 'Asignar pertenencias'. Below this is a message: 'No encontramos nada para mostrar aquí' followed by 'Agregue el primer elemento para verlo en esta lista.'

Editar usuario

- Desde el menú [Usuarios\Usuarios activos] pulsando sobre el “nombre” del usuario.
- Para asignar roles al usuario consultar el apartado [3.1.1.3 Segregación de funciones y tareas].



CCN-O365

[Restablecer contraseña](#)
[Bloquear inicio de sesión](#)
[Eliminar usuario](#)

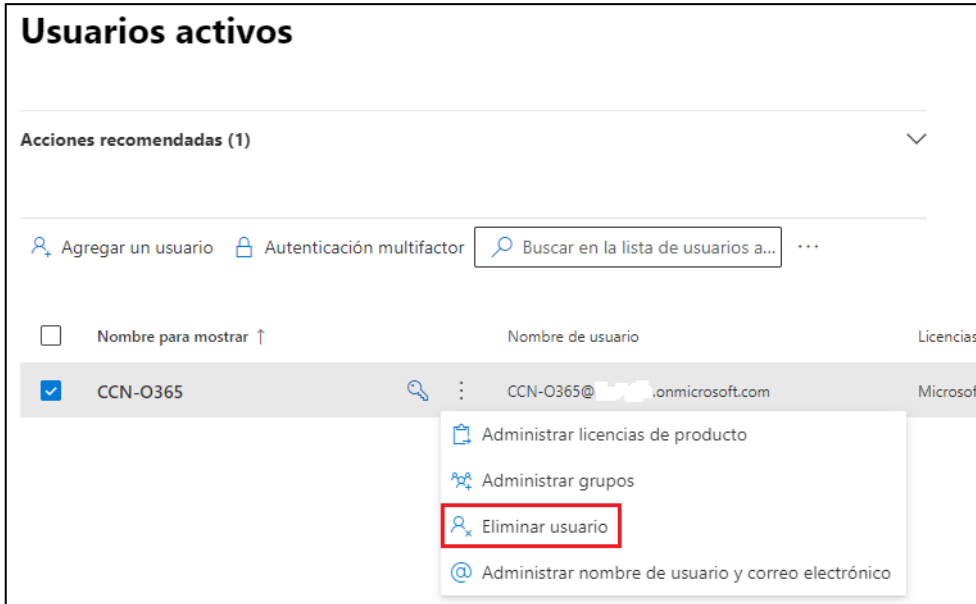
[Cambiar foto](#)

Cuenta
Dispositivos
Licencias y aplicaciones
Correo
OneDrive

| | |
|---|---|
| Nombre de usuario y correo electrónico CCN-O365@ .onmicrosoft.com Administrar nombre de usuario y correo electrónico | Alias Administrar nombre de usuario y correo electrónico |
| Último inicio de sesión Ver los últimos 7 días | Cerrar sesión ⓘ Infirme a este usuario de todas las sesiones de Microsoft 365. Cerrar sesión en todas las sesiones |
| Dirección de correo electrónico alternativa No se ha proporcionado ninguna Agregar dirección | Grupos Administrar grupos |
| Roles Sin acceso de administrador Administrar roles | Administrador No se ha proporcionado ninguno Agregar administrador |
| Información de contacto | |
| Nombre para mostrar CCN-O365 | Nombre CCN-O365 |
| Número de teléfono Administrar información de contacto | Apellidos |
| Activaciones de Microsoft 365 ⓘ Ver activaciones de Microsoft 365 | Autenticación multifactor Administrar la autenticación multifactor |

Eliminar usuario

Desde el menú [Usuarios\Usuarios activos] pulsando sobre el icono “Más opciones” del usuario.



Usuarios activos

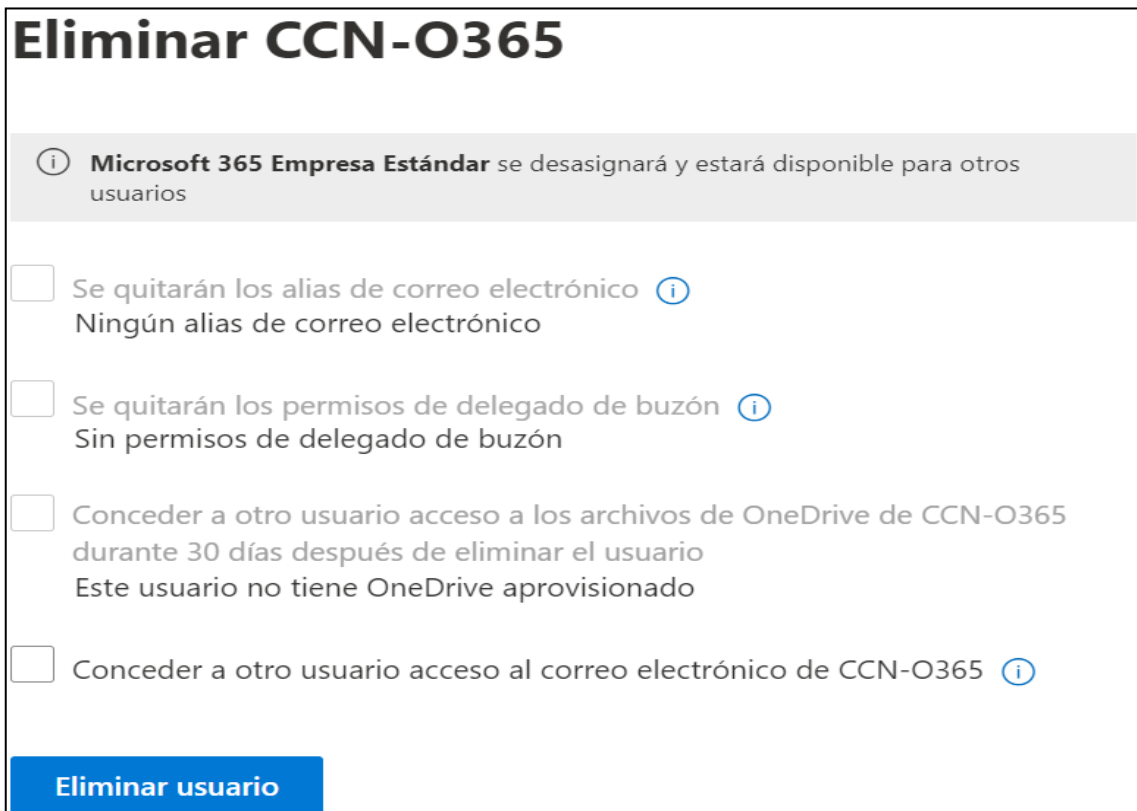
Acciones recomendadas (1) ▾

🔍 Agregar un usuario 🔒 Autenticación multifactor 🔍 Buscar en la lista de usuarios a... ⋮

| <input type="checkbox"/> | Nombre para mostrar ↑ | Nombre de usuario | Licencias |
|-------------------------------------|-----------------------|-----------------------------|-----------|
| <input checked="" type="checkbox"/> | CCN-O365 | CCN-O365@...onmicrosoft.com | Microsoft |

- 📄 Administrar licencias de producto
- 👤 Administrar grupos
- 👤 Eliminar usuario**
- 📧 Administrar nombre de usuario y correo electrónico

Nos saldrá la siguiente ventana. Click en Eliminar usuario.



Eliminar CCN-O365

Microsoft 365 Empresa Estándar se desasignará y estará disponible para otros usuarios

- Se quitarán los alias de correo electrónico ⓘ
Ningún alias de correo electrónico
- Se quitarán los permisos de delegado de buzón ⓘ
Sin permisos de delegado de buzón
- Conceder a otro usuario acceso a los archivos de OneDrive de CCN-O365 durante 30 días después de eliminar el usuario
Este usuario no tiene OneDrive provisionado
- Conceder a otro usuario acceso al correo electrónico de CCN-O365 ⓘ

Eliminar usuario

Se deberá mover los archivos que quiera conservar dentro del período de retención establecido para los archivos de OneDrive. **De forma predeterminada, el período de retención es de 30 días.**

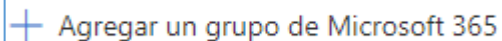
Crear grupo

En la sección **grupos** del Centro de administración de Microsoft 365, puede crear y administrar estos tipos de grupos:

- Los **grupos de Office 365** se usan para la colaboración entre usuarios, tanto dentro como fuera de la compañía.
- Los **grupos de distribución** se usan para enviar notificaciones a un grupo de personas.
- Los **grupos de seguridad** se usan para conceder acceso a los recursos de SharePoint.
- Los **grupos de seguridad habilitados para correo** se usan para conceder acceso a los recursos de SharePoint y enviar notificaciones por correo electrónico a dichos usuarios.
- Los **buzones compartidos** se usan cuando varias personas necesitan tener acceso al mismo buzón, como la información de la empresa o la dirección de correo electrónico de soporte técnico.

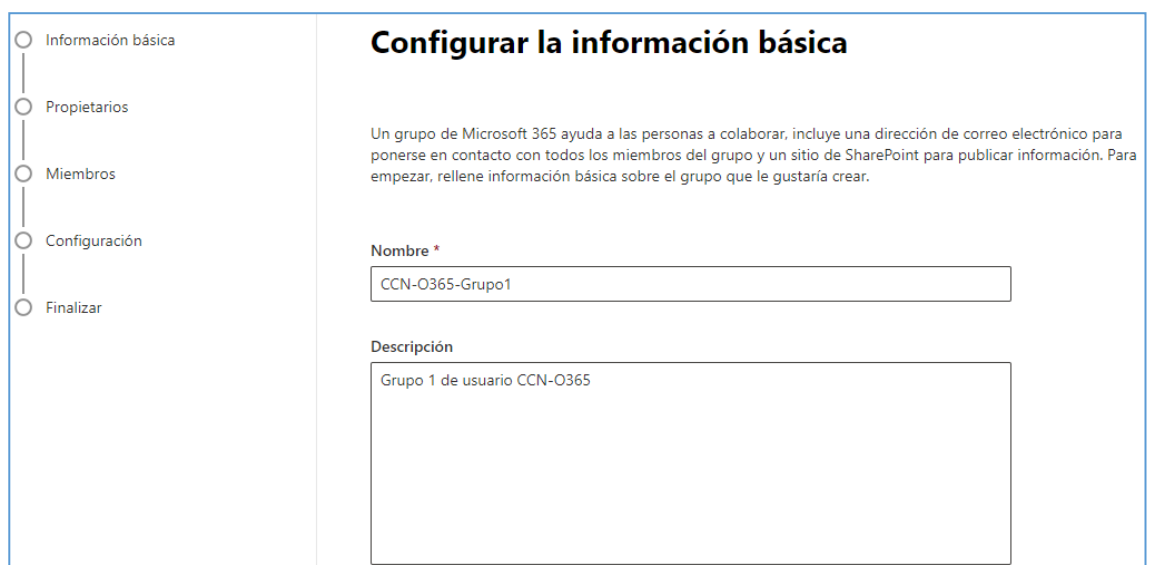
Es importante activar la “Auditoría de buzones compartidos” para permitir la trazabilidad en estos buzones, como se describe en la guía [CCN-STIC-885C - Guía de configuración segura para Exchange Online].

a) Agregar grupo.



Desde el menú [Teams y grupos], pulsar la opción Grupos y equipos activos, una vez dentro pulsar el icono “Agregar un grupo de Microsoft 365”.

b) Cumplimentar información del grupo.



El formulario muestra un menú de navegación a la izquierda con los siguientes ítems: Información básica (seleccionado), Propietarios, Miembros, Configuración y Finalizar. El contenido principal está titulado "Configurar la información básica" y contiene una descripción: "Un grupo de Microsoft 365 ayuda a las personas a colaborar, incluye una dirección de correo electrónico para ponerse en contacto con todos los miembros del grupo y un sitio de SharePoint para publicar información. Para empezar, rellene información básica sobre el grupo que le gustaría crear." Hay dos campos de entrada: "Nombre *" con el valor "CCN-O365-Grupo1" y "Descripción" con el valor "Grupo 1 de usuario CCN-O365".

c) Desde este apartado se agrega el propietario

- Información básica
- Propietarios**
- Miembros
- Configuración
- Finalizar

Asignar propietarios

Los propietarios del grupo tienen permisos exclusivos. Pueden agregar o quitar miembros, eliminar conversaciones de la bandeja de entrada compartida y cambiar la configuración del grupo. Los propietarios del grupo también pueden cambiar el nombre del grupo, actualizar la descripción y mucho más.

i Usted debe tener al menos un propietario. Le recomendamos que agregue dos propietarios para que uno pueda ayudar cuando el otro esté ausente. Si planea agregar Microsoft Teams a este grupo, todos los propietarios deben tener una licencia que incluya Teams. [Más información](#)

+ Asignar propietarios

Mostrar nombre Estado de Te...

C CCN-O365
CCN-O365@.onmicrosoft.com 🗑️

d) Desde este apartado se agrega los miembros del grupo

- Información básica
- Propietarios
- Miembros**
- Configuración
- Finalizar

Agregar miembros

Los miembros del grupo tienen acceso a todos los elementos del grupo, incluido el contenido del grupo como mensajes de correo electrónico, archivos y un calendario compartido. De forma predeterminada, los miembros del grupo pueden invitar a los invitados a unirse a su grupo, pero no pueden modificar la configuración del grupo. [Más información sobre los miembros del grupo que pueden hacer](#)

+ Agregar miembros

Mostrar nombre Estado de Te...

TU Test User
TestUser@.onmicrosoft.com 🗑️

e) Configuración del grupo

- Información básica
- Propietarios
- Miembros
- Configuración**
- Finalizar

Editar configuración

i Podrá cambiar la configuración, como Permitir remitentes externos o Enviar copias de las conversaciones del grupo a las bandejas de entrada de los miembros, después de crear el grupo. [Más información sobre todos los ajustes](#)

Los grupos de Microsoft 365 permiten que los equipos colaboren proporcionándole un correo electrónico de grupo y un área de trabajo compartida para las conversaciones, los archivos y los calendarios. Elija la configuración de su grupo de Microsoft 365.

Dirección de correo electrónico del grupo *

@ .onmicrosoft.com

Privacidad i

Público
v

Asignación de roles

Permitir que se asignen roles de administrador a este grupo

Esta configuración será permanente para este grupo. [Más información sobre la asignación de roles a grupos](#)

i La asignación de roles solo debe habilitarse cuando el grupo es Privado.

Agregar Microsoft Teams al grupo

Crear un equipo para este grupo

- 1) Añadimos un nombre al grupo
- 2) Privacidad:
 - Privado: Los grupos **privados** no están disponibles para que cualquier usuario se una a estos, y solo los propietarios del grupo pueden agregar miembros. Solo los miembros pueden acceder al contenido del grupo.
 - Público: Todos los usuarios pueden unirse a un grupo **público** sin necesidad de la aprobación de un propietario del grupo. Cualquier usuario puede acceder al contenido del grupo.

Nota: Si se requiere un mayor control sobre el acceso a la información del grupo por parte de los usuarios, entonces se recomienda el uso del valor Privado.

- 3) Para asignar roles al grupo
 - La opción de Privacidad debe estar en **Privado**.
 - La opción de **Agregar Microsoft Teams al grupo** debe estar desactivada.
- 4) Agregar Microsoft Teams al grupo
 - Activar esta opción si se requiere agregar un equipo de teams al grupo.

f) Revisar y terminar de agregar el grupo



The screenshot shows the 'Revisar y terminar de agregar el grupo' (Review and finish adding the group) step in the Microsoft 365 group configuration process. The left sidebar indicates the progress: 'Información básica', 'Propietarios', 'Miembros', and 'Configuración' are completed (checked), while 'Finalizar' is the current step (highlighted in blue). The main content area displays the following information:

- Tipo de grupo:** Microsoft 365 (with an 'Editar' link).
- Información básica:** Nombre: CCN-O365-Grupo1, Descripción: Grupo 1 de usuario CCN-O365 (with an 'Editar' link).
- Propietarios:** CCN-O365 (with an 'Editar' link).
- Miembros:** Test User (with an 'Editar' link).
- Configuración:** Correo electrónico: ccn-o365_grupo@...onmicrosoft.com, Privacidad: Público, Asignación de roles: Deshabilitado, Agregar Microsoft Teams: Sí (with an 'Editar' link).

g) Revisar y finalizar



Información básica
 Propietarios
 Miembros
 Configuración
 Finalizar

CCN-O365-Grupo1 grupo creado

CCN-O365-Grupo1 grupo aparecerá en la lista de equipos activos y grupos en un plazo de 5 minutos.

Ahora que se ha creado el grupo, puede cambiar esta configuración:

- Envíe copias de conversaciones y eventos del grupo a las bandejas de entrada de sus miembros.
- Permitir que los usuarios ajenos a la organización envíen correo electrónico a este grupo
- Ocultar de la lista global de direcciones de mi organización

¿Quiere obtener más información?


[Usar los grupos para colaborar de forma eficaz](#)

Pasos siguientes

[Agregar otro grupo Microsoft 365 \(recomendado\)](#)

Gestionar miembros de un grupo

- a) Desde el menú [Grupos y equipos activos] pulsando sobre el nombre del grupo, se despliega el panel del grupo con distintas pestañas. Seleccionar la pestaña *Pertenencia* y luego dentro *Miembros*.



Activar equipos y grupos

CCN-O365-grupo1

Público equipo

Correo electrónico | Abrir en Teams | Eliminar

CCN-O365-grupo1

General | **Pertenencia** | Canales | Configuración

Propietarios

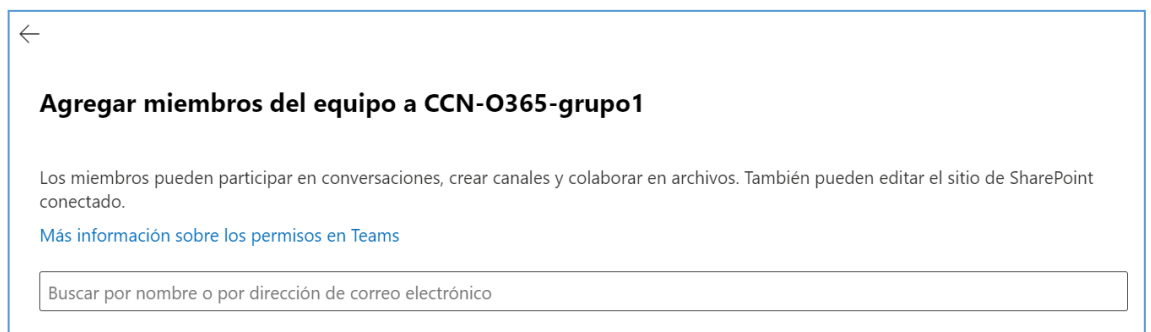
Miembros

Agregar miembros a este equipo

Este equipo no tiene miembros. Empiece a agregar miembros para que puedan trabajar en conjunto en Teams

[Agregar miembros](#)

- b) Buscamos los usuarios a través del nombre o del correo electrónico y hacer click en agregar.



←

Agregar miembros del equipo a CCN-O365-grupo1

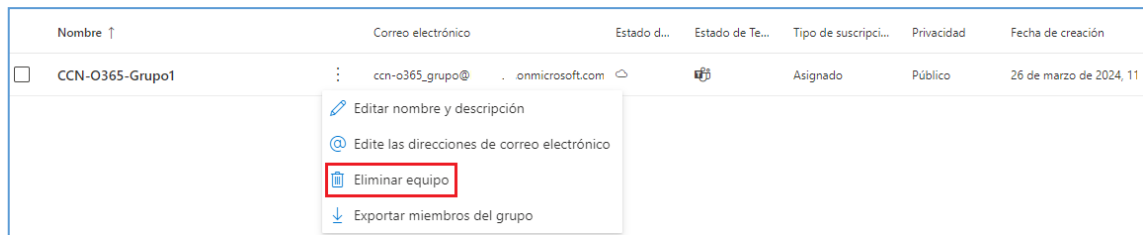
Los miembros pueden participar en conversaciones, crear canales y colaborar en archivos. También pueden editar el sitio de SharePoint conectado.

[Más información sobre los permisos en Teams](#)

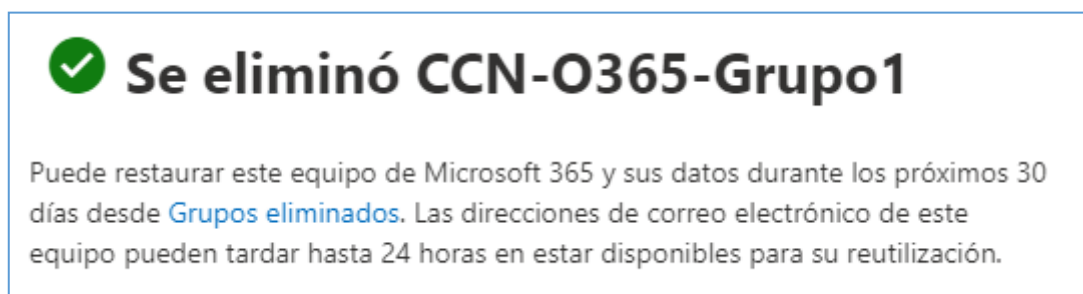
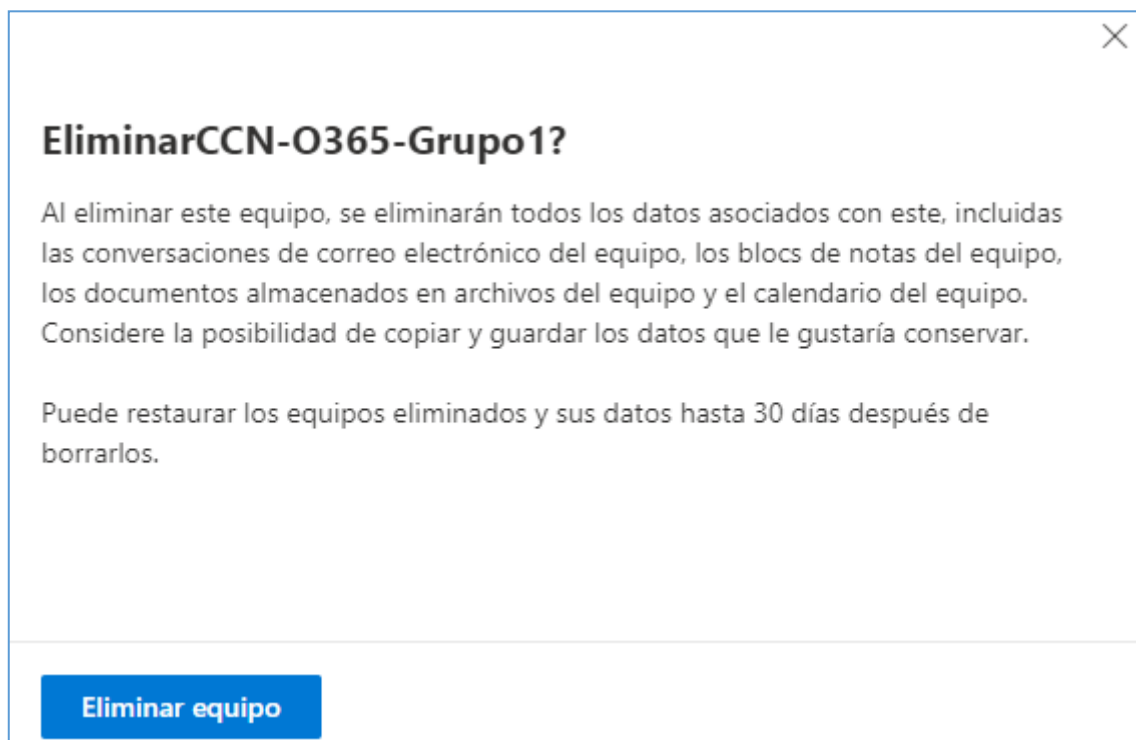
Buscar por nombre o por dirección de correo electrónico

Eliminar grupo

Desde el menú [Teams y grupos/ Grupos y equipos activos], seleccionar el grupo a eliminar y desde más opciones, click en Eliminar equipo.



Click en Eliminar equipo.



Powershell de Office 365

Para la ejecución de los siguientes scripts se requiere el módulo de Microsoft Graph PowerShell SDK para windows PowerShell.

Crear una cuenta de usuario individual

Ver Anexo A en el final del documento.

Crear varias cuentas de usuario

Ver Anexo B en el final del documento.

3.1.1.2 REQUISITOS DE ACCESO

Los mecanismos de acceso a los recursos se detallan en las guías específicas de cada servicio: Sharepoint Online [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online], Exchange Online [CCN-STIC-885C - Guía de configuración segura para Exchange Online] y Teams [CCN-STIC 885D - Guía de configuración segura para Microsoft Teams].

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Roles de administración

La suscripción de O365 incluye un conjunto de roles de administrador que se pueden asignar a los usuarios de la organización. Cada rol de administrador se asigna a funciones empresariales comunes y proporciona a los usuarios permisos para realizar tareas específicas en los centros de administración.

Como los administradores tienen acceso a los datos y archivos sensibles, Microsoft recomienda seguir estas directrices para mantener los datos de la organización más seguros.

| Recomendación | ¿Por qué es importante? |
|--|---|
| Tener de 2 a 4 administradores globales | Los administradores globales tienen acceso casi ilimitado a la configuración de su organización y a la mayoría de sus datos. Se recomienda limitar el número de administradores globales tanto como sea posible. Un Administración global puede bloquear accidentalmente su cuenta y requerir un restablecimiento de contraseña. Otra Administración global o una Administración de autenticación con privilegios pueden restablecer la contraseña de un Administración global. Por lo tanto, se recomienda tener al menos una Administración global más o una Administración de autenticación con privilegios en caso de que un Administración global bloquee su cuenta. |

| | |
|--|---|
| <p>Asignar el rol menos permisivo</p> | <p>Asignar el rol menos permisivo significa conceder a los administradores solo el acceso que necesitan para realizar el trabajo. Por ejemplo, si quiere que alguien restablezca las contraseñas de los empleados, no debe asignar el rol de administrador global ilimitado, debe asignar un rol de administrador limitado, como administrador de contraseñas o administrador del departamento de soporte técnico.</p> |
| <p>Requerir la autenticación multifactor para administradores</p> | <p>Es una buena idea requerir MFA para todos los usuarios, pero definitivamente se debe exigir a los administradores usar la MFA para iniciar sesión. MFA hace que los usuarios usen un segundo método de identificación para comprobar su identidad. Los administradores pueden tener acceso a gran parte de los datos de clientes y empleados. Si necesita MFA, incluso si la contraseña del administrador se pone en peligro, la contraseña no sirve para nada sin el segundo método de identificación. Al activar la MFA, la próxima vez que el usuario inicie sesión, deberá proporcionar una dirección de correo electrónico y un número de teléfono alternativos para recuperar la cuenta.</p> |

Asignar roles de administrador a un usuario



Desde el centro de administración, ir a los detalles del usuario y administrar funciones para asignar un rol al usuario.

Administrar roles de administrador

Los roles de administrador permiten a los usuarios realizar acciones en el centro de administración. Los administradores globales tienen permiso para administrar todos los productos y servicios, mientras que los administradores personalizados solo tienen los permisos que usted elija. Para reducir el nivel de riesgo en su organización, limite el número de administradores globales y, en su lugar, asigne roles de administrador personalizado.

Más información sobre roles de administración

Usuario (sin acceso de administrador) ⓘ

Administrador global

Debe tener al menos dos administradores globales en la organización para, en caso necesario, poder restablecer otra cuenta de administrador global. Para todos los demás administradores, asigne roles de administrador especial.

Administrador global ⓘ

Usuarios y grupos

Administrador de control de usuarios ⓘ

Administrador de servicios ⓘ

Administrador del servicio de asistencia ⓘ

Facturación

Administrador de facturación ⓘ

Roles especiales comunes

Administrador de Exchange ⓘ

Administrador de servicios de Teams ⓘ

Administrador de SharePoint ⓘ

Roles adicionales

Administrador de comunicaciones de Teams ⓘ

Roles disponibles en el centro de administración de Microsoft 365

El centro de administración Microsoft 365 permite administrar más de 30 roles de Entra ID. Sin embargo, estos roles son un subconjunto de las funciones disponibles en portal de Entra ID.

Usualmente es suficiente con asignar los siguientes roles a la organización:

| Rol de administrador | ¿A quién se le debe asignar este rol? |
|-------------------------------------|---|
| Administrador de facturación | <p>Asigne el rol de administrador de facturación a los usuarios que hagan compras, administren suscripciones y solicitudes de servicio y supervisen el estado del servicio.</p> <p>Los administradores de facturación también pueden:</p> <ul style="list-style-type: none"> - Administrar todos los aspectos de la facturación - Crear y administrar vales de soporte técnico en el portal de Entra ID. |
| Administrador de Exchange | <p>Asigne el rol de administrador de Exchange a los usuarios que necesiten ver y administrar los buzones de correo de sus usuarios, los grupos de Microsoft 365 y Exchange Online.</p> <p>Los administradores de Exchange también pueden:</p> <ul style="list-style-type: none"> - Recuperar elementos eliminados en un buzón de usuario - Configurar los delegados "Enviar como" y "Enviar en nombre de" |
| Administrador de Fabric | <p>Asigne el rol de administrador de Fabric a los usuarios que necesiten hacer lo siguiente:</p> <ul style="list-style-type: none"> - Administración de todas las características de administrador para Microsoft Fabric y Power BI - Informe sobre el uso y el rendimiento - Revisión y administración de auditorías |

| | |
|---------------------------------------|---|
| <p>Administrador global</p> | <p>Asigne el rol de administrador global a los usuarios que necesiten acceso global a la mayoría de las características de administración y datos en los servicios en línea de Microsoft.</p> <p>Dar acceso global a demasiados usuarios supone un riesgo para la seguridad y se recomienda tener entre dos y cuatro administradores globales.</p> <p>Solo los administradores globales pueden:</p> <ul style="list-style-type: none"> - Restablecer las contraseñas de todos los usuarios - Agregar y administrar dominios - Desbloquear a otro administrador global <p>Nota: La persona que se registró en Microsoft servicios en línea se convierte automáticamente en administrador global.</p> |
| <p>Lector global</p> | <p>Asigne el rol de lector global a los usuarios que necesiten ver la configuración y las funciones de administración en los centros de administración que el administrador global puede ver. El administrador del lector global no puede editar ninguna configuración.</p> |
| <p>Administrador de grupos</p> | <p>Asigne el rol de administrador de grupos a los usuarios que necesiten administrar la configuración de todos los grupos en los centros de administración, incluido el Centro de administración de Microsoft 365 y el Centro de administración de Microsoft Entra.</p> <p>Los administradores de grupos pueden:</p> <ul style="list-style-type: none"> - Crear, editar, eliminar y restaurar los grupos de Microsoft 365 - Crear y actualizar las directivas de creación, expiración y nomenclatura de grupos - Creación, edición, eliminación y restauración Microsoft Entra grupos de seguridad |

| | |
|---|---|
| <p>Administrador del departamento de soporte técnico</p> | <p>Asigne el rol de administrador del departamento de soporte técnico a los usuarios que necesiten que hacer lo siguiente:</p> <ul style="list-style-type: none"> - Restablecer contraseñas - Forzar a los usuarios a cerrar sesión - Administrar solicitudes de servicio - Supervisar el estado del servicio <p>Nota: el administrador del departamento de soporte técnico solo puede ayudar a usuarios que no son administradores y a usuarios que tienen asignados estos roles: Lector de directorios, Invitador de usuarios invitados, Administrador del departamento de soporte técnico, Lector del centro de mensajes y Lector de informes.</p> |
| <p>Administrador de licencias</p> | <p>Asigne el rol de administrador de licencias a los usuarios que necesiten asignar y quitar licencias a usuarios y editar su ubicación de uso.</p> <p>Los administradores de licencias también pueden:</p> <ul style="list-style-type: none"> - Volver a procesar asignaciones de licencia para licencias basadas en grupos - Asignar licencias de producto a grupos de licencias basadas en grupos |
| <p>Lector de privacidad del centro de mensajes</p> | <p>Asigne el rol de lector de privacidad del Centro de mensajes a los usuarios que necesiten leer mensajes y actualizaciones de privacidad y seguridad en el Centro de mensajes de Microsoft 365. Los lectores de privacidad del centro de mensajes pueden recibir notificaciones por correo electrónico relacionadas con la privacidad de los datos, en función de sus preferencias, y pueden cancelar la suscripción mediante las preferencias del Centro de mensajes. Solo los administradores globales y los lectores de privacidad del Centro de mensajes pueden leer los mensajes de privacidad de datos. Este rol no tiene permiso para ver, crear o administrar solicitudes de servicio.</p> <p>Los lectores de privacidad del centro de mensajes también pueden:</p> <ul style="list-style-type: none"> - Supervisar todas las notificaciones en el Centro de mensajes, incluidos los mensajes de privacidad de datos - Ver grupos, dominios y suscripciones |

| | |
|--|---|
| Lector del Centro de mensajes | <p>Asigne el rol de Lector del Centro de mensajes a los usuarios que necesiten hacer lo siguiente:</p> <ul style="list-style-type: none"> - Supervisar las notificaciones del Centro de mensajes - Obtener resúmenes semanales por correo electrónico de las publicaciones y actualizaciones del Centro de mensajes - Compartir publicaciones del Centro de mensajes - Tener acceso de solo lectura a Microsoft Entra servicios, como usuarios y grupos |
| Administrador de migración | <p>Asigne el rol Administrador de migración de Microsoft 365 a los usuarios que necesiten realizar las siguientes tareas:</p> <ul style="list-style-type: none"> - Use el Administrador de migración en el Centro de administración de Microsoft 365 para administrar la migración de contenido a Microsoft 365, incluidos los sitios de Teams, OneDrive para la Empresa y SharePoint, desde diversos orígenes, como Google Drive, Dropbox y Box. - Seleccione orígenes de migración, cree inventarios de migración (como listas de usuarios de Google Drive), programe y ejecute migraciones y descargue informes. - Cree nuevos sitios de SharePoint si los sitios de destino aún no existen, cree listas de SharePoint en los sitios de administración de SharePoint y cree y actualice elementos en listas de SharePoint. - Administrar la configuración del proyecto de migración y el ciclo de vida de la migración para las tareas, así como administrar asignaciones de permisos de origen a destino. <p>Nota: Con este rol, solo puedes migrar desde Google Drive, Box, Dropbox y Egnyte. Este rol no permite migrar desde orígenes de recursos compartidos de archivos desde el Centro de administración de SharePoint. Use un administrador de SharePoint o un administrador global para migrar desde orígenes de recursos compartidos de archivos.</p> |
| Administrador de aplicaciones de Office | <p>Asigne el rol de administrador de aplicaciones de Office a los usuarios que necesiten hacer lo siguiente:</p> <ul style="list-style-type: none"> - Use el servicio Cloud Policy para Microsoft 365 para crear y administrar directivas basadas en la nube. - Crear y administrar solicitudes de servicio - Administrar el contenido novedades que los usuarios ven en sus aplicaciones de Microsoft 365 - Supervisar el estado del servicio |
| Escritor de mensajes de la organización | <p>Asigne el rol Escritor de mensajes de la organización a los usuarios que necesiten escribir, publicar, administrar y revisar los mensajes de la organización para los usuarios finales a través de superficies de productos de Microsoft.</p> |

| | |
|--|--|
| Aprobador de mensajes de la organización | Asigne el rol Aprobador de mensajes organizativos a los usuarios que necesiten revisar, aprobar o rechazar nuevos mensajes de la organización para su entrega en el Centro de administración de Microsoft 365 antes de que se envíen a los usuarios a través de superficies de productos de Microsoft. |
| Administrador de contraseñas | Asigne el rol de administrador de contraseñas a un usuario que necesite restablecer las contraseñas de los no administradores y los administradores de contraseñas. |
| Administrador de Power Platform | Asigne el rol de administrador de Power Platform a los usuarios que necesiten hacer lo siguiente: <ul style="list-style-type: none"> - Administrar todas las características de administración de Power Apps, Power Automate, Power BI, Microsoft Fabric y Prevención de pérdida de datos de Microsoft Purview - Crear y administrar solicitudes de servicio - Supervisar el estado del servicio |
| Lector de informes | Asigne el rol de lector de informes a los usuarios que necesiten hacer lo siguiente: <ul style="list-style-type: none"> - Ver datos de uso e informes de actividad en el Centro de administración de Microsoft 365 - Obtener acceso al paquete de contenido de adopción de Power BI - Obtener acceso a los informes de inicio de sesión y la actividad en Microsoft Entra ID - Ver datos devueltos por la API de informes de Microsoft Graph |
| Administrador de búsqueda | Asigne el rol de administrador Búsqueda a los usuarios que necesitan crear y administrar el contenido de los resultados de búsqueda y definir la configuración de consulta para mejorar los resultados de búsqueda dentro de la organización. El administrador de Búsqueda administra la configuración de búsqueda de Microsoft y puede realizar todas las tareas de administración de contenido que puede realizar un editor de Búsqueda. |
| Administrador de soporte técnico del servicio | Asigne el rol de administrador de soporte técnico de servicio como un rol adicional a los administradores o usuarios que necesiten hacer, además de su rol de administrador habitual, lo siguiente: <ul style="list-style-type: none"> - Abrir y administrar solicitudes de servicio - Ver y compartir publicaciones del centro de mensajes - Supervisar el estado del servicio |

| | |
|--|--|
| <p>Administrador de SharePoint</p> | <p>Asigne el rol de administrador de SharePoint a los usuarios que necesiten acceder y administrar el centro de administración de SharePoint Online.</p> <p>Los administradores de SharePoint también pueden:</p> <ul style="list-style-type: none"> - Crear y eliminar sitios - Administrar colecciones de sitios y la configuración global de SharePoint |
| <p>Administrador de Teams</p> | <p>Asigne el rol de administrador de Teams a los usuarios que necesiten acceder y administrar el Centro de administración de Teams.</p> <p>El administrador de Teams también puede:</p> <ul style="list-style-type: none"> - Administrar reuniones - Administrar puentes de conferencia - Administrar la configuración de toda la organización, incluida la federación, la actualización de equipos y la configuración de cliente de equipos |
| <p>Administrador de usuarios</p> | <p>Asigne el rol de administrador de usuarios a los usuarios que necesiten hacer lo siguiente para todos los usuarios:</p> <ul style="list-style-type: none"> - Agregar usuarios y grupos - Asignar licencias - Administrar las propiedades de la mayoría de los usuarios - Crear y administrar vistas de usuarios - Actualizar las directivas de expiración de contraseña - Administrar solicitudes de servicio - Supervisar el estado del servicio <p>El administrador de usuario también puede realizar las siguientes acciones para los usuarios que no sean administradores y para los usuarios que tengan asignados los siguientes roles: Lector de directorios, Invitador de usuarios invitados, Administrador del departamento de soporte técnico, Lector del centro de mensajes y Lector de informes:</p> <ul style="list-style-type: none"> - Administrar nombres de usuario - Eliminar y restaurar usuarios - Restablecer contraseñas - Forzar a los usuarios a cerrar sesión - Actualizar claves de dispositivo (FIDO) |
| <p>Administrador de éxito de la experiencia del usuario</p> | <p>Asigne el rol Administrador de éxito de experiencia de usuario a los usuarios que necesitan acceder a Experience Insights, la puntuación de adopción y el Centro de mensajes en el Centro de administración de Microsoft 365. Este rol incluye los permisos del rol Lector de informes de resumen de uso.</p> |

El portal de Entra ID tiene más roles que los disponibles en el Centro de administración de Microsoft 365.

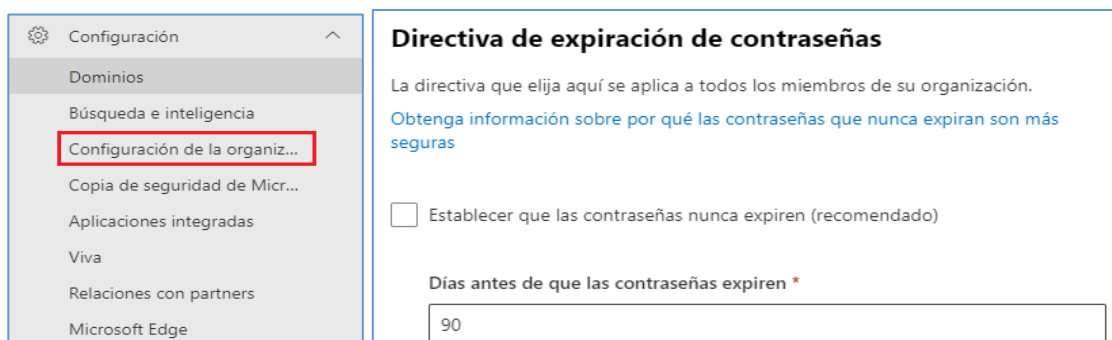
Desde Entra ID es posible crear roles personalizados. Se necesita Entra ID Premium P1 o P2.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Más información en las guías específicas de cada servicio: Sharepoint Online [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online], Exchange Online [CCN-STIC-885C - Guía de configuración segura para Exchange Online] y Teams [CCN-STIC 885D - Guía de configuración segura para Microsoft Teams].

3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Desde el Centro de administración de Microsoft 365 en el menú [Configuración\configuración de la organización\Seguridad y Privacidad] se pueden establecer **Directivas de expiración de contraseñas** para todos los usuarios de la organización.



Se recomienda activar la opción Establecer que las contraseñas nunca expiren (recomendado).

Desde Office 365 sólo se pueden modificar estos parámetros, cuyos valores por defecto son:

Días antes de que las contraseñas expiren: 90

Nota: Las notificaciones de expiración de contraseñas ya no se admiten en las aplicaciones Centro de administración de Microsoft 365 y Microsoft 365.

Para una gestión más avanzada hay que recurrir a Entra ID. Consultar guía [CCN-STIC-884A - Guía de configuración segura para Azure].

Powershell

Desde PS se pueden consultar y/o modificar un parámetro relacionado con la contraseña del usuario:

- PasswordNeverExpires: si la contraseña nunca expira.

Listado de usuarios con información de caducidad

```
Get-MgUser -All | Select-Object UserPrincipalName,
@{N="PasswordNeverExpires";E={$_.PasswordPolicies -contains
"DisablePasswordExpiration"}}
```

Modificar parámetros de contraseñas

Se recomienda aplicar el siguiente comando:

```
Update-MgUser -UserId <user ID> -PasswordPolicies DisablePasswordExpiration
```

Nota: Se recomienda configurar el parámetro PasswordNeverExpires en los entornos de Producción de la empresa.

Cómo ya se ha comentado, para una configuración avanzada de la política de contraseña hay que recurrir a la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

A continuación, se desglosan las características de las cuentas de usuario de Entra ID, y los comandos para modificarlas:

| Propiedad | Requerimiento de UPN (User Principal Name) |
|--|---|
| Caracteres permitidos | Caracteres en mayúsculas (A - Z) Caracteres en minúsculas (a - z) Números (0 - 9) Símbolos: - @ # \$ % ^ & * - _ ! + = [] { } \ : ' , . ? / ` ~ " () ; < > - espacio en blanco |
| Caracteres no permitidos en las contraseñas | Caracteres unicode Espacios |
| Longitud de la contraseña | Las contraseñas requieren lo siguiente - Una longitud mínima de ocho caracteres - 256 caracteres como máximo. |
| Complejidad de la contraseña | Las contraseñas requieren tres de las cuatro categorías siguientes: - Caracteres en mayúsculas - Caracteres en minúsculas - Números - Símbolos Nota: La comprobación de complejidad de la contraseña no es necesaria para los tenants de Education. |
| Contraseña no usada recientemente | Cuando un usuario cambie su contraseña, la nueva contraseña no debería ser la misma que la contraseña actual. |
| La protección de contraseñas de Microsoft Entra no ha prohibido la contraseña | La contraseña no puede estar en la lista global de contraseñas prohibidas de la protección de contraseñas de Microsoft Entra ni en la lista personalizable de contraseñas prohibidas específicas de la organización. |

Activar la autenticación multifactor (MFA)

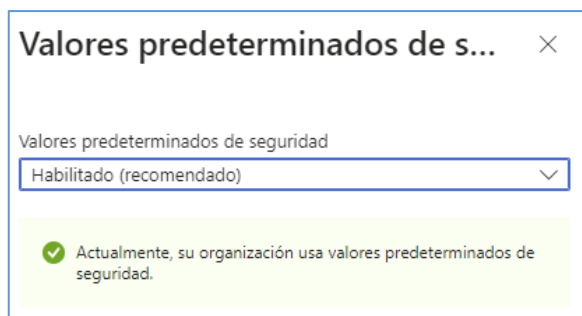
| Elemento | Al estar habilitado | Al estar deshabilitado | Método de autenticación secundario |
|--|---|--|--|
| Security defaults | No se pueden usar directivas de acceso condicional | Se pueden usar directivas de acceso condicional | Aplicación Microsoft Authenticator |
| Directivas de acceso condicional | Si hay alguno habilitado, no puede habilitar los valores predeterminados de seguridad. | Si se deshabilitan todos, puede habilitar los valores predeterminados de seguridad | Especificado por el usuario durante el registro de MFA |
| MFA heredada por usuario (no recomendado) | Invalida los valores predeterminados de seguridad y las directivas de acceso condicional que requieren MFA en cada inicio de sesión | Invalidado por valores predeterminados de seguridad y directivas de acceso condicional | Especificado por el usuario durante el registro de MFA |

Como se describe en el apartado [3.1.1.3 Segregación de funciones y tareas] es importante habilitar MFA al menos para los usuarios con el rol de administración. Para ello:

Security defaults

Para activar el MFA a través de este método:

- Iniciar sesión en el [Centro de administración Microsoft Entra](#) como administrador de seguridad como mínimo.
- Navegar a **Información general > Propiedades**.
- Seleccionar **Administrar los valores predeterminados de seguridad**.
- Cambiar los valores predeterminados de Seguridad a **Habilitado**.



- Click en guardar.

MFA heredada por usuario (no recomendado)

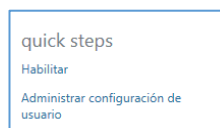
- Acceder al menú [Usuarios\Usuarios Activos].
- Pulsar el icono “Autenticación multifactor” de la barra superior.



- Se accede a un nuevo panel de administración:



- Marcar un usuario con el check correspondiente y habilitar o deshabilitar el MFA en el panel derecho.



Nota: El método Per-user MFA será deprecado el 30 de septiembre de 2025 y será sustituido por Authentication methods de Entra ID. Para migrar al nuevo método, ver el siguiente enlace; [Migración a la directiva de métodos de autenticación - Microsoft Entra ID | Microsoft Learn](#)

Directivas de acceso condicional

Las directivas de acceso condicional son un conjunto de reglas que especifican las condiciones en las que se evalúan y permiten los inicios de sesión. Por ejemplo, puede crear una directiva de acceso condicional que indique lo siguiente:

- Si el nombre de la cuenta de usuario es miembro de un grupo de usuarios a los que se han asignado los roles de administrador de Exchange, de usuarios, de contraseñas, de seguridad, de SharePoint o global, requerir MFA antes de permitir el acceso.

Esta directiva le permite exigir la MFA en función de la pertenencia a grupos, en lugar de intentar configurar cuentas de usuario individuales para la MFA cuando se asignan o se quitan estos roles de administrador.

También puede usar directivas de acceso condicional para funcionalidades más avanzadas, como requerir MFA para aplicaciones específicas o que el inicio de sesión se realice desde un dispositivo compatible, como el equipo portátil que ejecuta Windows 10.

Para más información consultar [CCN-STIC-884A - Guía de configuración segura para Azure]

Powershell de Office 365

Planificación de los métodos de autenticación

Los administradores pueden elegir los métodos de autenticación que quieren que estén disponibles para los usuarios. Es importante habilitar más de un método de autenticación para que los usuarios tengan disponible un método alternativo en caso de que su método principal no esté disponible. Los métodos siguientes están disponibles para que los administradores los habiliten:

- a) **FIDO2 security key:** El usuario conecta la clave de seguridad FIDO2 en su equipo, Windows detecta la llave de seguridad FIDO2, entonces el usuario realiza su gesto para desbloquear la clave privada almacenada en el enclave seguro de la llave de seguridad FIDO2.

Para más información: [Inicio de sesión sin contraseña de Microsoft Entra - Microsoft Entra ID | Microsoft Learn](#)

- b) **Notificación a través de aplicación móvil:** Se envía una notificación push a la aplicación Microsoft Authenticator del dispositivo móvil. El usuario ve la notificación y selecciona Aprobar para completar la comprobación. Las notificaciones push a través de una aplicación móvil proporcionan la opción menos intrusiva para los usuarios.

Para más información: [Método de autenticación de Microsoft Authenticator - Microsoft Entra ID | Microsoft Learn](#)

- c) **Código de verificación desde aplicación móvil:** Una aplicación móvil como la de Microsoft Authenticator genera un nuevo código de verificación de OATH cada 30 segundos. El usuario escribe el código de verificación en la interfaz de inicio de sesión. La opción de aplicación móvil puede utilizarse independientemente de si el teléfono tiene una señal de telefonía móvil o datos.

Para más información: [Método de autenticación de Microsoft Authenticator - Microsoft Entra ID | Microsoft Learn](#)

- d) **SMS:** Se envía al usuario un mensaje de texto que contiene un código de verificación; después, se le pide al usuario que escriba el código de verificación en la interfaz de inicio de sesión.

Para más información: [Métodos de autenticación de teléfono - Microsoft Entra ID | Microsoft Learn](#)

- e) **Pase de acceso temporal (TAP):** El pase de acceso temporal (TAP) es un código de acceso de tiempo limitado que puede configurarse para usarse una o varias veces. Los usuarios pueden iniciar sesión con un TAP para incorporar otros métodos de autenticación sin contraseña, como Microsoft Authenticator, FIDO2 y Windows Hello para empresas.

Para más información: [Configuración de un pase de acceso temporal en Id. de Microsoft Entra para registrar métodos de autenticación sin contraseña - Microsoft Entra ID | Microsoft Learn](#)

- f) **Tokens de hardware OATH (versión preliminar):** Microsoft Entra ID admite el uso de tokens OATH-TOTP SHA-1 que actualizan los códigos cada 30 o 60 segundos. Los clientes pueden adquirir estos tokens a través de proveedores de terceros. Los tokens OATH de hardware están disponibles para usuarios con una licencia Microsoft Entra ID P1 o P2.

Los tokens de hardware TOTP de OATH suelen incluir una clave secreta, o valor de inicialización, programada previamente en el token. Estas claves deben introducirse en Microsoft Entra ID tal como se describe en los pasos siguientes. Las claves secretas están limitadas a 128 caracteres, que no son compatibles con algunos tokens. La clave secreta solo puede contener los caracteres a-z o A-Z y los dígitos 2-7, y debe estar codificada en base 32.

Para más información: [Método de autenticación de token OATH - Microsoft Entra ID | Microsoft Learn](#)

Nota: La versión preliminar solo se admite en nubes globales de Entra ID y Entra ID Government.

- g) **Tokens de software OATH:** Los tokens de software OATH suelen ser aplicaciones, como la aplicación Microsoft Authenticator y otras aplicaciones de autenticador. Microsoft Entra ID genera la clave secreta o valor de inicialización, que se introduce en la aplicación y se usa para generar cada OTP.

Para más información: [Método de autenticación de token OATH - Microsoft Entra ID | Microsoft Learn](#)

- h) **Llamada al teléfono:** Se realiza una llamada de voz automática al usuario. El usuario responde a la llamada y pulsa # en el teclado del teléfono para aprobar su autenticación. La llamada a teléfono es un método alternativo excelente para los códigos de verificación o notificación de una aplicación móvil.

Para más información: [Métodos de autenticación de teléfono - Microsoft Entra ID | Microsoft Learn](#)

- i) **Email OTP:** La característica de código de acceso de un solo uso por correo electrónico es una manera de autenticar a los usuarios de colaboración B2B cuando no se pueden autenticar a través de otros medios, como Microsoft Entra ID, la cuenta Microsoft (MSA) o los proveedores de identidades sociales. Cuando un usuario invitado B2B intenta canjear la invitación o iniciar sesión en los

recursos compartidos, puede solicitar un código de acceso temporal, que se envía a su dirección de correo electrónico. A continuación, escribe el código de acceso para continuar con el inicio de sesión.

Para los usuarios internos del tenant, este método solamente se puede utilizar para la recuperación de la contraseña.

Para más información [Autenticación de código de acceso de un solo uso para usuarios invitados de B2B - Microsoft Entra External ID | Microsoft Learn](#)

- j) **Autenticación basada en certificados:** La autenticación basada en certificados (CBA) de Microsoft Entra habilita a los clientes para permitir o requerir que los usuarios se autenticen directamente con certificados X.509 en Microsoft Entra ID para aplicaciones e inicio de sesión en el explorador. Esta característica permite a los clientes adoptar una autenticación resistente a la suplantación de identidad (phishing) y autenticarse con un certificado X.509 en su infraestructura de clave pública (PKI).

Para más información [Introducción a la autenticación basada en certificados de Microsoft Entra - Microsoft Entra ID | Microsoft Learn](#)

Más información de cómo configurar los distintos métodos de autenticación en la guía [CCN-STIC-884A - Guía de configuración segura para Azure.]

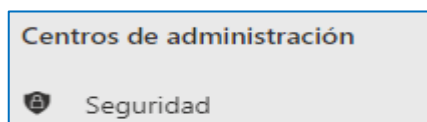
3.1.1.6 MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Ver el apartado **3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS)**

3.1.2 EXPLOTACIÓN

Office 365, al ser un software ofrecido como servicio (SaaS), **siempre estará actualizado**. Es decir, el servicio es mantenido permanentemente por **Microsoft**, encargándose de las actualizaciones y parches, así como de establecer los mecanismos de detección y protección ante amenazas, cumpliendo con los requisitos Esquema Nacional de Seguridad en su categoría ALTA.

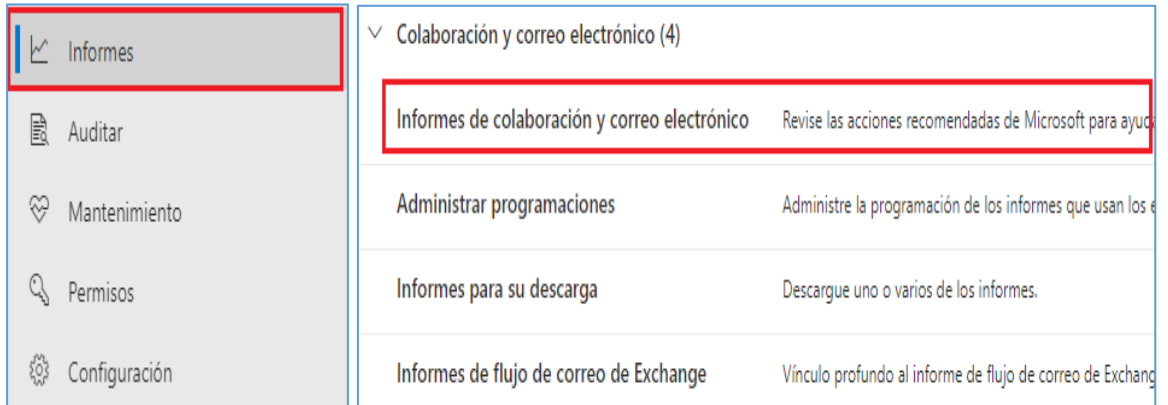
En esta sección se explicará el funcionamiento y las características del Centro de Seguridad al que se accede desde el portal de Administración.



3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

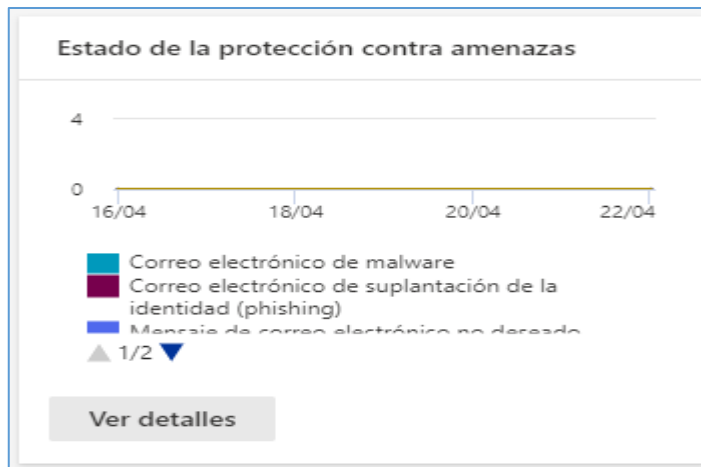
Si la organización dispone de las licencias correspondientes podrá ver el informe de "Estado de protección contra amenazas". El informe de estado de protección contra amenazas proporciona información sobre las amenazas detectadas antes de la entrega de correo electrónico, que abarca tecnologías de detección relevantes, tipos de directivas y acciones de entrega.

- a) Desde el Centro de Seguridad de Office 365 menú [Informes\Informes de colaboración y correo electrónico].



The screenshot shows the Office 365 Security Center interface. On the left, a navigation menu is visible with the following items: Informes (highlighted with a red box), Auditar, Mantenimiento, Permisos, and Configuración. On the right, the 'Colaboración y correo electrónico (4)' section is expanded, showing a list of reports. The first report, 'Informes de colaboración y correo electrónico', is highlighted with a red box and includes the subtext 'Revise las acciones recomendadas de Microsoft para ayudar a...'. Other reports listed include 'Administrar programaciones', 'Informes para su descarga', and 'Informes de flujo de correo de Exchange'.

- b) Click en el botón [Ver detalle] de la tarjeta [Estado de protección contra amenazas]:



Desde este informe se puede ver:

- Ver datos por Información general
- Ver datos por correos electrónicos de suplantación de identidad (phishing)
- Ver datos por correo electrónico de Malware
- Ver datos por correo electrónico de Correo no deseado
- Ver datos por contenido de software malintencionado
- Ver datos por invalidación del sistema

Para más sobre este informe [Ver informes de Defender para Office 365 - Microsoft Defender for Office 365 | Microsoft Learn](#)

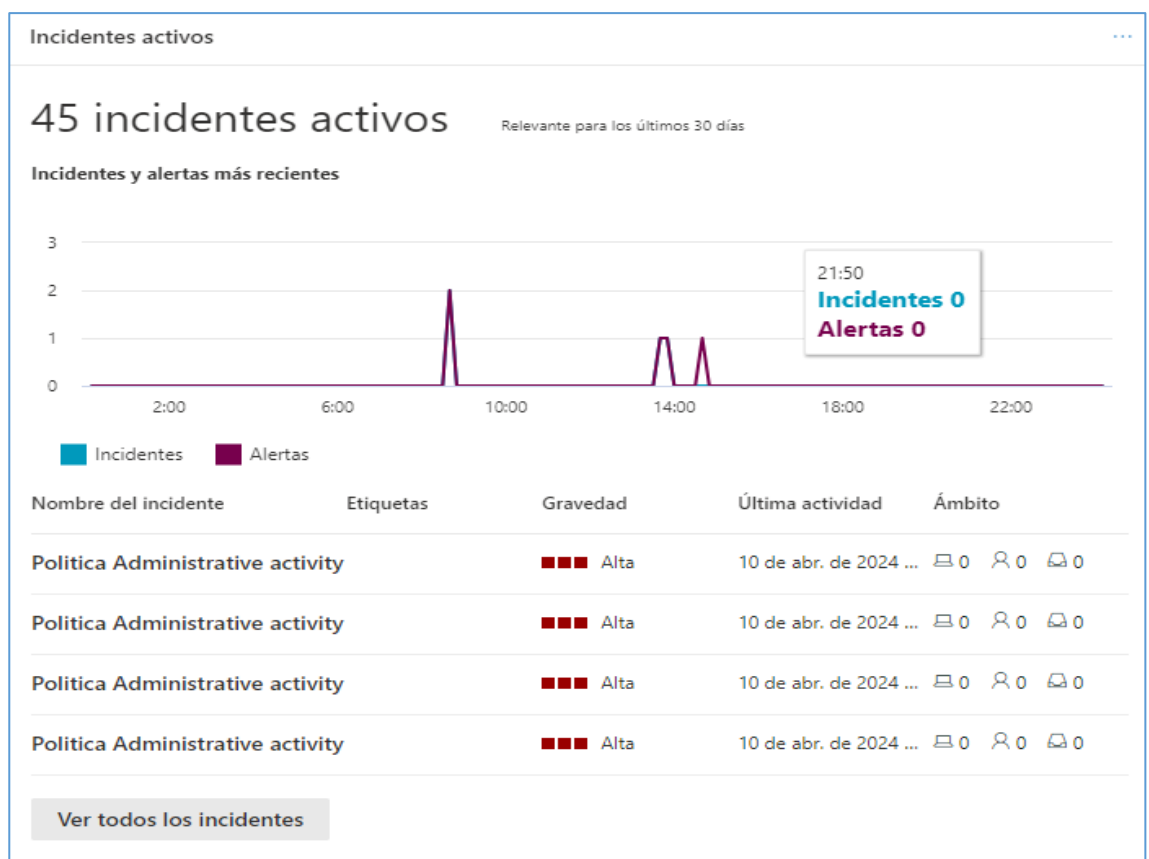
Más información en la guía [CCN-STIC-885C - Guía de configuración segura para Exchange Online].

3.1.2.2 GESTIÓN DE INCIDENTES

Otros informes relevantes relacionados con la gestión de incidentes y accesibles desde el Centro de Seguridad son:

- Panel de alertas. [Inicio] Widget del panel principal

<https://security.microsoft.com/homepage>



- Panel de informes. Menú [Informes].

<https://security.microsoft.com/securityreports>

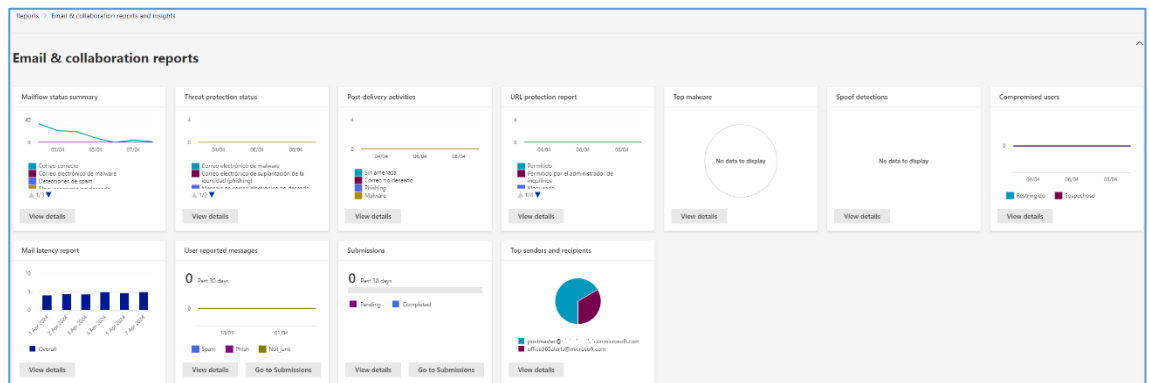
| Informes | |
|--|--|
| Vea información sobre las tendencias de seguridad y realice un seguimiento del estado de protección de identidades, datos, dispositivos, aplicaciones e infraestructura. | |
| 17 elementos | |
| Nombre | Descripción |
| General (2) | |
| Informe de seguridad | Vea información sobre las tendencias de seguridad y realice un seguimiento del estado de protección de identidades, datos, dispositivos, aplicaciones e infraestructura. |
| Recursos de consulta | Revise cómo las consultas de búsqueda consumen recursos y vea cómo evitar la limitación debido al uso excesivo. |
| Extremos (7) | |
| Estado del dispositivo | Supervisar el estado del dispositivo, el estado del software antivirus, las versiones de actualización del antivirus y las plataformas del sistema operativo. |
| Dispositivos vulnerables | Vea información acerca de los dispositivos vulnerables en su organización, tales como su exposición a vulnerabilidades por nivel de gravedad, aprovechamiento, edad y más. |
| Resumen de seguridad mensual | Vea un informe ejecutivo mensual que muestra una instantánea del estado de protección de su organización y el trabajo realizado para evitar y responder a ciberamenazas. |
| Protección web | Obtenga información sobre la actividad web y las amenazas web detectadas en la organización. |
| Firewall | Ver las conexiones bloqueadas por el firewall, incluyendo los dispositivos relacionados, por qué se han bloqueado y qué puertos se han usado |
| Control de dispositivos | En este informe se muestran los datos de uso de contenido medios de su organización. |
| Reglas de reducción de la superficie expuesta a ataques | Vea información acerca de las detecciones, la configuración incorrecta y las exclusiones sugeridas en su entorno. |
| Colaboración y correo electrónico (4) | |
| Informes de colaboración y correo electrónico | Revise las acciones recomendadas de Microsoft para ayudar a mejorar la seguridad del correo electrónico y la colaboración. |
| Administrar programaciones | Administre la programación de los informes que usan los equipos de seguridad para mitigar y solucionar amenazas para la organización. |
| Informes para su descarga | Descargue uno o varios de los informes. |
| Informes de flujo de correo de Exchange | Vínculo profundo al informe de flujo de correo de Exchange en el Centro de administración de Exchange. |
| Aplicaciones en la nube (1) | |
| Informes exportados | Exportaciones generadas para datos, directivas y archivos de Cloud App Discovery, Control de aplicaciones de acceso condicional. |
| Identidades (1) | |
| Administración de informes | Descargue uno o varios informes de Defender for Identity o programe un informe para que se envíe periódicamente por correo electrónico. |

- Informes para su descarga. Menú [Informes\Informes para su descarga].

<https://security.microsoft.com/ReportsForDownload>

| | |
|--------------------------------------|---|
| Informes > Informes para su descarga | |
| <h2>Informes para su descarga</h2> | |
| <u>Personalizado (una vez)</u> | |
| Descargue los informes desde aquí | |
| Actualizar | 0 elementos <input type="text" value="Buscar"/> |
| <input type="checkbox"/> | Fecha de inicio |
| | Nombre |
| | Tipo de informe |
| | Último envío |
| | Estado |
| No hay datos disponibles | |

- Panel de Flujo de correo. Menú [Flujo de correo\Panel].
<https://security.microsoft.com/emailandcollabreport>



3.1.2.3 REGISTRO DE LA ACTIVIDAD

En lo relativo al registro de la actividad de usuarios y administradores se requiere la activación de la **Auditoría** de Office 365.

Cuando se activa la búsqueda de registros de auditoría en el Centro de Seguridad, la actividad de usuario y administrador de la organización se registra en el registro de auditoría y se conserva durante 180 días.

Activar/Desactivar registro de auditoría

Se debe tener asignado el **rol de Audit Logs or View-Only Audit Logs** para activar o desactivar la búsqueda de registros de auditoría en su organización de Office 365. De forma predeterminada, este rol se asigna a los grupos de roles administración de cumplimiento y administración de la organización en la página permisos del centro de administración de Exchange. Los administradores globales de Office 365 son miembros del grupo de funciones de administración de la organización en Exchange Online.

- Desde el Centro de Seguridad de Office 365 menú [Auditar], pulsar el botón “Grabar la actividad de usuarios y administradores”.

Auditar

📄 Obtener información sobre la auditoría

Nueva búsqueda
Directivas de retención de auditoría

Grabar la actividad de usuarios y administradores

Búsquedas completadas **1** | Búsquedas activas **0** | Búsquedas activas sin filtrar **0**

Intervalo de fecha y hora (UTC) *

Inicio

Fin

Búsqueda de palabras clave

Escriba la palabra clave que desea buscar.

Unidades de administración

Elegir las unidades de administración que se van...

Actividades: nombres descriptivos

Elegir qué actividades buscar

Actividades: nombres de operación

Escriba los valores de la operación, separados por c...

Tipos de registros

Seleccione los tipos de registros que quiere buscar

Nombre de la búsqueda

Dar un nombre a la búsqueda

Usuarios

Agregar a los usuarios cuyos registros de auditoría d...

Archivo, carpeta o sitio

Escriba todo o parte del nombre de un archivo, sitio...

Cargas de trabajo

Escriba las cargas de trabajo que desea buscar

Buscar
Borrar todo

- b) Nos saldrá un pop-up solicitando confirmación, Pulsar “Sí”.

Nota: Pueden pasar varias horas desde que se activa el registro de auditoría hasta que estén accesibles los datos en la búsqueda.

Powershell de Office 365

- a) Conexión a Exchange Online mediante PowerShell.
- b) Ejecutar el siguiente comando de PowerShell para activar/desactivar la búsqueda de registros de auditoría en Office 365:

1. Activar auditoría:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

2. Desactivar auditoría:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $false
```

Consultar registro de auditoría

Permite buscar en el registro de auditoría lo que hacen los usuarios y administradores de la organización: actividades relacionadas con el correo electrónico, grupos, documentos, permisos, servicios de directorio y mucho más.

Auditar

[Obtener información sobre la auditoría](#)

Nueva búsqueda
Directivas de retención de auditoría

Búsquedas completadas: 1
Búsquedas activas: 0
Búsquedas activas sin filtrar: 0

Intervalo de fecha y hora (UTC) *

Inici: Apr 09 00:00

Fin: Apr 10 00:00

Búsqueda de palabras clave

Escriba la palabra clave que desea buscar.

Unidades de administración

Elegir las unidades de administración que se van...

Actividades: nombres descriptivos

Elegir qué actividades buscar

Actividades: nombres de operación

Escriba los valores de la operación, separados por c...

Tipos de registros

Seleccione los tipos de registros que quiere buscar

Nombre de la búsqueda

Dar un nombre a la búsqueda

Usuarios

Agregar a los usuarios cuyos registros de auditoría d...

Archivo, carpeta o sitio

Escriba todo o parte del nombre de un archivo, sitio...

Cargas de trabajo

Escriba las cargas de trabajo que desea buscar

Buscar
Borrar todo

Nota: Para realizar búsquedas en el registro de auditoría deben pasar al menos 24 h.

En el desplegable de Actividades se muestran todas las búsquedas posibles relacionadas con el registro de auditoría y clasificadas por temas. Ejemplo de consulta relacionada con la descarga de ficheros:

Buscar información de consulta: Wed, 01 Nov 2023 00:00:00 GMT a Wed, 10 Apr 2024 00:00:00 GMT , filemodified , ,
 Recuento total de resultados: 186 elementos

Exportar

| Fecha (UTC) | Dirección IP | Usuario | Tipo de registro | Actividad | Elemento | Unidades de administra... | Detalles |
|--------------------------|-----------------------------|-----------------|------------------|-------------------------|-----------------------------|-------------------------------|---|
| 3 de abr. de 2024 7:35 | 188.26.212. | jaime.gonzalez@ | cloud... | SharePointFileOperation | Se ha modificado el archivo | CollabHome.aspx | Se modificó en "SitePages" |
| 3 de abr. de 2024 7:35 | 188.26.212 | jaime.gonzalez@ | cloud... | SharePointFileOperation | Se ha modificado el archivo | CollabHome.aspx | Se modificó en "SitePages" |
| 15 de mar. de 2024 11:48 | 2401:1111:1009001:1761:9120 | aserna@ | cloudlab.ornl... | SharePointFileOperation | Se ha modificado el archivo | ~tmpAC_Listado PVP subscri... | Se modificó en "Documents/Apps/Microsoft Forms/Usuarios Externos - CloudLab/Question" |
| 30 de ene. de 2024 10:22 | 32.182.179 | ines.martinez@ | cloudlab... | SharePointFileOperation | Se ha modificado el archivo | documentos-compartidos.as... | Se modificó en "SitePages" |
| 30 de ene. de 2024 10:22 | 32.182.179 | ines.martinez@ | cloudlab... | SharePointFileOperation | Se ha modificado el archivo | venture.aspx | Se modificó en "SitePages" |

Protección de los registros de actividad

A través del uso de roles de usuarios se puede securizar quién puede consultar la información del registro de actividad. Los roles definidos para tal fin son:

- Administradores globales.
- Administradores de Exchange.
- Administradores de SharePoint
- Administradores de Teams.
- Lector de informes.

API de Actividad de administración de Office 365

A parte del Centro de Seguridad Office 365, existe una API de Actividad de administración de Office 365 para recuperar información sobre acciones y eventos de usuario, administrador, sistema y directivas de los registros de actividad de Office 365 y Entra ID.

La API de Actividad de administración de Office 365 es un servicio web REST que se puede usar para desarrollar soluciones mediante cualquier lenguaje y entorno de hospedaje que admita HTTPS y certificados X.509. La API se basa en Microsoft Entra ID y el protocolo OAuth2 para la autenticación y autorización. Para acceder a la API desde la aplicación, primero debe registrarla en Microsoft Entra ID y configurarla con los permisos adecuados. Esto permitirá que la aplicación solicite los tokens de acceso OAuth2 que necesita para llamar a la API. Para obtener más información, vea [Get started with Office 365 Management APIs \(Introducción a las API de administración de Office 365\)](#).

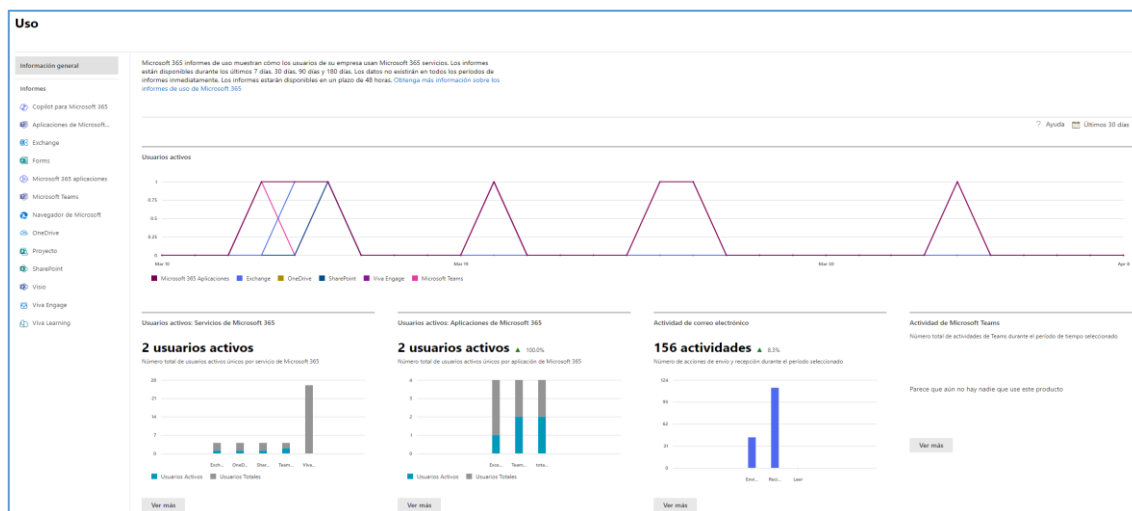
Para obtener información sobre los datos que devuelve la API de Actividad de administración de Office 365, vea: [Esquema de la API de Actividad de administración de Office 365 | Microsoft Learn](#)

Informes de actividades en el centro de administración de Microsoft 365

Otra manera de obtener información de cómo los usuarios de la organización usan los servicios de Office 365 es a través del Centro de administración de Microsoft 365, menú [Informes/Uso]. Por ejemplo, se puede identificar quién está usando mucho un servicio, quién alcanza las cuotas o quién es posible que no necesite una licencia de Office 365 en absoluto.

Los informes pueden obtenerse para los últimos 7, 30, 90 o 180 días. Pulsando sobre cada widget del informe se profundiza en la información suministrada, bajando a un nivel de más detalle.

Nota: los datos no estarán disponibles para todos los períodos de informes al instante (usualmente a las 48 horas).



3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

En cuanto a la protección de las comunicaciones, cabe reseñar que se usan los protocolos criptográficos para conexiones TLS, integrados en Office 365 de manera automática. Esto es así cuando:

- Los usuarios trabajan con archivos guardados en OneDrive For Business o SharePoint Online.
- Los usuarios comparten archivos en reuniones en línea y conversaciones de mensajería instantánea.
- Los usuarios se comunican por correo electrónico.

Todas las comunicaciones de Office 365 están cifradas.

3.2.2 MONITORIZACIÓN DEL SISTEMA

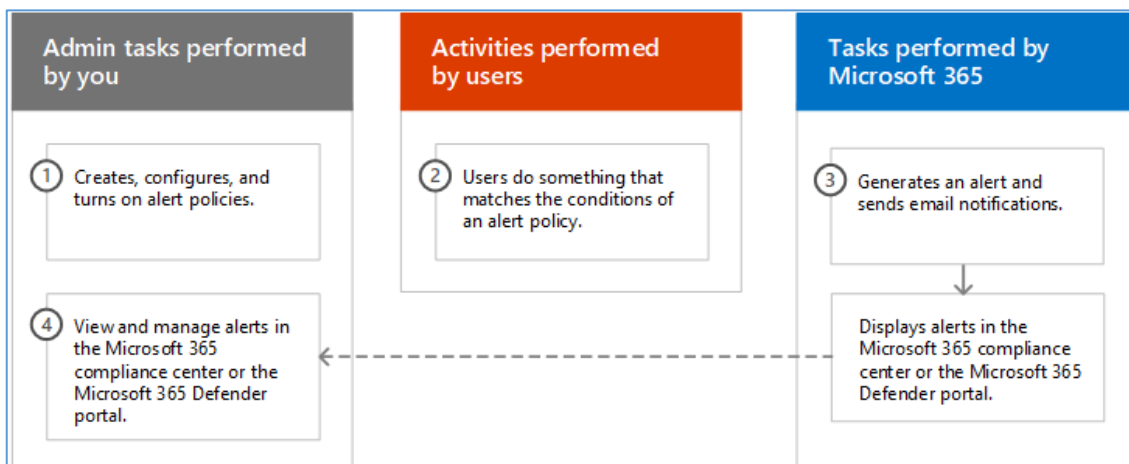
Es posible definir **alertas** en Office 365 a través del Centro de Seguridad de Office 365.

Se pueden usar las alertas de actividad para **enviar notificaciones de correo electrónico** a responsables del sistema cuando los usuarios realizan actividades específicas en Office 365. Las alertas de actividad son similares a la búsqueda de eventos en el registro de auditoría de Office 365, excepto que se enviará un mensaje

de correo electrónico cuando se produzca un evento en el que se haya creado una alerta.

Cómo funcionan las directivas de alerta

A continuación, se presenta una introducción rápida sobre cómo funcionan las directivas de alertas y las alertas que se desencadenan cuando la actividad de usuario o de administrador cumpla las condiciones de una directiva de alerta.



- Un administrador de la organización crea, configura y activa una directiva de alertas mediante la página **Directivas de alerta** del portal de Purview o del portal de Microsoft Defender. También se puede crear directivas de alerta mediante el cmdlet *New-ProtectionAlert* en PowerShell de seguridad & Purview.
- Un usuario realiza una actividad que coincide con las condiciones de una directiva de alerta. En el caso de ataques de malware, los mensajes de correo electrónico infectados enviados a los usuarios de su organización desencadenan una alerta.
- Microsoft 365 genera una alerta que se muestra en la página Alertas en el Portal de Purview o en el portal de Defender. Además, si las notificaciones por correo electrónico están habilitadas para la directiva de alertas, Microsoft envía una notificación a una lista de destinatarios. Las alertas que un administrador u otros usuarios pueden ver que en la página Alertas están determinadas por los roles asignados al usuario.
- Un administrador administra las alertas en el Portal de Purview. La administración de alertas consiste en asignar un estado de alerta para ayudar a realizar un seguimiento y administrar cualquier investigación.

Ver/editar directivas de alerta de sistema

Con las directivas de alerta es posible realizar el seguimiento de las actividades de administradores y usuarios, amenazas de malware o incidentes de pérdida de datos en la organización. Después de elegir la actividad sobre la que se requiere el aviso, se puede afinar la directiva agregando condiciones, decidiendo cuándo activar la alerta y quién debería recibir las notificaciones.

- a) Acceder al menú [Reglas y directivas\Directivas de alerta] desde el Centro de Seguridad de Office 365.

Directiva de alerta Más información

Las alertas de flujo de correo se han movido al nuevo Centro de administración de Exchange. A partir de octubre de 2021, los clientes solo podrán crear, ver o editar alertas de flujo de correo en el nuevo Centro de administración de Exchange. Probar ahora

+ Nueva directiva de alertas Administrar alertas de actividad Actualizar 50 elementos Filtrar

| <input type="checkbox"/> Nombre | Gravedad | Tipo ↓ | Categoría | Fecha de modificación (UTC +02:00) | Etiquetas |
|--|-----------------|---------|----------------------------|------------------------------------|-----------|
| <input type="checkbox"/> MIP AutoLabel simulation completed | ■■■ Bajo | Sistema | Administración de amenazas | 9 de mar. de 2021 16:38 | - |
| <input type="checkbox"/> Suspicious email sending patterns detected | ■■■ Medio | Sistema | Administración de amenazas | 11 de feb. de 2020 18:07 | - |
| <input type="checkbox"/> Email messages removed after delivery | ■■■ Informativo | Sistema | Administración de amenazas | 12 de abr. de 2022 13:26 | - |
| <input type="checkbox"/> Email messages from a campaign removed after delivery | ■■■ Informativo | Sistema | Administración de amenazas | 12 de abr. de 2022 13:26 | - |
| <input type="checkbox"/> Admin triggered user compromise investigation | ■■■ Medio | Sistema | Administración de amenazas | 3 de ago. de 2021 11:37 | - |

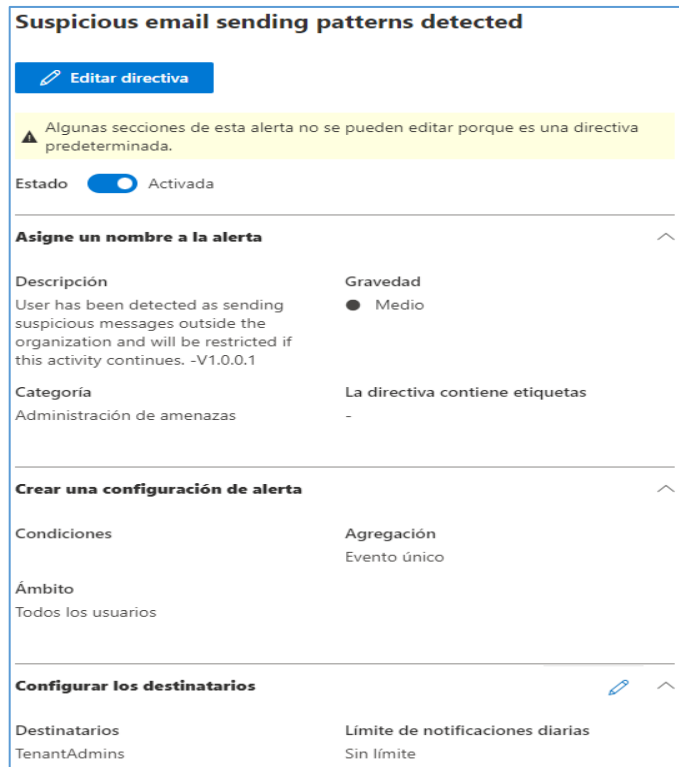
- b) Marcar las alertas sobre las cuales se quiere realizar el seguimiento de la lista de alertas predefinidas. Las alertas predefinidas se pueden activar o desactivar y cambiar parte de su configuración.

| <input type="checkbox"/> Nombre | Gravedad | Tipo ↓ | Categoría | Fecha de modificación (UTC +02:00) | Etiquetas |
|--|-----------------|---------|----------------------------|------------------------------------|-----------|
| <input type="checkbox"/> MIP AutoLabel simulation completed | ■■■ Bajo | Sistema | Administración de amenazas | 9 de mar. de 2021 16:38 | - |
| <input type="checkbox"/> Suspicious email sending patterns detected | ■■■ Medio | Sistema | Administración de amenazas | 11 de feb. de 2020 18:07 | - |
| <input type="checkbox"/> Email messages removed after delivery | ■■■ Informativo | Sistema | Administración de amenazas | 12 de abr. de 2022 13:26 | - |
| <input type="checkbox"/> Email messages from a campaign removed after delivery | ■■■ Informativo | Sistema | Administración de amenazas | 12 de abr. de 2022 13:26 | - |

Más información de las alertas predeterminadas en la documentación de Microsoft. [Directivas de alertas de Microsoft 365 | Microsoft Learn](#)

- c) Pulsar sobre una directiva concreta para acceder a sus propiedades.

Por ejemplo, la directiva “Suspicious email sending patterns detected” la cual se activa cuando se detecta que un usuario ha enviado un correo o correos con texto con patrones sospechosos.



Suspicious email sending patterns detected

Editar directiva

Algunas secciones de esta alerta no se pueden editar porque es una directiva predeterminada.

Estado Activada

Asigne un nombre a la alerta

| | |
|---|---------------------------------|
| Descripción | Gravedad |
| User has been detected as sending suspicious messages outside the organization and will be restricted if this activity continues. -V1.0.0.1 | ● Medio |
| Categoría | La directiva contiene etiquetas |
| Administración de amenazas | - |

Crear una configuración de alerta

| | |
|--------------------|--------------|
| Condiciones | Agregación |
| Ámbito | Evento único |
| Todos los usuarios | |

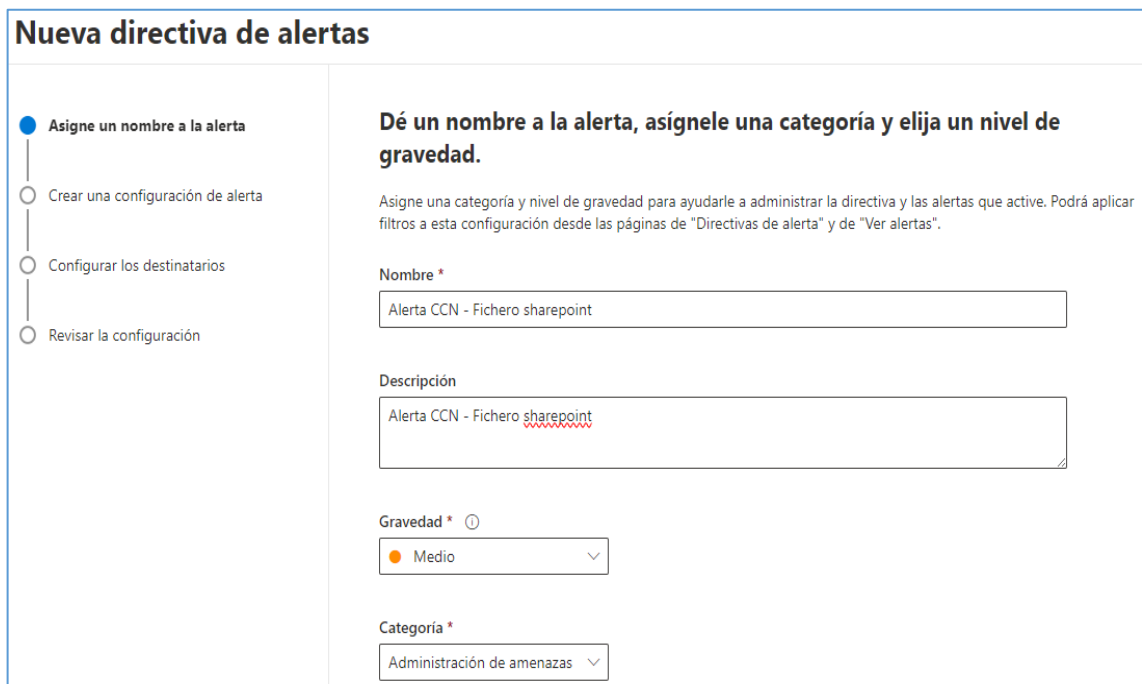
Configurar los destinatarios

| | |
|---------------|----------------------------------|
| Destinatarios | Límite de notificaciones diarias |
| TenantAdmins | Sin límite |

Crear directivas de alerta personalizadas

Para crear una **directiva de alerta personalizada** pulsar el botón “Nueva directiva de alertas”, en el menú [Reglas y directivas\Directivas de alertas]. Como ejemplo se va a crear una directiva para el borrado sospechoso de ficheros word en una ubicación concreta (sitio de Sharepoint CCN-SPO-SITIO1).

- a) Asignar un nombre.



Nueva directiva de alertas

- Asigne un nombre a la alerta
- Crear una configuración de alerta
- Configurar los destinatarios
- Revisar la configuración

Dé un nombre a la alerta, asígnele una categoría y elija un nivel de gravedad.

Asigne una categoría y nivel de gravedad para ayudarle a administrar la directiva y las alertas que active. Podrá aplicar filtros a esta configuración desde las páginas de "Directivas de alerta" y de "Ver alertas".

Nombre *
Alerta CCN - Fichero sharepoint

Descripción
Alerta CCN - Fichero sharepoint

Gravedad * ⓘ
● Medio

Categoría *
Administración de amenazas

b) Crear configuración de alerta.

¿Sobre qué se quiere enviar alertas? Seleccionar una **actividad**:

Nueva directiva de alertas

Asigne un nombre a la alerta
 Crear una configuración de alerta
 Configurar los destinatarios
 Revisar la configuración

Elija una actividad, condiciones y cuándo se debe activar la alerta
 Solo puede elegir una actividad, pero puede agregar condiciones para refinar qué se detectará.

¿Sobre qué quiere enviar alertas?

La actividad es

Seleccione una actividad

Pantalla capturada
 Actividades de archivos y carpetas

- Se ha accedido al archivo
- Se ha protegido el archivo
- Se ha desprotegido el archivo
- Se ha copiado el archivo
- Se ha eliminado el archivo**
- Se ha descartado la desprotección del archivo
- Se ha descargado el archivo
- Se ha modificado el archivo

Cuando el volumen de las actividades que coincidan sea poco frecuente

Activada Todos los usuarios

Agregar condiciones:

Para la mayoría de las actividades, se puede definir condiciones adicionales que deben cumplirse para desencadenar una alerta. Las condiciones comunes incluyen referencias a direcciones IP (por lo que se desencadena una alerta cuando el usuario realiza la actividad en un equipo con una dirección IP específica o dentro de un intervalo de direcciones IP), usuarios concretos, nombres de archivos, urls de sitios o extensiones de archivos.

Nueva directiva de alertas

Asigne un nombre a la alerta
 Crear una configuración de alerta
 Configurar los destinatarios
 Revisar la configuración

Elija una actividad, condiciones y cuándo se debe activar la alerta
 Solo puede elegir una actividad, pero puede agregar condiciones para refinar qué se detectará.

¿Sobre qué quiere enviar alertas?

La actividad es

Se ha eliminado el archivo

El usuario elimina un documento de un sitio.

+ Agregar condición

General: La dirección IP es
 Usuario: El usuario es
 Usuario: Las etiquetas de usuario son
 Archivo: El nombre de archivo es alcance un umbral
 Archivo: La dirección URL de la colección de sitios es actividades
 Archivo: La extensión de archivo es minutos

Cuando el volumen de las actividades que coincidan sea poco frecuente

Activada Todos los usuarios

En el ejemplo:

^ Archivo: La extensión de archivo es 🗑️

Como cualquiera de ▾

txt, doc*, pptx

AND

^ Archivo: La dirección URL de la colección de sitios es 🗑️

Como cualquiera de ▾

https://*.sharepoint.com/sites/CCN-SPO-SITIO1

¿Cómo quiere que se active la alerta?

¿Cómo quiere que se active la alerta?

Cada vez que una actividad coincide con la regla

Cuando el volumen de las actividades que coincidan alcance un umbral

Mayor que o igual a actividades

En los últimos minutos

Activada ▾

Cuando el volumen de las actividades que coincidan sea poco frecuente

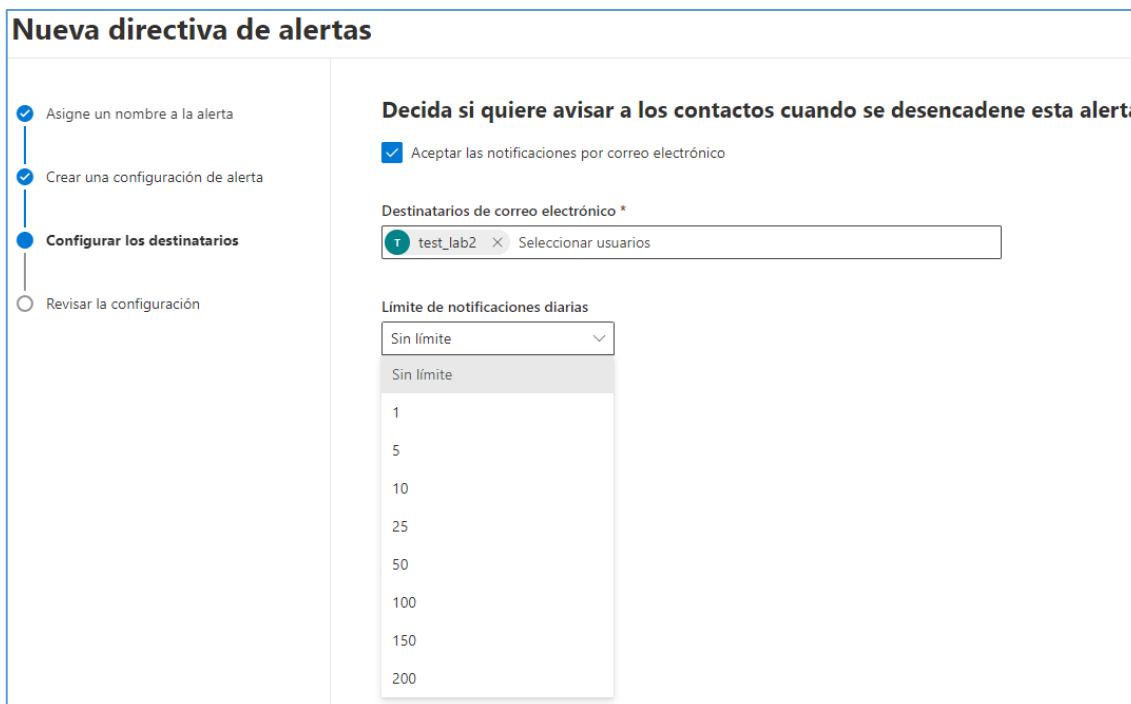
Activada ▾

Puede configurar una configuración que defina la frecuencia con la que se puede producir una actividad antes de que se desencadene una alerta.

Puede configurar una directiva para generar una alerta cada vez que una actividad coincide con las condiciones de la directiva, cuando se supera un umbral determinado.

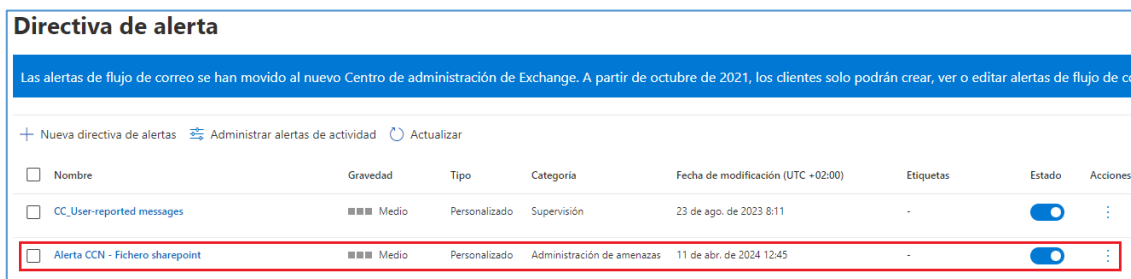
Puede configurar la directiva para generar una alerta cuando la aparición de la actividad que la alerta está realizando se vuelve inusual para su organización. Si selecciona la configuración en función de una actividad inusual, Microsoft establece un valor de línea base que define la frecuencia normal de la actividad seleccionada. El establecimiento de esta línea base tarda hasta siete días, durante los cuales no se generarán alertas. Una vez establecida la línea base, se desencadena una alerta cuando la frecuencia de la actividad a la que realiza el seguimiento la directiva de alerta supera en gran medida el valor de línea base.

c) Configurar los destinatarios



Consultar directivas de alertas

Desde el menú [Alertas\Directivas de alertas] pueden consultarse las directivas personalizadas, así como todas las directivas predeterminadas en el Centro de Seguridad de Office 365.



| Nombre | Gravedad | Tipo | Categoría | Fecha de modificación (UTC +02:00) | Etiquetas | Estado | Acciones |
|---------------------------------|----------|---------------|----------------------------|------------------------------------|-----------|--------|----------|
| CC_User-reported messages | Medio | Personalizado | Supervisión | 23 de ago. de 2023 8:11 | - | On | ⋮ |
| Alerta CCN - Fichero sharepoint | Medio | Personalizado | Administración de amenazas | 11 de abr. de 2024 12:45 | - | On | ⋮ |

3.2.3 PROTECCIÓN DE LA INFORMACIÓN

3.2.3.1 CALIFICACIÓN DE LA INFORMACIÓN

En este apartado se tratarán principalmente los mecanismos que ofrece Office 365 para calificar la información y aplicar políticas determinadas. En concreto:

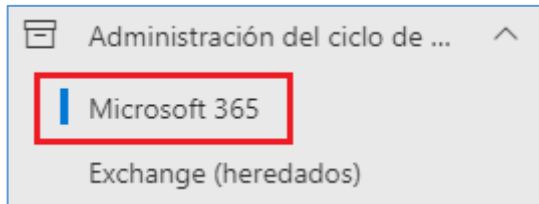
Tipos de información confidencial.

- **Ciclo de vida del dato** (Conocido anteriormente como Políticas de retención): La administración del ciclo de vida de datos de Microsoft Purview (anteriormente gobernanza de información de Microsoft) le proporciona herramientas y capacidades para conservar el contenido que necesita conservar y eliminar el que no.

- **DLPs (Data Loss Prevention).** Con estas políticas de Prevención de Pérdida de Datos se puede identificar, supervisar y proteger información sensible en todo Office 365.
- **Sensitivity labels.** Permiten clasificar, cifrar, agregar marcadores y controlar accesos en documentos y correos electrónicos en Office 365.

POLÍTICAS DE RETENCIÓN

Definición de etiquetas de retención



Estas etiquetas se definen en el Portal de Purview de Office 365, en el menú [Administración del ciclo de vida de datos\Microsoft 365\Etiquetas], una vez dentro y se utilizan para aplicar políticas de retención a correos de Exchange y documentos de SharePoint y OneDrive. Se puede definir el tiempo que el correo o el documento debe retenerse, o el tiempo después del cual debe borrarse. Además, las retenciones se pueden aplicar a partir de la fecha de creación, de última modificación, o a partir de la fecha de aplicación de la etiqueta.

También se puede declarar un documento como Registro para impedir que sea editado o borrado.

Las etiquetas pueden aplicarse **automáticamente** según las condiciones establecidas en el Portal de Purview de Office 365, y los usuarios también pueden aplicar estas etiquetas directamente en las aplicaciones Office, así como en SharePoint o OneDrive.

Las **etiquetas de retención** tienen que ver con el cumplimiento, y se aplican a correos o documentos en una ubicación determinada.

Ejemplo: en el departamento comercial se precisa aplicar políticas de retención sobre documentos diversos:

- Presupuestos: retención de 5 años después de la fecha límite del presupuesto.
- Contratos: retención de 10 años después de la fecha de finalización del contrato.
- Hojas de producto: declarado como registro (no borrar).

Consulta y modificación de etiquetas de retención

- Acceder a la pestaña de [Etiquetas].
- Seleccionar una etiqueta.

Administración del ciclo de vida de datos

Información general Directivas de retención **Etiquetas** Directivas de etiquetas Ámbitos de adaptación Búsqueda de directiva ...

Cree etiquetas para los elementos que necesiten excepciones a las directivas de retención. Entre las excepciones se incluyen la ampliación del período de retención de documentos específicos o la prevención de que determinados correos electrónicos se eliminen permanentemente, por ejemplo. Si necesita aún más opciones de etiqueta, use Administración de registros > Plan de archivos para administrar el contenido. [Más información sobre el uso de etiquetas de retención para excepciones](#)

+ Crear una etiqueta Publicar etiquetas Importar Exportar Actualizar 4 elementos EtiquetaRe

| <input type="checkbox"/> Nombre | Duración de retención | Última modificación |
|---|-----------------------|--------------------------|
| <input type="checkbox"/> EtiquetaRetencion 3 | 7 años | 26 de oct. de 2020 14:06 |
| <input type="checkbox"/> EtiquetaRetencion 1 | 5 años | 22 de oct. de 2020 12:45 |
| <input type="checkbox"/> EtiquetaRetencion 4 sin publicar | 7 años | 28 de oct. de 2020 20:19 |
| <input type="checkbox"/> EtiquetaRetencion 2 | 10 años | 26 de oct. de 2020 13:44 |

- Editar etiqueta. En el panel derecho pulsar el botón “Editar etiqueta”. Definimos la configuración de etiqueta.

Modificar etiqueta de retención

Nombre
 Configuración de la etiqueta
 Período
 Finalizar

Definir la configuración de etiqueta

Aplicaremos la configuración que elija a los elementos etiquetados

- Conservar elementos para siempre o durante un período específico**
Los elementos no se conservarán, pero cuando alcancen la antigüedad que se especifique, se eliminarán de donde estén almacenados.
- Aplicar acciones después de un período específico**
Los elementos etiquetados no se conservarán. Puede decidir si se deben eliminar o volver a etiquetar cuando finalice el período que especifique en el paso siguiente.
- Solo elementos de etiqueta**
Elija esta configuración si solo desea clasificar los elementos etiquetados. Los elementos no se conservarán y los usuarios no podrán editarlos, moverlos ni eliminarlos.

- Configuramos el periodo de retención

Definir el período de retención

Especifique cuánto tiempo debe durar el período de retención.

Conservar elementos para

5 años

Iniciar el período de retención basado en

La última vez que se modificaron los elementos

+ Crear nuevo tipo de evento

e) Configuramos la acción a ejecutar después del periodo

Elegir lo que sucede después del período de retención

Esta configuración determina qué ocurre con los elementos cuando finaliza el período de retención.

- Eliminar elementos automáticamente**
Quitaremos permanentemente los elementos etiquetados desde cualquier lugar en el que se almacenen.
- Iniciar una revisión para eliminación**
Permita que los revisores para eliminación que asigne en el paso siguiente decidan si los elementos se pueden eliminar de forma segura o si se deben realizar otras acciones (como cambiar el período de retención). [Más información](#)
- Cambiar la etiqueta**
Puede ampliar el período eligiendo una etiqueta existente con la que reemplazar esta. [Más información acerca de reetiquetado de elementos](#)
- Seleccionar un flujo de Power Automate**
Personalice lo que sucede con los elementos etiquetados con un flujo de Power Automate. Puede ejecutar un flujo para satisfacer una necesidad empresarial específica, como mover elementos etiquetados a una ubicación determinada o enviar notificaciones de correo electrónico. [Más información sobre cómo ejecutar un flujo de Power Automate](#)
- Desactivar la configuración de retención**
Los elementos etiquetados no se conservarán ni eliminarán cuando se desactive su configuración de retención. Tendrá que quitar manualmente los elementos que desee eliminar.

Una vez termine el periodo de retención establecido en la etiqueta, se debe elegir qué hacer con el elemento etiquetado:

- **Eliminar elementos automáticamente.** Se quitarán permanentemente los elementos etiquetados desde cualquier lugar en el que se almacenen.
- **Iniciar una revisión para su eliminación.** Permite que revisores para eliminación que se asignen decidan si los elementos se pueden eliminar o si deben realizar otras acciones.
- **Cambiar la etiqueta.** Se puede ampliar el periodo de retención aplicando otra etiqueta.
- **Seleccionar un flujo de Power Automate.** Se puede ejecutar un flujo de Power Automate para satisfacer una necesidad empresarial específica.
- **Desactivar la configuración de retención.** Con esta opción los elementos etiquetados no se conservarán ni eliminarán cuando se desactive su configuración de retención.

Creación de una etiqueta de retención

a) Acceder al menú [Etiquetas] y pulsamos el botón “Crear una etiqueta”.

Administración del ciclo de vida de datos

Información general Directivas de retención Etiquetas Directivas de etiqu

Cree etiquetas para los elementos que necesiten excepciones a las directivas de retención. Entre archivos para administrar el contenido. [Más información sobre el uso de etiquetas de retención](#)

+ Crear una etiqueta Publicar etiquetas Importar Exportar Actualizar

b) Asignar nombre a la etiqueta.

- Nombre
- Configuración de la etiqueta
- Período
- Finalizar

Asigne un nombre a la etiqueta de retención

Este es el nombre de la etiqueta que verán los usuarios en las aplicaciones donde se publicó (como Outlook, SharePoint y OneDrive). Asegúrese de seleccionar un nombre que les ayude a comprender su finalidad.

① Cree etiquetas con Administración de registros para tener acceso a más opciones de configuración de etiquetas. [Crear una etiqueta con Administración de registros.](#)

Nombre *

Descripción para usuarios

Descripción para administradores

c) Definimos la configuración de la etiqueta.

- Nombre
- Configuración de la etiqueta
- Período
- Finalizar

Definir la configuración de etiqueta

Aplicaremos la configuración que elija a los elementos etiquetados

- Conservar elementos para siempre o durante un periodo específico**
Los elementos no se conservarán, pero cuando alcancen la antigüedad que se especifique, se eliminarán de donde estén almacenados.
- Aplicar acciones después de un periodo específico**
Los elementos etiquetados no se conservarán. Puede decidir si se deben eliminar o volver a etiquetar cuando finalice el período que especifique en el paso siguiente.
- Solo elementos de etiqueta**
Elija esta configuración si solo desea clasificar los elementos etiquetados. Los elementos no se conservarán y los usuarios no podrán editarlos, moverlos ni eliminarlos.

d) Configurar el periodo de retención de la etiqueta.

- Nombre
- Configuración de la etiqueta
- Período
- Finalizar

Definir el período de retención

Especifique cuánto tiempo debe durar el período de retención.

Conservar elementos para

Iniciar el período de retención basado en

- Cuando se crearon los elementos
- La última vez que se modificaron los elementos
- Cuando los elementos se etiquetaron
- Employee activity (tipo de evento)
- Empleo finalizado (tipo de evento)
- Expiration or termination of contracts and agreements (tipo de even...
- Product lifetime (tipo de evento)

e) Configuramos la acción a suceder después del periodo de retención

- Nombre
- Configuración de la etiqueta
- Periodo**
- Configuración después del periodo
- Finalizar

Elegir lo que sucede después del período de retención

Esta configuración determina qué ocurre con los elementos cuando finaliza el período de retención.

- Eliminar elementos automáticamente**
Quitaremos permanentemente los elementos etiquetados desde cualquier lugar en el que se almacenen.
- Iniciar una revisión para eliminación**
Permita que los revisores para eliminación que asigne en el paso siguiente decidan si los elementos se pueden eliminar de forma segura o si se deben realizar otras acciones (como cambiar el período de retención). [Más información](#)
- Cambiar la etiqueta**
Puede ampliar el período eligiendo una etiqueta existente con la que reemplazar esta. [Más información acerca de reetiquetado de elementos](#)
- Seleccionar un flujo de Power Automate**
Personalice lo que sucede con los elementos etiquetados con un flujo de Power Automate. Puede ejecutar un flujo para satisfacer una necesidad empresarial específica, como mover elementos etiquetados a una ubicación determinada o enviar notificaciones de correo electrónico. [Más información sobre cómo ejecutar un flujo de Power Automate](#)
- Desactivar la configuración de retención**
Los elementos etiquetados no se conservarán ni eliminarán cuando se desactive su configuración de retención. Tendrá que quitar manualmente los elementos que desee eliminar.

f) Revisar y Crear.

- Nombre
- Configuración de la etiqueta
- Período
- Finalizar**

Revisar y finalizar

Nombre

Nombre
CCN-ETIQUETA-RETENCION1
[Editar](#)

Descripción para usuarios
CCN-ETIQUETA-RETENCION1
[Editar](#)

Descripción para administradores
ETIQUETA de retención para presupuestos.
[Editar](#)

Configuración de retención

| Período de retención | Acción de retención |
|----------------------------------|--|
| 7 años Editar | Conservar y eliminar Editar |

Basado en
Basado en fecha en la que se creó
[Editar](#)

- Nombre
- Configuración de la etiqueta
- Período
- Finalizar

✔ Se creó la etiqueta de retención

Crear la etiqueta sólo es el primer paso para clasificar y controlar el contenido. Para que esta etiqueta esté disponible para todos los usuarios de su organización, publíquela en ubicaciones seleccionadas o aplíquela automáticamente a contenido específico.

Siguientes pasos

- Publicar esta etiqueta en las ubicaciones de Microsoft 365**
Crear una directiva de etiquetas para que esta etiqueta esté disponible en ubicaciones como Exchange y OneDrive. Cuando se publican, los usuarios pueden aplicarla manualmente a su contenido o establecerla como la etiqueta predeterminada para contenedores de contenido (como las bibliotecas de documentos de SharePoint o las carpetas de correo electrónico).
- Aplicar esta etiqueta automáticamente a un tipo de contenido específico**
Crear una directiva de etiquetado automático para aplicar la etiqueta al contenido que coincida con determinadas condiciones, como contenido que incluya información confidencial específica.
- No hacer nada**
Puede publicarlo o aplicarlo automáticamente al contenido más adelante.

Directivas de etiquetas (Publicar etiquetas)

Una vez creada la etiqueta, el siguiente paso para poder utilizarla es “Publicar etiqueta”.

- a) se puede hacer desde la misma pestaña de Etiquetas, haciendo click en “Publicar etiqueta” o desde la pestaña “Directiva de etiquetas”.

Administración del ciclo de vida de datos

Información general Directivas de retención **Etiquetas** Directivas de etiquetas Ámbitos de adaptación Búsqueda de directiva ...

Cree etiquetas para los elementos que necesiten excepciones a las directivas de retención. Entre las excepciones se incluyen la ampliación del período de retención de documentos específicos o la prevención de que determinados correos electrónicos se eliminen permanentemente, por ejemplo. Si necesita aún más opciones de etiqueta, use Administración de registros > Plan de archivos para administrar el contenido. [Más información sobre el uso de etiquetas de retención para excepciones](#)

1 elemento

| <input type="checkbox"/> Nombre | Duración de retención | Última modificación |
|--|-----------------------|--------------------------|
| <input type="checkbox"/> CCN-ETIQUETA-RETENCION1 | 7 años | 16 de abr. de 2024 13:25 |

- b) Elegir las etiquetas.

Publique etiquetas para que los usuarios puedan aplicarlas a su contenido.

- Elija las etiquetas para publicar**
- Unidades administrativas
- Ámbito
- Asignar un nombre a la directiva
- Finalizar

Elija las etiquetas para publicar

Elija las etiquetas que desea publicar en las aplicaciones de su organización para que los usuarios puedan aplicarlas a su contenido. Si no ve las etiquetas que desea, podrá crear una nueva.

* Elija las etiquetas para publicar

Elegir una etiqueta

1 elemento

| <input type="checkbox"/> Nombre | Retención |
|--|-----------------------------|
| <input type="checkbox"/> CCN-ETIQUETA-RETENCION1 | 7 años conservar + suprimir |

Agregar

Cancelar

- c) Elegir ámbito de directiva, es decir, si se aplicara a todo el Directorio o a una unidad de Administración en concreto.

- Elija las etiquetas para publicar
- Unidades administrativas**
- Ámbito
- Asignar un nombre a la directiva
- Finalizar

Ámbito de directiva

Elija las unidades de administración a las que quiere aplicar esta directiva. Las selecciones afectarán a las opciones que tenga en el paso de selección de ubicaciones.

+ Agregar o quitar unidades de administración

Unidades de administración

Directorio completo

- d) Elegir tipo de directiva de retención

- Elija las etiquetas para publicar
- Unidades administrativas
- Ámbito**
- Asignar un nombre a la directiva
- Finalizar

Elija el tipo de directiva de retención que quiere crear

Las ubicaciones se pueden especificar dinámicamente con un ámbito adaptable mediante atributos o propiedades, o bien, si conoce las ubicaciones de destino específicas, puede seleccionarlas individualmente en una lista. Una ventaja de usar un ámbito adaptable para determinar las ubicaciones de destino es que se actualizará automáticamente donde se aplique en función de los atributos o propiedades que defina.

- Adaptable**
Después de seleccionar ámbitos de directiva adaptables, que consisten en atributos o propiedades (por ejemplo, "Departamento" o "Dirección URL del sitio") que definen los usuarios, grupos o sitios de la organización, elegirá ubicaciones admitidas que contengan el contenido que quiera conservar. La directiva se actualizará automáticamente para que coincida con los criterios definidos en los ámbitos.
- Estático**
Elegirá las ubicaciones que incluyen el contenido que desea conservar. Si las ubicaciones cambian después de que se haya creado esta directiva (por ejemplo, si se ha agregado o quitado un sitio de SharePoint), tendrá que actualizar la directiva de forma manual.

- e) Elegir ubicaciones.

- Elija las etiquetas para publicar
- Unidades administrativas
- Ámbito**
- Publicar para usuarios y grupos
- Asignar un nombre a la directiva
- Finalizar

Seleccionar dónde quiere publicar la noticia

Cuando se publique, los usuarios de su organización podrán aplicar esta etiqueta a los elementos de las ubicaciones que elija.

1 Puede configurar conectores de datos para importar contenido de aplicaciones que no son de Microsoft, como Slack, WhatsApp, entre otras, y úselo con esta solución. [Configurar ahora](#)

- Todas las ubicaciones. Incluye el contenido del correo electrónico de Exchange, los grupos de Office 365 y los documentos de OneDrive y SharePoint.
- Permíteme elegir ubicaciones específicas.

| Estado | Ubicación | Incluido | Excluido |
|--|---|---|--------------------------------|
| <input checked="" type="checkbox"/> Activada | Buzones de Exchange | Todo buzones de correo Editar | Ninguno Editar |
| <input type="checkbox"/> Desactivada | Sitios clásicos y de comunicación de SharePoint | | |
| <input checked="" type="checkbox"/> Activada | Cuentas de OneDrive | Todo cuentas del usuario Editar | Ninguno Editar |
| <input checked="" type="checkbox"/> Activada | Buzones de grupo y sitios de Microsoft 365 | Todo grupos de microsoft 365 Editar | Ninguno Editar |

Hay que tener en cuenta que, en **Exchange**, las etiquetas de retención de aplicación automática (tanto para consultas como para tipos de información sensible) **solo se aplican en los nuevos mensajes enviados** (datos en tránsito), no en todos los elementos que ya están presentes en el buzón (datos en reposo).

Además, las etiquetas de retención de aplicación automática para tipos de información sensible se aplican a todos los buzones (no se pueden seleccionar buzones específicos).

f) Dar un nombre a la directiva.

- Elija las etiquetas para publicar
- Unidades administrativas
- Ámbito
- Asignar un nombre a la directiva**
- Finalizar

Asignar un nombre a la directiva

Nombre *

Descripción

CCN-DIRECTIVA-RETENCION1

g) Revisar y Publicar.

- Elija las etiquetas para publicar
- Unidades administrativas
- Ámbito
- Asignar un nombre a la directiva
- Finalizar**

Finalizar

⚠ La mayoría de las etiquetas estarán disponibles para sus usuarios en una semana. Las etiquetas aparecerán en Outlook y Outlook en la Web solo para buzones con al menos 10 MB de datos.

Elija las etiquetas para publicar
 Se publicará 1 etiqueta (estará disponible) para que los usuarios puedan clasificar su contenido
 CCN-ETIQUETA-RETENCION1 7 años conservar + suprimir
[Editar](#)

Se aplica al contenido en estas ubicaciones
 Buzones de Exchange (Todo Destinatarios)
 Cuentas de OneDrive (Todo Sitios)
 Buzones de grupo y sitios de Microsoft 365 (Todo Grupos)
[Editar](#)

Nombre
 CCN-DIRECTIVA-RETENCION1
[Editar](#)

Descripción
 CCN-DIRECTIVA-RETENCION1
[Editar](#)

Nota: Las etiquetas tardarán hasta 1 día en mostrarse a los usuarios. Las etiquetas aparecerán en Outlook y Outlook Web App solo para los buzones que tengan al menos 10 MB de datos.

Puede consultarse la nueva directiva en la pestaña correspondiente:

Administración del ciclo de vida de datos

Información general
Directivas de retención
Etiquetas
Directivas de etiquetas
Ámbitos de adaptación
Búsqueda de directiva
...

Cree directivas de etiquetas de retención para publicar o aplicar etiquetas automáticamente. La publicación de etiquetas en ubicaciones específicas (como Exchange o SharePoint) permite a los usuarios aplicar etiquetas manualmente a su contenido. Cuando aplique etiquetas automáticamente, las aplicaremos al contenido que coincida con sus condiciones. Más información sobre etiquetado automático y directivas de etiquetas de publicación

Publicar etiquetas

Aplicar automáticamente una etiqueta

Actualizar

1 elemento

| Nombre | Estado | Tipo | Creado por | Última m... | Última modificación |
|---|---|----------|------------|-------------|---------------------|
| <input type="checkbox"/> CCN-DIRECTIVA-RETENCION1 | ⋮ Habilitado | Publicar | | | 16/4/2024 |

Uso de las directivas de retención

Más información en las guías específicas de cada servicio: Sharepoint Online [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online], Exchange Online [CCN-STIC-885C - Guía de configuración segura para Exchange Online].

DLPs (DATA LOSS PREVENTION)

Con estas políticas de Prevención de Pérdida de Datos se puede identificar, supervisar y proteger información sensible en todo Office 365. Por ejemplo, puede configurar directivas para asegurarse de que la información en correos electrónicos y documentos no se comparta con los contactos inadecuados.

Ejemplos de datos susceptibles de aplicación:

- Datos financieros
- Información de identificación personal
 - Tarjetas de crédito
 - Números de Seguridad Social
 - Registros Médicos, etc.

Elementos de una directiva DLP

- Dónde proteger el contenido: ubicaciones como Exchange Online, SharePoint Online y sitios de OneDrive para la Empresa, así como mensajes de chat y canales de Microsoft Teams.
- Cuándo y cómo proteger el contenido aplicando reglas compuestas de:
 - **Condiciones** que el contenido debe cumplir antes de que se aplique la regla. Por ejemplo, una regla se puede configurar para que busque solo contenido que incluya números de seguridad social y que se haya compartido con personas de fuera de su organización.
 - **Acciones** que quiere que la regla realice automáticamente cuando se encuentra contenido que coincide con las condiciones. Por ejemplo, una regla se puede configurar para bloquear el acceso a un documento y enviar una notificación por correo electrónico al usuario y al responsable de cumplimiento.

Por ejemplo, se podría tener una directiva DLP que ayude al tratamiento de datos relativos a la salud.

| | |
|----------------------|--|
| ¿el qué? | Proteger los datos de salud |
| ¿dónde? | En todos los sitios de SharePoint Online y OneDrive para la Empresa |
| ¿condiciones? | Al buscar cualquier documento que contenga información sensible y que se comparte con personas de fuera de la organización |
| ¿acciones? | Bloquear el acceso al documento y enviar una notificación |

Estos requisitos se almacenan como reglas individuales y se agrupan de forma conjunta como directiva DLP para simplificar la administración y la creación de informes.

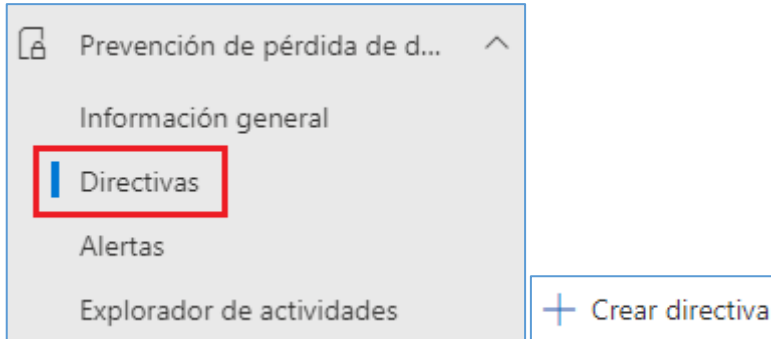
Casos de uso de una DLP

Con una directiva DLP se puede:

- **Identificar información sensible en varias ubicaciones**, como Exchange Online, SharePoint Online, OneDrive para la empresa y Microsoft Teams. Por ejemplo, identificar cualquier documento que contenga un número de tarjeta de crédito, o bien supervisar solo los sitios de personas específicas.
- **Evitar el uso compartido accidental de información sensible**. Por ejemplo, identificar cualquier documento o correo electrónico que contenga un registro de mantenimiento compartido con personas de fuera de la organización y, a continuación, bloquear automáticamente el acceso a ese documento o impedir que se envíe el correo electrónico.
- **Supervisar y proteger información sensible** en las versiones de escritorio de Excel, PowerPoint y Word. Al igual que en Exchange Online, SharePoint Online y OneDrive para la empresa, estos programas de escritorio de Office incluyen las mismas capacidades para identificar información sensible y aplicar directivas de DLP. DLP proporciona supervisión continua cuando las personas comparten contenido en estos programas de Office.
- **Ayudar a los usuarios a aprender a cumplir** sin interrumpir el flujo de trabajo. Puede educar a sus usuarios acerca de las directivas DLP y ayudar a que sigan manteniendo el cumplimiento normativo sin bloquear su trabajo. Por ejemplo, si un usuario intenta compartir un documento que contiene información sensible, una directiva DLP puede enviarle una notificación por correo electrónico y mostrarle una sugerencia de directiva en el contexto de la biblioteca de documentos que le permite invalidar la directiva si tiene una justificación comercial. Las mismas sugerencias de directiva también aparecen en Outlook en la web, Outlook, Excel, PowerPoint y Word.
- **Ver informes de DLP** que muestran contenido que coincide con las directivas DLP de su organización. Para evaluar si la organización está cumpliendo con una directiva DLP, puede ver cuántas coincidencias tienen la directiva y la regla a lo largo del tiempo. Si una directiva DLP permite a los usuarios invalidar una sugerencia de directiva e informar de un falso positivo, también puede ver qué han informado los usuarios.

Crear una nueva política DLP

- a) Desde el Centro de Seguridad de Office 365 en el menú [Prevención de pérdida de datos\Directiva], pulsar el botón “Crear una directiva”.



- b) Elegir reglamento del sector o crear una política a medida.

Seleccionar la opción Personalizado para crear una directiva personalizada:



- c) Asignar nombre y descripción.

Asignar un nombre a la directiva

Cree una directiva DLP para detectar datos confidenciales en las ubicaciones y aplicar acciones de protección cuando las condiciones coincidan.

Nombre *

Descripción

- d) Elegir ámbito de directiva, es decir, si se aplicara a todo el Directorio o a una unidad de Administración en concreto.

- Plantilla o directiva personalizada
- Nombre
- Unidades administrativas**
- Localizaciones
- Configuración de directiva
- Modo de directiva
- Finalizar

Asignar unidades administrativas

Elija las unidades de administración a las que quiere asignar esta directiva. Las unidades de administración se crean en Microsoft Entra ID y restringen la directiva a un conjunto específico de usuarios o grupos. Las selecciones afectarán a las opciones de ubicación disponibles en el paso siguiente.

Si desea asignar esta directiva a todos los usuarios y grupos, seleccione "Siguiente" y continúe. [Más información sobre unidades de administración](#)

+ Agregar o quitar unidades de administración

Unidades de administración

Directorio completo

- e) Elegir ubicaciones.

Una directiva DLP puede buscar y proteger información sensible en todo Office 365, independientemente de si esa información se encuentra en Exchange Online, SharePoint Online, OneDrive para la Empresa o Microsoft Teams. Puede elegir proteger el contenido en el correo electrónico de Exchange, y los mensajes de canales y chats de Microsoft Teams, y todas las bibliotecas de SharePoint o OneDrive, o bien seleccionar ubicaciones específicas para una directiva.

- Plantilla o directiva personalizada
- Nombre
- Unidades administrativas
- Localizaciones**
- Configuración de directiva
- Modo de directiva
- Finalizar

Elegir dónde aplicar la directiva

Se aplicará la directiva a los datos almacenados en las ubicaciones que elija.

ⓘ Si los permisos del grupo de roles están restringidos a un conjunto específico de usuarios o grupos, solo podrá aplicar esta directiva a esos usuarios o grupos. [Obtenga más información sobre los permisos del grupo de roles.](#) ✕

[Ver grupos de roles](#)

ⓘ La protección de la información confidencial en los repositorios locales (sitios de SharePoint y recursos compartidos de archivos) está ahora en vista previa. Tenga en cuenta que hay pasos previos necesarios para admitir esta nueva capacidad. [Más información sobre los requisitos previos](#)

⚠ Algunos de los dispositivos de los usuarios no están actualizados. [Ver más detalles](#)

| Ubicación | Ámbito | |
|--|-----------------------------|------------------------|
| <input checked="" type="checkbox"/> Correo electrónico de Exchange | Todos grupos | Editar |
| <input checked="" type="checkbox"/> Sitios de SharePoint | Todos sitios | Editar |
| <input checked="" type="checkbox"/> Cuentas de OneDrive | Todos usuarios y grupos | Editar |
| <input type="checkbox"/> Mensajes de chat y canal de Teams | Activar ubicación al ámbito | |
| <input type="checkbox"/> Dispositivos | Activar ubicación al ámbito | |
| <input type="checkbox"/> Instancias | Activar ubicación al ámbito | |
| <input type="checkbox"/> Repositorios locales | Activar ubicación al ámbito | |
| <input type="checkbox"/> Áreas de trabajo de Power BI | Activar ubicación al ámbito | |

Si se elige incluir o excluir sitios de SharePoint o cuentas de OneDrive específicos, una directiva DLP no puede contener más de 100 inclusiones y exclusiones. Aunque este límite exista, se puede superar este límite aplicando una directiva para toda la organización o una directiva que se aplique a ubicaciones completas.

f) Definir reglas.

Definir configuración de directiva

Decida si desea utilizar la configuración predeterminada de la plantilla seleccionada para configurar rápidamente una directiva o configurar reglas personalizadas para perfeccionar aún más su directiva.

- Revise y personalice la configuración predeterminada de la plantilla. ⓘ
 Crear o personalizar reglas de DLP avanzadas ⓘ

Personalizar reglas de DLP avanzadas

Las reglas se componen de condiciones y acciones que definen los requisitos de protección de esta directiva. Puede modificar las reglas existentes o crear unas nuevas.

+ Crear regla

0 elementos

Nombre

Estado

No se han creado reglas

Las reglas son las que **aplican los requisitos empresariales en el contenido** de su organización. Una directiva contiene **una o más reglas**, y cada regla consta de las condiciones y acciones. Para cada regla, cuando se cumplen las condiciones, **las acciones se realizan automáticamente**. Las reglas se ejecutan **secuencialmente**, comenzando por la regla de mayor prioridad de cada directiva.

Una regla también proporciona opciones para notificar a los usuarios (con sugerencias de directiva y notificaciones por correo electrónico) y los administradores (con informes de incidentes por correo electrónico) de que el contenido ha coincidido con la regla.

Crear regla

Use reglas para definir el tipo de información confidencial que protege en los datos. Si el contenido coincide con muchas reglas, se aplicará la más restrictiva. [Más información sobre las reglas.](#)

Nombre *

Descripción

Condiciones

Aplicaremos esta directiva en el contenido que coincida con estas condiciones.

+ Agregar condición ▾

Excepciones

No aplicaremos esta regla al contenido que coincida con una de estas excepciones.

+ Agregar excepción ▾

Acciones

Use las acciones para proteger el contenido cuando se cumplan las condiciones.

+ Agregar una acción ▾

Notificaciones al usuario
 Use las notificaciones para informar a los usuarios y para enseñarles a usar correctamente la información confidencial.
 Desactivado
 Las notificaciones no se usarán para actividades en Exchange, SharePoint, OneDrive, Teams y Microsoft Exchange local.

Reemplazos de usuario
 Permitir invalidaciones a partir de servicios de M365
 Permite a los usuarios invalidar las restricciones de directiva en Fabric (incluido Power BI), Exchange, SharePoint, OneDrive y Teams.

Informes de incidentes
 Utilice este nivel de gravedad en las alertas e informes de administración:
 Envíe una alerta a los administradores cuando se produzca una coincidencia con una regla.
 Activado
 Enviar alertas de correo electrónico a estos usuarios (opcional)

 Recopilar el archivo original como evidencia para todas las actividades de archivo seleccionadas en el punto de conexión

Enviar alerta cada vez que una actividad coincide con la regla
 Enviar alerta cuando el volumen de las actividades que coincidan alcance un umbral
 Instancias que son mayores o iguales que actividades coincidentes
 Volumen mayor o igual que MB
 Durante los últimos minutos
 Para

Use los informes de incidentes de correo electrónico para que se le envíe una notificación cuando se produzca una coincidencia con una directiva.
 Desactivado

Opciones adicionales
 Si existe una coincidencia para esta regla, detenga el procesamiento de reglas y directivas DLP adicionales.
 Establezca el orden en el que se seleccionará esta regla para la evaluación
 Prioridad:

f1. Condiciones

Las condiciones son importantes porque determinan los tipos de información que está buscando y cuándo se debe realizar una acción.

Las condiciones se centran en el contenido, como el tipo de información sensible que está buscando, y también en el contexto, como con quién se comparte el documento.

Puede usar condiciones para asignar acciones diferentes a distintos niveles de riesgo. Por ejemplo, el contenido sensible compartido internamente podría ser de menor riesgo y necesitar menos acciones que el contenido sensible compartido con personas de fuera de la organización.

Nota: Dependiendo de las localizaciones seleccionadas, en el apartado “Condiciones”, veremos más o menos opciones.

Condiciones

Defina las condiciones que deben cumplirse para que se aplique esta directiva. Incluya contenido, remitentes y destinatarios específicos que quiera que detecte la regla. Para reglas más complejas, cree grupos para excluir o incluir elementos. [Más información sobre cómo funciona el generador de condiciones](#)

+ Agregar condición ▼ Agregar grupo

| | |
|---|---|
| El contenido incluye | |
| El contenido se comparte desde Microsoft 365 | |
| La propiedad del documento es | Condiciones. |
| No se pudo examinar el documento | |
| El documento o los datos adjuntos están protegidos con contraseña | |
| El documento no finalizó el análisis | usar correctamente la información confidencial. |
| La extensión de archivo es | |
| El nombre del documento contiene palabras o frases | it, OneDrive, Teams y Microsoft Exchange local. |
| El tamaño del documento es igual o mayor que | |

Una directiva DLP puede ayudar a proteger información sensible, lo que se define como un tipo de información sensible. Office 365 incluye definiciones para muchos tipos comunes de información sensible en muchas regiones diferentes que están listas para su uso, como números de tarjeta de crédito, números de cuentas bancarias, números de identificación nacionales y números de pasaporte.

f2. Acciones

Cuando el contenido coincide con una condición en una regla, se pueden aplicar acciones para proteger automáticamente el contenido.

Nota: Dependiendo de las localizaciones seleccionadas, en el apartado “Acciones”, veremos más o menos opciones.

Acciones

Use las acciones para proteger el contenido cuando se cumplan las condiciones.

+ Agregar una acción ▼

Restringir el acceso o cifrar el contenido en las ubicaciones de Microsoft 365

Acciones

Use las acciones para proteger el contenido cuando se cumplan las condiciones.

Restringir el acceso o cifrar el contenido en las ubicaciones de Microsoft 365

- Impedir que los usuarios reciban correo electrónico o accedan a archivos compartidos de SharePoint, OneDrive y Teams, y a elementos de Power BI.
De forma predeterminada, los usuarios no pueden enviar chats de Teams y mensajes de canal que incluyan el tipo de contenido que se está protegiendo. Sin embargo, puede elegir a quién se le impide recibir correos electrónicos o acceder a archivos compartidos desde SharePoint, OneDrive y Teams, o elementos de Power BI.
- Bloquear a todos. ⓘ
- Bloquear solo a personas externas a la organización. ⓘ

- Bloquear el uso compartido para los usuarios y restringir el acceso al contenido compartido.

De forma predeterminada, los usuarios no podrán enviar a otros usuarios mensajes de correo electrónico, chats de Teams ni mensajes del canal que incluyan el tipo de contenido que está protegiendo. Pero se puede elegir quién tiene acceso a los archivos compartidos de

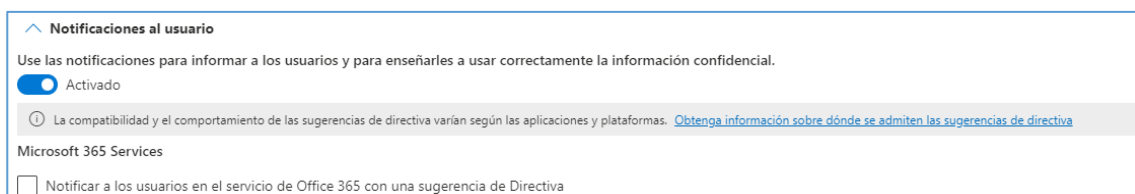
SharePoint y OneDrive. También decidir si se quiere permitir que los usuarios puedan ignorar las restricciones de la directiva.

Bloquear estos usuarios para que no tengan acceso al contenido de SharePoint, OneDrive y Teams:

- Todos. Solo el propietario del contenido, el último usuario que lo modificó y el administrador del sitio seguirán teniendo acceso
- Solo los usuarios fuera de la organización. Los usuarios de la organización seguirán teniendo acceso.

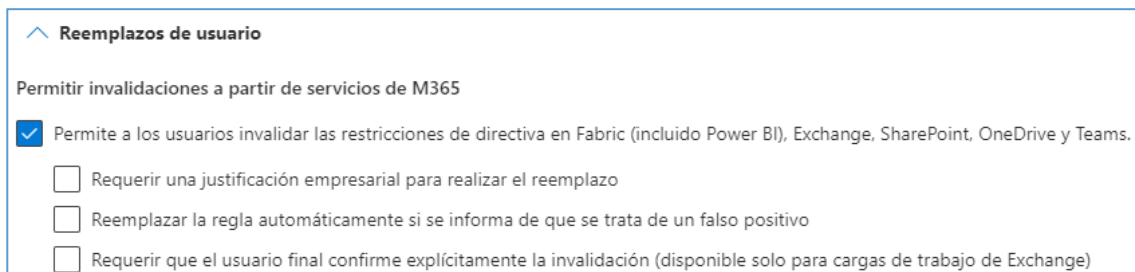
f3. Notificaciones de usuario e invalidaciones de usuario

Se puede utilizar notificaciones de usuario e invalidaciones de usuario para concienciarles sobre las directivas DLP y ayudarles a que sigan manteniendo el cumplimiento normativo sin bloquear su trabajo.



f4. Reemplazos de usuarios

Esta opción permite a los usuarios invalidar las restricciones de la directiva configurada en el apartado “Acciones”.



f5. Informes de incidentes

Cuando una regla coincide, es posible enviar un informe de incidentes a su responsable de cumplimiento normativo (o a la persona que elija) con los detalles del evento.

Informes de incidentes

Utilice este nivel de gravedad en las alertas e informes de administración:

Envíe una alerta a los administradores cuando se produzca una coincidencia con una regla.

Activado

Enviar alertas de correo electrónico a estos usuarios (opcional)

[+ Agregar o quitar grupos](#)

Recopilar el archivo original como evidencia para todas las actividades de archivo seleccionadas en el punto de conexión [Agregar almacenamiento](#)

Enviar alerta cada vez que una actividad coincide con la regla

Enviar alerta cuando el volumen de las actividades que coincidan alcance un umbral

Instancias que son mayores o iguales que actividades coincidentes

Volumen mayor o igual que MB

Durante los últimos minutos

Para

Use los informes de incidentes de correo electrónico para que se le envíe una notificación cuando se produzca una coincidencia con una directiva.

Desactivado

f6. Opciones adicionales

Opciones adicionales

Si existe una coincidencia para esta regla, detenga el procesamiento de reglas y directivas DLP adicionales.

Establezca el orden en el que se seleccionará esta regla para la evaluación

Prioridad:

g) Modo de directiva

- Plantilla o directiva personalizada
- Nombre
- Unidades administrativas
- Localizaciones
- Configuración de directiva
- Modo de directiva**
- Finalizar

Modo de directiva

Puede probar esta directiva antes de activarla para comprobar si necesita mejoras o si cumple todos sus objetivos. Si activa la directiva inmediatamente, puede editarla más adelante y probar de forma segura esos cambios en modo de simulación.

ⓘ En este tiempo, el modo de simulación no es soportado para estas ubicaciones seleccionadas: Repositorios de archivo locales, Microsoft Defender for Cloud Apps.

Ejecutar la directiva en modo de simulación
 Le mostraremos los elementos que coinciden con las condiciones de la directiva para ayudarle a evaluar su impacto. Los datos no se verán afectados: la directiva permanece desactivada mientras está en modo de simulación. [Obtener más información sobre el modo de simulación](#)

Mostrar sugerencias de directiva en modo de simulación.

Activar la directiva si no se edita en los quince días posteriores a la simulación

Active la directiva inmediatamente
 Una vez creada la directiva, tardará hasta una hora antes de que se apliquen los cambios.

Dejar la directiva desactivada
 Decida probar o activar la directiva más adelante.

h) Revisar y finalizar

- Plantilla o directiva personalizada
- Nombre
- Unidades administrativas
- Localizaciones
- Configuración de directiva
- Modo de directiva
- Finalizar

Revisar y finalizar

Cree la directiva si estos detalles parecen correctos. De lo contrario, ajuste la configuración para satisfacer mejor sus necesidades.

La información que se protegerá
Directiva personalizada
[Editar](#)

Nombre
CCN-DLP-1
[Editar](#)

Descripción
CCN-DLP-1
[Editar](#)

Localizaciones

! Considere la posibilidad de agregar Teams como ubicación para proteger el uso compartido accidental de información confidencial en los mensajes de Teams.

[Actualizar ubicaciones](#)

Correo electrónico de Exchange
Sitios de SharePoint
Cuentas de OneDrive
Mensajes de chat y canal de Teams
Dispositivos
Microsoft Defender for Cloud Apps
Repositorios locales
[Editar](#)

Configuración de directiva
Regla-DLP
[Editar](#)

¿Quiere activar la directiva después de su creación?
Pruébelo primero. No aplique acciones, pero muestre sugerencias de directiva a los usuarios.
[Editar](#)

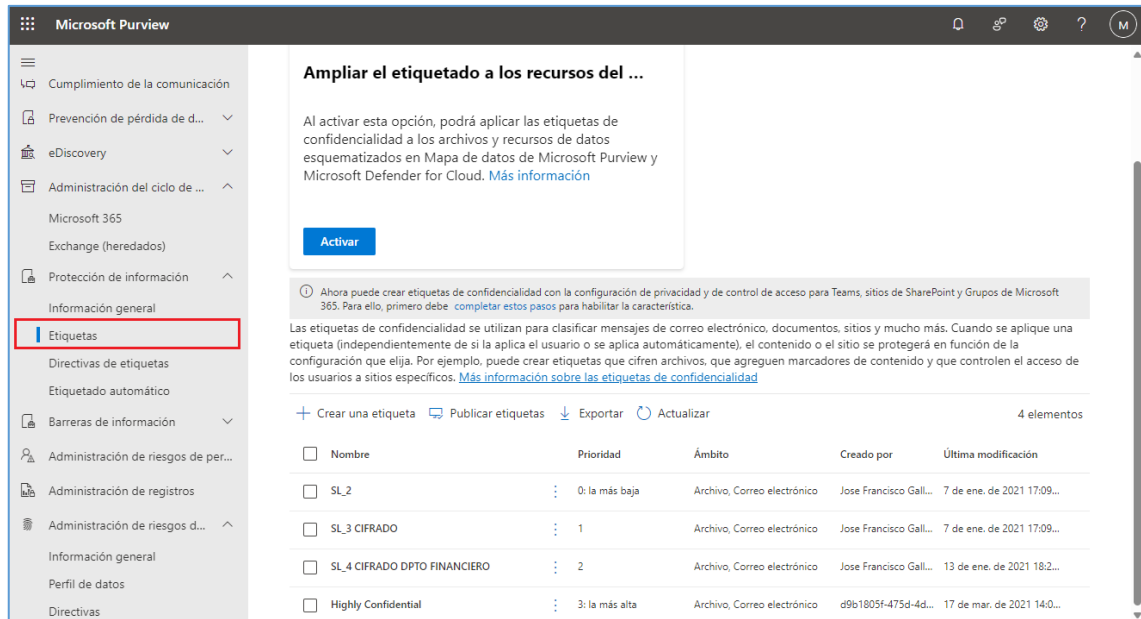
PROTECCIÓN DE LA INFORMACIÓN DE MICROSOFT PURVIEW (ETIQUETAS DE SENSIBILIDAD)

Las sensitivity labels se utilizan para clasificar mensajes de correo electrónico, documentos, sitios y mucho más. Cuando se aplique una etiqueta (independientemente de si la aplica el usuario o se aplica automáticamente), el contenido o el sitio se protegerá en función de la configuración que se elija. Por ejemplo, pueden crearse etiquetas que cifren archivos, que agreguen marcadores de contenido y que controlen el acceso de los usuarios a sitios específicos.

Nota: Las sensitivity labels son distintas de las etiquetas de retención (se usan para conservar o eliminar el contenido en función de las directivas que se definan).

Crear sensitivity labels

Abrir el Portal de Purview de Office 365, menú [Protección de la información\Etiquetas].



- En primer lugar, se debe **establecer una taxonomía** para definir los diferentes niveles de contenido sensible. Lo mejor es usar nombres o términos comunes que tengan sentido para los usuarios. Por ejemplo, se puede empezar con las etiquetas por defecto: Personal, Public, General, Confidential y Highly Confidential.
- Después, **definir qué puede hacer cada etiqueta**. Configurar las opciones de protección que se quiere asociar a cada etiqueta. Por ejemplo, el contenido con un nivel de sensibilidad menor (una etiqueta "General") podría simplemente tener un encabezado o pie de página aplicados, mientras que al contenido con un nivel de sensibilidad mayor (una etiqueta "Confidential") se le podrían aplicar marcas de agua, encriptación para asegurarse de que solo los usuarios con privilegios pueden acceder a él.
- Y, por último, **definir quién obtiene las etiquetas**. Después de definir las etiquetas de la organización, se publican en una directiva de etiqueta que controla qué usuarios y grupos pueden ver esas etiquetas. Una misma etiqueta puede reutilizarse: definirla una vez y después incluirla en varias directivas de etiqueta asignadas a diferentes usuarios. Pero para que una etiqueta pueda asignarse a un contenido, primero debe publicarse dicha etiqueta para que esté disponible en las aplicaciones de Office y otros servicios.

Ejemplo de creación de sensitivity labels:

Los archivos etiquetados estarán protegidos dondequiera que se lleven, tanto si están guardados en la nube o como si están descargados en un equipo.

- a) Desde el Portal de Purview de Office 365, menú [Protección de la información\Etiquetas]. Pulsar el botón: “Crear una etiqueta”.

| <input type="checkbox"/> Nombre | Prioridad | Ámbito |
|---|----------------|--|
| <input type="checkbox"/> SL_2 | 0: la más baja | Archivo, Correo electrónico |
| <input type="checkbox"/> SL_3 CIFRADO | 1 | Archivo, Correo electrónico |
| <input type="checkbox"/> SL_4 CIFRADO DPTO FINANCIERO | 2 | Archivo, Correo electrónico |
| <input type="checkbox"/> Highly Confidential | 3 | Archivo, Correo electrónico |
| <input type="checkbox"/> CCN-Etiqueta-Confidencial1 | 4: la más alta | Archivo, Correo electrónico, Reuniones |

- b) Complimentar el siguiente formulario con el nombre que tendrá la etiqueta, la prioridad, la descripción y el color.

Nueva etiqueta de confidencialidad

- Detalles de la etiqueta**
 - Ámbito
 - Elementos
 - Grupos y sitios
 - Recursos de datos esquematizados (versión preliminar)
 - Finalizar

Proporcionar detalles básicos para esta etiqueta

La configuración de protección que elija para esta etiqueta se aplicará de inmediato a los elementos o contenedores de contenido a los que se aplique. Los archivos etiquetados estarán protegidos allá donde vayan, tanto si se guardan en la nube como si se descargan en un equipo.

Nombre *

Nombre para mostrar *

Prioridad de etiqueta

De forma predeterminada, a esta etiqueta se le asignará la prioridad más alta, pero puede cambiarla después de crearla.

Descripción para usuarios *

Descripción sobre CCN Etiqueta-Confidencial1 para usuarios

Descripción para administradores

Descripción sobre CCN Etiqueta-Confidencial1 para administradores

Color de la etiqueta

c) **Ámbito**

Aquí se elige a que tipo de elementos aplicara esta etiqueta.

Nueva etiqueta de confidencialidad

- Detalles de la etiqueta
- Ámbito**
- Elementos
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

Definir el ámbito de esta etiqueta

Las etiquetas se pueden aplicar directamente a elementos (como archivos, correos electrónicos y reuniones), contenedores como sitios de SharePoint y Teams, elementos de Fabric y Power BI, activos de datos esquematizados, etc. Indíquenos dónde desea que se utilice esta etiqueta para poder configurar los ajustes de protección aplicables. [Más información sobre los ámbitos de etiquetas](#)

Elementos
Tenga en cuenta que la restricción del ámbito solo a archivos o correos electrónicos podría afectar a la configuración del control de acceso y a dónde se puede aplicar la etiqueta. [Más información](#)

- Archivos
Proteja los archivos creados en Word, Excel, PowerPoint y mucho más.
- Correos electrónicos
Proteja los mensajes enviados desde cualquier versión de Outlook.
- Reuniones
Proteja los eventos del calendario y las reuniones programadas en Outlook y Teams.

Grupos y sitios
Configure la privacidad, el control de acceso y otras opciones para etiquetados protegidos de Teams, los grupos de Microsoft 365 y los sitios de SharePoint.

Recursos de datos esquematizados (versión preliminar)
Aplique etiquetas a archivos y recursos de datos esquematizados en el Mapa de datos de Microsoft Purview. Los recursos de datos esquematizados incluyen SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, etc.

d) **Elementos - Cifrado**

d1. Cifrado - Para cifrar elementos elegimos la opción "Controlar acceso".

- Detalles de la etiqueta
- Ámbito
- Elementos**
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

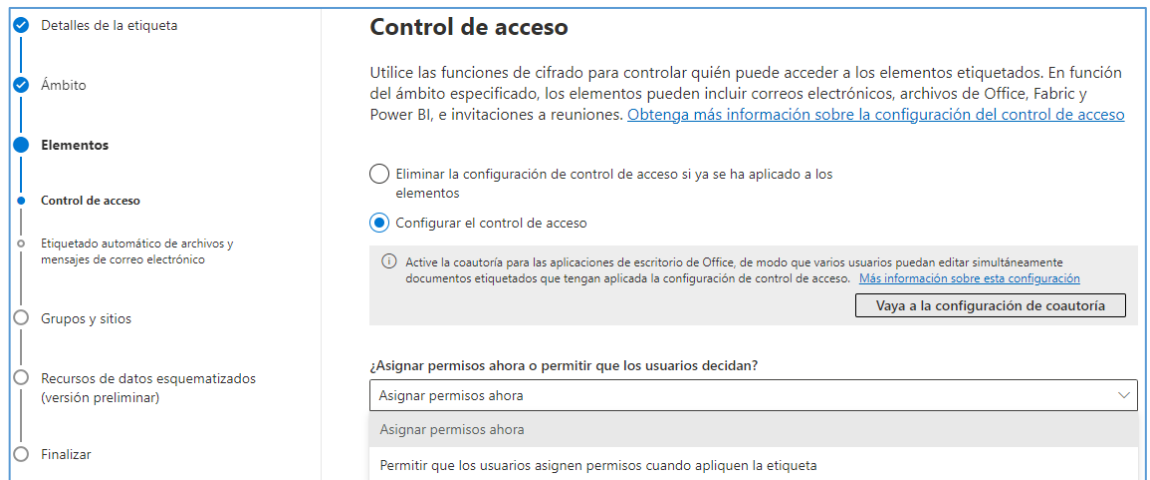
Elija la configuración de protección para los tipos de elementos seleccionados

Los ajustes de protección que configure se aplicarán cuando la etiqueta se aplique a los elementos en Microsoft 365.

- Controlar acceso**
Controlar quién puede acceder a los elementos etiquetados y verlos.
- Aplicar marcado de contenido**
Agregue encabezados, pies de página y marcas de agua personalizadas a los elementos etiquetados.
- Proteger reuniones y chats de Teams**
Configure las opciones de protección para reuniones y chats de Teams.

Proteger reuniones y chats de Teams
Configure las opciones de protección para reuniones y chats de Teams.

d2. ¿Asignar permisos ahora o permitir que los usuarios decidan?

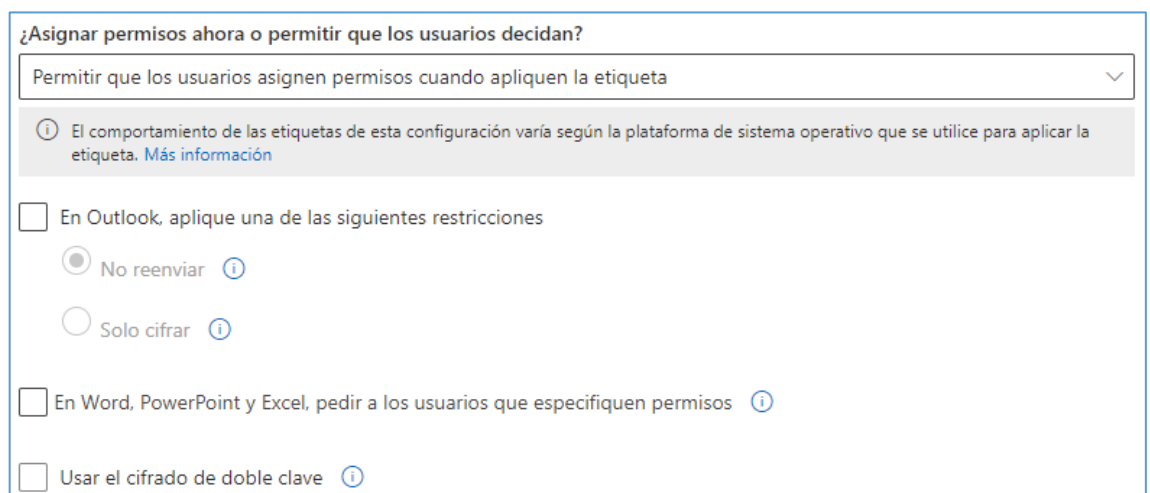


The screenshot shows the 'Control de acceso' (Access Control) configuration page. On the left is a navigation pane with the following items: Detalles de la etiqueta, Ámbito, Elementos, Control de acceso (selected), Etiquetado automático de archivos y mensajes de correo electrónico, Grupos y sitios, Recursos de datos esquematizados (versión preliminar), and Finalizar. The main content area is titled 'Control de acceso' and includes the following text: 'Utilice las funciones de cifrado para controlar quién puede acceder a los elementos etiquetados. En función del ámbito especificado, los elementos pueden incluir correos electrónicos, archivos de Office, Fabric y Power BI, e invitaciones a reuniones. [Obtenga más información sobre la configuración del control de acceso](#)'.

Below this text are two radio buttons: 'Eliminar la configuración de control de acceso si ya se ha aplicado a los elementos' (unselected) and 'Configurar el control de acceso' (selected). Under the selected option, there is a sub-section with a heading '¿Asignar permisos ahora o permitir que los usuarios decidan?' and a dropdown menu currently set to 'Asignar permisos ahora'. Below the dropdown are two more options: 'Asignar permisos ahora' and 'Permitir que los usuarios asignen permisos cuando apliquen la etiqueta'.

d3. Asignar permisos ahora

Esta opción determina exactamente los permisos para el contenido con esa etiqueta y los usuarios que los obtendrán.



The screenshot shows the expanded dropdown menu for '¿Asignar permisos ahora o permitir que los usuarios decidan?'. The selected option is 'Permitir que los usuarios asignen permisos cuando apliquen la etiqueta'. Below this is an information icon and text: 'El comportamiento de las etiquetas de esta configuración varía según la plataforma de sistema operativo que se utilice para aplicar la etiqueta. [Más información](#)'. There are three main options, each with a checkbox and an information icon: 'En Outlook, aplique una de las siguientes restricciones' (unchecked), 'En Word, PowerPoint y Excel, pedir a los usuarios que especifiquen permisos' (unchecked), and 'Usar el cifrado de doble clave' (unchecked). Under the first option, there are two radio buttons: 'No reenviar' (selected) and 'Solo cifrar' (unselected).

- **En Outlook, aplique una de las siguientes restricciones:**
 - **No reenviar:** Cuando los usuarios aplican la etiqueta a un correo electrónico en Outlook, los destinatarios podrán leer el mensaje, pero no podrá reenviar, imprimir ni copiar el contenido. El remitente tiene permiso total para sus mensajes y todas las respuestas.
 - **Solo cifrar:** Cuando los usuarios aplican la etiqueta a un correo en Outlook, el correo se cifra y los destinatarios deben autenticarse. Los destinatarios no tienen restricciones, excepto que no pueden quitar el cifrado.
- **En Word, PowerPoint y Excel, pedir a los usuarios que especifiquen permisos:** Cuando los usuarios aplican la etiqueta a los archivos de Word, PowerPoint o Excel, aparece un cuadro de diálogo en el que se

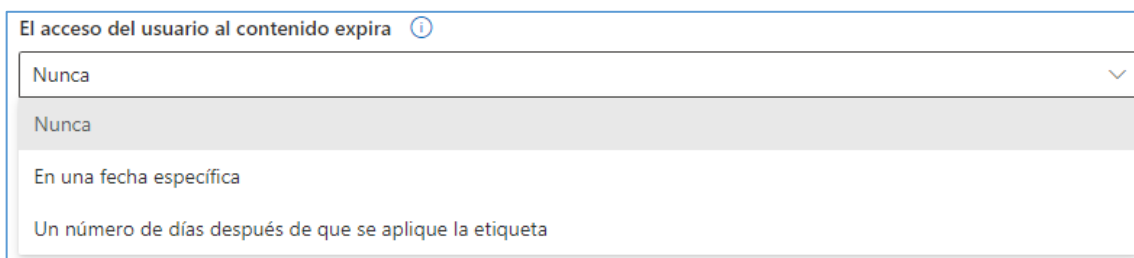
les pide que elijan uno de los niveles de permisos predefinidos, especifiquen los usuarios o grupos a los que se aplican y, de forma opcional, establezcan una fecha de expiración para el archivo etiquetado.

- **Usar el cifrado de doble clave:** Active DKE si desea utilizar dos llaves para controlar aún más el acceso a los elementos etiquetados. Microsoft almacena una clave en Azure y usted tiene la otra. Tenga en cuenta que, si activa esta opción, no podrá editar la etiqueta una vez creada.

d4. Permitir a los usuarios asignar permisos al aplicar la etiqueta al contenido.

De esta forma, puede permitir a los usuarios de su organización cierta flexibilidad que pueden necesitar para colaborar y llevar a cabo su trabajo.

1. El acceso del usuario al contenido expira



El acceso del usuario al contenido expira ⓘ

Nunca

Nunca

En una fecha específica

Un número de días después de que se aplique la etiqueta

Si desea limitar el tiempo que los usuarios pueden acceder al contenido con esta etiqueta, especifique una fecha o un número de días en los que el acceso deba vencer. Más información:

- Después de este tiempo, los usuarios no podrán abrir archivos que tengan esta etiqueta aplicada. Sin embargo, para los correos electrónicos, la expiración no siempre se aplica debido a los mecanismos de almacenamiento en caché usados por algunos clientes de correo electrónico.
- Si especifica una fecha, es efectiva la medianoche en la zona horaria actual.
- Si especifica un número de días, la hora comienza en el momento en que se aplica la etiqueta al contenido.

2. Permitir acceso sin conexión

Permitir acceso sin conexión ⓘ

Siempre ▼

Siempre

Nunca

Solo durante un número de días

Si especifica que el contenido etiquetado nunca esté disponible sin conexión o que solo esté disponible sin conexión durante un número de días, cuando se alcanza ese umbral, los usuarios deben volver a autenticarse y su acceso se registra. Cuando esto sucede, si sus credenciales no se almacenan en caché, se pedirá a los usuarios que inicien sesión en Microsoft 365 para poder abrir el documento o el correo electrónico.

3. Asignar permisos a usuarios y grupos específicos

Aquí se asignan los permisos a usuarios específicos para que solo ellos puedan interactuar con contenido que tenga esta etiqueta aplicada.

Asignar permisos a usuarios y grupos específicos * ⓘ

[Asignar permisos](#)

Asignar permisos

Se asignarán permisos para utilizar el contenido con esta etiqueta aplicada solo a los usuarios o grupos que elija. Puede elegir entre los permisos existentes (como copropietario, coautor y revisor) o personalizarlos para satisfacer sus necesidades.

- + [Agregar todos los usuarios y grupos de su organización](#)
- + [Agregar cualquier usuario autenticado](#) ⓘ
- + [Agregar usuarios o grupos](#)
- + [Agregar dominios o direcciones de correo electrónico específicos](#) ⓘ

0 elementos

Permisos asignados a [Eliminar](#)

No hay datos disponibles

[Elegir permisos](#)

Coautor
 Mostrar contenido, Visualizar permisos, Editar contenido, Guardar, Imprimir, Copiar y extraer contenido, Responder, Responder a todos, Reenviar, Permitir macros

4. Usar el cifrado de doble clave

 Usar el cifrado de doble clave ⓘ

Active DKE si desea utilizar dos llaves para controlar aún más el acceso a los elementos etiquetados. Microsoft almacena una clave en Azure y usted tiene la otra. Tenga en cuenta que, si activa esta opción, no podrá editar la etiqueta una vez creada. Para más información ver [Aplicar cifrado mediante etiquetas de confidencialidad | Microsoft Learn](#)

e) Elementos - Marcado de contenido

Nueva etiqueta de confidencialidad

- ✓ Detalles de la etiqueta
- ✓ Ámbito
- **Elementos**
- Marcado de contenido
- Etiquetado automático de archivos y mensajes de correo electrónico
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

Marcado de contenido

Agregue encabezados, pies de página y marcas de agua personalizadas al contenido que tenga esta etiqueta aplicada. [Más información sobre el marcado de contenido](#)

ⓘ Todas las marcas de contenido se aplicarán a los documentos, pero solo se aplicarán la cabecera y el pie de página a los mensajes de correo electrónico. Si decide configurar los ajustes de reunión para esta etiqueta, el encabezado y el pie de página también se aplicarán a las invitaciones de reunión.

Marcado de contenido

Marcado de contenido

Agregar una marca de agua
Personalizar texto

Agregar un encabezado
Personalizar texto

Agregar un pie de página
Personalizar texto
Test CCN

Se pueden asignar encabezados, pies o marcas de agua que se agregará al documento o correo electrónico.

f) Etiquetado automático

Nueva etiqueta de confidencialidad

- ✓ Detalles de la etiqueta
- ✓ Ámbito
- **Elementos**
- ✓ Control de acceso
- **Etiquetado automático de archivos y mensajes de correo electrónico**
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

Etiquetado automático de archivos y mensajes de correo electrónico

Quando los usuarios editen archivos de Office o redacten, respondan o reenvíen correos electrónicos de Outlook con contenido que cumpla las condiciones que elija aquí, aplicaremos automáticamente esta etiqueta o recomendamos que la apliquen por su cuenta. [Más información sobre el etiquetado automático para Microsoft Purview](#)

ⓘ Para aplicar esta etiqueta automáticamente a los archivos que ya están guardados (en SharePoint y OneDrive) o los mensajes de correo electrónico que ya han sido procesados por Exchange, debe crear una directiva de etiquetado automático. [Más información sobre directivas de etiquetado automático](#)

Etiquetado automático para archivos y mensajes de correo electrónico

Etiquetado automático para archivos y mensajes de correo electrónico

^ Detectar contenido que cumpla estas condiciones

+ Agregar condición ^

Quando el contenido coincida con estas condiciones

Aplicar automáticamente la etiqueta

Las etiquetas automáticas y recomendadas funcionan de forma diferente en los elementos de Office 365 que en los archivos almacenados en dispositivos Windows. [Más información](#)

Mostrar este mensaje a los usuarios cuando se aplique la etiqueta ⓘ

Escriba un texto o déjelo en blanco para mostrar el mensaje predeterminado

Cuando se detecte contenido sensible en el correo electrónico o en los documentos que cumplan las condiciones que se elija, se puede aplicar automáticamente esta etiqueta o mostrar un mensaje a los usuarios que les recomiende que la apliquen ellos mismos.

g) Parámetros de protección de los grupos y sitios.

Esta configuración se aplica a equipos, grupos y sitios que tengan esta etiqueta aplicada. Pero no se aplica directamente a los archivos almacenados en estos contenedores.

Nueva etiqueta de confidencialidad

- Detalles de la etiqueta
- Ámbito
- Elementos
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

Definir los parámetros de protección de los grupos y sitios

Esta configuración se aplica a equipos, grupos y sitios que tengan esta etiqueta aplicada. Pero no se aplica directamente a los archivos almacenados en estos contenedores. [Más información acerca de esta configuración](#)

Privacidad y acceso de usuarios externos
Controle el nivel de acceso que tendrán los usuarios internos y externos a la etiqueta equipos y grupos de Microsoft 365.

Uso compartido externo y acceso condicional
Controle el uso compartido externo y configure las opciones de acceso condicional para proteger los sitios de SharePoint etiquetados.

Detectabilidad de equipos privados y configuración de canal compartido
Decida si los equipos privados se podrán detectar en las búsquedas y controle los tipos de equipos que se pueden invitar a canales compartidos.

h) Etiquetado automático para recursos de datos esquematizados

Nueva etiqueta de confidencialidad

- Detalles de la etiqueta
- Ámbito
- Elementos
- Grupos y sitios
- Recursos de datos esquematizados (versión preliminar)
- Finalizar

Etiquetado automático para recursos de datos esquematizados (versión preliminar)

Aplique automáticamente esta etiqueta a los recursos de datos esquematizados en el Mapa de datos de Microsoft Purview que contengan los tipos de información confidencial que elija aquí. Puede etiquetar automáticamente las columnas de base de datos en SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS y otros orígenes de datos regidos por el Mapa de datos de Microsoft Purview. [Más información acerca del etiquetado automático para los recursos de datos esquematizados](#)

Etiquetado automático para recursos de datos esquematizados (versión preliminar)

Publicar sensitivity labels

Una vez creada la etiqueta se publica, así estará disponible en aplicaciones de Office (Word, Excel, PowerPoint y Outlook), sitios de SharePoint y Teams, y grupos de Office 365 de usuarios específicos.

a) Pulsar el botón “Publicar etiqueta”.

| + Crear una etiqueta Publicar etiquetas ↓ Exportar ↻ Actualizar | | | | | |
|---|----------------|--|--------------------------------------|-----------------------------|--|
| <input type="checkbox"/> Nombre | Prioridad | Ámbito | Creado por | Última modificación | |
| <input type="checkbox"/> SL_2 | 0: la más baja | Archivo, Correo electrónico | Jose Francisco Gallardo Bernal | 7 de ene. de 2021 17:09:29 | |
| <input type="checkbox"/> SL_3 CIFRADO | 1 | Archivo, Correo electrónico | Jose Francisco Gallardo Bernal | 7 de ene. de 2021 17:09:29 | |
| <input type="checkbox"/> SL_4 CIFRADO DPTO FINANCIERO | 2 | Archivo, Correo electrónico | Jose Francisco Gallardo Bernal | 13 de ene. de 2021 18:24:21 | |
| <input type="checkbox"/> Highly Confidential | 3 | Archivo, Correo electrónico | d9b1805f-475d-4dfc-b6b8-d8fda3fed... | 17 de mar. de 2021 14:06:07 | |
| <input type="checkbox"/> CCN-Etiqueta-ConfidencialI | 4: la más alta | Archivo, Correo electrónico, Reuniones | Mohammad Hassan Nazir Kosar | 18 de abr. de 2024 1:19:49 | |

b) Seleccionar las etiquetas desde el asistente de publicación (panel derecho).

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos
- Configuración
- Nombre
- Finalizar

Elija etiquetas de confidencialidad para publicar

Cuando se publiquen, las etiquetas que elija aquí estarán disponibles en aplicaciones de Office (Word, Excel, PowerPoint y Outlook), sitios de SharePoint y Teams, y Grupos de Microsoft 365 de usuarios específicos.

Etiquetas de confidencialidad para publicar

CCN-Etiqueta-Confidencial1

[Editar](#)

c) Ámbito

- Etiquetas para publicar
- Unidades administrativas**
- Usuarios y grupos
- Configuración
- Nombre
- Finalizar

Asignar unidades administrativas

Elija las unidades de administración a las que quiere asignar esta directiva. Las unidades de administración se crean en Microsoft Entra ID y restringen la directiva a un conjunto específico de usuarios o grupos. Las selecciones afectarán a las opciones de ubicación disponibles en el paso siguiente.

Si desea asignar esta directiva a todos los usuarios y grupos, seleccione "Siguiente" y continúe. [Más información sobre unidades de administración](#)

[+](#) Agregar o quitar unidades de administración

Unidades de administración

Directorio completo

d) Elegir usuarios o grupos

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos**
- Configuración
- Nombre
- Finalizar

Publicar para usuarios y grupos

Las etiquetas que seleccione estarán disponibles para los usuarios, los grupos de distribución, los grupos de seguridad habilitados para correo y los Grupos de Microsoft 365 que elija aquí.

× Si los permisos del grupo de roles están restringidos a un conjunto específico de usuarios y grupos, solo podrá publicar etiquetas para esos usuarios y grupos. [Obtenga más información sobre los permisos del grupo de roles.](#)

[Ver grupos de roles](#)

| Ubicación | Ámbito |
|---|---|
| <input checked="" type="checkbox"/> Usuarios y grupos | Todos usuarios y grupos Editar |

e) Configuración de la directiva

Se puede tener una etiqueta de forma predeterminada, una etiqueta obligatoria o requerir a los usuarios que justifiquen las acciones en su extremo.

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos
- Configuración**
- Nombre
- Finalizar

Configuración de la directiva

Configure las opciones de las etiquetas incluidas en esta directiva.

- Los usuarios deben proporcionar una justificación para quitar una etiqueta o rebajar su clasificación**
Los usuarios deberán proporcionar una justificación antes de quitar una etiqueta o reemplazarla por una que tenga un número de orden inferior. Puede usar el explorador de actividades para revisar los cambios de las etiquetas y el texto de justificación.
- Requiere que los usuarios apliquen una etiqueta a su correo electrónico y documentos**
Se requerirá que los usuarios apliquen etiquetas para poder guardar documentos o enviar correos electrónicos (solo si estos elementos no tienen una etiqueta aplicada).

× El soporte y el comportamiento de esta configuración varían en las distintas aplicaciones y plataformas. [Más información sobre la administración de etiquetas de confidencialidad](#)
- Requerir a los usuarios que apliquen una etiqueta al contenido de Fabric y Power BI**
Se requerirá a los usuarios que apliquen etiquetas al contenido sin etiquetar que hayan creado o editado en Fabric y Power BI. [Más información sobre el etiquetado obligatorio en Fabric y Power BI](#)
- Proporciona a los usuarios un vínculo a una página de ayuda personalizada.**
Si creó un sitio web dedicado a ayudar a los usuarios a comprender cómo utilizar etiquetas en su organización, escriba la dirección URL aquí. [Más información acerca de esta página de ayuda](#)

f) Configuración predeterminada para documentos

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos
- Configuración**
- Documentos
- Correos electrónicos
- Reuniones
- Fabric y Power BI
- Nombre
- Finalizar

Configuración predeterminada para documentos

Aplicar una etiqueta predeterminada a los documentos

La etiqueta que elija se aplicará automáticamente a los documentos de Word, Excel y PowerPoint cuando se creen o modifiquen. Los usuarios siempre podrán seleccionar una etiqueta diferente que coincida mejor con la confidencialidad de su documento. [Obtenga información sobre qué versiones de la aplicación de Office admiten esta configuración](#)

Etiqueta predeterminada

Ninguno

Ninguno

CCN-Etiqueta-Confidencial1

g) Configuración predeterminada para los correos electrónicos

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos
- Configuración**
- Documentos
- Correos electrónicos**
- Reuniones
- Fabric y Power BI
- Nombre
- Finalizar

Configuración predeterminada para los correos electrónicos

Aplicar una etiqueta predeterminada a los correos electrónicos

La etiqueta que elija se aplicará automáticamente a los correos electrónicos nuevos y existentes sin etiquetar. Los usuarios siempre pueden cambiar la etiqueta predeterminada antes de enviar el mensaje. [Obtenga información sobre qué versiones de Outlook admiten esta configuración](#)

Etiqueta predeterminada

Igual que el documento

Igual que el documento

Ninguno

CCN-Etiqueta-Confidencial1

Heredar etiqueta de datos adjuntos

Si se aplica una etiqueta a un correo electrónico, se agrega un archivo adjunto con una etiqueta de mayor prioridad a un correo electrónico, esta configuración reemplaza la etiqueta existente por la etiqueta de los datos adjuntos. Si se agregan varios datos adjuntos etiquetados, se aplicará la etiqueta de prioridad más alta. Si el correo electrónico aún no está etiquetado, heredará la etiqueta de prioridad más alta de los datos adjuntos. [Más información sobre la herencia de etiquetas](#)

El correo electrónico hereda la etiqueta de máxima prioridad de los archivos adjuntos

h) Configuración predeterminada para reuniones y eventos de calendario

- Etiquetas para publicar
- Unidades administrativas
- Usuarios y grupos
- Configuración**
- Documentos
- Correos electrónicos
- Reuniones**
- Fabric y Power BI

Configuración predeterminada para reuniones y eventos de calendario

Aplicar una etiqueta predeterminada a las reuniones y eventos del calendario

La etiqueta que elija se aplicará automáticamente a eventos de calendario y reuniones nuevos y existentes sin etiquetar. Los usuarios siempre pueden cambiar la etiqueta predeterminada antes de crear el evento o la reunión. [Obtenga información sobre qué clientes de Teams y Outlook admiten esta configuración](#)

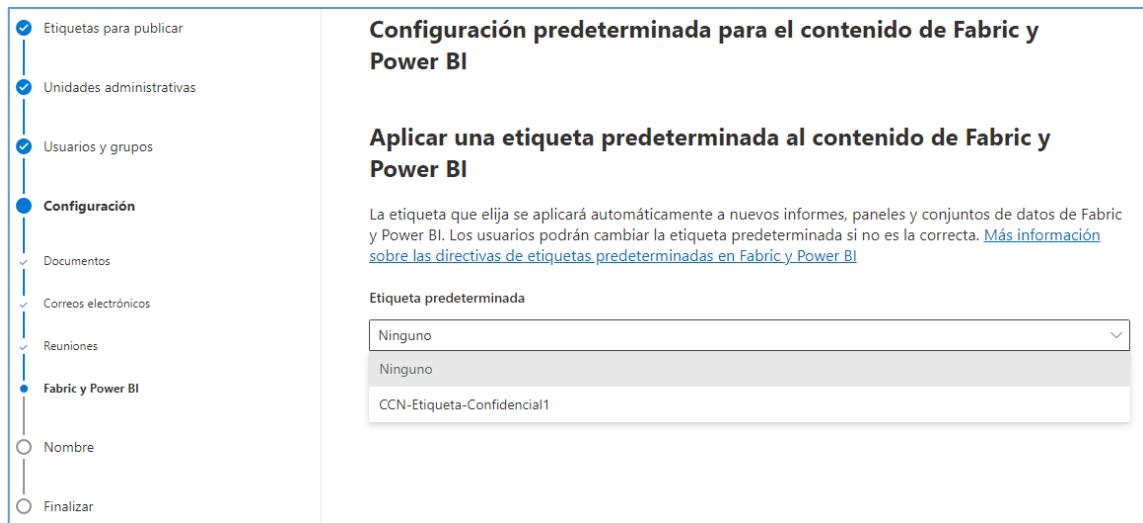
Etiqueta predeterminada

Ninguno

Ninguno

CCN-Etiqueta-Confidencial1

i) Configuración predeterminada para el contenido de Fabric y Power BI



Etiquetas para publicar

Unidades administrativas

Usuarios y grupos

Configuración

Documentos

Correos electrónicos

Reuniones

Fabric y Power BI

Nombre

Finalizar

Configuración predeterminada para el contenido de Fabric y Power BI

Aplicar una etiqueta predeterminada al contenido de Fabric y Power BI

La etiqueta que elija se aplicará automáticamente a nuevos informes, paneles y conjuntos de datos de Fabric y Power BI. Los usuarios podrán cambiar la etiqueta predeterminada si no es la correcta. [Más información sobre las directivas de etiquetas predeterminadas en Fabric y Power BI](#)

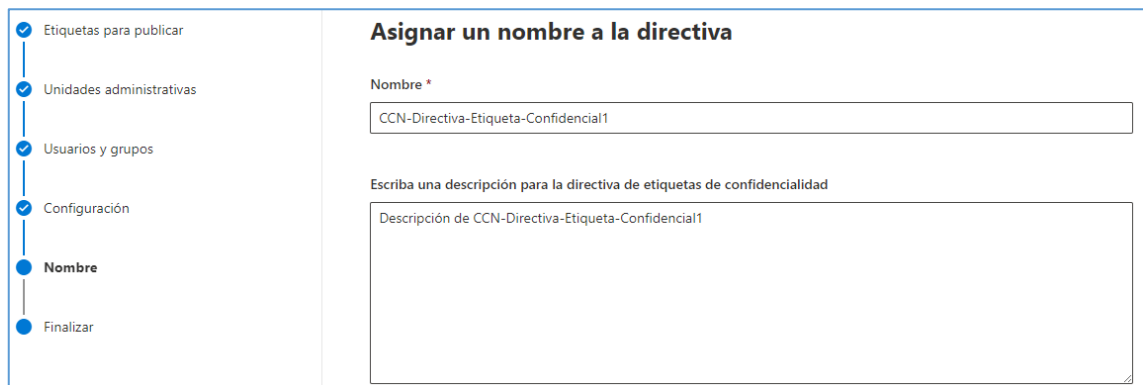
Etiqueta predeterminada

Ninguno

Ninguno

CCN-Etiqueta-Confidencial1

j) Nombrar la directiva.



Etiquetas para publicar

Unidades administrativas

Usuarios y grupos

Configuración

Nombre

Finalizar

Asignar un nombre a la directiva

Nombre *

CCN-Directiva-Etiqueta-Confidencial1

Escriba una descripción para la directiva de etiquetas de confidencialidad

Descripción de CCN-Directiva-Etiqueta-Confidencial1

3.2.3.2 LIMPIEZA DE DOCUMENTOS

Al compartir una copia electrónica de determinados documentos de Office365 o al exponer cierta documentación en internet, es una buena práctica revisar los documentos en busca de datos ocultos, información personal y en general cualquier metadato que pudiera estar asociado. Es posible eliminar esta información a través del Inspector de documentos, característica que se accede desde las propias aplicaciones de Word, Excel, PowerPoint o Visio.

3.2.3.3 COPIAS DE SEGURIDAD

En el Modelo de responsabilidad compartida de Office 365 de Microsoft donde se especifica qué es responsabilidad de Microsoft y qué responsabilidad del cliente en materia de copias de seguridad.

No existe una solución global de respaldo de Office 365. Consultar las guías específicas de los servicios para información más concreta.

3.2.4 PROTECCIÓN DE LOS SERVICIOS

3.2.4.1 PROTECCIÓN FRENTE A DENEGACIÓN DE SERVICIO

Office 365 ofrece un sistema avanzado de detección de amenazas y sistemas de mitigación para proteger la infraestructura subyacente de los ataques de denegación de servicio (DoS) y prevenir la interrupción de servicio a los clientes.

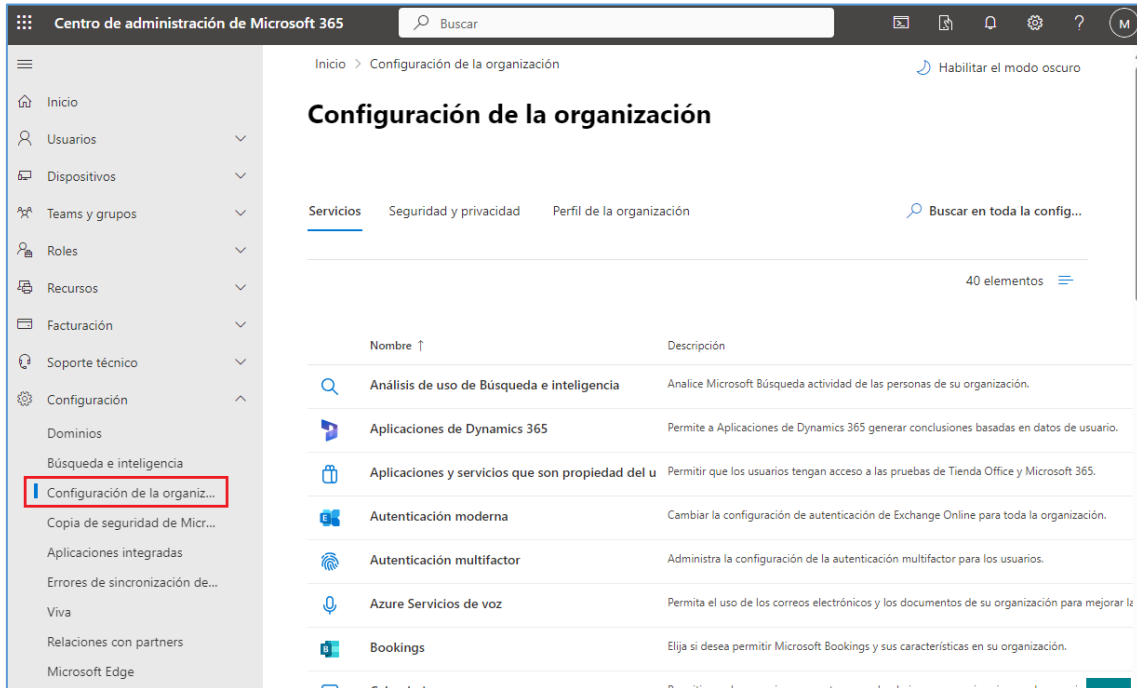
El sistema de defensa DDoS de Azure está diseñado no solo para resistir ataques desde el exterior, sino también desde otros tenants de Azure. Los mecanismos de limitación de peticiones de Exchange Online y SharePoint Online forman parte de un enfoque de varias capas para defenderse contra ataques DoS.

Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure] para obtener más información sobre el sistema de defensa DDoS de Azure.

4. OTRAS CONSIDERACIONES DE SEGURIDAD

4.1 SERVICIOS Y COMPLEMENTOS

Es interesante, de cara a tener un mayor control sobre las operaciones que puedan realizar los usuarios, restringir o habilitar el uso de ciertos servicios y complementos adicionales que puedan estar disponibles para los usuarios de Office 365. Este control se realiza desde el Centro de administración de Microsoft 365, menú [Configuración\Configuración de la organización].



5. CARACTERÍSTICAS DISPONIBLES POR LICENCIAMIENTO

| Administración de cuentas de usuario | Microsoft 365 Empresa Básico y Estándar | Microsoft 365 Empresa Premium | Office 365 E1 | Microsoft 365 E3 y Office 365 E3 | Microsoft 365 E5 y Office 365 E5 | Microsoft 365 F1 | Microsoft 365 F3 y Office 365 Enterprise F3 |
|--|---|-------------------------------|---------------|----------------------------------|----------------------------------|------------------|---|
| Identidad en la nube, identidad federada o autenticación multifactor | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Configuración de escritorio de Office 365 | Sí | Sí | No | Sí | Sí | No | No |
| Eliminar cuentas y restablecer contraseñas de usuario de Microsoft 365 o mediante Windows PowerShell | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Los usuarios pueden cambiar su propia contraseña | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Administración de licencias | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Informes de actividad del centro de Administración | Microsoft 365 Empresa Básico y Estándar | Microsoft 365 Empresa Premium | Office 365 E1 | Microsoft 365 E3 y Office 365 E3 | Microsoft 365 E5 y Office 365 E5 | Microsoft 365 F1 | Microsoft 365 F3 y Office 365 Enterprise F3 |
| Informes de actividad | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| API de informes de uso de Microsoft Graph | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Microsoft Graph API (BETA) | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Confianza | Microsoft 365 Empresa Básico y Estándar | Microsoft 365 Empresa Premium | Office 365 E1 | Microsoft 365 E3 y Office 365 E3 | Microsoft 365 E5 y Office 365 E5 | Microsoft 365 F1 | Microsoft 365 F3 y Office 365 Enterprise F3 |
| Office 365 Cloud App Security | No | No | No | No | Sí | No | No |
| Detección de Microsoft Defender for Cloud Apps | No | Sí | No | Sí (solo M365 E3) | Sí | Sí | Sí (solo M365 F3) |
| Microsoft Defender for Cloud Apps | No | No | No | No | Sí (solo M365 E5) | No | No |
| Microsoft Defender para Office 365 | No | Sí | No | No | Sí | No | No |

| | | | | | | | |
|--|----|----|----|----|----|----|----|
| Caja de seguridad del cliente de Microsoft Purview | No | No | No | No | Sí | No | No |
| Clave de cliente de Microsoft Purview | No | No | No | No | Sí | No | No |
| Microsoft Purview eDiscovery (Premium) | No | No | No | No | Sí | No | No |
| Auditoría de Microsoft Purview (estándar) | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Auditoría de Microsoft Purview (Premium) | No | No | No | No | Sí | No | No |
| Puntuación de seguridad de Microsoft Office 365 Threat Intelligence | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| | No | No | No | No | Sí | No | No |

6. GLOSARIO Y ABREVIATURAS

A continuación se describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

| Término | Definición |
|--|---|
| AD DS | <i>Active Directory Domain Services</i> (Servicios de dominio de Directorio Activo). |
| Microsoft Entra ID | <i>Conocido anteriormente como Azure Active Directory.</i> |
| Azure RMS | <i>Azure Rights Management (Azure RMS).</i> |
| Centro de Administración de Microsoft 365 | Portal de Administración de Office 365. Accesible desde la url: admin.microsoft.com . |
| CSP | <i>Cloud Service Provider</i> |
| DDoS | <i>Distributed Denial of Service</i> (Ataque de Denegación de Servicio Distribuido), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. |
| ENS | <i>Esquema Nacional de Seguridad.</i> |
| MFA | <i>Multifactor Authentication</i> (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una <i>app</i> , <i>sms</i> , etc. |
| Microsoft Intune | Microsoft Intune es un servicio de administración de movilidad empresarial (EMM) basado en nube que ayuda a los empleados a ser productivos mientras mantiene protegidos los datos corporativos. Al igual que otros servicios de Azure, Microsoft Intune está disponible en el portal de Azure. Intune permite: <ul style="list-style-type: none"> - Administrar los dispositivos móviles y los equipos que los empleados usan para tener acceso a datos de la empresa. - Administrar las aplicaciones móviles que usa la plantilla. - Proteger la información de la empresa al ayudar a controlar la manera en que los empleados tienen acceso a ella y la comparten. - Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad de la empresa |
| O365 | <i>Office 365.</i> |
| PowerShell | PowerShell (originalmente llamada Windows PowerShell) es una interfaz de consola (<i>CLI</i>) con posibilidad de escritura y unión de comandos por medio de instrucciones (<i>scripts</i>). |
| PS | <i>PowerShell.</i> |
| SaaS | <i>Software as a Service</i> (Software como Servicio). Modelo de distribución de software donde el soporte lógico y los datos que |

| | |
|--------------------------|---|
| | maneja se alojan en servidores de una compañía de TIC, y se accede vía internet. |
| Sensitivity label | <i>Etiqueta de sensibilidad.</i> Permiten clasificar, cifrar, agregar marcadores y controlar accesos en documentos y correos electrónicos en Office 365. |
| Tenant | Un <i>tenant</i> de Office 365 es un espacio reservado en la nube de Microsoft desde el que tendremos acceso a los recursos y servicios que Microsoft ofrece. |
| TLS | TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos. |

7. ANEXO A. CREAR UNA CUENTA DE USUARIO INDIVIDUAL

```

Import-Module Microsoft.Graph.Users
Connect-MgGraph -Scopes "User.ReadWrite.All"

$params_CreateUsers = @{
    accountEnabled = $true
    displayName = "Adele Vance"
    givenName = "Adele"
    surname = "Vance"
    mailNickname = "Adelev"
    userPrincipalName = "Adelev@domain.com"
    usageLocation = "ES"
    passwordProfile = @{
        forceChangePasswordNextSignIn = $true
        password = "CONTRASEÑA"
    }
}

$params_AddLicnese = @{
    addLicenses = @(
        @{
            disabledPlans = @(
                # "39b5c996-467e-4e60-bd62-46066f572726"
            )
            skuId = "f245ecc8-75af-4f8e-b61f-27d8114de5f3"
        }
    )
    removeLicenses = @(
    )
}

# Comando para crear el usuario
New-MgUser -BodyParameter $params_CreateUsers

# Comando para asignar la licencia
Set-MgUserLicense -UserId "Adelev@domain.com" -BodyParameter $params_AddLicnese

# Una vez terminado el proceso, nos desconectamos de la sesión.
Disconnect-MgGraph
  
```

- a) **Import-Module Microsoft.Graph.Users:** Con la primera línea importamos el módulos
- b) **Connect-MgGraph -Scopes "User.ReadWrite.All":** Nos conectamos a Microsoft Graph con el rol de lectura y escritura de usuarios.
- c) **\$params_CreateUsers:** En este array añadimos los datos del usuario.
- d) **passwordProfile:**
 - a. **forceChangePasswordNextSignIn:** Al poner en true esta línea estamos indicando que el usuario debe cambiar la contraseña en el siguiente inicio de sesión.
 - b. **Password:** Aquí se debe escribir la contraseña del usuario. Por defecto exige que la contraseña sea fuerte.
- e) **\$params_AddLicnese:** En este array añadimos las opciones de las licencias.
 - a. **addLicenses:**
 - i. **disabledPlans:** Si hay algún plan de la licencia que se desea desactivar, se debiera escribir el skuID de ese plan dentro de este array.
 - ii. **skuId:** Escribimos el skuID de la licencia a asignar.

- b. **removeLicenses = @():** Si el usuario ya tuviese alguna licencia asignada y hubiera que quitarla, se deberá escribir el skuID de esta licencia.
- f) **New-MgUser -BodyParameter \$params_CreateUsers:** Este comando crea el usuario.
- g) **Set-MgUserLicense -UserId "AdeleV@domain.com" -BodyParameter \$params_AddLincese:** Este comando asigna la licencia al usuario creado.
- h) **Disconnect-MgGraph:** Este comando termina la conexión con Microsoft Graph.

8. ANEXO B. CREAR VARIAS CUENTAS DE USUARIO

- a) Crear un archivo de valores separados por comas (CSV) que contenga la información necesaria de la cuenta de usuario. Por ejemplo:

```

Usuario 1,Usuario,1,Usuario1,Usuario1@dominio.com,ES,f245ecc8-75af-4f8e-b61f-27d8114de5f3,AcugWKQ4_{94
Usuario 2,Usuario,2,Usuario2,Usuario2@dominio.com,ES,f245ecc8-75af-4f8e-b61f-27d8114de5f3,AcugWKQ4_{94
Usuario 3,Usuario,3,Usuario3,Usuario3@dominio.com,ES,f245ecc8-75af-4f8e-b61f-27d8114de5f3,AcugWKQ4_{94
  
```

- b) Ejecutar desde PowerShell:

```

Import-Module Microsoft.Graph.Users
Connect-MgGraph -Scopes "User.Readwrite.All"

$UsersList = Import-Csv -Path "C:\Users\\Downloads\CCN\users.csv" -
Delimitter ","

foreach ($User in $UsersList) {
    $params_CreateUsers = @{
        accountEnabled = $true
        displayName = $User.displayName.Trim()
        givenName = $User.givenName.Trim()
        surname = $User.surname.Trim()
        mailNickname = $User.mailNickname.Trim()
        userPrincipalName = $User.userPrincipalName.Trim()
        usageLocation = $User.usageLocation.Trim()
        passwordProfile = @{
            forceChangePasswordNextSignIn = $true
            password = $User.password.Trim()
        }
    }

    $params_AddLincese = @(
        addLicenses = @(
            @{
                disabledPlans = @(
                )
                skuId = $User.license.Trim()
            }
        )
        removeLicenses = @(
        )
    )

    # Comando para crear el usuario
    New-MgUser -BodyParameter $params_CreateUsers

    # Comando para asignar la licencia
    Set-MgUserLicense -UserId $User.userPrincipalName.Trim() -BodyParameter
    $params_AddLincese
}

# Una vez terminado el proceso, nos desconectamos de la sesión.
Disconnect-MgGraph
  
```

- a) **Import-Module Microsoft.Graph.Users:** Con la primera línea importamos el módulos
- b) **Connect-MgGraph -Scopes "User.ReadWrite.All":** Nos conectamos a Microsoft Graph con el rol de lectura y escritura de usuarios.
- c) **\$UsersList:** Aquí se añadirá la ruta del CSV de los usuarios
- d) **\$params_CreateUsers:** En este array añadimos los datos del usuario.
- e) **passwordProfile:**
 - a. **forceChangePasswordNextSignIn:** Al poner en true esta línea estamos indicando que el usuario debe cambiar la contraseña en el siguiente inicio de sesión.
 - b. **Password:** Aquí se debe escribir la contraseña del usuario. Por defecto exige que la contraseña sea fuerte.
- f) **\$params_AddLicense:** En este array añadimos las opciones de las licencias.
 - a. **addLicenses:**
 - i. **disabledPlans:** Si hay algún plan de la licencia que se desea desactivar, se deberá escribir el skuID de ese plan dentro de este array.
 - ii. **skuId:** Escribimos el skuID de la licencia a asignar.
 - b. **removeLicenses = @():** Si el usuario ya tuviese alguna licencia asignada y hubiera que quitarla, se deberá escribir el skuID de esta licencia.
- g) **New-MgUser -BodyParameter \$params_CreateUsers:** Este comando crea el usuario.
- h) **Set-MgUserLicense -UserId "<>" -BodyParameter \$params_AddLicense:** Este comando asigna la licencia al usuario creado.
- i) **Disconnect-MgGraph:** Este comando termina la conexión con Microsoft Graph.

9. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización podrá valorar qué medidas de las propuestas se cumplen.

| Control ENS | Configuración | Estado | |
|-------------|---|---|---|
| Op | Marco Operacional | | |
| Op.acc | Control de Acceso | | |
| Op.acc.1 | Identificación Se ha configurado el uso de cuentas y la asignación de licencias a usuarios. Cada usuario debe disponer de un acceso nominal y personal a Office 365 que permita su identificación de forma única. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| Op.acc.3 | Segregación de funciones y tareas Se ha asignado adecuadamente los roles de administración. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |

| | | | |
|------------------------------|---|---|---|
| <p>Op.acc.5 Op.acc.6</p> | <p>Mecanismo de autenticación</p> <p>Se ha habilitado <u>Multi-Factor Authentication</u> (MFA) para los usuarios de la organización y externos.</p> | <p>Aplica:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Cumple:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |
| <p>op.exp</p> | <p>Explotación</p> | | |
| <p>op.exp.6</p> | <p>Protección frente a código dañino</p> <p>Se han habilitado y configurado una o varias medidas de protección del correo electrónico como Antispam, Antispoofing, Antiphishing y Antimalware.</p> | <p>Aplica:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Cumple:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |

| | | | |
|----------|---|---|---|
| | | | |
| op.exp.6 | Protección frente a código dañino | | |
| | <p>Se comprueba periódicamente la detección de amenazas en tiempo real, accesible desde el <i>Centro de Seguridad de Office 365</i>, y se genera el informe pertinente.</p> <p><i>* Si la organización dispone de las licencias correspondientes.</i></p> | <p>Aplica:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Cumple:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |
| op.exp.7 | Gestión de incidentes | | |
| | <p>Se ha revisado el panel de incidentes y han aplicado las medidas necesarias para corregirlas.</p> | <p>Aplica:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Cumple:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |
| op.exp.8 | Registro de la actividad | | |
| | <p>Se ha comprobado que el registro de Auditoría está activado y capturando eventos.</p> | <p>Aplica:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Cumple:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> |
| | | <p>Evidencias Recogidas:</p> <p><input type="checkbox"/> Si <input type="checkbox"/> No</p> | <p>Observaciones:</p> |

| | | | |
|----------|--|---|---|
| | | | |
| op.exp.8 | Registro de la actividad | | |
| | Se ha securizado la consulta del registro de actividad mediante el establecimiento de los roles adecuados. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| op.mon | Monitorización del sistema | | |
| | Se han configurado alertas en el <i>Centro de Seguridad de Office 365</i> . | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |

| | | | |
|-----------|---|---|---|
| mp | Medidas de Protección | | |
| mp.info | Protección de la información | | |
| mp.info.2 | Calificación de la información | | |
| | Se han aplicado políticas de retención. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| mp.info.2 | Calificación de la información | | |
| | Se han aplicado políticas de DLPs. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| mp.info.2 | Calificación de la información | | |
| | Se han aplicado <i>sensitivity labels</i> . | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |

| | | | |
|-----------|---|---|---|
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| mp.info.5 | Limpieza de documentos | | |
| | Se ha eliminado información personal y en general cualquier metadato que pudiera estar asociado a los documentos. *Mediante la herramienta Inspector de documentos (característica que se accede desde las propias aplicaciones de Word, Excel, PowerPoint o Visio) o aplicaciones de terceros. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| mp.info.6 | Copias de seguridad | | |
| | Se dispone de planes específicos de copias de seguridad de la información en aquellos servicios en donde se admita. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| mp.s | Protección de los servicios | | |
| mp.s.8 | Protección frente a denegación de servicio | | |
| | Se ha tenido en cuenta la información detallada en la guía [CCN-STIC-884A - Guía de configuración segura para Azure] sobre el <i>sistema de defensa DDoS de Azure</i> . | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |

| | | | |
|--|--|---|---|
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |
| | Servicios y complementos | | |
| | Se ha controlado los servicios y complementos disponibles para los usuarios. | Aplica: <input type="checkbox"/> Si <input type="checkbox"/> No | Cumple: <input type="checkbox"/> Si <input type="checkbox"/> No |
| | | Evidencias Recogidas: <input type="checkbox"/> Si <input type="checkbox"/> No | Observaciones: |



CCN-STIC 885A



Guía de configuración segura para Office 365

