

Guía de Seguridad de las TIC CCN-STIC 885A

Guía de configuración segura para Office 365



DICIEMBRE 2019

Edita:



2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.13 16:37:40 +01'00'

© Centro Criptológico Nacional, 2019

NIPO: 083-19-261-6

Fecha de Edición: diciembre de 2019

Plain Concepts ha participado en la realización y modificación del presente documento y sus anexos. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

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.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019



Félix Sanz Roldán

Secretario de Estado

Director del Centro Criptológico Nacional

ÍNDICE

1. OFFICE 365	6
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA	6
1.2 DEFINICIÓN DE LA SOLUCIÓN	6
1.3 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL	7
2. DESPLIEGUE DE OFFICE 365	9
2.1 ADMINISTRADOR – CONFIGURACIÓN INICIAL	9
2.2 USUARIO FINAL - PRIMEROS PASOS	12
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	22
3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS	22
3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO	26
3.1.1.5 MECANISMOS DE AUTENTICACIÓN	26
3.1.1.6 ACCESO LOCAL	30
3.1.1.7 ACCESO REMOTO	30
3.1.2 EXPLOTACIÓN	30
3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO	30
3.1.2.2 REGISTRO DE ACTIVIDAD	31
3.1.2.3 GESTIÓN DE INCIDENTES	34
3.1.2.4 PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	36
3.2 MEDIDAS DE PROTECCIÓN	37
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES	37
3.2.2 MONITORIZACIÓN DEL SISTEMA	37
3.2.3 PROTECCIÓN DE LA INFORMACIÓN	42
3.2.3.1 CALIFICACIÓN DE LA INFORMACIÓN	42
3.2.3.2 CIFRADO	69
3.2.3.3 LIMPIEZA DE DOCUMENTOS	70
3.2.3.4 COPIAS DE SEGURIDAD	70
3.2.4 PROTECCIÓN DE LOS SERVICIOS	71

3.2.4.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO.....71

4. OTRAS CONSIDERACIONES DE SEGURIDAD 71

4.1 SERVICIOS Y COMPLEMENTOS.....71

5. CARACTERÍSTICAS DISPONIBLES POR LICENCIAMIENTO 72

6. GLOSARIO Y ABREVIATURAS 74

7. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD 76

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 conjuntamente 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-823 Servicios en la Nube.
- CCN-STIC-884A - Guía de configuración segura para Azure.
- ENS Real Decreto BOE-A-2010-1330.

1.2 Definición 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 *Microsoft Azure*.



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

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

En la fecha de esta guía, el *Módulo Azure Active Directory para Graph* no reemplaza completamente la funcionalidad de los cmdlets del *Módulo Microsoft Azure Active Directory para Windows PowerShell* para la administración de usuarios, grupos y licencias. En muchos casos, deberá usarse ambas versiones. Pueden instalarse ambas versiones de forma segura en el mismo equipo.

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 Azure; y *ejecución remota de PowerShell*, instalando los módulos necesarios en el equipo cliente del administrador. La seguridad de una conexión de comunicación remota de PowerShell se contempla desde dos perspectivas:

- Autenticación inicial. Mediante un usuario con los derechos adecuados para la administración del servicio.
- 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. La compatibilidad con la versión de 32 bits del *Módulo de Microsoft Azure Active Directory para Windows PowerShell* se discontinuó en octubre de 2014. Es necesario así mismo, usar la versión 5.1 o posterior de PowerShell. Más información sobre requerimientos previos de plataformas en: <https://docs.microsoft.com/es-es/office365/enterprise/powershell/connect-to-office-365-powershell>.

Instalar módulo de PowerShell de Azure Active Directory para Graph

1. Instalar el software necesario

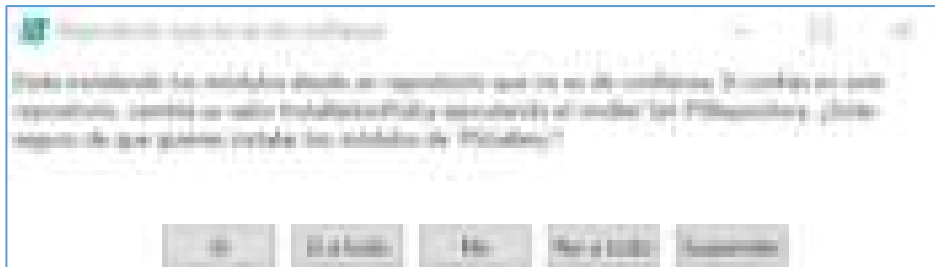
Estos pasos son necesarios una sola vez en el equipo físico desde cual se va a administrar el *tenant* de Office 365, no cada vez que se conecta.

1. Abrir un símbolo del sistema de Windows PowerShell con privilegios elevados (ejecutar Windows PowerShell como administrador).

- En la ventana de comandos de Windows PowerShell (como administrador), ejecutar este comando:

```
# Install-Module -Name AzureAD
```

Si se pregunta si se quiere instalar un módulo desde un repositorio que no es de confianza, escribir “Y” y presionar ENTRAR.



Esto ocurre porque de forma predeterminada, la *Galería* de PowerShell no está configurada como un repositorio de confianza. Responder *Sí* o *Sí a todo*.

Para **actualizar** una nueva versión del módulo ejecutar el comando anterior con el parámetro *Force*:

```
# Install-Module -Name AzureAD -Force
```

Nota: Se recomienda realizar actualizaciones mensuales.

2. Conectarse a Azure AD para la suscripción de Office 365

Para conectarse a Azure AD para la suscripción de Office 365 con un nombre de cuenta y contraseña o con la autenticación multifactor (MFA), ejecutar este comando desde un símbolo del sistema de Windows PowerShell:

```
# Connect-AzureAD
```

En la sección [2.1. Administrador – configuración inicial] se explica cómo obtener las credenciales de acceso de *administración*.

Instalar módulo Microsoft Azure Active Directory para Windows PowerShell

Los comandos del Módulo Microsoft Azure Active Directory para Windows PowerShell tienen **Mso** en el nombre de su *cmdlet*.

1. Instalar el software necesario

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.

- Instalar la versión de 64 bits de *Microsoft Online Services* - Ayudante para el inicio de sesión: *Ayudante para el inicio de sesión de Microsoft Online Services* para profesionales de TI (RTW).
- Instalar el *Módulo Microsoft Azure Active Directory* para Windows PowerShell siguiendo estos pasos:

- Abrir un símbolo del sistema de Windows PowerShell con privilegios elevados (ejecute Windows PowerShell como administrador).
- Ejecutar el comando:

```
# Install-Module MSOnline
```

- Aceptar la instalación del proveedor de NuGet.
- Aceptar la instalación del módulo desde PSGallery.

Para **actualizar** una nueva versión del módulo ejecutar el comando anterior con el parámetro *Force*:

```
# Install-Module MSOnline -Force
```

Nota: Se recomienda realizar actualizaciones mensuales.

2. Conectarse a Azure AD para la suscripción de Office 365

Para conectarse a Azure AD para la suscripción de Office 365 con un nombre de cuenta y contraseña o con la autenticación multifactor (MFA), ejecutar este comando desde un símbolo del sistema de Windows PowerShell

```
# Connect-MsolService
```

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].

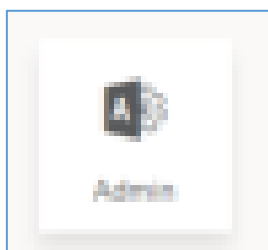
Office 365 se encuentra englobado en la categoría de servicio **SaaS** (Software as a Service). El CSP (Microsoft) es el encargado de ofrecer al cliente el software como un servicio.

2.1 Administrador – configuración inicial

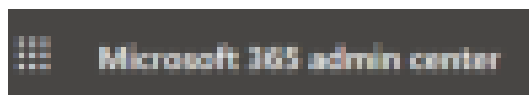
1. Acceder al portal de Office 365 con usuario administrador.

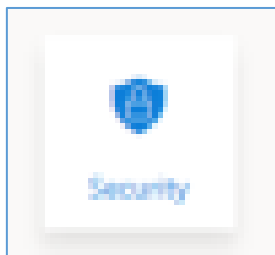
El usuario *administrador* podrá acceder al portal Office 365 a través de la misma *url* que el *usuario final*: portal.office365.com.

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](#).

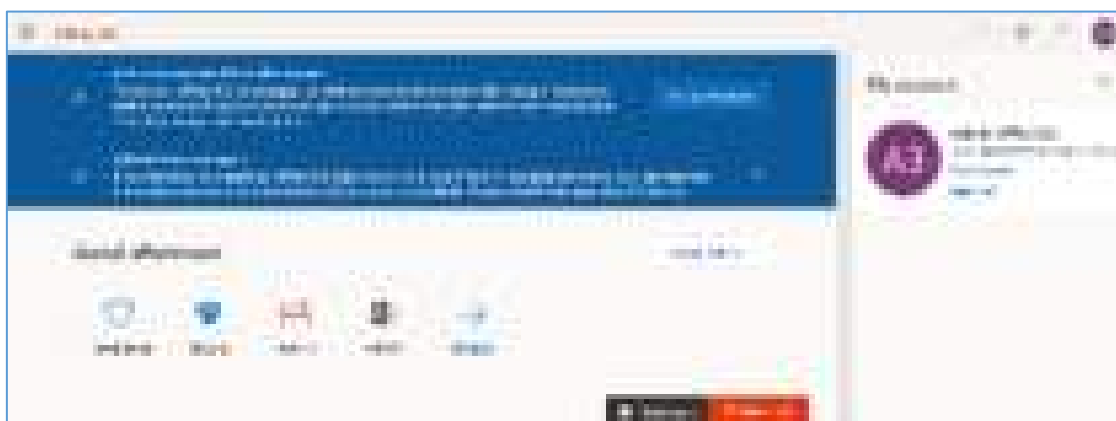




Y un icono de *seguridad*, para acceder al [Centro de Seguridad y Cumplimiento de Office 365](#).



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.



2. Cambiar el idioma a español.

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



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

3. 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.

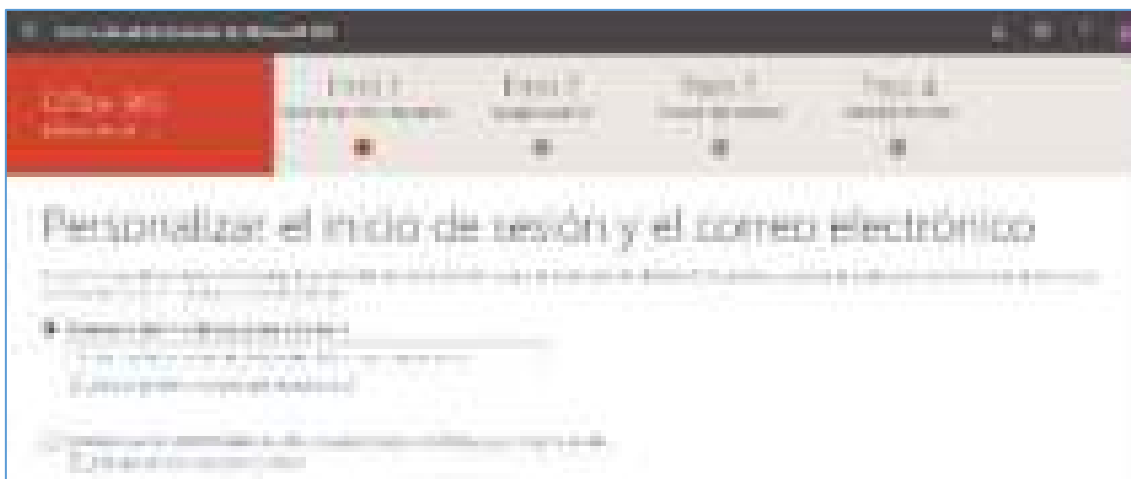
Si no se dispone de un **dominio profesional** puede aparecer un mensaje avisando de la conveniencia de establecer uno para personalizar las cuentas de correo electrónico.

Pulsar el botón “Ir a instalación”:



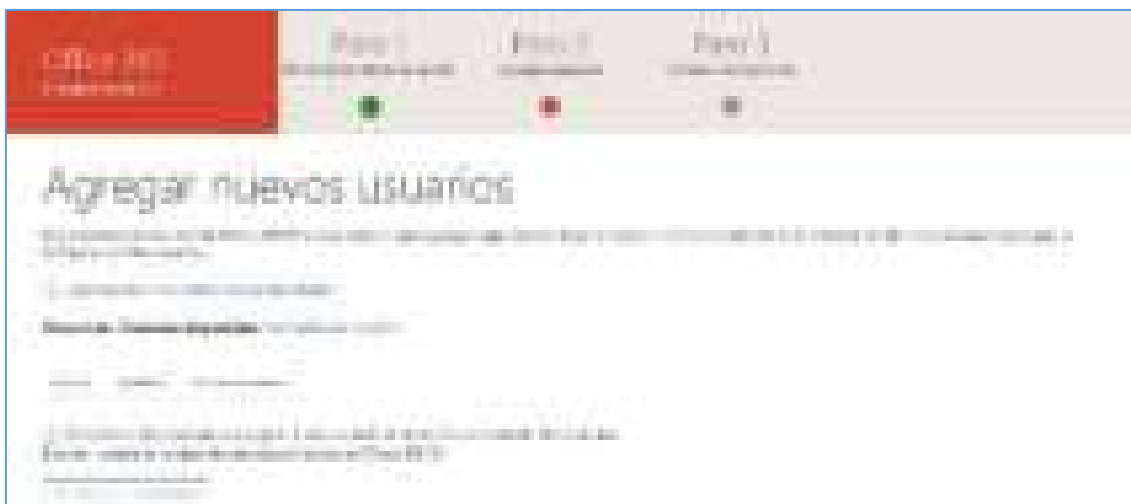
3.1. Personalizar el inicio de sesión y correo electrónico.

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

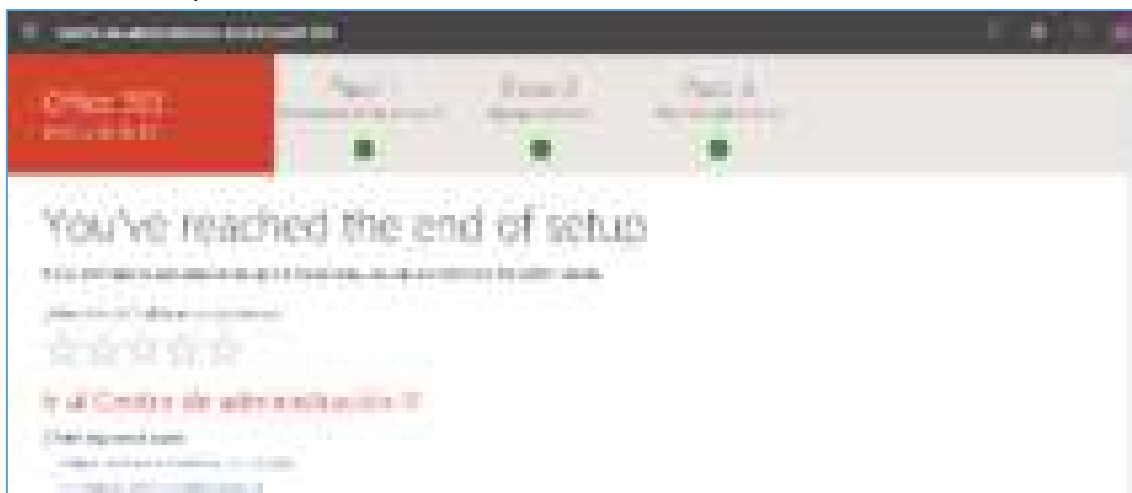


3.2. Agregar nuevos usuarios.

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



3.3. Fin del proceso de instalación.



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

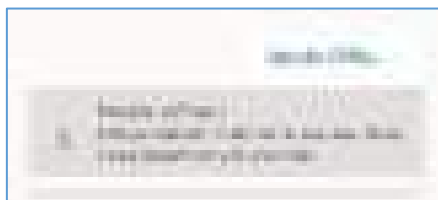
2.2 Usuario final - primeros pasos

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:

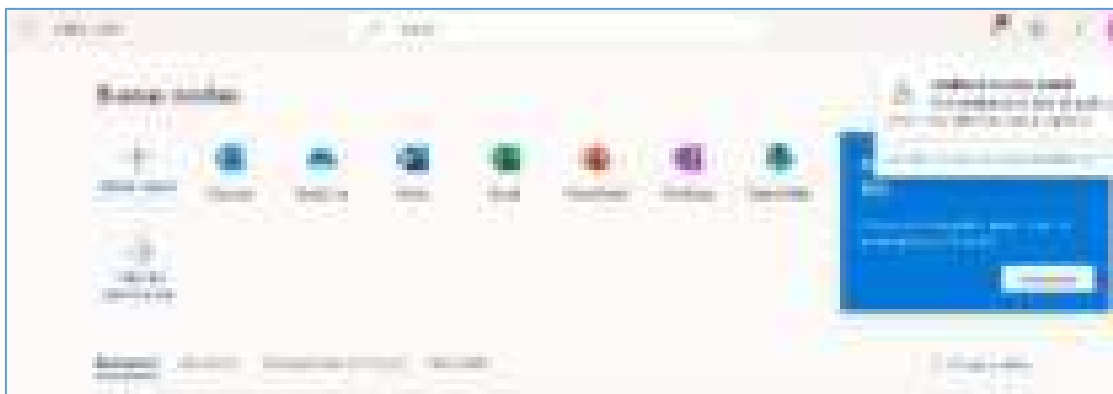


Desde el propio panel de Office 365 se permite instalar la versión de escritorio de las aplicaciones.

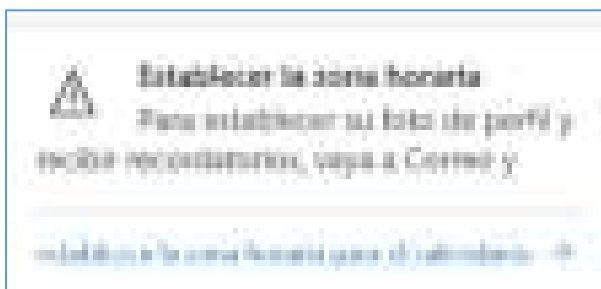


Nota: para la configuración de seguridad de la versión de escritorio de las aplicaciones Office remitirse a la Guía CCN-STIC más actualizada (CCN-STIC-585 en el momento de edición de la presente guía).

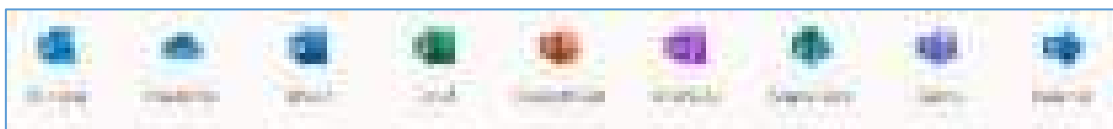
Una vez asignadas la licencia al usuario final, y tras logarse en el portal de Office 365, se mostrará una página de inicio con los iconos de todas las aplicaciones a las que se tiene acceso, y algunos mensajes de aviso.



Es aconsejable establecer el *idioma* y la *zona horaria*.



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 *Azure Active Directory (Azure AD)*, 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].

3.1.1.1.1 Modelos de gestión de identidades

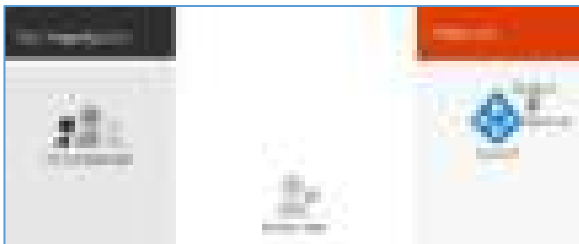
En esta sección se abordarán los distintos modelos y mecanismos para la gestión de identidades en Office 365. Principalmente nos centraremos en dos: *modelo identidad sólo nube* (que será tomado como referencia en esta guía) y *modelo de identidad híbrida*.

A continuación, se muestra una tabla con las características de ambos modelos.

	Identidad solo de nube	Identidad híbrida
Definición	La cuenta de usuario solo existe en el tenant de Azure Active Directory (Azure AD) para su suscripción a Microsoft 365.	La cuenta de usuario existe en AD DS y una copia también se encuentra en el tenant de Azure AD para su suscripción a Microsoft 365. La cuenta de usuario en Azure AD también puede incluir una versión <i>hash</i> de la contraseña de la cuenta de usuario.
Cómo autentica Microsoft 365 las credenciales de usuario	El tenant de Azure AD para su suscripción a Microsoft 365 realiza la autenticación con la cuenta de identidad de nube.	El tenant de Azure AD 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 *Azure AD*. 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 *Azure AD* para acceder a los servicios en la nube de Office 365.

Azure AD 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 *Azure AD*, se puede administrar las identidades de nube con herramientas como el *Centro de administración de Microsoft 365* y *Windows PowerShell* con el módulo *Azure Active Directory PowerShell* para *Graph*.

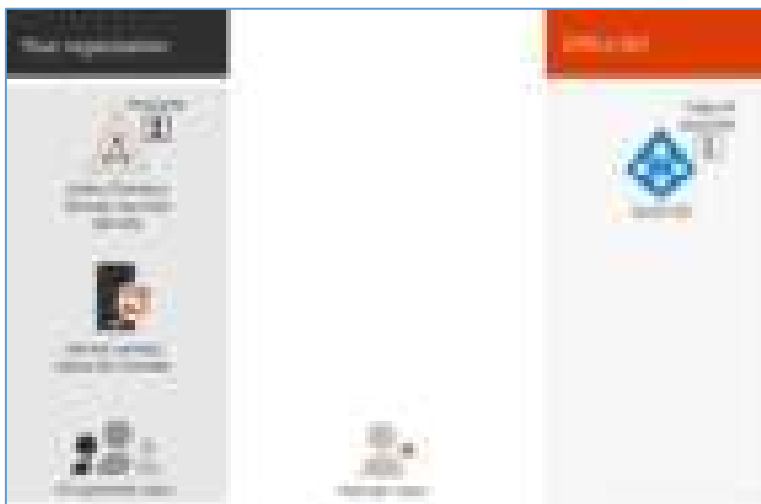
Modelo identidad híbrido

La identidad híbrida usa cuentas que se originan en un *AD DS* local y tienen una copia en el tenant de *Azure AD* 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 *Azure AD*. Pero los cambios realizados en cuentas basadas en la nube en *Azure AD*, como nuevas cuentas de usuario, no se sincronizan con *AD DS*.

Azure AD 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 *Azure AD*. *Azure AD 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 *Azure AD*.

Estos son los componentes de la identidad híbrida.



El *tenant* de *Azure AD* 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 *Azure AD*.

3.1.1.1.2 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 *Azure Active Directory* (Azure AD) de la suscripción a Office 365.

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

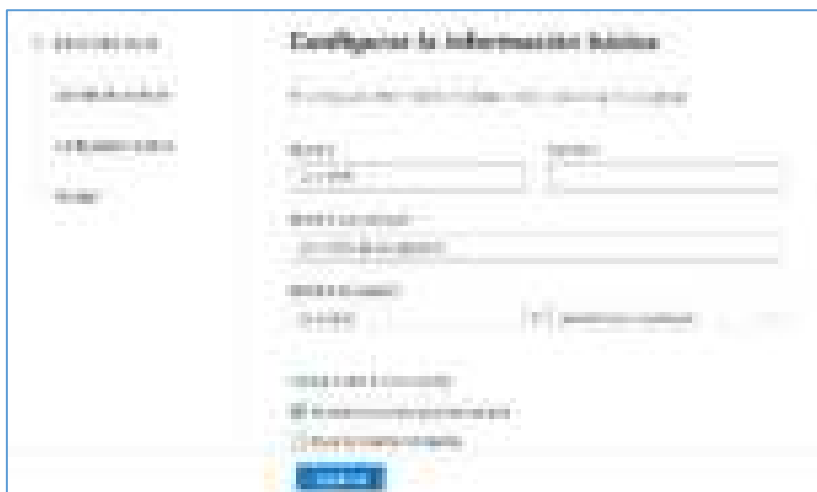
- Centro de administración de Microsoft 365
- PowerShell de Office 365

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.

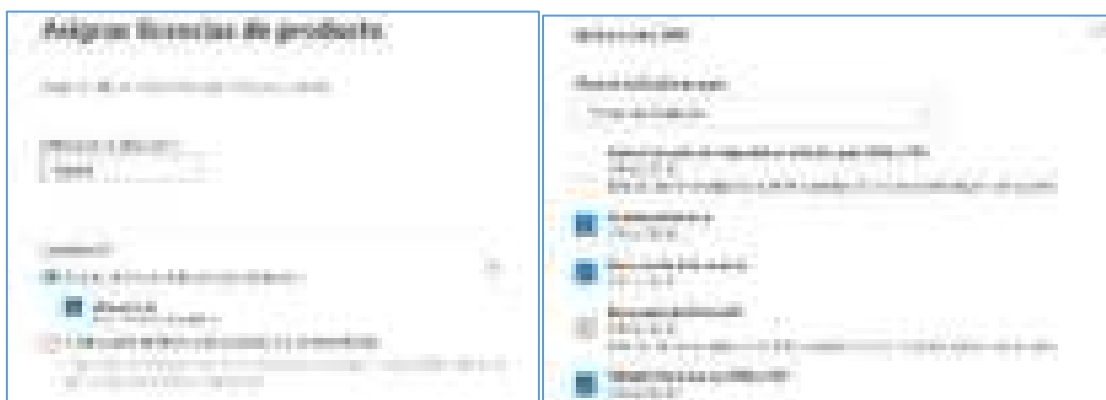
Creación de usuarios

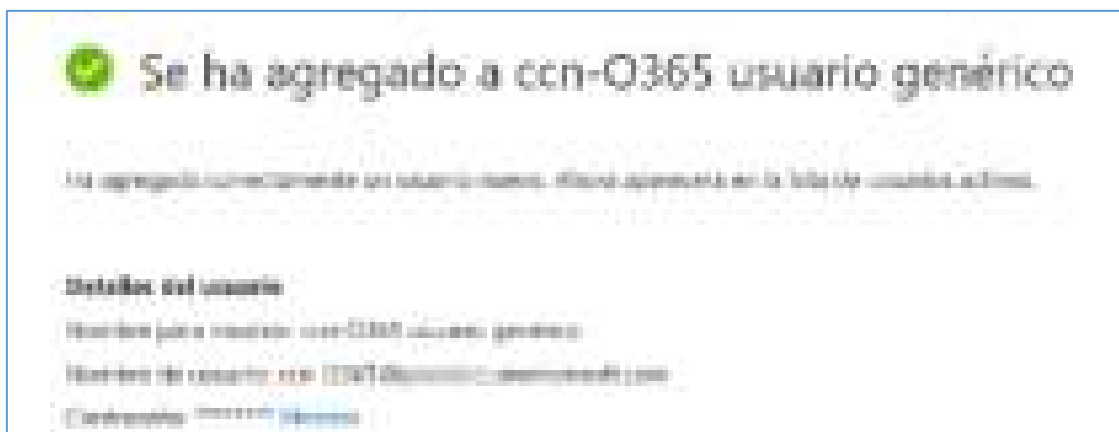
1. Desde el menú [Usuarios\Usuarios activos] pulsar el icono “Agregar un usuario”, y rellenar el formulario.



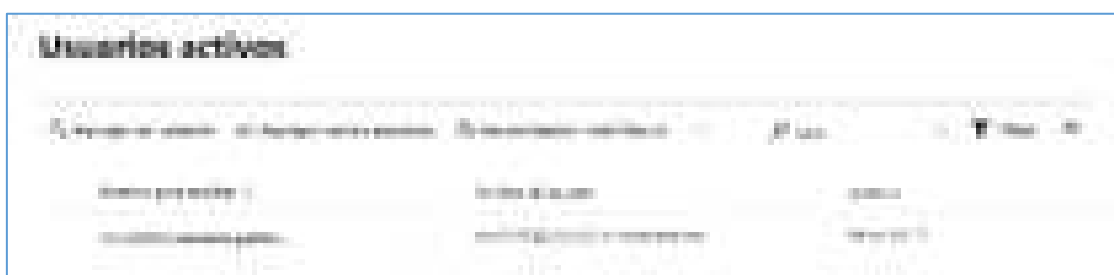
Nota: mas información sobre gestión de contraseñas en el apartado [3.1.1.5 Mecanismos de autenticación].

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



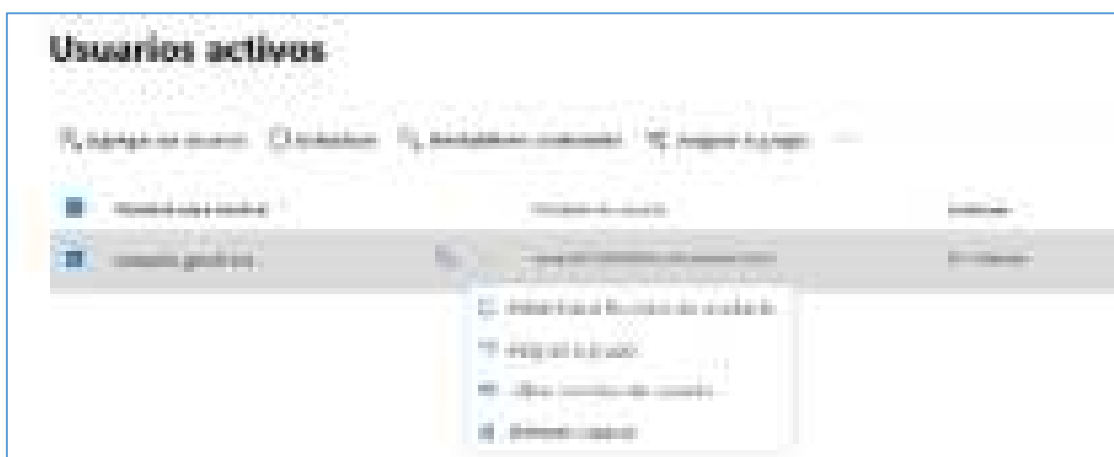


3. Para comprobar que el usuario se ha creado correctamente revisar la lista de “usuarios activos”.



Operaciones básicas sobre usuarios

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

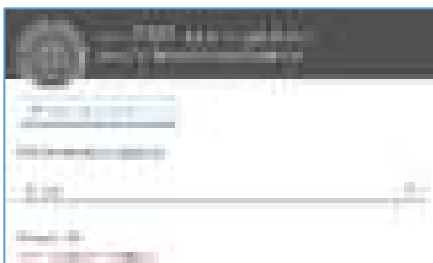


Administrar licencias

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.



Asignar usuario a grupo



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

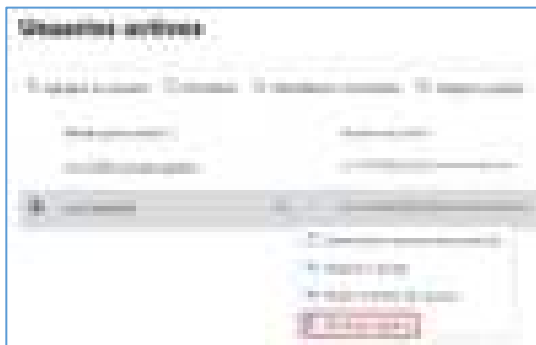
Editar usuario

1. Desde el menú [Usuarios\Usuarios activos] pulsando sobre el “nombre” del usuario.

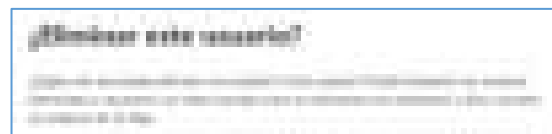


2. Para asignar *roles* al usuario consultar el apartado [3.1.1.3 Segregación de funciones y tareas].

Eliminar usuario



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

1. Agregar grupo.



Desde el menú [Grupos] pulsar el icono “Agregar un grupo”.

2. Cumplimentar información del grupo.



Aunque el mensaje de la opción de **privacidad** indica que no puede cambiarse una vez creado el grupo, en las nuevas actualizaciones ya se permite. Los valores posibles son:

- *Privado*: sólo los miembros pueden ver el contenido del grupo.
- *Público*: cualquiera puede ver el contenido del grupo.

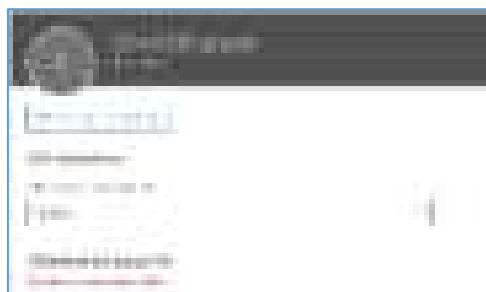
Nota: Se recomienda el uso del valor *Privado* para incrementar el control sobre el acceso a la información del grupo por parte de los usuarios.

Gestionar miembros de un grupo

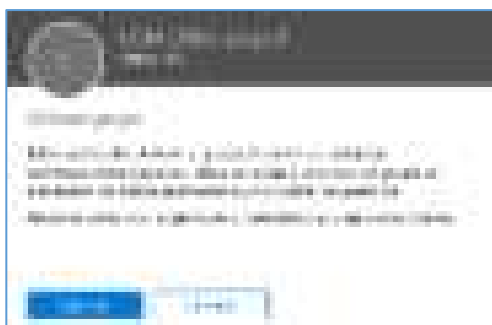
1. Desde el menú [Grupos] pulsando sobre el nombre del grupo, se despliega el panel del grupo con distintas pestañas. Seleccionar la pestaña “Miembros”.



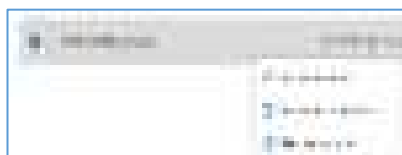
2. Después pulsar sobre el *link* “Ver todos los miembros y administrarlos”.



Eliminar grupo



Desde el menú [Grupos] pulsando sobre el icono “Más opciones” del grupo.



Powershell de Office 365

Para la ejecución de los siguientes scripts se requiere el módulo de *Microsoft Azure Active Directory* para windows *PowerShell*.

Crear una cuenta de usuario individual

```
# New-MsolUser -DisplayName <display name> -FirstName <first name> -LastName
<last name> -UserPrincipalName <sign-in name> -UsageLocation <ISO 3166-1
alpha-2 country code> -LicenseAssignment <licensing plan name> [-Password
<Password>]
```

Ejemplo:

```
# New-MsolUser -DisplayName "John Doe" -FirstName John -LastName Doe -
UserPrincipalName johndoe@contoso.onmicrosoft.com -UsageLocation US
```

Crear varias cuentas de usuario

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

```
UserPrincipalName,FirstName,LastName,DisplayName,UsageLocation,AccountSkuId
Claudel@contoso.onmicrosoft.com,Claude,Loiselle,ClaudeLoiselle,US,contoso:ENTERPRISEPACK
LynneB@contoso.onmicrosoft.com,Lynne,Baxter,Lynne Baxter,US,contoso:ENTERPRISEPACK
ShawnM@contoso.onmicrosoft.com,Shawn,Melendez,Shawn Melendez,US,contoso:ENTERPRISEPACK
```

2. Ejecutar desde PowerShell:

```
# Import-Csv -Path <Input CSV File Path and Name> | foreach {New-MsolUser -
DisplayName $_.DisplayName -FirstName $_.FirstName -LastName $_.LastName -
UserPrincipalName $_.UserPrincipalName -UsageLocation $_.UsageLocation -
LicenseAssignment $_.AccountSkuId [-Password $_.Password]} | Export-Csv -
Path <Output CSV File Path and Name>
```

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].

3.1.1.3 Segregación de funciones y tareas

Roles de administración

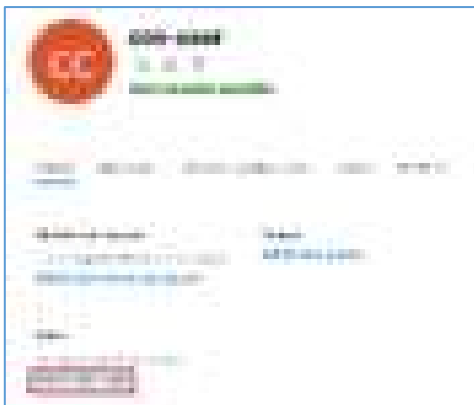
La suscripción de O365 incluye un conjunto de *roles de administrador* que se pueden asignar a los usuarios de la organización. Cada rol de administrador se asigna a funciones empresariales comunes y proporciona a los usuarios permisos para realizar tareas específicas en los centros de administración.

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	Como solo otro administrador global puede restablecer la contraseña de un administrador global, se recomienda tener al menos dos administradores globales en la organización en caso de bloqueo de cuenta. Pero el administrador global tiene casi un acceso ilimitado a la configuración de la organización y a la mayoría de los datos, por lo que también se recomienda no tener más de 4 administradores globales porque es una amenaza de seguridad.
Asignar el rol <i>menos permisivo</i>	La asignación del rol menos permisivo implica conceder a los administradores los permisos mínimos necesarios para realizar el trabajo. Por ejemplo, si se desea que alguien restablezca las contraseñas de los empleados, no se debería asignar el rol de <i>administrador global</i> ilimitado, sino el de <i>administrador de contraseñas</i> .
Requerir MFA para administradores	Es buena práctica requerir MFA en el inicio de sesión para todos los usuarios, pero es necesario al menos para los administradores. El MFA hace que los usuarios escriban un segundo método de identificación para comprobar que son quienes dicen que son.

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 acceso para administrar todas las propiedades y funciones, mientras que los administradores personalizadas solo tienen las permisos de administración. Para reducir el riesgo de riesgo por su implementación, todos el número de administradores globales en su base, asignar roles de administrador personalizadas.

Para información sobre roles de administración:

☐ [Guía de roles de administración](#) ⓘ

Administración global

Este tipo de roles de administración permite a los usuarios para el nivel máximo, como administrador global. Los roles de administración global, como el administrador global, se pueden asignar a usuarios.

☐ [Administración global](#) ⓘ

Usuarios y grupos

☐ [Administración de usuarios de usuarios](#) ⓘ

☐ [Administración de grupos](#) ⓘ

☐ [Administración de grupos de usuarios](#) ⓘ

Recursos

☐ [Administración de recursos](#) ⓘ

Roles específicos de usuarios

☐ [Administración de Exchange](#) ⓘ

☐ [Administración de usuarios de Skype](#) ⓘ

☐ [Administración de SharePoint](#) ⓘ

Roles administrativos

☐ [Administración de la configuración de temas](#) ⓘ

Roles disponibles en el centro de administración de Microsoft 365

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

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

Rol de administrador	¿A quién se le debe asignar este rol?
----------------------	---------------------------------------

Administrador global	Asignar el rol de <i>administrador global</i> a los usuarios que necesitan acceso global a la mayoría de las características y datos de administración en Microsoft Online Services. Proporcionar demasiados usuarios el acceso global es un riesgo para la seguridad y se recomienda tener entre 2 y 4 administradores globales. Solo los administradores globales pueden: -Restablecer contraseñas para todos los usuarios -Agregar y administrar dominios Nota: La persona que se registró en Microsoft Online Services se convierte automáticamente en un administrador global.
Administrador de facturación	Asignar el rol de administrador de facturación a los usuarios que necesiten hacer lo siguiente: -Suscripciones y licencias de compra -Suscripciones de actualización -Pagar por servicios -Recibir notificaciones por correo electrónico para facturas -Administrar solicitudes de servicio -Supervisar el estado del servicio
Administrador del Departamento de soporte técnico	Asignar el rol de administrador del Departamento de soporte técnico a los usuarios que necesiten hacer lo siguiente: -Contraseñas de REST -Obligar a los usuarios a cerrar sesión -Administrar solicitudes de servicio -Supervisar el estado del servicio Nota: el administrador del Departamento de soporte solo puede ayudar a los usuarios que no son administradores y a los usuarios que tienen asignados estos roles: lector de directorios, invitado, administrador de soporte, lector del centro de mensajes y lector de informes.
Administrador de licencias	Asignar el rol de administrador de licencias a los usuarios que necesiten hacer lo siguiente: -Administrar las licencias asignadas a los usuarios -Administrar las licencias asignadas a grupos mediante licencias basadas en grupos. -Editar la ubicación de uso para los usuarios Nota: este rol no da permiso para comprar o administrar suscripciones, agregar o administrar grupos o editar propiedades de usuario, excepto para la ubicación de uso.
Lector de informes	Asignar el rol de lector de informes a los usuarios que necesiten hacer lo siguiente: - Ver los datos de uso y los informes de actividad - Obtener acceso al paquete de contenido de adopción de Power BI. -Ver los informes y la actividad de inicio de sesión -Ver datos devueltos por la API de informes de Microsoft Graph

Administrador del usuario

Asignar el rol de administrador de usuarios a los usuarios que necesiten hacer lo siguiente para todos los usuarios:

- Agregar usuarios y grupos
- Asignar licencias
- Administrar la mayoría de las propiedades de los usuarios
- Crear y administrar vistas de usuario
- Actualizar directivas de expiración de contraseñas
- Administrar solicitudes de servicio
- Supervisar el estado del servicio

El administrador del usuario también puede realizar las siguientes acciones para los usuarios que no son administradores y para los usuarios que tienen asignados los siguientes roles: lector de directorios, invitado, administrador de soporte, lector del centro de mensajes, lector de informes:

- Administrar nombres de usuario
- Eliminar y restaurar usuarios
- Restablecer contraseñas
- Obligar a los usuarios a cerrar sesión
- Actualizar las claves de dispositivo (FIDO)

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

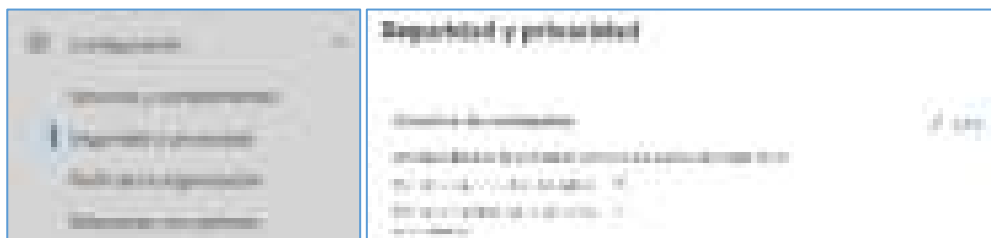
Desde *Azure AD* es posible crear roles personalizados. Se necesita *Azure AD Premium P1* o *P2*.

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].

3.1.1.5 Mecanismos de autenticación

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



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

- Días antes de que las contraseñas expiren

90

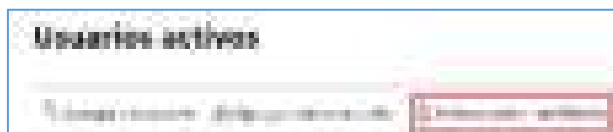
- Días antes de notificar a un usuario acerca de la caducidad 14

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

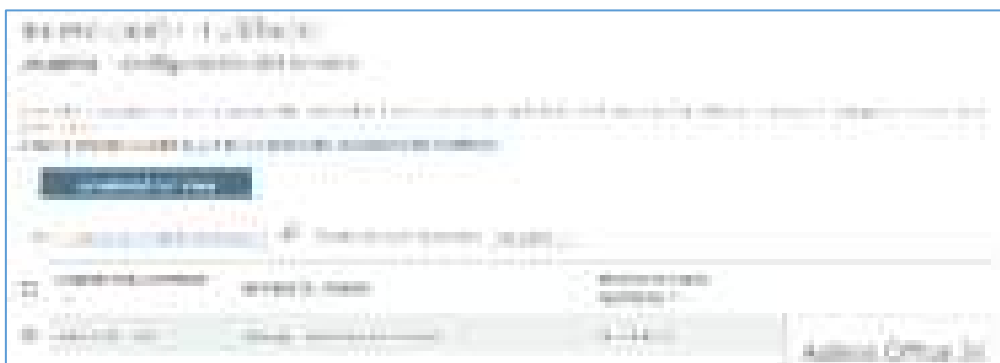
Activar la autenticación multifactor (MFA)

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:

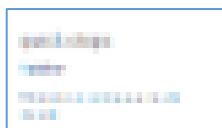
1. Acceder al menú [Usuarios\Usuarios Activos].
2. Pulsar el icono “Autenticación multifactor” de la barra superior.



3. Se accede a un nuevo panel de administración:



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



Nota: También es posible realizar una actualización en masa marcando varios usuarios a la vez.

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:

- 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.

- 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.

- 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.

- Mensaje de texto al teléfono.

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.

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

Powershell

Desde PS se pueden consultar y/o modificar tres parámetros relacionados con las contraseñas de los usuarios:

- *StrongPasswordRequired*: si requiere contraseña fuerte. Ver tabla más abajo.
- *PasswordNeverExpires*: si la contraseña nunca expira.
- *ForceChangePassword*: si se exige cambiar la contraseña en el siguiente inicio de sesión.

Listado de usuarios con información de complejidad y caducidad

```
# Get-MsolUser | ft -auto UserPrincipalName, StrongPasswordRequired,  
PasswordNeverExpires
```

Modificar parámetros de contraseñas

Se recomienda aplicar el siguiente comando:

```
# Set-MsolUser -UserPrincipalName "User Principal Name"  
-StrongPasswordRequired $true  
-PasswordNeverExpires $false
```

Nota: no se recomienda el uso del 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 *Azure Active Directory*, y los comandos para modificarlas:

Propiedad	Requerimiento de UPN (User Principal Name)
Caracteres permitidos	Mayúsculas: A-Z Minúsculas: a-z Números: 0-9 Caracteres especiales: @ # \$ % ^ & * _ ! + = [] { } \ : ' , . ? / ` ~ " () ;
Caracteres no permitidos en las contraseñas	Caracteres unicode Espacios
Restricciones de contraseñas	Mínimo de 8 caracteres y máximo de 16. Solamente para “ strong password ”: Usar 3 de los siguientes 4 grupos: Minúsculas Mayúsculas Números (0-9) Símbolos (mostrados anteriormente)
Expiración de la password	Valor por defecto: 90 días. El valor es configurable usando el <i>cmdlet</i> de Power Shell de AAD: <i>Set-MsolPasswordPolicy</i>
Notificación de caducidad de las contraseñas:	Valor por defecto: 14 días (antes de que la password expire). El valor es configurable usando el <i>cmdlet</i> de PowerShell de AAD: <i>Set-MsolPasswordPolicy</i>
Caducidad de contraseñas	Valor por defecto: false. El valor se puede configurar individualmente para cuentas de usuario usando el <i>cmdlet</i> : <i>Set-MsolUser</i>
Historial de contraseñas	La última contraseña no puede ser usada cuando el usuario actualiza la password.
Reseteo del historial de contraseñas	La última contraseña puede usarse nuevamente cuando el usuario la ha olvidado.

Bloqueo de cuenta	Después de 10 intentos con contraseñas erróneas, el usuario es bloqueado durante 1 minuto. Posterioros intentos infructuosos incrementan dicho tiempo de bloqueo.
--------------------------	---

3.1.1.6 Acceso local

Se requiere establecer un “doble factor de autenticación” (MFA) y tener una política adecuada de gestión de credenciales, que se describen en el apartado [3.1.1.5 Mecanismos de autenticación]. Así mismo, se requiere un registro de intentos de accesos con éxito y fallidos al sistema, descritos en el apartado [3.1.2.2 Registro de actividad] de la presente guía. Adicionalmente se puede controlar el acceso a Office 365 mediante directivas de acceso condicional o reglas en ADFS, como se describe en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.7 Acceso remoto

A destacar en este punto que Office 365 es una solución *cloud* accesible por el usuario final a través de internet. Se aplicará el cifrado de datos tal y como se describe en el apartado [3.2.3.2 Cifrado].

3.1.2 Explotación

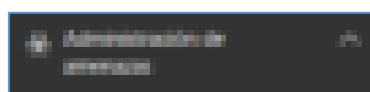
Office 365, al ser un software ofrecido como servicio (SaaS), **siempre estará actualizado**. Es decir, el servicio es mantenido permanentemente por **Microsoft**, encargándose de las actualizaciones y parches, así como de establecer los mecanismos de detección y protección ante amenazas, cumpliendo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



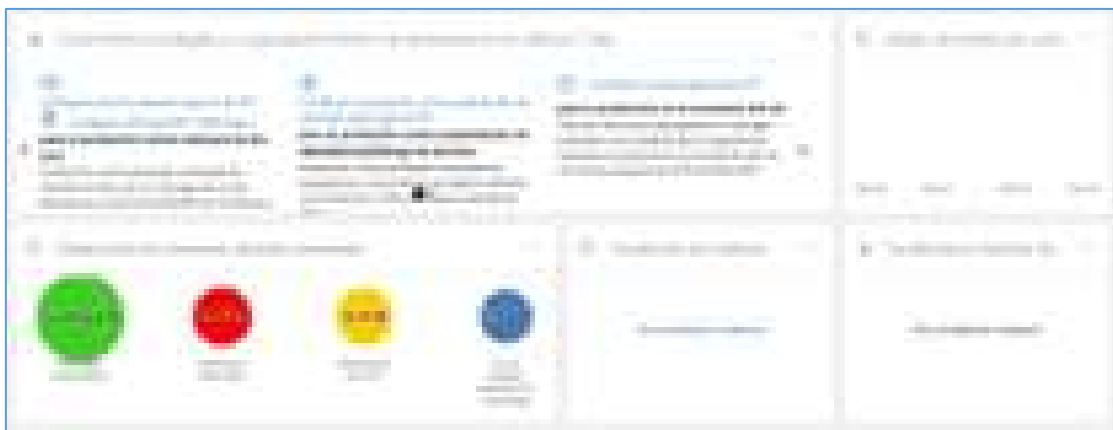
En esta sección se explicará el funcionamiento y las características del *Centro de Seguridad y cumplimiento de Office 365*, al que se accede desde el portal de *Administración*.

3.1.2.1 Protección frente a código dañino

Si la organización dispone de *Office 365 Advanced Threat Protection* (Office 365 ATP) tendrá un explorador de detecciones en tiempo real, accesible desde el *Centro de Seguridad y cumplimiento de Office 365*.



En el panel de [Administración de amenazas\Panel] se muestra el estado general:



En el explorador [Administración de amenazas\Explorador] se dispone de un informe detallado donde pueden realizarse las siguientes acciones:

- Ver *malware* detectado por las características de seguridad de Office 365.
- Ver datos sobre direcciones *url* de suplantación de identidad y hacer clic en veredicto.
- Iniciar un proceso de investigación y respuesta automatizado desde una vista en el explorador.
- Investigar el correo electrónico malintencionado, etc.

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

3.1.2.2 Registro de 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 y cumplimiento de Office 365*, la actividad de usuario y administrador de la organización se registra en el registro de auditoría y se conserva durante *90 días*.

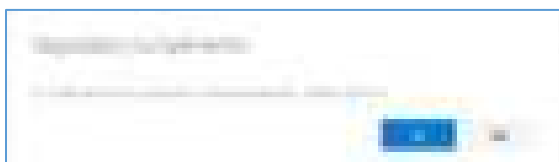
Activar/Desactivar registro de auditoría

Se debe tener asignado el **rol registros de auditoría** en Exchange Online 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.

1. Desde el *Centro de Seguridad y cumplimiento de Office 365* menú [Buscar\Búsqueda de registros de auditoría], pulsar el botón “Activar Auditoría”.



2. 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

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

Activar auditoría:

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

Desactivar auditoría:

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

Consultar registro de auditoría

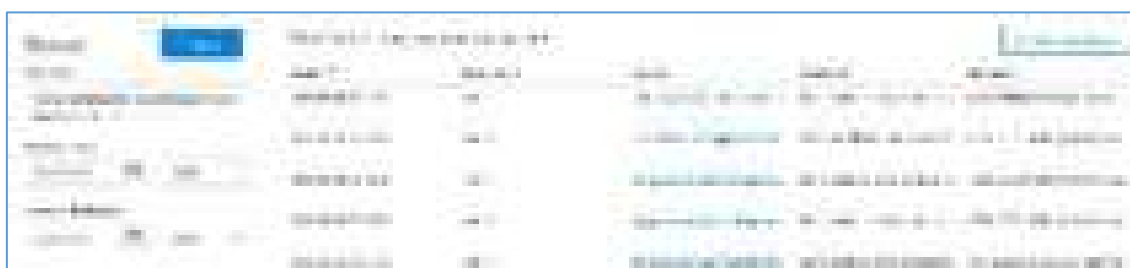
Permite buscar en el registro de auditoría lo que hacen los usuarios y administradores de la organización: actividades relacionadas con el correo electrónico, grupos, documentos, permisos, servicios de directorio y mucho más.



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

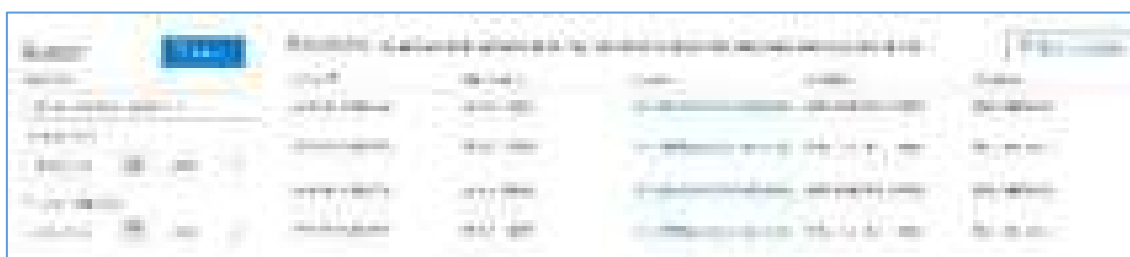
En el desplegable de *Actividades* se muestran todas las búsquedas posibles relacionadas con el registro de auditoría y clasificadas por temas.

Ejemplo de consulta relacionada con las *credenciales*:



Actividad	Fecha	Tipo de registro	Resultado
Agregar credencial	2023-01-01 10:00:00	Evento de auditoría	Se agregó la credencial con éxito.
Eliminar credencial	2023-01-01 10:05:00	Evento de auditoría	Se eliminó la credencial con éxito.
Actualizar credencial	2023-01-01 10:10:00	Evento de auditoría	Se actualizó la credencial con éxito.

Ejemplo de consulta relacionada con el *acceso a ficheros*:



Actividad	Fecha	Tipo de registro	Resultado
Acceso a archivo	2023-01-01 10:00:00	Evento de auditoría	Se accedió al archivo con éxito.
Descarga de archivo	2023-01-01 10:05:00	Evento de auditoría	Se descargó el archivo con éxito.
Carga de archivo	2023-01-01 10:10:00	Evento de auditoría	Se cargó el archivo con éxito.

API de Actividad de administración de Office 365

A parte del *Centro de Seguridad y cumplimiento de 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 Azure AD.

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. Para mayor información, consultar la documentación siguiente de Microsoft:

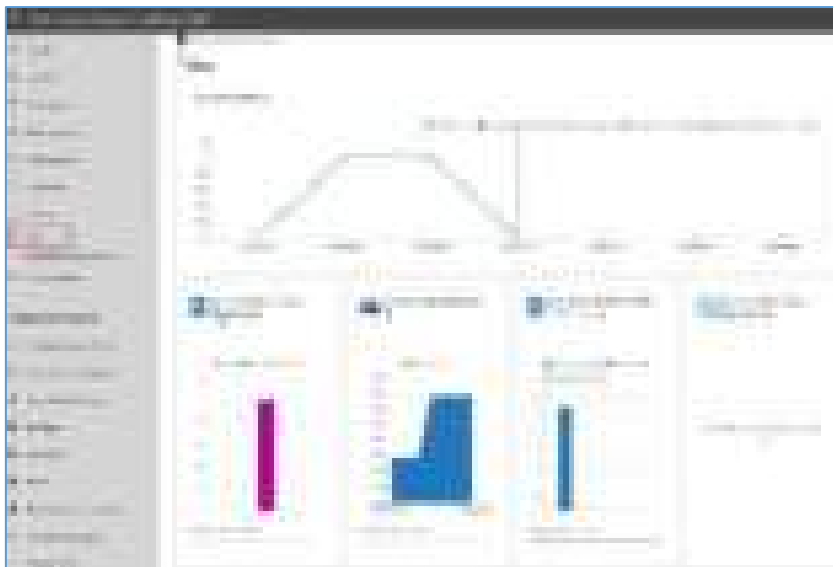
url: docs.microsoft.com/es-es/office365/securitycompliance/office-365-management-activity-api

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).



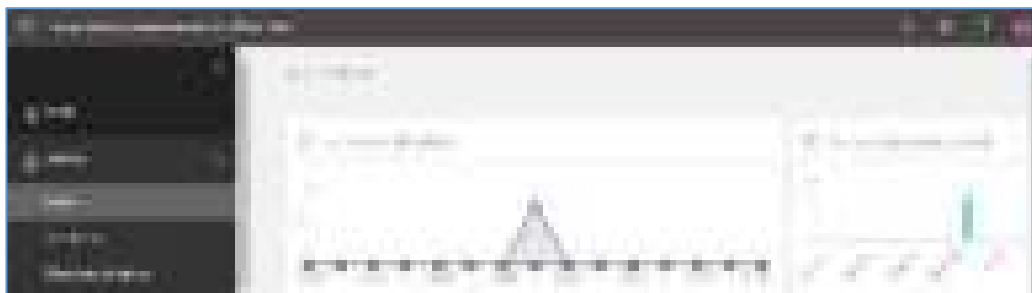
3.1.2.3 Gestión de incidentes

Ver apartado [3.1.2.1 Protección frente a código dañino] donde se explica cómo acceder a los informes de “Administración de Amenazas”.

Otros informes relevantes relacionados con la gestión de incidentes y accesibles desde el *Centro de Seguridad y Cumplimiento de Office 365* son:

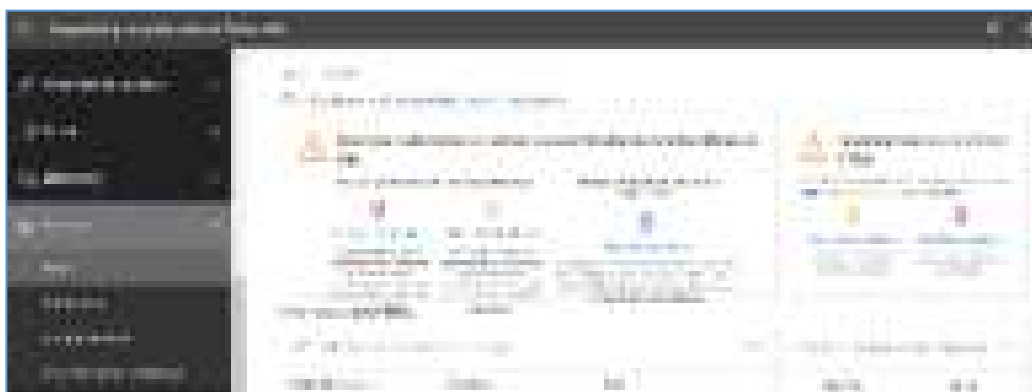
- Panel de alertas. Menú [Alertas\Panel].

<https://protection.office.com/alertsdashboard>



- Panel de informes. Menú [Informes\Panel].

<https://protection.office.com/insightdashboard>



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

<https://protection.office.com/ReportsForDownload>



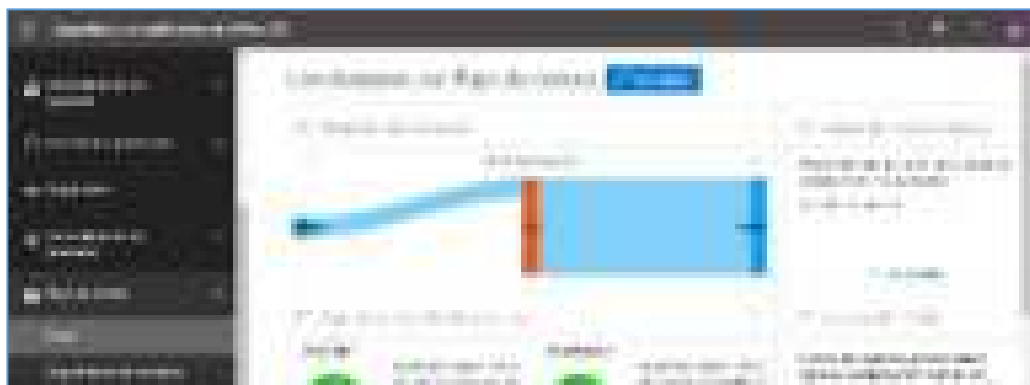
- Búsqueda e investigación. *Widget* del panel principal.

<https://protection.office.com/searchandinvestigation/dashboard>



- Panel de Flujo de correo. Menú [Flujo de correo\Panel].

<https://protection.office.com/mailflow/dashboard>



3.1.2.4 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 Skype Empresarial.
- Lector de informes.

Cuando un usuario o administrador realiza una actividad auditada, se genera un registro de auditoría y se almacena en el registro de auditoría de Office 365 de la organización. **La cantidad de tiempo que se retiene un registro de auditoría**, y que por tanto puede aparecer en las búsquedas, depende de la suscripción a Office 365 y, específicamente, del tipo de licencia que se ha asignado a un usuario específico.

Office 365 E3: Los registros de auditoría se conservan durante **90 días**. Eso significa que puede buscar el registro de auditoría para las actividades que se han realizado en los últimos 90 días.

Office 365 E5: Los registros de auditoría también se conservan durante 90 días.

Nota: A fecha de edición de esta guía Microsoft está trabajando en ampliar el período de retención a 1 año para usuarios con licencia E5 o E3 con la licencia complementaria “Cumplimiento Avanzado de Office 365”.

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.

En realidad, todas las comunicaciones de Office 365 están cifradas: Clientes de correo (POP, IMAP, SMTP-TLS), Clientes Outlook (MAPI-HTTPS), Navegadores (Web HTTPS), Dispositivos móviles (ActiveSync HTTPS), Teams y Skype (SIP-TLS). No es necesario realizar ninguna configuración adicional, pero es importante indicar que, a partir de junio 2020, se eliminará soporte de TLS 1.0 y 1.1. Esto tiene implicaciones directas en los clientes.

Ver: <https://docs.microsoft.com/en-us/office365/troubleshoot/security/prepare-tls-1.2-in-office-365>.

3.2.2 Monitorización del sistema

Es posible definir **alertas** en Office 365 a través del *Centro de Seguridad y cumplimiento de Office 365*, menú [Alertas].

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 cumple las condiciones de una directiva de alerta.



1. Un administrador crea, configura y activa una directiva de alerta mediante la página directivas de alerta en el *Centro de Seguridad y cumplimiento de Office 365*. También puede crear directivas de alerta con el cmdlet **New-ProtectionAlert**.
2. 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 que se envían a los usuarios de su organización activan una alerta.
3. Office 365 genera una alerta que se muestra en el menú [Alertas\Ver alertas] del *Centro de Seguridad y cumplimiento de Office 365*. Además, si las notificaciones de correo electrónico están habilitadas para la Directiva de alertas, Office 365 envía una notificación a una lista de destinatarios. Las alertas que un administrador u otros usuarios pueden ver que en la página ver alertas está determinada por los roles asignados al usuario.
4. Un administrador administra alertas en el *Centro de Seguridad y cumplimiento de Office 365*. La administración de alertas consiste en asignar un estado de alerta para ayudar a realizar un seguimiento y administrar cualquier investigación.

Creación de una directiva de alerta

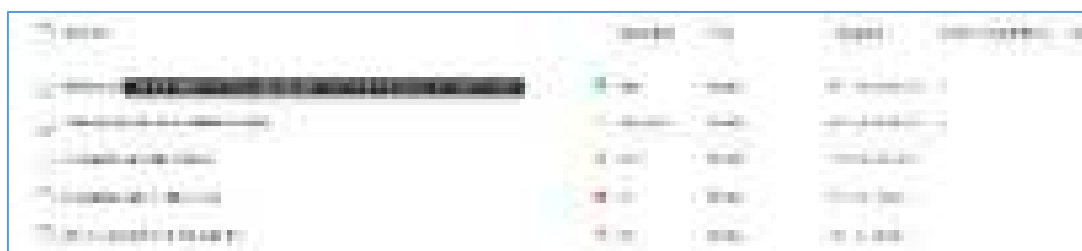
Con las directivas de alerta es posible realizar el seguimiento de las actividades de administradores y usuarios, amenazas de malware o incidentes de pérdida de datos en la organización. Después de elegir la actividad sobre la que se requiere el aviso, se puede afinar la directiva agregando condiciones,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

1. Acceder al menú [Alertas\Directivas de alerta] desde el *Centro de Seguridad y cumplimiento de Office 365*.



2. 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.



3. Pulsar sobre una directiva concreta para acceder a sus propiedades.



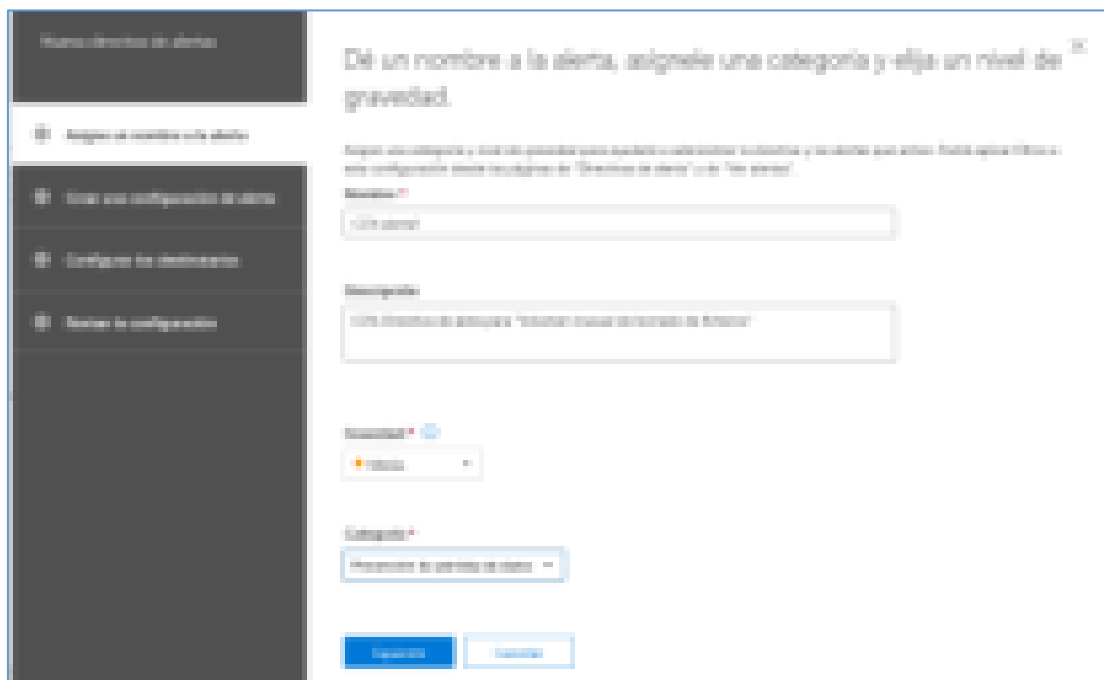
Por ejemplo la directiva “Unusual volume of file deletion” la cual se activa cuando se detecta que un usuario ha borrado un número inusual de ficheros.

Más información de las alertas predeterminadas en la documentación de Microsoft.

<https://docs.microsoft.com/es-es/office365/securitycompliance/alert-policies>

Para crear una **directiva de alerta personalizada** pulsar el botón “Nueva directiva de alerta”, en el menú [Alertas\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).

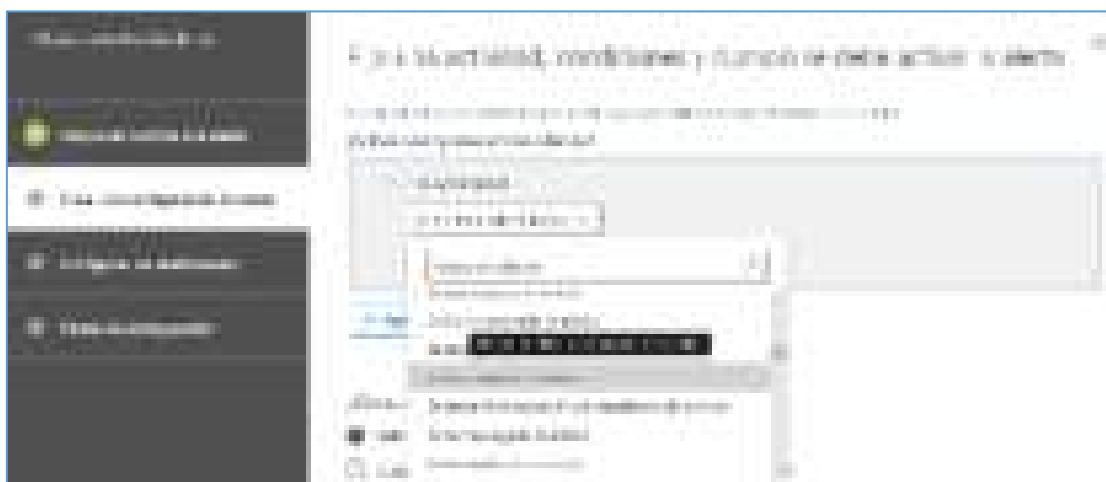
1. Asignar un nombre.



2. Crear configuración de alerta.

¿Sobre qué se quiere enviar alertas?

Seleccionar una **actividad**:



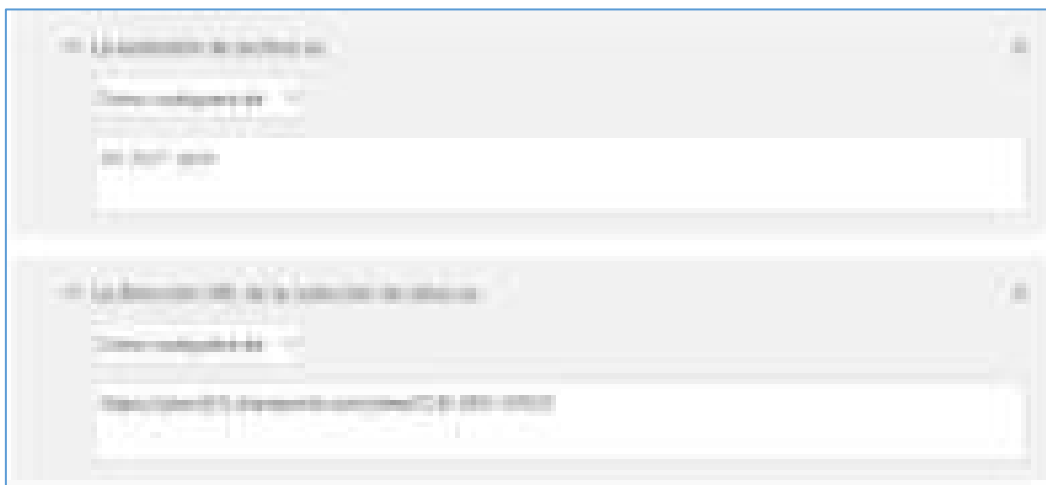
Agregar **condiciones**:

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

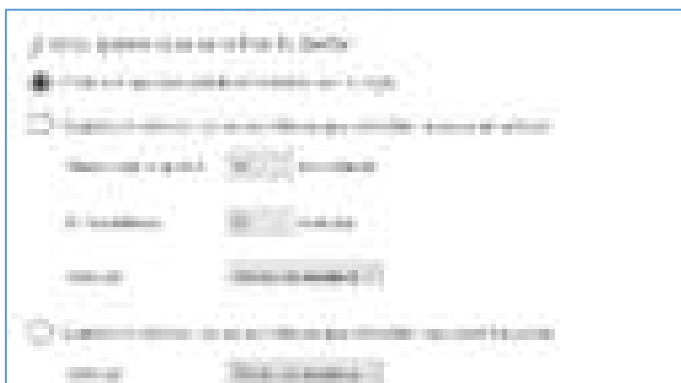
realiza la actividad en un equipo con una dirección IP específica o dentro de un intervalo de direcciones IP), usuarios concretos, nombres de archivos, urls de sitios o extensiones de archivos.



En el ejemplo:



¿Cómo quiere que se active la alerta?

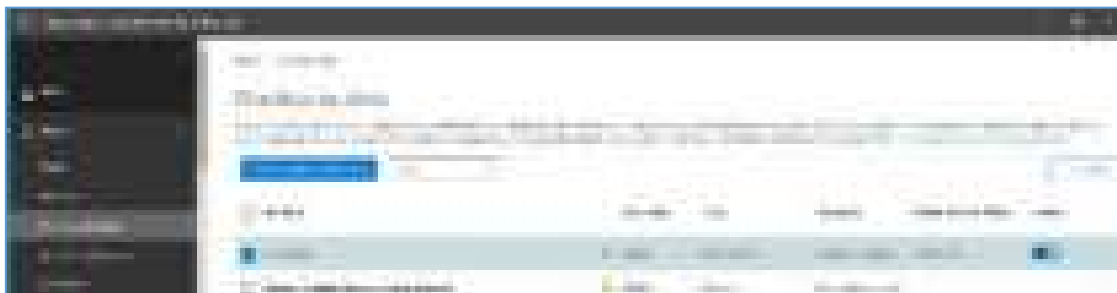


3. Configurar los destinatarios



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 y cumplimiento de Office 365*.



3.2.3 Protección de la información

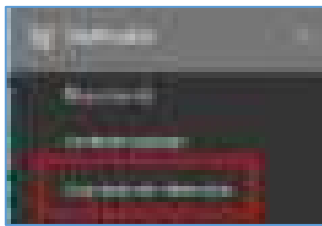
3.2.3.1 Calificación de la información

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

- **Políticas de retención** que puede aplicarse sobre el *tenant*. Para determinar qué hacer con la información una vez cumplido un período de tiempo determinado.
- **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.

3.2.3.1.1 Políticas de retención

Definición de etiquetas de retención



Estas etiquetas se definen en el *Centro de Seguridad y cumplimiento de Office 365*, en el menú [Clasificación\Etiquetas de retención], 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 *Centro de Seguridad y cumplimiento de Office 365*, y los usuarios también pueden aplicar estas etiquetas directamente en las aplicaciones Office, así como en SharePoint o OneDrive.

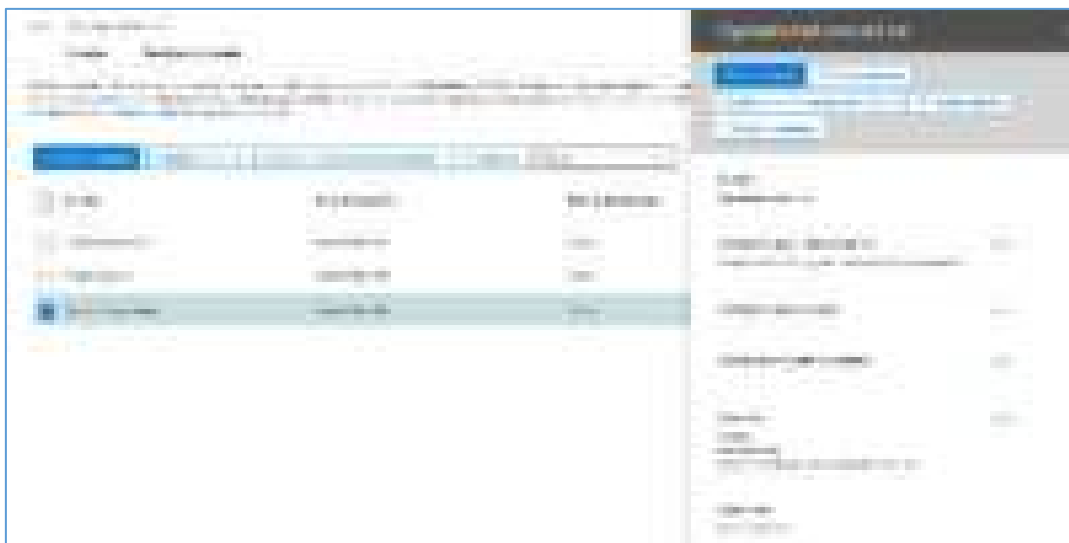
Las **etiquetas de retención** tienen que ver con el cumplimiento, y se aplican a correos o documentos en una ubicación determinada.

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

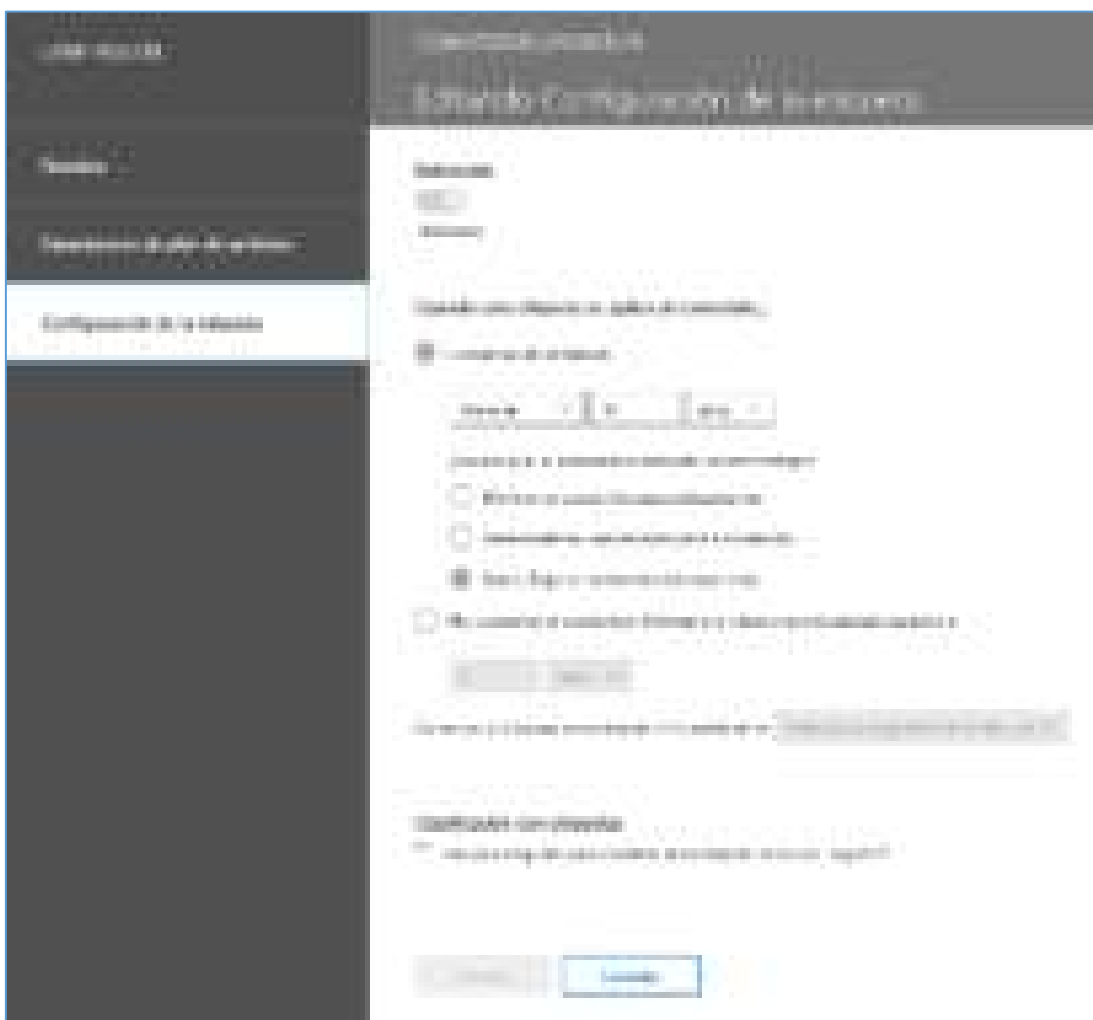
- Presupuestos: retención de 5 años después de la fecha límite del presupuesto.
- Contratos: retención de 10 años después de la fecha de finalización del contrato.
- Hojas de producto: declarado como registro (no borrar).

Consulta y modificación de etiquetas de retención

1. Acceder al menú [Clasificación\Etiquetas de retención].
2. Seleccionar una etiqueta.

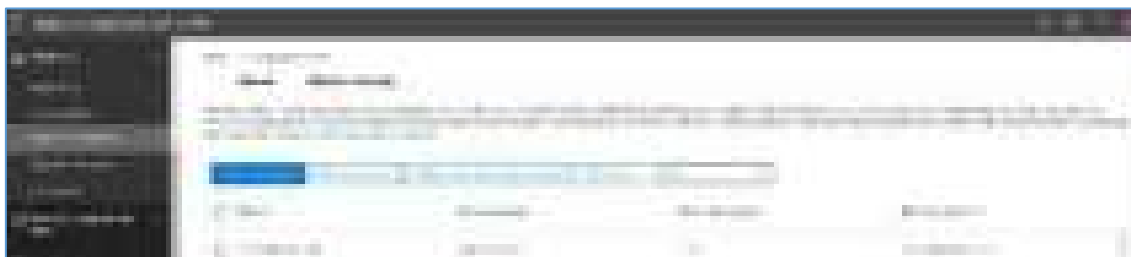


3. Editar etiqueta. En el panel derecho pulsar el botón “Editar etiqueta”.



Creación de una etiqueta de retención

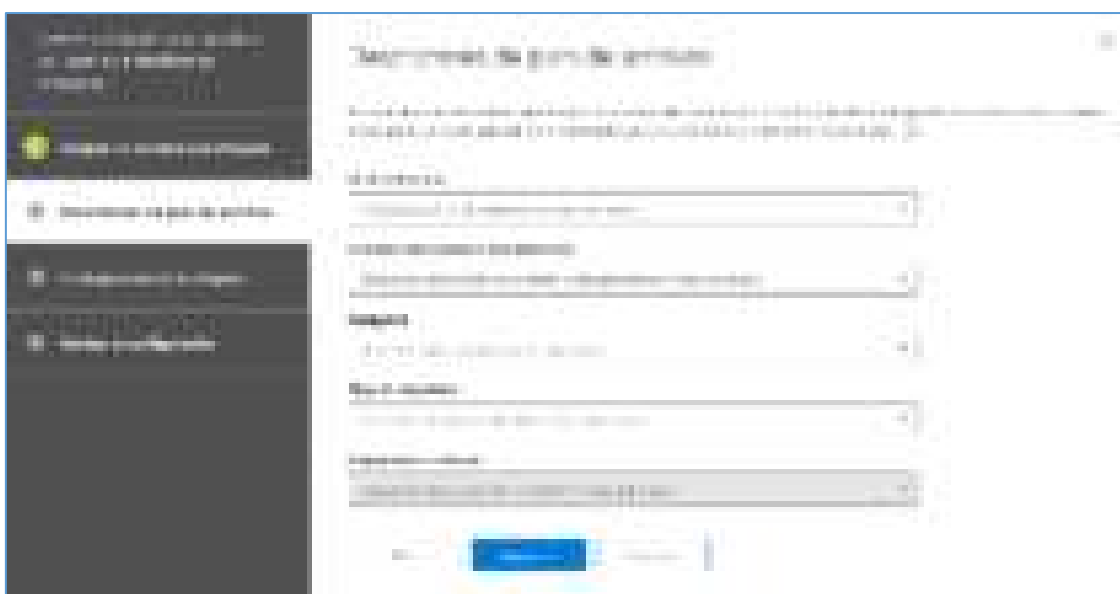
1. Acceder al menú [Clasificación\Etiquetas de retención].



2. Pulsar el botón “Crear una etiqueta”.
3. Asignar nombre a la etiqueta.



4. Para aplicación automática y cumplimiento regulatorio.

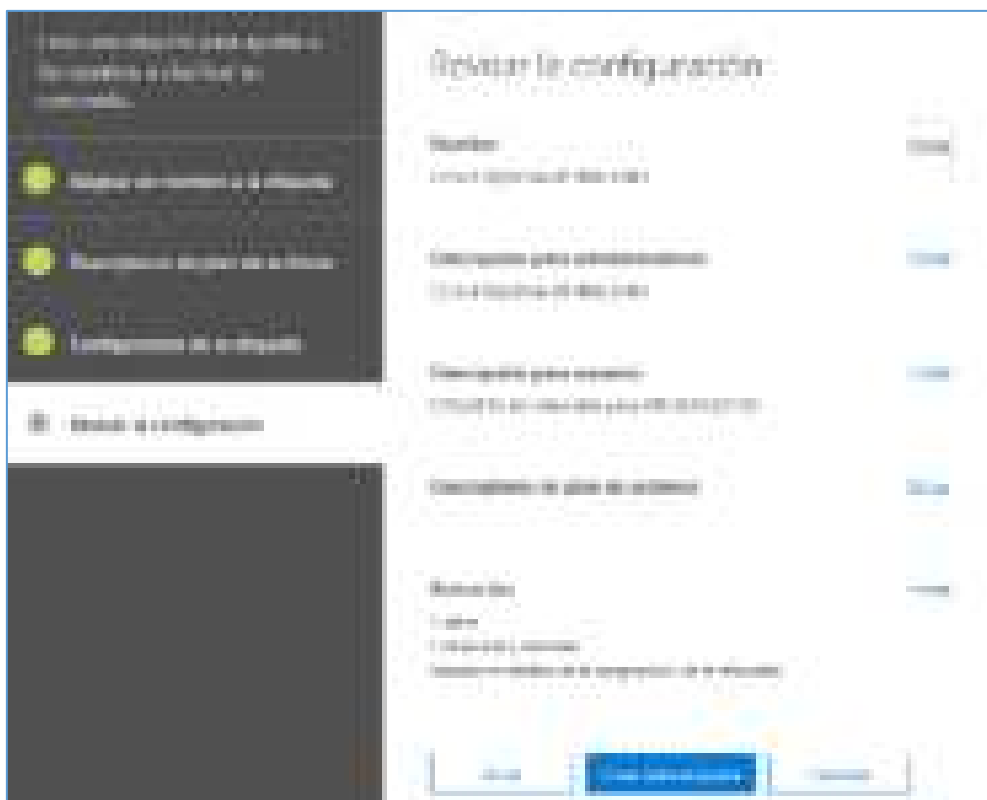


Pulsar “Siguiente”.

5. Configurar la etiqueta.

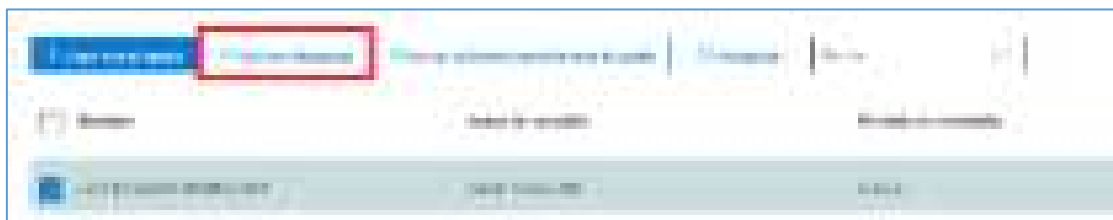


6. Revisar y Crear.

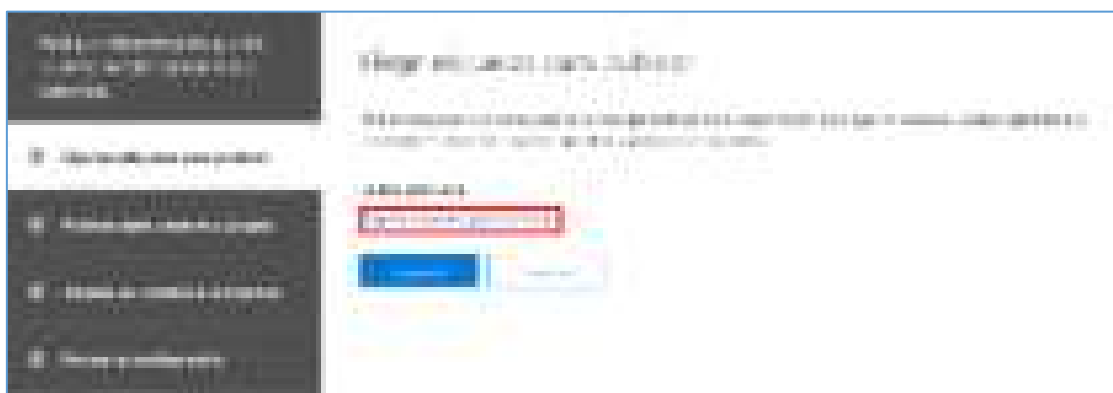


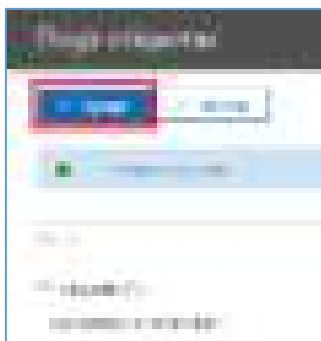
Publicar etiquetas

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



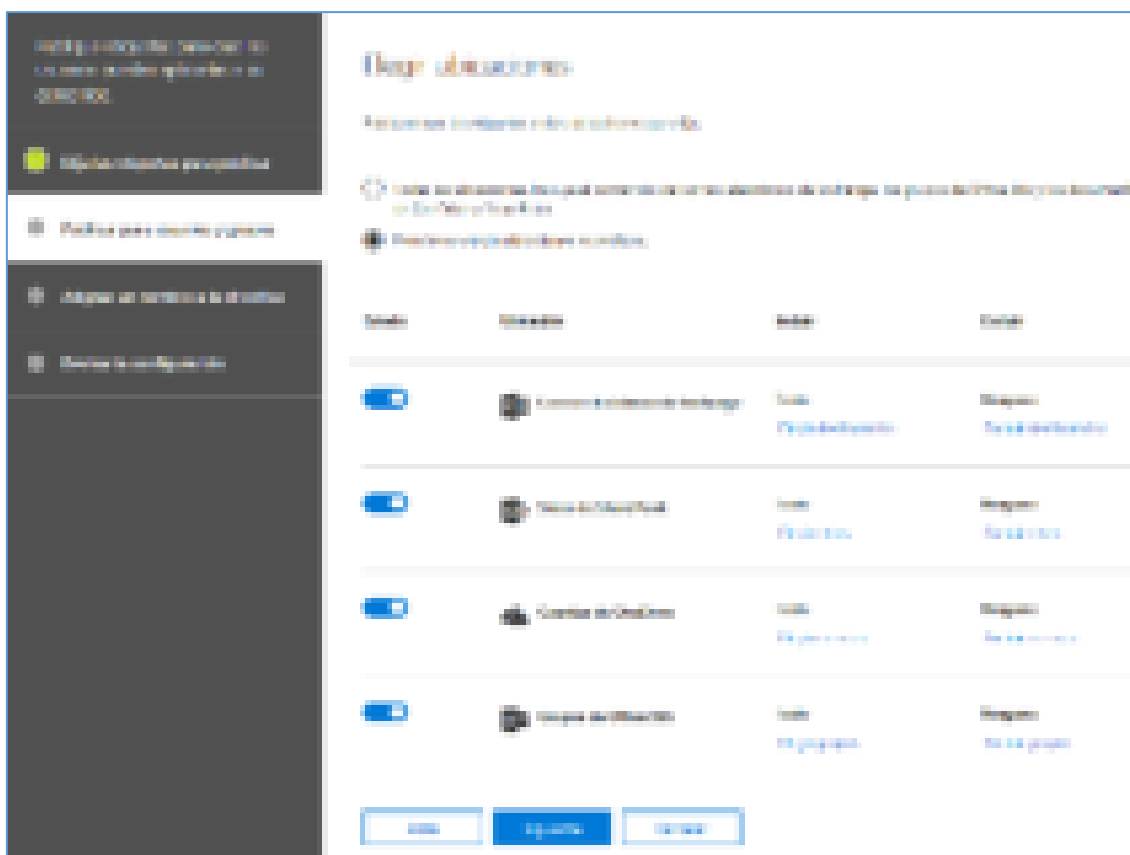
1. Elegir las etiquetas.





2. Elegir ubicaciones.

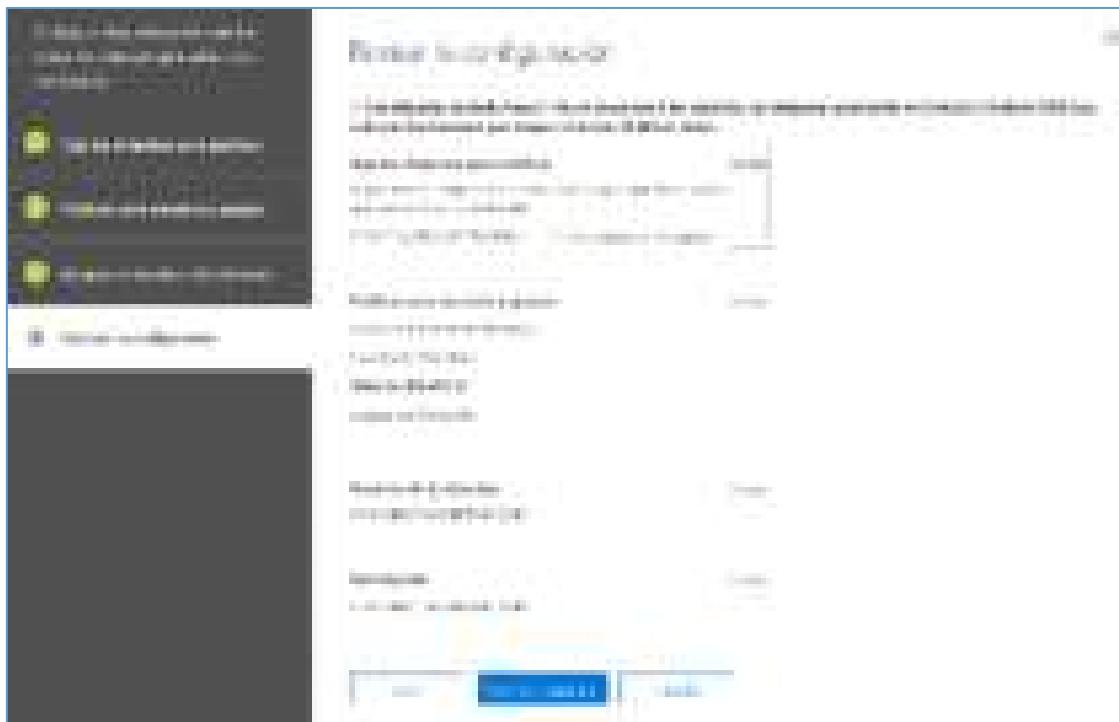
- Hay que tener en cuenta que, en **Exchange**, las etiquetas de retención de aplicación automática (tanto para consultas como para tipos de información sensible) **solo se aplican en los nuevos mensajes enviados** (datos en tránsito), no en todos los elementos que ya están presentes en el buzón (datos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



3. Dar un nombre a la directiva.

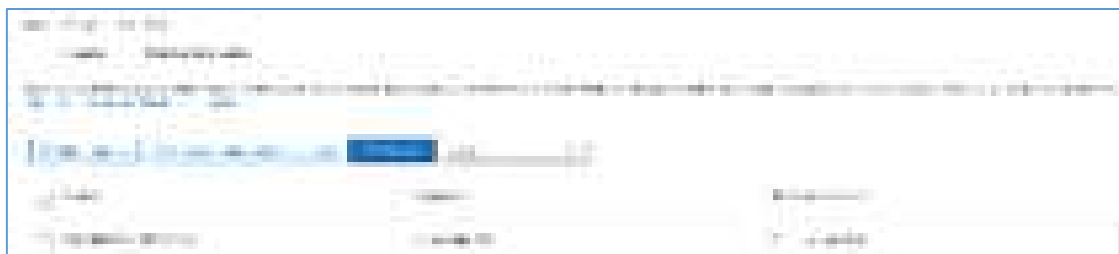


4. Revisar y Publicar.



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:



Uso de las políticas 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].

3.2.3.1.2 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.
- *Cuando 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.

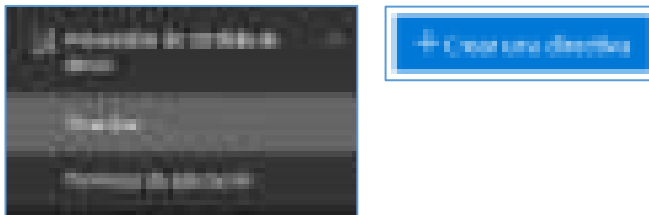
Puede educar a sus usuarios acerca de las directivas DLP y ayudar a que sigan manteniendo el cumplimiento normativo sin bloquear su trabajo. Por ejemplo, si un usuario intenta compartir un documento que contiene información sensible, una directiva DLP puede enviarle una notificación por correo electrónico 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

1. Desde el *Centro de Seguridad y cumplimiento de Office 365* en el menú [Prevención de pérdida de datos\Directiva], pulsar el botón “Crear una directiva”.

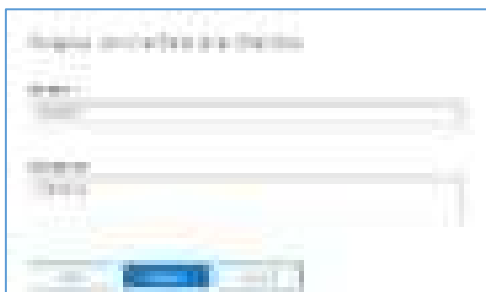


2. Elegir reglamento del sector o crear una política *a medida*.

Seleccionar la opción *Custom policy* para crear una directiva personalizada:



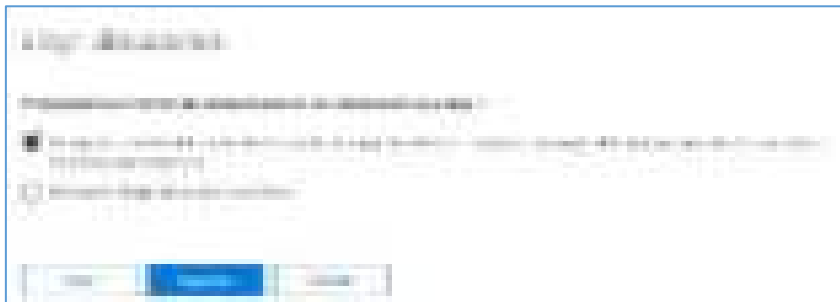
3. Asignar nombre y descripción.



4. 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.

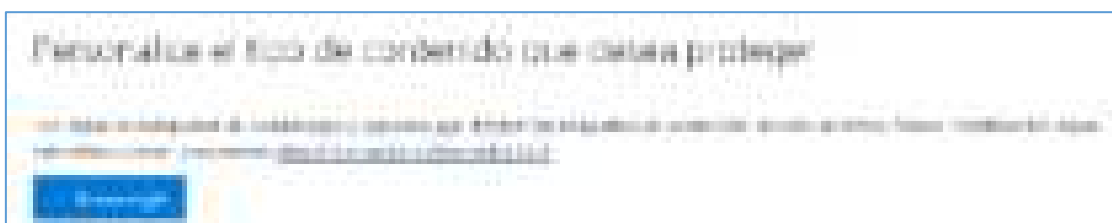


O seleccionar ubicaciones específicas:



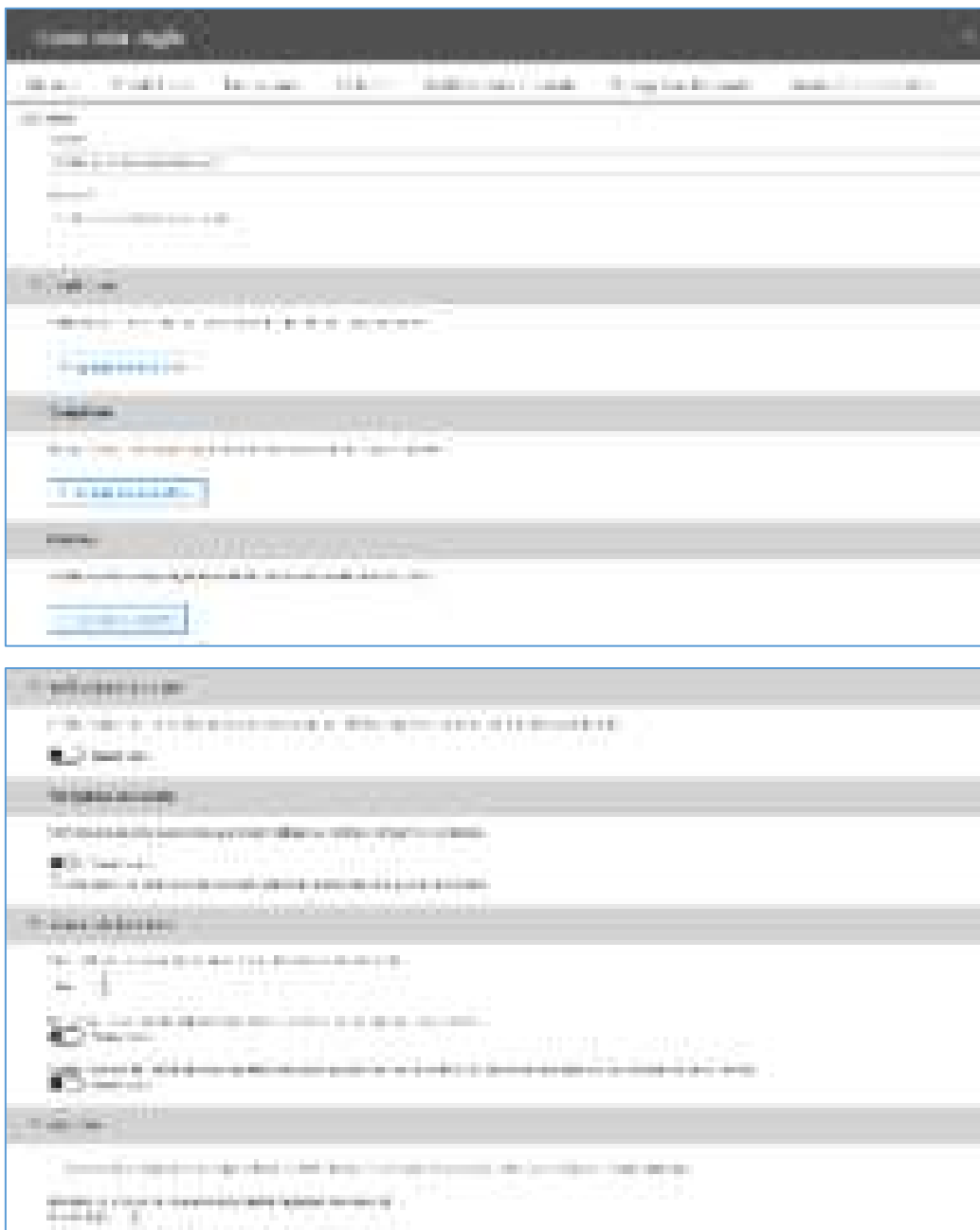
Si se elige incluir o excluir sitios de SharePoint o cuentas de OneDrive específicos, una directiva DLP no puede contener más de 100 inclusiones y exclusiones. Aunque este límite exista, se puede superar este límite aplicando una directiva para toda la organización o una directiva que se aplique ubicaciones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

5. Definir 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.



a. 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.

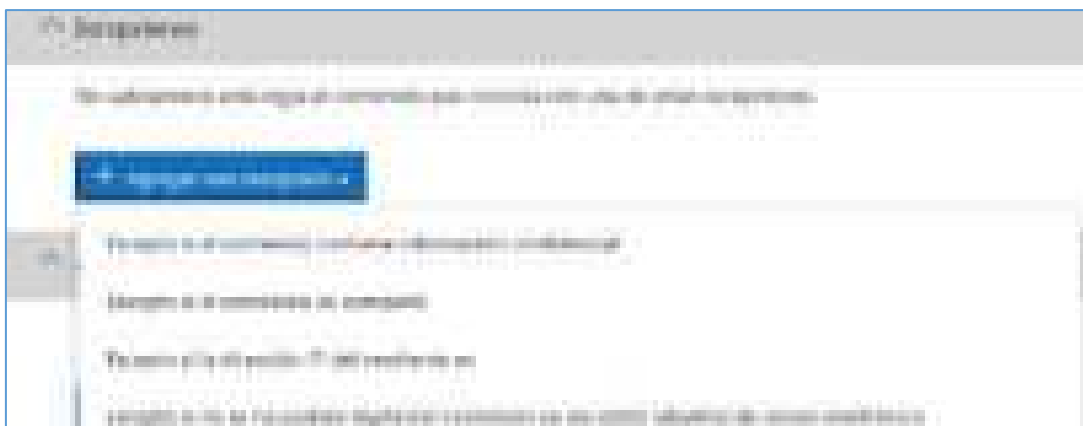


Las condiciones disponibles ahora pueden determinar si:

- El contenido incluye un tipo de información sensible.
- El contenido incluye una **etiqueta**.
- El contenido **se comparte** con personas de fuera o dentro de la organización.

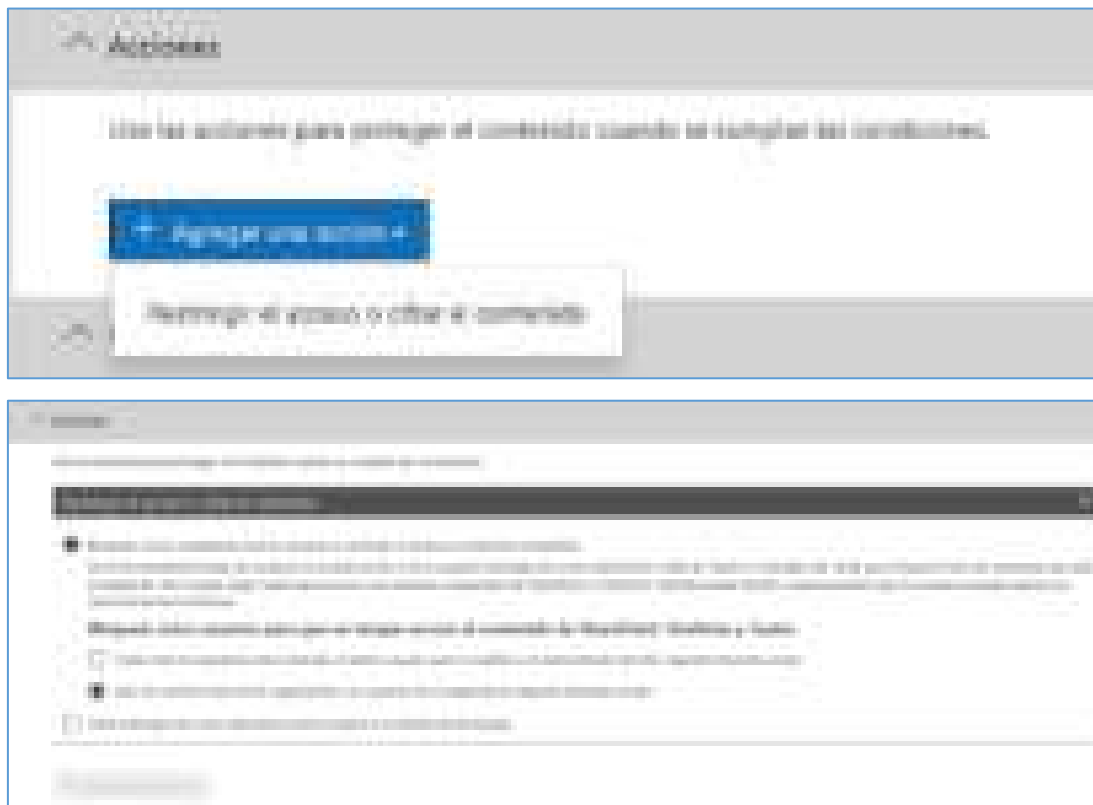
Una directiva DLP puede ayudar a proteger información sensible, lo que se define como un **tipo de información sensible**. Office 365 incluye definiciones para muchos tipos comunes de información sensible en muchas regiones diferentes que están listas para su uso, como números de tarjeta de crédito,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

b. Excepciones



c. Acciones

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



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

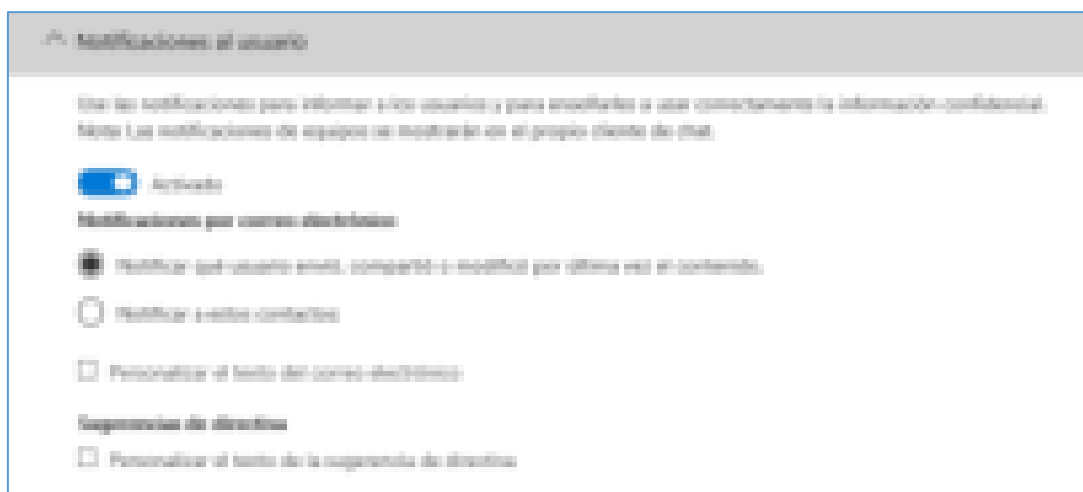
De forma predeterminada, los usuarios no podrán enviar a otros usuarios mensajes de correo electrónico, chats de Teams ni mensajes del canal que incluyan el tipo de contenido que está protegiendo. Pero se puede elegir quién tiene acceso a los archivos compartidos de SharePoint y OneDrive. También decidir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

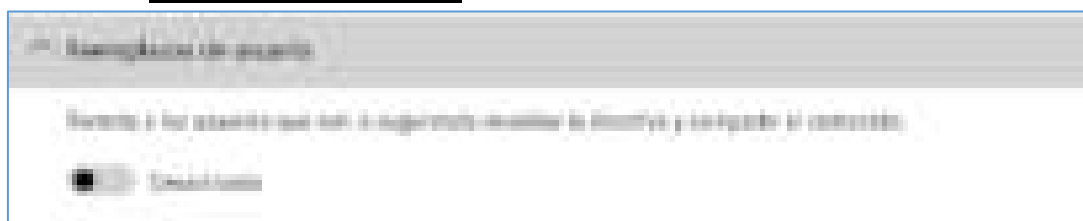
- Todos. Solo el propietario del contenido, el último usuario que lo modificó y el administrador del sitio seguirán teniendo acceso
 - Solo los usuarios fuera de la organización. Los usuarios de la organización seguirán teniendo acceso.
- Cifrar mensajes de correo electrónico (solo se aplica a contenido de Exchange).

a. 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.

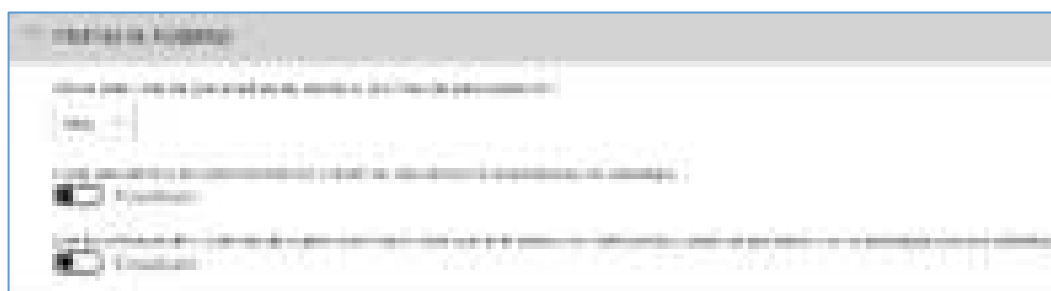


b. Reemplazos de usuarios



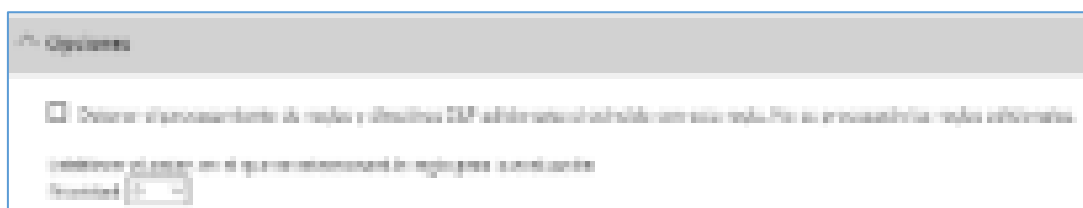
c. Informes de incidentes

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.

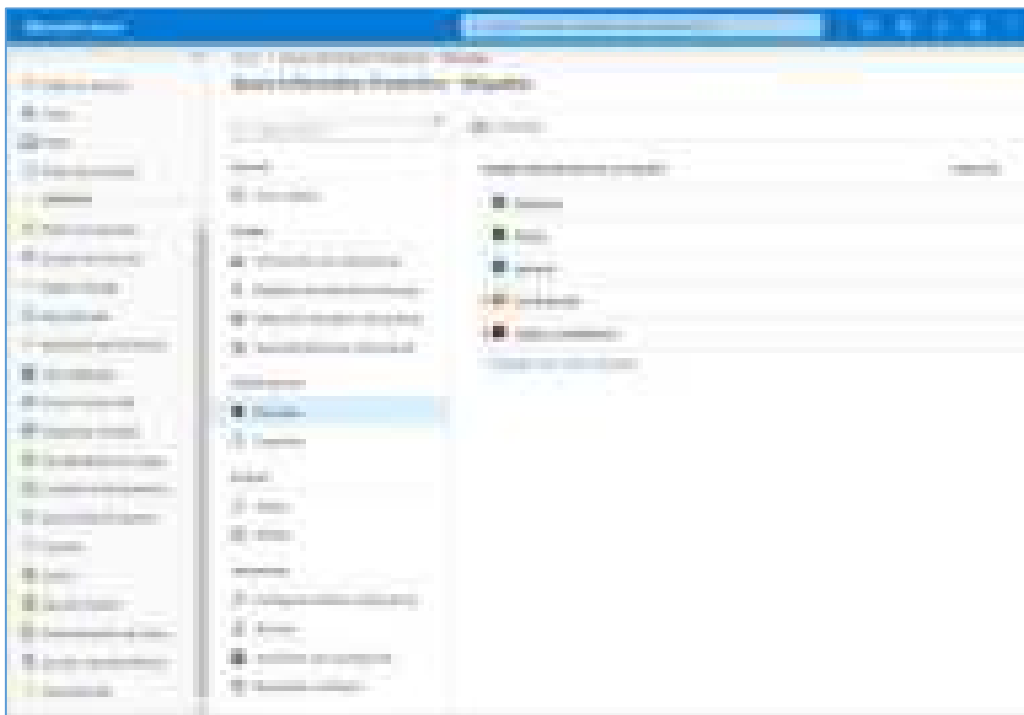
d. Opciones



3.2.3.1.3 Azure Information Protection

Azure Information Protection, también conocido como AIP, es una solución basada en la nube que permite a las organizaciones clasificar y, opcionalmente, proteger sus documentos y correos electrónicos mediante la aplicación de **etiquetas**. Las etiquetas las pueden aplicar automáticamente los administradores, quienes definen reglas y condiciones, los usuarios manualmente, o bien una combinación en la que los usuarios reciben recomendaciones.

Se configura en el portal de Azure.



Se necesita instalar un cliente en cada equipo para incluir la funcionalidad en las aplicaciones de escritorio como word y excel. Aparecerá un nuevo icono: *Protect*.



Office 365

cuenta, además, con una solución similar llamada **Office 365 Sensitivity labels**, accesible desde el Centro de Seguridad y Cumplimiento. Se recomienda usar esta segunda opción que se gestiona desde el propio portal del *Centro de Seguridad y Cumplimiento* y no desde el portal de Azure, y parece ser la evolución natural de las anteriores. En la fecha de edición de esta guía ambas opciones son válidas.

3.2.3.1.4 Office 365 Sensitivity labels (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 *Centro de Seguridad y cumplimiento de Office 365*, menú [Clasificación\Etiquetas de confidencialidad].



- 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.

1. Desde el *Centro de Seguridad y cumplimiento de Office 365*, menú [Clasificación\Etiquetas de confidencialidad]. Pulsar el botón: **“Crear una etiqueta”**.



2. **Asignar un nombre a la etiqueta.**

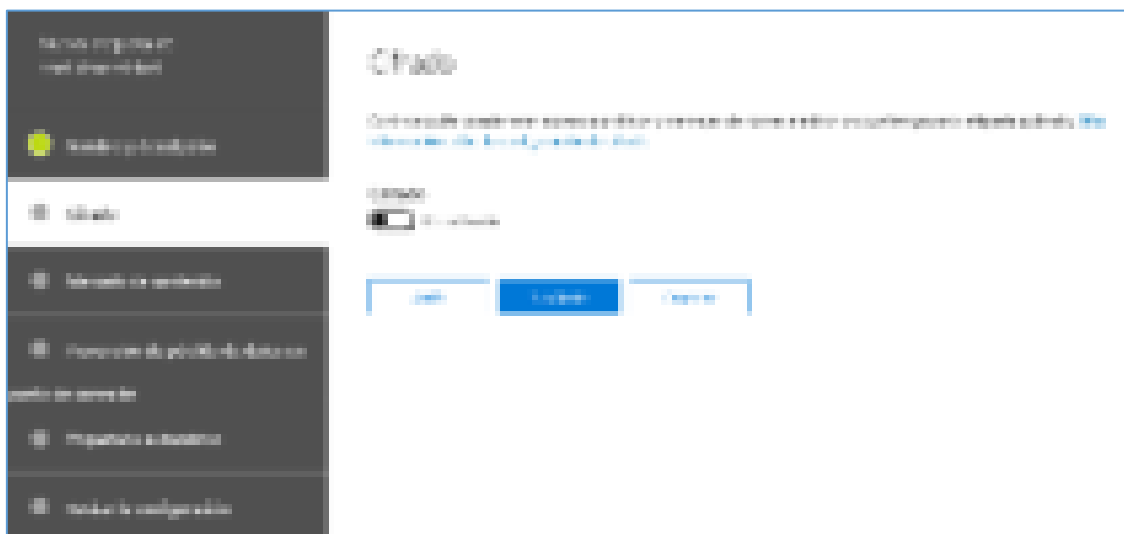


3. **Cifrado.**

Cuando se encripta un documento o correo electrónico, el acceso al contenido está restringido, por lo que:

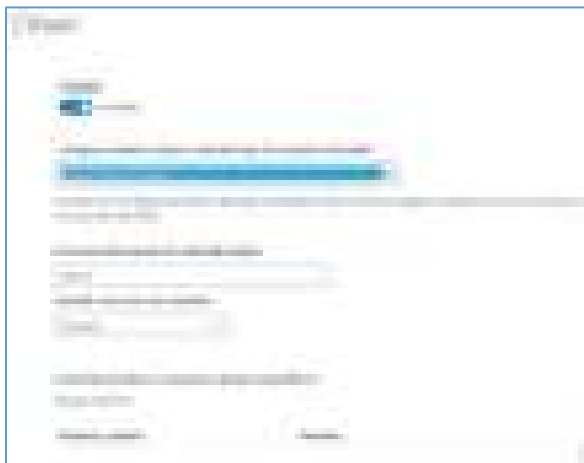
- Se puede desencriptar solo por los usuarios autorizados por la configuración de encriptado de la etiqueta.
- Permanece encriptado independientemente de dónde resida, dentro o fuera de la organización, incluso si cambia el nombre del archivo.
- Se encripta tanto en reposo (por ejemplo, en una cuenta de OneDrive o Sharepoint) como en tránsito (por ejemplo, un correo electrónico enviado).

Activar o desactivar el control en función del grado de sensibilidad del documento.



Si activamos el cifrado se despliegan nuevas opciones, en función de si se asignan los permisos en este momento o se postergan cuando los usuarios apliquen las etiquetas:

3.1. *Asignar permisos ahora.*

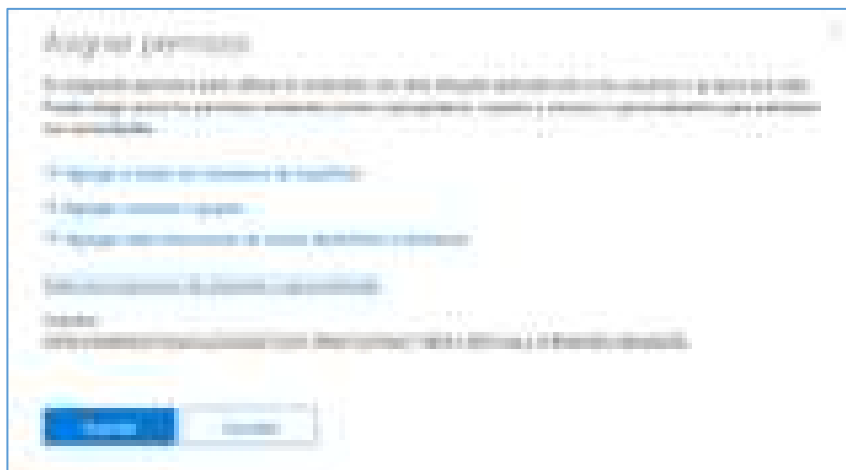


- Determinar si el acceso del usuario al **contenido expira** o establecer un límite.

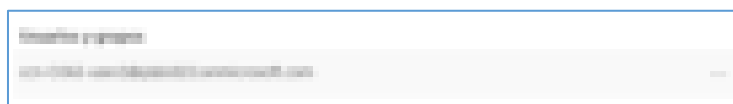
- Establecer el siguiente parámetro a "Nunca", para evitar **accesos sin conexión**:



- Pulsar sobre "Asignar permisos".



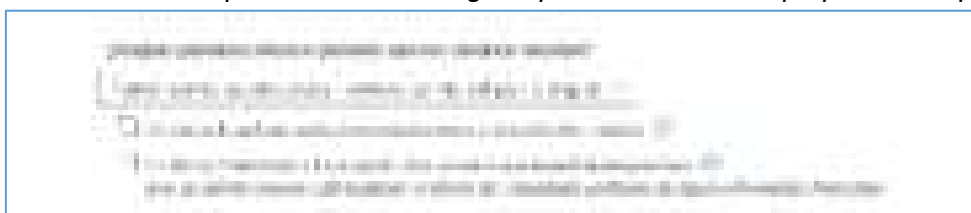
- Se asignarán permisos para utilizar el contenido con esta etiqueta aplicada solo a los usuarios o grupos que se elija.



- Se puede elegir entre los permisos existentes (como copropietario, coautor y revisor) o personalizarlos.



3.2. Permitir que los usuarios asignen permisos cuando apliquen la etiqueta.



Ejemplo: Se ha configurado el cifrado para que se asignen permisos de “Visualizador” a toda la organización, que el acceso al contenido caduque después de 30 días y que no se permita acceso sin conexión.



4. Marcado de contenido.



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

5. Prevención de pérdida de datos en punto de conexión.



Dejar opción por defecto. La configuración de DLP para las aplicaciones de Office 365 aún no están disponibles a la fecha de edición de esta guía.

6. Etiquetado automático.



El etiquetado automático solo se admite en las aplicaciones de Office cuando está instalado el *cliente de etiquetado unificado de Azure Information Protection*.

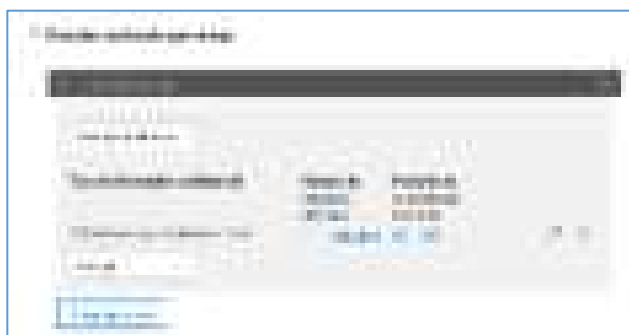
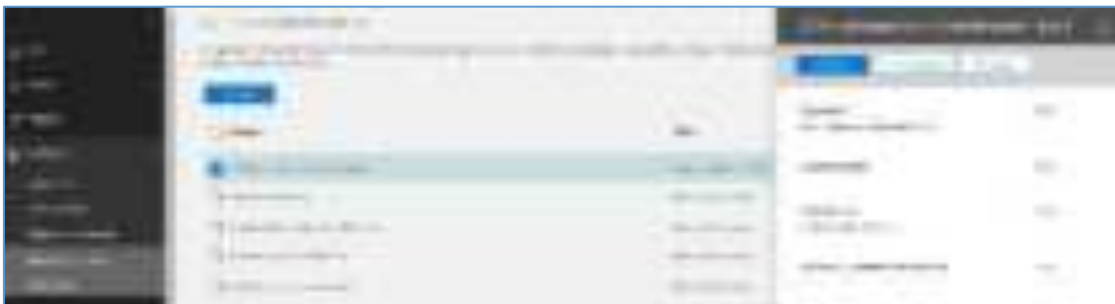
Cuando se detecte contenido sensible en el correo electrónico o en los documentos que cumplan las condiciones que se elija, se puede aplicar automáticamente esta etiqueta o mostrar un mensaje a los usuarios que les recomiende que la apliquen ellos mismos.

Si se activa el etiquetado automático:



En “Detectar contenido que incluya”, agregaremos *Tipos de información confidencial* que se definen en el menú [Clasificación\Tipos de información confidencial]. Existen muchos tipos definidos: tarjetas de crédito, números de pasaporte, etc. o pueden crearse tipos personalizados.

Por ejemplo, se creará el tipo CCN-Information-Confidencial-Tipo1, que busca coincidencias de las palabras clave: *confidencial* y *top secret*.



Y asignamos este tipo a la *sensitivity labels*.

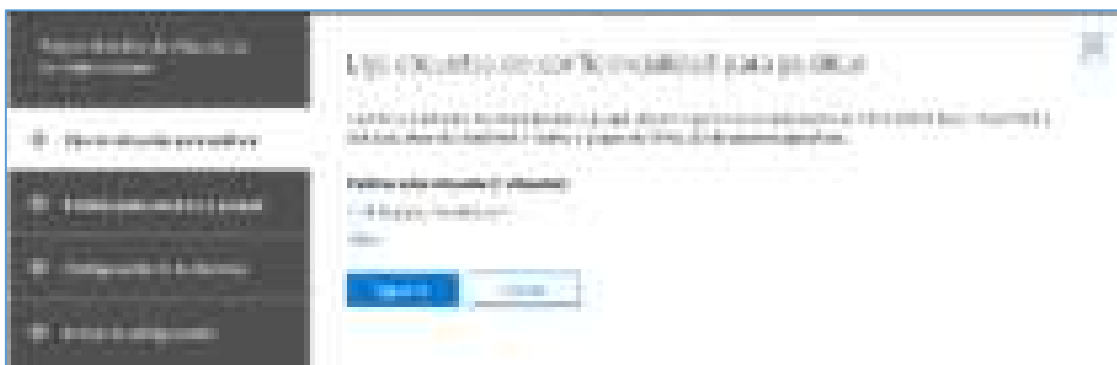
Publicar *sensitivity labels*

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.

1. Pulsar el botón “Publicar etiqueta”.



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

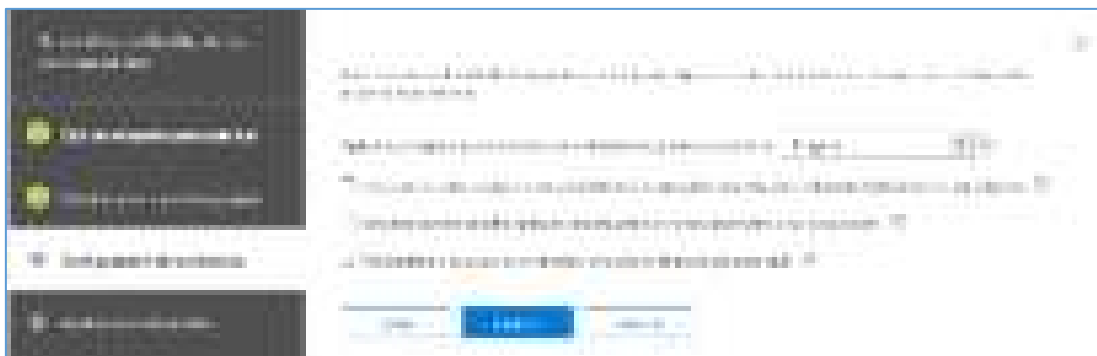


3. Elegir usuarios o grupos.

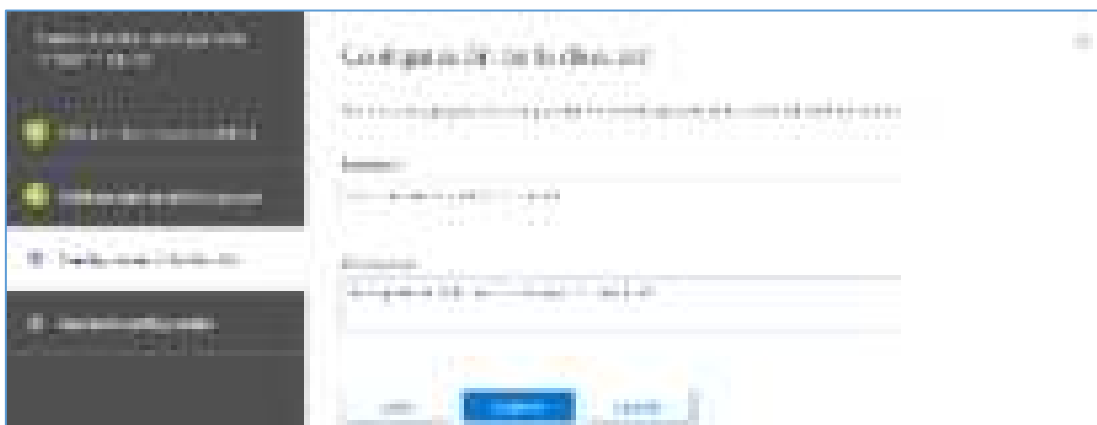


4. Configuración de la directiva.

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



5. Nombrar la directiva.



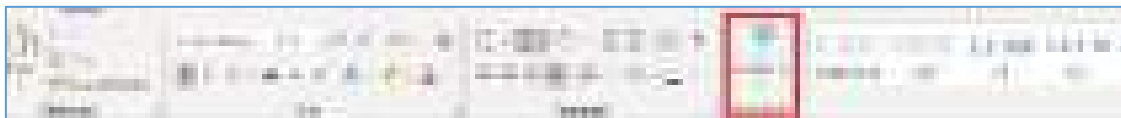
Instalar cliente para *sensitivity labels*

Existen dos clientes relacionados con las *sensitivity labels*: cliente de *Azure Information Protection*, y cliente ***Azure Information Protection unified labeling***. Se recomienda la instalación del segundo para el uso de las *sensitivity labels* tal y como se han descrito en la sección anterior (es decir, a través del *Centro de Seguridad y cumplimiento de Office 365*).

Nota: Puede ser confusa la nomenclatura utilizada por Microsoft, pero el primer cliente iría asociado a las etiquetas creadas desde el portal de Azure con *Azure Information Protection* (AIP) y el segundo para las *sensitivity labels* creadas desde *Centro de Seguridad y cumplimiento de Office 365* (CSC). Microsoft incorpora mecanismos para migrarlas desde AIP al CSC.

Para la instalación del cliente *Azure Information Protection unified labeling*: descargar ***AzInfoProtection_UL.exe*** desde el *Centro de descargas de Microsoft*, y ejecutarlo como administrador del equipo.

Tras su instalación, aparecerá en las aplicaciones de escritorio el nuevo icono:



3.2.3.2 Cifrado

Además de proteger los datos de clientes en reposo, Microsoft usa tecnologías de cifrado para proteger los datos de clientes de Office 365 en tránsito.

Por datos en tránsito nos estamos refiriendo:

- Cuando un equipo cliente se comunica con un servidor de Office 365.
- Cuando un servidor de Office 365 se comunica con otro servidor de Office 365.
- Cuando un servidor de Office 365 se comunica con un servidor que no es Office 365 (por ejemplo, Exchange online que entrega el correo electrónico a un servidor de correo electrónico externo).

Como el cifrado en Office 365 puede realizarse con diferentes tecnologías y métodos, no hay un único lugar en el que activar o configurar el cifrado.

Así por ejemplo el administrador de **Exchange Online**, tiene varias opciones para configurar el cifrado de correo electrónico. Entre ellos se incluyen usar el cifrado de mensajes de Office 365 con **Azure Rights Management** (Azure RMS) para permitir que los usuarios envíen mensajes cifrados dentro o fuera de la organización. Para más información consultar la guía específica del servicio de Exchange Online.

Controlar los datos en Office 365 con la clave de cliente

Con la clave de cliente, se puede controlar las claves de cifrado de la organización y, después, configurar Office 365 para usarlas y cifrar los datos en reposo en los centros de datos de Microsoft. Es decir, la clave de cliente permite a los clientes agregar una capa de cifrado que les pertenece, con sus claves. Los datos en reposo incluyen datos de Exchange Online y Skype Empresarial que se almacenan en buzones y archivos en SharePoint Online y OneDrive para la Empresa. Se debe configurar Azure antes de poder usar la clave de cliente de Office 365.

Consultar guía [CCN-STIC-884A - Guía de configuración segura para Azure] y guías específicas de los servicios.

3.2.3.3 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.

3.2.3.4 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 la 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\Servicios y complementos].



5. CARACTERÍSTICAS DISPONIBLES POR LICENCIAMIENTO

En la siguiente tabla se relacionan las características referenciadas en esta guía y su disponibilidad en función de los planes de Office 365 contratados por la organización.

Característica	Office 365 Enterprise E1	Office 365 Enterprise E3	Office 365 Enterprise E5
Acceso al Centro de Seguridad y Cumplimiento	Sí	Sí	Sí
Office 365 Cloud App Security	No	No	Sí
Administración de amenazas , tales como filtrado de correo y antimalware.	Sí	Sí	Sí
Administración avanzada de amenazas (ATP) , tales como el explorador de amenazas para las campañas de suplantación de identidad. Nota: la protección contra amenazas avanzada está disponible en Office 365 Enterprise E5 y como un servicio independiente para Office 365 Enterprise E1 y Office 365 Enterprise E3.	No	No	Sí
Data Loss Prevention (DLP). Prevención de pérdida de datos para Exchange Online, SharePoint Online y OneDrive para la empresa. Nota: incluye los archivos almacenados en repositorios de Microsoft Teams. Hay disponible un complemento DLP que se puede agregar a cualquier SKU que tenga Exchange o SharePoint/OneDrive.	No	Sí	Sí
Data Loss Prevention (DLP). Prevención de pérdida de datos para mensajes de chat y canales de Microsoft Teams	No	No	Sí
Etiquetas de sensibilidad Nota: las <i>etiquetas de sensibilidad</i> también se incluyen en Azure Information Protection P1 y P2.	No	Sí	Sí
Gobierno de datos Nota: el gobierno de datos permite a los usuarios crear, publicar y aplicar manualmente etiquetas a los documentos.	Sí	Sí	Sí
Gobierno de datos avanzado Nota: el gobierno de datos avanzado permite conservar información importante y eliminar información poco relevante mediante la clasificación de la información basándose en una directiva de retención o eliminación o en ambas. Incluye acciones inteligentes/automatizadas, como la	No	No	Sí

aplicación automática de etiquetas a datos, la aplicación de etiquetas basadas en <i>tipos de datos sensibles</i> o consultas y el uso de filtros de importación inteligentes. También incluye la característica de <i>supervisión</i> para revisar las comunicaciones de los empleados con fines de seguridad y cumplimiento.			
Búsqueda de contenido	Sí	Sí	Sí
casos de eDiscovery	Sí	Sí	Sí
Archivado	Sí *límite de 50 GB	Sí * ilimitado	Sí * ilimitado
Auditoría unificada Nota: se puede usar la API de actividad de administración 365 de Office para recuperar eventos del registro de auditoría unificado.	Sí	Sí	Sí
Políticas de retención	Sí *se necesita una licencia de EXO (plan 2) para aplicar una directiva de retención a un buzón de usuario.	Sí	Sí
Políticas de supervisión	No	No	Sí

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
AAD	<i>Azure Active Directory</i> (Directorio Activo de Azure).
AD DS	<i>Active Directory Domain Services</i> (Servicios de dominio de Directorio Activo).
AIP	<i>Azure Information Protection</i> .
Azure AD	<i>Azure Active Directory</i> .
Azure RMS	<i>Azure Rights Management</i> (Azure RMS).
Centro de Administración de Microsoft 365	Portal de Administración de Office 365. Accesible desde la url: admin.microsoft.com .
CSC	Centro de Seguridad y Cumplimiento de Office 365.
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: - 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. 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	Configuracion		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:	Cumple:
		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas:	Observaciones:
		☐ Si ☐ No	
Op.acc.3	Segregación de funciones y tareas		
	Se ha asignado adecuadamente los roles de administración.	Aplica:	Cumple:

		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación		
	Se ha habilitado <u>Multi-Factor Authentication</u> (MFA) para los usuarios de la organización.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.6	Acceso local		
	Se han configurado directivas de acceso condicional para que los usuarios y dispositivos que se conectan desde las redes de la organización dispongan de un acceso menos restrictivo que aquellos que se conectan desde Internet, identificando correctamente las direcciones IPs y redes de origen	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.7	Acceso remoto		
	El acceso remoto se entiende como acceso desde Internet (cualquier IP). Se recomienda reforzar la seguridad cuando se accede desde Internet (<i>solo equipos administrados, MFA, conformidad de dispositivos, etc.</i>).	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp	Explotacion		
op.exp.6	Protección frente a código dañino		
	Se han habilitado y configurado una o varias medidas de protección del correo electrónico como Antispam, Antispoofing, Antiphishing y Antimalware.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.6	Protección frente a código dañino		
	Se comprueba periódicamente la detección de amenazas en tiempo real, accesible desde el <i>Centro de Seguridad y cumplimiento de Office 365</i> , y se genera el informe pertinente. * Si la organización dispone de <i>Office 365 Advanced Threat Protection</i> (Office	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

	365 ATP).		
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.8	Registro de la actividad de los usuarios		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.10	Protección de los registros de actividad		
	Se ha securizado la consulta del registro de actividad mediante el establecimiento de los roles adecuados.	Aplica: Si No	Cumple: Si No

		☐	☐	☐	☐
		Evidencias Recogidas:		Observaciones:	
		☐	Si	☐	No
op.mon	Monitorización del sistema				
	Se han configurado alertas en el <i>Centro de Seguridad y cumplimiento de Office 365</i> .	Aplica:		Cumple:	
		☐	Si	☐	No
		☐	Si	☐	No
mp	Medidas de Protección				
mp.info	Protección de la información				
mp.info.2	Calificación de la información				

	Se han aplicado políticas de retención.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.2	Calificación de la información		
	Se han aplicado políticas de DLPs.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.2	Calificación de la información		

	Se han aplicado <i>sensitivity labels</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.3	Cifrado		
	Se ha aplicado un cifrado especial mediante etiquetas de sensibilidad a sitios de Sharepoint que precisan una protección especial. * Microsoft cifra automáticamente los datos en reposo y de manera transparente para el usuario. Para un cifrado adicional se pueden usar las <i>sensitivity labels</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	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: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.9	Copias de seguridad		
	Se dispone de planes específicos de copias de seguridad de la información en aquellos servicios en donde se admita.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s	Protección de los servicios		

mp.s.8	Protección frente a la 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: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
	Servicios y complementos		
	Se ha controlado los servicios y complementos disponibles para los usuarios.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones: