

Guía de Seguridad de las TIC CCN-STIC 885A

Guía de configuración segura para Office 365





Edita:



© 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, que ha sido financiado por Microsoft.

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.



Guía de configuración segura para Office 365

<u>PRÓLOGO</u>

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.

Diciembre de 2019

Félix Sanz Roldán Secretario de Estado Director del Centro Criptológico Nacional



Guía de configuración segura para Office 365

<u>ÍNDICE</u>

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	6
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	25
3.1.1.5 MECANISMOS DE AUTENTICACIÓN	25
3.1.1.6 ACCESO LOCAL	29
3.1.1.7 ACCESO REMOTO	29
3.1.2 EXPLOTACIÓN	29
3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO	30
3.1.2.2 REGISTRO DE ACTIVIDAD	30
3.1.2.3 GESTIÓN DE INCIDENTES	33
3.1.2.4 PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	35
3.2 MEDIDAS DE PROTECCIÓN	36
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES	36
3.2.2 MONITORIZACIÓN DEL SISTEMA	36
3.2.3 PROTECCIÓN DE LA INFORMACIÓN	41
3.2.3.1 CALIFICACIÓN DE LA INFORMACIÓN	41
3.2.3.2 CIFRADO	67
3.2.3.3 LIMPIEZA DE DOCUMENTOS	68
3.2.3.4 COPIAS DE SEGURIDAD	68
3.2.4 PROTECCIÓN DE LOS SERVICIOS	69



	3.2.4.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO	.69
4.	OTRAS CONSIDERACIONES DE SEGURIDAD	69
4.	1 SERVICIOS Y COMPLEMENTOS	.69
5.	GLOSARIO Y ABREVIATURAS	70
6.	CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD	72



CCN-STIC 885A Guía

Guía de configuración segura para Office 365

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:

- <u>Autenticación inicial</u>. Mediante un usuario con los derechos adecuados para la administración del servicio.
- <u>Cifrado continuo de la comunicación</u>. 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 descontinuó 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 administrador 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).
- 2. 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.



CCN-STIC 885A Gu

Guía de configuración segura para Office 365



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 [3.1. 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 *Msol* 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).
- 2. 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*.

Microsoft 365 admin center



CCN-STIC 885A Guía de configuración segura para 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.

 Office 3	65										Q	\$?	A3
	Is this a br This is you assign a pr Then all yo	rand new Office r Office 365 hor roduct license to our apps will sho	e 365 license? me page. It's a lit o your own user a	tle empty at the account and to 1	moment. Click Ass the other users in y	ign Products to our organization.	Assign Pro	oducts		My accou	nt			×
▲	Still don't If you have it may take	see any apps? e just purchased e a few more mi	l an Office 365 su nutes before all :	ubscription, or if your apps are av	your IT admin has railable. Please refr	assigned one to you vi 2sh this page after 10 r	ery recently, minutes.	×		A3	Admin C admin@ My accou Sign out	office 36	55 onmicro	soft.c
Go	od afte	rnoon					Install Off	ice \vee						
	\bigcirc	(田	A 33	\rightarrow									
Co	mpliance	Security	Add-In	Admin	All apps									
						Fe	eedback	② Need help?	~					

2. Cambiar el idioma a español.

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

	Centro de administra	ación de Micro	osoft 365		Q	ŝ	?	A3
=			Contract	Finalizar la	Configuración)	×
ŵ	Inicio		Obtener aprice	de Office 3	Temas			
8	Usuarios	~	Personalizar	Empiece por configurar	Office	*	(h)*	
۶R	Grupos	~	Inicio de sesión	Le ayudaremos a configu professional para sus dir			201	
	Facturación	~		evitar repetir trabajo más direcciones de correo ele		A.	÷.	ų
0	Customize navigation			directiones de conco etc	Ver todo			
	Mostrar todo			Ir a instalación	Idioma			. 1
			\wp Buscar usuarios, grupos, opciones de co $+$	- Agregar tarjeta 👌 Modo oscuro 🛛 🦻 No	español (España, alfabe	tización		. 1
			Essentials		Guardar Cance	lar		~

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.



CCN-STIC 885A Gu

Guía de configuración segura para Office 365

Pulsar el botón "Ir a instalación":

	Centro de administraci	ón de N	icrosoft 365	Ф 🌍 ? Аз
= ଜ	Inicio		and a start and a start and a start a star	Finalizar la configuración de Office 365 E5
8	Usuarios	\sim	Person	Empiece por configurar su dominio
RR	Grupos	~		Le ayudaremos a configurar un nombre de dominio más professional para sus direcciones de correo electrónico y su sitio web. Es mejor hacer este cambio lo antes posible para
	Facturación	\sim		evitar repetir trabajo más tarde, por ejemplo cambiando direcciones de correo electrónico
0	Customize navigation			Ir a instalación
	Mostrar todo			

3.1. Personalizar el inicio de sesión y correo electrónico.

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

::: Centro de administración de Micr	rosoft 365				Q	ŝ	?	A3
Office 365 Instalación de E5	Paso 1 Personalizar inicio de sesión	Paso 2 Agregar usuarios	Paso 3 Obtener aplicaciones	Paso 4 Conectar dominio				^
Personalizar el inicio de sesión y el correo electrónico El dominio que elija se mostrará en la parte de su dirección de correo electrónico que viene después del símbolo @. Su usuario y su personal usarán esa dirección para iniciar sesión y es así como los clientes le enviarán correos electrónicos.								
Escriba el nombre de un dominio de su	propiedad. Por ejemplo, suempresa.com							
Escriba el nombre de un dominio de su propiedad. Por ejemplo, suempresa.com. Q ¿Qué es un dominio y por qué necesita uno? O Continúe usando pueste Lonmicrosoft.com para el correo electrónico y el inicio de sesión. Q ¿Por qué debería usar este dominio?								

3.2. Agregar nuevos usuarios.

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

Office 365 Instalación de E5	Paso 1 Personalizar inicio de sesión	Paso 2 Agregar usuarios	Paso 3 Obtener aplicaciones					
Agregar nuevos usuarios Asignaremos una licencia de Office 365 E5 a cada usuario que agregue aquí. Cuando haya terminado, le proporcionaremos la información de inicio de sesión para que la								
 ¿Qué sucede si no realiza esta acci Tiene 0 de 1 licencias disponibles. V 	ón ahora? er todos los usuarios.							
Nombre Apellidos Nombre de usuario								
+ Adquirir una licencia								

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:

 Office 365		Q	0	?	D
۵	¿Es la primera vez que usa Office 365? Esta es su página principal de Office 365; desde aquí puede ver todas sus aplicaciones de Office 365 y obtener acceso a ellas. Si la página princip vacía, la razón podría ser que se le ha asignado la licencia de usuario hace muy poco. Espere 10 minutos y actualice esta página. Si sigue sin ver ninguna aplicación, póngase en contacto con su departamento de TI. Ellos pueden ayudarle para que todo funcione correctamente.	al está	×		Â
Bue	enos días In	stalar Office	×		
Com	inplemento Todas las aplicaciones				

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.



Guía de configuración segura para Office 365

 Office 365		ş	O Buscar					₽ ⊗ ? <mark>(</mark>
Buenas no	ches							Establecer la zona horaria Para establecer su foto de perfil y recibir recordatorios, vaya a Correo y
+	O		w	×	2	N	5	Aj establezca la zona horaria para el calendario. $ ightarrow$
Iniciar nuevo	Outlook	OneDrive	Word	Excel	PowerPoint	OneNote	SharePoint	365
\rightarrow								Obtenga las conocidas aplicaciones de escritorio en su PC o Mac.
Todas las aplicaciones								Entendido
Recientes Ar	nclados Co	ompartidos con	nigo Desc	ubrir				→ Cargar y abrir

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*.

	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.
ldeal 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.

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

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.



Guía de configuración segura para Office 365

<u>Administración</u>

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:



Guía de configuración segura para Office 365

- 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.

Agregar un usuario

Información básica	Configurar la información básica							
C Licencias de producto	Para empezar, rellene información básica sobre el usuario que va a agregar.							
O Configuración opcional	Nombre Apellidos							
Finalizar	ccn-0365							
	Nombre para mostrar *							
	ccn-O365 usuario generico							
	Nombre de usuario *							
	ccn-O365 @ parall.onmicrosoft.com ~							
	Configuración de contraseñas							
	Generar contraseña automáticamente							
	🔿 Dejarme crear la contraseña							
	Siguiente							

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.

Asignar licencias de producto	Aplicaciones (34)
Asigne las licencias que desea que tenga este usuario.	Mostrar aplicaciones para: Todas las licencias
Seleccione la ubicación * España V	Administración de dispositivos móviles para Office 365 Office 365 E5 Esta aplicación se asigna a nivel de organización. No se puede asignar por usuario.
Licencias (1) * Asignar una licencia de producto al usuario 	 Office 365 E5 Barreras de información Office 365 E5
Office 365 E5 0 de 1 licencias disponibles Orear usuario sin licencia de producto (no se recomienda) Es posible que tengan acceso limitado o que no tengan acceso a Office 365 hasta que asigne una licencia de producto.	Búsqueda de Microsoft Office 365 E5 Esta aplicación se asigna a nivel de organización. No se puede asignar por usuario. Cifrado Premium en Office 365 Office 365 E5





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

Usuarios activos			
$\mathcal{R}_{\!\!\!\!\!\!\!\!\!\!}$ Agregar un usuario $\ \ g_{\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!}^{\mathcal{R}}$ Agregar varios usuarios	Autenticación multifactor	, C ccn × ▼ Filtra	ar 🚍
Nombre para mostrar \uparrow	Nombre de usuario	Licencias	
ccn-O365 usuario genér	ccn-O365@p	Office 365 E5	

Operaciones básicas sobre usuarios

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

Usuarios activos					
Agregar un usuario 💍 Actualizar	\mathbb{Q}_{k} Restablecer contraseña $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$				
✓ Nombre para mostrar ↑	Nombre de usuario	Licencias			
< usuario genérico	🔍 : usuario@ 3.onmicrosoft.com	Sin licencia			
	🛱 Administrar licencias de producto				
	🗚 Asignar a grupo				
	🛋 Editar nombre de usuario				
	📋 Eliminar usuario				



Guía de configuración segura para Office 365

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.

Usuarios activos	ccn-O365 usuario genérico
우, Agregar un usuario 💍 Actualizar 🛛 …	Cambiar foto
✓ Nombre para mostrar ↑	
 ccn-0365 usuario genér 	Cuenta Dispositivos Licencias y aplicaciones Correo OneDrive
	Seleccione la ubicación * España
	Licencias (1)
	Office 365 E5 0 de 1 licencias disponibles

Asignar usuario a grupo

CC ccn-O365 usuario genérico ccn-O365@, ccn-O365@, ccn-O360@, ccn-O360@, ccn-O360@, ccn-O360@, ccn-O366@, ccn-O360@, ccn-O3
+ Agregar pertenencias Pertenencia a grupos
Buscar $ ho$
Grupos (0) No se encontraron resultados

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

Usuarios activos	
우, Agregar un usuario 🛛 Actuali	izar 🔍 Restablecer contraseña 🛱 Asignar a grupo
Nombre para mostrar ↑	Nombre de usuario
ccn-O365 usuario genér	ccn-O365@onmicrosoft.com
ccn-usuario2	🔍 : ccn-usuario2@onmicrosoft.com
	📫 Administrar licencias de producto
	🗯 Asignar a grupo
	🔿 Editar nombre de usuario
	📋 Eliminar usuario

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

¿Eliminar este usuario?

¿Seguro de que desea eliminar con-usuario2 como usuario? Puede restaurar los usuarios eliminados y recuperar sus datos excepto para los elementos de calendario y alias, durante un máximo de 30 días.

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.

Agregar un grupo



Guía de configuración segura para Office 365

CCN-O365-grupo1 Office 365	×
Agregar un grupo	
Тіро	
Office 365 V	
Nombre *	
CCN-O365-grupo1	
Dirección de correo electrónico del grupo *	
ccn-O365-grupo1 @onmicrosoft.com V	
Disponible	
Descripción	
Grupo 1 de usuarios CCN-O365	
Privacidad *	
Privado: solo los miembros pueden ver el contenido del grupo	No puede cambiar la configuración de privacidad después
Público: cualquiera puede ver el contenido del grupo	de crear el grupo.
con-O365 usuario genérico con-O365@	
Cambiar esta configuración después de crear el grupo	
Envíe copias de conversaciones y eventos del grupo a las bandejas	
de entrada de sus miembros. Decartivado	
Permitir que personas que no pertenezcan a la organización envíen correos electrónicos al grupo	
Desactivado	
Agregar Cancelar	

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".

Grupos Los grupos de distribución y los grupos de seguridad habilitados para correo pueden tardar hasta una hora expanser en la lista de grupos. Si aún no ve su grupo nuevo, vaya al centro de administración de Echange. Más información sobre los lupos de grupo	CCN-0365-grupo1 Grupo Private • 0 miembros
R Agregar un grupo O'Actualizar 🖉 Editar nombre 🛱 Editar descripción 🗃 Eliminar grupo	General Miembros Configuración Microsoft Teams
CCN-0365-grupo1 : con-0365-grupo1@juumit.comicrosoft.co Office 365	Propietarios (1) cen-0365 usuario genérico cen-0365@j onmicrosoft.com
	Ver todos los propietarios y administrarios Miembros (0)
	Ver todos los miembros y administratlos



Guía de configuración segura para Office 365

2. Después pulsar sobre el link "Ver todos los miembros y administrarlos".

$\left(\begin{array}{c} \\ \end{array} \right)$	Unice 565			
+ Agreg	ar miembros]		
Ver miem	bros			
Miembros de	la búsqueda			
D			Q	

Eliminar grupo

CCN-STIC 885A

CCN-0365-grupo1 Office 365	D
Eliminar grupo	IC
Eliminar grupo Está a punto de eliminar el grupo. Si continúa, todas las conversaciones, archivos, blocs de notas y eventos del grupo se eliminarán de forma permanente y no podrá recuperarlos. Antes de continuar, copie todo el contenido que quiera conservar.	
Eliminar Cancelar	

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

•	CCN-O365-grupo1	: ccn-O365-grupo
		🖉 Editar nombre
		🗒 Editar descripción
		📋 Eliminar 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:



Guía de configuración segura para Office 365

```
# 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</i> permisivo	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 permiso para administrar todos los productos y servicios, mientras que los administradores personalizados solo tienen los permisos que usted elija. Para reducir el nivel de riesgo en su organización, limite el número de administradores globales y, en su lugar, asigne roles de administrador personalizado.

Más información sobre roles de administración

Usuario (sin	acceso	de	administrador)	(j)

Administrador global

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

Administrador global 🛈

Usuarios y grupos

Administrador de control de usuarios 🛈

Administrador de servicios 🛈

Administrador del servicio de asistencia 🛈

Facturación

Administrador de facturación	Û)
------------------------------	---	---

Roles especiales comunes

Administrador de Exchange 🛈

Administrador de servicios de Teams 🛈

Administrador de SharePoint (i)

Roles adicionales

Administrador de comunicaciones de Teams 🛈



Roles disponibles en el centro de administración de Microsoft 365

El centro de administración Microsoft 365 permite administrar más de 30 roles de *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 <i>rol de 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.



CCN-STIC 885A Guía de configuración segura para Office 365

ø	Configuración ^	Seguridad y privacidad	
	Servicios y complementos		
	Seguridad v privacidad	Directiva de contraseñas	
	beganada y privaciada	Establezca directivas de contraseñas para todos los usuarios de la organización.	
	Perfil de la organización	Días antes de que las contraseñas expiren 90	
	Relaciones con partners	Días antes de notificar a un usuario acerca 14 de la caducidad	

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:

au	autenticación multifactor								
usu	iarios configuració	on del servicio							
	5								
Nota	solo los usuarios con licencia p	ara usar Microsoft Online Services pueden usar Multi-Factor A	Authentication. Más información aco	erca de la asignación de licencias a					
Antes	s de empezar, consulte la guía d	e implementación de autenticación multifactor.							
	actualización en masa								
Ve	r: Usuarios con inicio de sesión	peri 🗸 👂 Estado de Multi-Factor Auth: Cualquiera 🗸							
	NOMBRE PARA MOSTRAR	NOMBRE DE USUARIO	ESTADO DE MULTI- FACTOR AUTH						
	Admin Office 365	admin@plain823.onmicrosoft.com	Deshabilitada	Admin Office 365					

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.



Guía de configuración segura para Office 365

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:



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 <i>AAD</i> : Set-MsolPasswordPolicy
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: Set-MsolPasswordPolicy



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. Posteriores 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.

Centros de administración

Seguridad y cumplimiento

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*.



Guía de configuración segura para Office 365

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:

$\&$ Cómo hemos protegido su organización frente a las amenazas en los últimos 7 días \cdots							└── Estado de protección cont ···		
Configurar archivos adjunto Configurar ATP para para la protección contr cero Protección contra amenaza malware de día cero en me electrónico y archivos de St	os seguros de ATP SPO, ODB, Teams ra malware de día s avanzadas de nsajes de correo narePoint, OneDrive y	Configurar la protección con identidad (phishing) de ATP para la protección contra identidad (phishing) de d Protección contra amenazas suplantación y de phishing d con protección contra amenaz	tra suplantación de suplantación de lía cero avanzadas de e objetivo definido uzas avanzada de	Configurar vínculos seguros de ATP para la protección en el momento del clic Vínculos maliciosos bloqueados en mensajes entrantes y en el ámbito de su organización mediante la protección en el momento del clic de Vínculos seguros de ATP de Office 365	>	08/20	08/22	08/24	08/26
└── Detecciones de a	menazas globale	s semanales		└── Tendencias de malware		& Se	detectaro	n familias d	e •••
63-81 mil M Mensajes examinados	Amenazas detenidas	9.59 M Bloqueado por ATP	3.09 M Se ha quitado después de la entreoa	No se detectó malware			No se dete	ectó malware	

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".

🎽 Flujo de correo 🛛 🗸	Inicio > Búsqueda de registros de auditoría	
	Búsqueda de registros de auditoría	×
	Para utilizar esta función, active la auditoría para que podamos empezar a re Lusuario en su organización. Al activada la actividad se anotará en el registro	gistrar la actividad de administrador y de auditoría de Office 365 y estará
,O Buscar 🔨	disponible para su visualización en un informe.	
Búsqueda de contenido ⊏	¿Necesita averiguar si un usuario eliminó un documento o si un administrador resta Office 365 para conocer lo que hacen los usuarios y administradores de la organizar grupos, documentos, permisos, servicios de directorio y mucho más. Más informaci	oleció la contraseña de un usuario? Busque en el registro de auditoría de ión. Encontrará actividades relacionadas con el correo electrónico, on acerca de cómo hacer búsquedas en el registro de auditoría
Búsqueda de registros de	Deputtodes	
auditoría	Buscar ² Borrar Resultados	
Aplicaciones de	Actividades Pecha Dirección	IP Usuario Actividad Elemento Detalle
productividad	actividades 👻	
P	Fecha de inicio	ina busqueda para ver los resultado
🕞 eDiscovery 🗸 🗸	2019-08-20	
⊬ Informes ∨	Fecha de finalización 2019-08-28 Image: 00.00 V	

2. Pulsar "Sí".

Seguridad y cumplimiento		
La configuración de la organización necesita actualizarse. ¿Desea continuar	?	
	Sí	No

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.



Guía de configuración segura para Office 365

Búsqueda de registros de auditoría

¿Necesita averiguar si un usuario eliminó un documento o si un administrador restableció la contraseña de un usuario? Busque en el registro de auditoría de Office 365 para conocer lo que hacen los usuarios y administradores de la organización. Encontrará actividades relacionadas con el correo electrónico, grupos, documentos, permisos, servicios de directorio y mucho más. Más información acerca de cómo hacer búsquedas en el registro de auditoría

Buscar	り Borrar		Resultados						
Como inició los registros de l	Como inició los registros de las actividades de		Fecha 🔻	Dirección IP	Usuario	Actividad	Elemento	Detalle	
usuario y de administración h horas, es posible que algunas	nace menos de 24 s actividades no se								
muestren todavía en los resu	ltados de la búsqueo	la.	Fiec	utar una	búsqued	a para ve	r los resu	resultados	
Actividades			LJCC	acar ana	babqaca		1001004	10005	
Mostrar resultados para actividades 🔻	a todas las								
Fecha de inicio									
2019-08-27	00:00 ~	 							
Fecha de finalización									
2019-08-28	00:00 ~	·							
Usuarios									
Mostrar resultados para	todos los usuario								
Archivo, carpeta o sitio 🕕									
Agregue todo o parte d archivo o carpeta, o UR	le nombre de L de sitio.								
Q Buscar									

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:

Buscar ් Borrar	Resultados se han encontr	rado resultados de 5			▼ Filtrar resultados
Actividades	Fecha 🔻	Dirección IP	Usuario	Actividad	Elemento D
Se ha restablecido la contraseña de un usuario, (3) 💌	2019-09-03 11:42:31	<null></null>	admin@konmicrosoft.co	Se ha restablecido la contraseña	ccn-O365@
Fecha de inicio	2019-08-29 10:03:32	<null></null>	CCN-USER1-ADM@j	Se ha modificado una contraseñ	CCN-USER1-ADM@on
2019-08-01 🗰 00:00 ∨	2019-08-29 09:16:46	<null></null>	fim_password_service@support	Se ha restablecido la contraseña	CCN-USER2-ADM@3.on
Fecha de finalización 2019-10-04 00:00 ✓	2019-08-29 09:15:22	<null></null>	fim_password_service@support	Se ha restablecido la contraseña	CCN-USER1-ADM@j
	2019-08-29 09:11:42	<null></null>	fim_password_service@support	Se ha restablecido la contraseña	ccn-usuario2@onmicro

Ejemplo de consulta relacionada con el acceso a ficheros:

Buscar	Borrar	Resultados se han encontrado resultados de 150 (Hay más elementos disponibles, desplácese hacia abajo para ver más.)					
Actividades		Fecha 💌	Dirección IP	Usuario	Actividad	Elemento	
Se ha accedido al archivo 🕞		2019-09-18 03:35:29	52.142.112.247	ccn-o365@	Se ha accedido al archivo	Documento.docx	
Fecha de inicio	1:00 ×	2019-09-18 03:25:50	52.142.112.247	ccn-o365@	Se ha accedido al archivo	Documento.docx	
Fecha de finalización		2019-09-18 03:24:49	52.156.193.220	ccn-o365@onmicrosof	Se ha accedido al archivo	Documento.docx	
2019-10-04 🗰 00):00 ~	2019-09-18 03:15:11	52.142.114.208	ccn-o365@onmicrosof	Se ha accedido al archivo	Documento.docx	



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:



Guía de configuración segura para Office 365

Panel de alertas. Menú [Alertas\Panel].

https://protection.office.com/alertsdashboard

Seguridad y cumplimiento de Office 3	Q 🕸 ? 🔼	
< ^	Inicio > Alertas	
命 ^{Inicio}	M Tendenrias de alertas	Malertas activas por graved
🛕 Alertas 🔨		
Panel	8	0.5
Ver alertas Directivas de alerta		o

Panel de informes. Menú [Informes\Panel].

Seguridad y cumplimiento de Office 365 Inicio > Panel Privacidad de los datos Conclusiones y recomendaciones principales O Buscar Dominios suplantados con errores de autenticación durante los últimos 30 Suplantaciones en los últimos \wedge 7 días días 🛱 eDiscovery Revisar pares de dominios sospechosos Revisar pares de dominios no La inteligencia de suplanta y dominios que se indican tegió a los us 0 0 0 0 0 Pares de dominios Pares de dominios Pares de domin La inteligencia contra la La inteligencia contra la suplantación de la identidad suplantación de la identidad La inte ha recibido señales ha recibido señales recibid importantes que indican que adversada sup indican que adores de sub indican que adversada sup indican que dom gencia contra la suplantación de la reñales significativas que indicaban Panel Administrar Informes disponibles programaciones └── Informes recientes de descarga Cómo se aplicaron las etiquetas Informes para su descarga Fecha de inicio \smallsetminus Tipo Nombre 100 % 0 %

https://protection.office.com/insightdashboard

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

https://protection.office.com/ReportsForDownload

	E Seguridad y cumplimiento de Office 365							Q		
÷	Administración de amenazas	× ^	Inicio > Informes para su de	escarga						
	Flujo de correo	~	Descargue los informes desde a	iquí						
A	Privacidad de los datos	~	Ver Solicitudes de informes per	rsonalizados 🔻	Buscar					
Q	Buscar	~	✓ Fecha de inicio	Nombre		Tipo de informe	Dirección	Últim	o envío	\sim
Ģ	, eDiscovery	\sim			No hay datos disp	onibles				
⊵	Informes	^								
	Panel									
	Administrar									
	programaciones									
	Informes para su descarga									

Búsqueda e investigación. Widget del panel principal.

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



Guía de configuración segura para Office 365



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

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

:::: Seguridad y cumplimiento d	д 🏼 ? 🔥				
Administración de 🔨 🔨	 Conclusiones del flujo de correo	Í.			
A Information governance	🗠 Mapa de flujo de correo 🛛 …	└── Estado del flujo de correo ···			
- Currentation	< 2019-10-16 (UTC) >	Estado del flujo de correo en los dominios principales de la organización.			
		plain823.onmicrosoft 🗸			
ی Administración de می مسافقه م مسافقه مسافقه م	internet 0365 internet				
- Rich Is source		+ Ver detalles			
Flujo de correo /	✓ Flujo de correo entrante y saliente	└── Clientes SMTP Auth ····			
Panel	De salida: 7 De entrada; 8				
Seguimiento de mensajes	La semana pasada, Office La semana pasada, Office 365 revibio 7 mensajes, de 365 recibio 8 mensajes, de	Número de usuarios que han enviado mensajes mediante SMTP Auth en los últimos 7 días. Aquí puedo investigas las			

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

Cómo funcionan las directivas de alerta

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




- 1. Un administrador crea, configura y activa una directiva de alertas 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.*



Guía de configuración segura para Office 365

	Seguridad y cumplimiento de Office 365							¢ ?	
	< ^	Inicio > Alert policies							
ŵ	Inicio	Directivas de alerta							
♪	Alertas ^	Use las directivas de alerta para realizar el seguimi pérdida de datos en su organización. Después de e condiciones decidiendo cuándo activar la alerta y	ento de las act elegir la activid quién debería	tividades de admi lad sobre la que c recibir las notifica	nistradores y usuar juiere que se le avis	ios, amenazas de malw se, refine la directiva ag pación sobre las directiv	are o inc regando vas de ali	identes d ertas	e
	Panel		the second						
	Ver alertas	+ Nueva directiva de alertas							
	Directivas de alerta		,	l					
	Administrar las alertas	Nombre	Graved	Тіро	Categoría	Fecha de modific	. Estad	do	
	avanzadas	Malware campaign detected and bl	Baja	Sistema	Administraci	-			
x ^R	Permisos	Email reported by user as malware	Informati	Sistema	Administraci	-			
E	Clasificación 🗸	Unusual volume of file deletion	Media	Sistema	Gobierno de	-			
٦ ٦	Prevención de pérdida de	Unusual external user file activity	Alta	Sistema	Gobierno de	-			

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.

Nombre	Gravedad Tipo Categoría Fecha d	e modificaci Esta
Malware carm This alert is triggered when any email message is reported as malware or phish by users -V1.0.0.2	Baja Sistema Administración de a	
Email reported by user as malware or phish	Informativo Sistema Administración de a	
Unusual volume of file deletion	Media Sistema Gobierno de datos -	
Unusual external user file activity	Alta Sistema Gobierno de datos -	
eDiscovery search started or exported	• Media Sistema Administración de a	

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/eses/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 <u>ejemplo</u> 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.

Nueva directiva de alertas	Dé un nombre a la alerta, asígnele una categoría y elija un nivel de $^{ imes}$ gravedad.
Asigne un nombre a la alerta	Asigne una categoría y nivel de gravedad para ayudarle a administrar la directiva y las alertas que active. Podrá aplicar filtros a esta configuración deede las nácions de "Directivas de alerta" y de "Ver alertas"
Crear una configuración de alerta	Nombre *
-	CCN-alerta1
Configurar los destinatarios	
	Descripción
Revisar la configuración	CCN. Directiva de aleta para "Volumen inusual de borrado de ficheros"
3	Gravedad * () • Media -
	Categoría *
	Prevención de pérdida de datos 🔻
	Siguiente Cancelar

2. Crear configuración de alerta.

¿Sobre qué se quiere enviar alertas?

Seleccionar una actividad:

Nueva directiva de alertas	Elija una actividad, condiciones y cuándo se debe activar la alerta	×
Asigne un nombre a la alerta	Solo puede elegir una actividad, pero puede agregar condiciones para refinar qué se detectará. ¿Sobre qué quiere enviar alertas?	
Crear una configuración de alerta	 * La actividad es Se ha eliminado el archivo 	
Configurar los destinatarios	Buscar actividades	
Revisar la configuración	+ Agra Se ha desprotegido el archivo Se ha c Un usuario elimina un documento de un sitio.	
	Se ha eliminado el archivo	
	¿COMO C Se descartó la extracción del repositorio del archivo	
	Cada Se ha descargado el archivo	
	Cuant Se na modificado el archivo	

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



Guía de configuración segura para Office 365

direcciones IP), usuarios concretos, nombres de archivos, urls de sitios o extensiones de archivos.

Nueva directiva de alertas	Elija una actividad, condiciones y cuándo se debe activa	ar la alerta
Signe un nombre a la alerta	Solo puede elegir una actividad, pero puede agregar condiciones para refinar qué se detectará. ¿Sobre qué quiere enviar alertas?	
Crear una configuración de alerta Configurar los destinatarios	 ^ * La actividad es Se ha eliminado el archivo ∨ Un usuario elimina un documento de un sitio. 	
Revisar la configuración	+ Agregar una condición 🗸 General	
	Dirección IP Usuario Usuario CArchivo Nombre de archivo Dirección URL de la colección de sitios 25	
	Extensión de archivo	

En el ejemplo:

CCN-STIC 885A

Como cualquiera de	×	
txt, doc*, pptx		
∧ La dirección URL de la	colección de sitios es	
Como cualquiera de	~	

¿Cómo quiere que se active la alerta?

¿Cómo quiere que se active la alerta?									
Cada vez que una activ	Cada vez que una actividad coincide con la regla								
O Cuando el volumen de las actividades que coincidan alcance un umbral									
Mayor que o igual a	15 actividades								
En los últimos	60 minutos								
Activado	Todos los usuarios $^{\vee}$								
O Cuando el volumen de las actividades que coincidan sea poco frecuente									
Activado	Todos los usuarios \vee								



CCN-STIC 885A Guía de configuración segura para Office 365

3. Configurar los destinatarios

Nueva directiva de alertas	Decida si quiere avisar a los contactos cuando se desencadene esta $^{ imes}$ alerta
🥝 Asigne un nombre a la alerta	Enviar notificaciones por correo electrónico Destinatarios de correo electrónico *
Crear una configuración de alerta	admin@lonmicrosoft.com ×
Configurar los destinatarios	Límite de notificaciones diarias Sin límites
Revisar la configuración	1 5 10 25 50 100 150 200

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*.

	III Seguridad y cumplimiento de Office 365 D						Q	۲	?		
		< ^	Inicio > Alert policies								
ທີ	Inicio		Directivas de alerta								
♪	Atertas Ng Atertas Use las directivas de alerta para realizar el seguimiento de las actividades de administradores y usuarios, amenazas de malvare o incidentes de péridida de datos en su organización. Después de elegir la sobre la que quiere que se le avise, refine la directiva agregando condiciones, decidiendo cuándo activar la alerta y quién debería recibir las notificaciones. Más información sobre las directivas de alertas						activida	d			
	Panel	н.	+ Nueva directiva de alertas Buscar 🔎							¶ Filt	rar
	Ver alertas		Nombre		Gravedad	Tino	Categoría	Facha da modificaci	Ertado		
	Directivas de alerta		Nonible		Glavedau	про	categoria	recha de modificaci	Estado		
	Administrar las alertas		CCN-alerta1	•	Media	Personalizado	Prevención de pérdi	9/9/19 18:00			
	avanzadas		Suspicious email sending patterns detected	•	Media	Sistema	Administración de a				

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.



Guía de configuración segura para 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.

<u>Ejemplo</u>: *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.

Inicio > Etiquetas de	retención				Operational procedure
Etiquetas Cuando se publican, las e contenido se conservará determinada. Más inform	Directivas de etiquetas etiquetas aparecen en las aplicacion en función de la configuración que nación sobre las etiquetas de reten	nes de los usuarios, como Outlook, ShareP • haya elegido, Por ejemplo, puede crear et ción	oint y OneDrive. Cu: tiquetas que conser	ando se aplique una etiqueta a un ven el contenido durante un perío	Cottar etiqueta Cottar etiqueta
+ Crear una etiqueta	Publicar etiquetas	Aplicar automáticamente una etiqueta Autor de creación	O Actualizar	Buscar ,	Nombre Operational procedure
Contract agreen	nent I	Admin Office 365 Admin Office 365		5 años 3 años	Descripción para administradores Editar Retains content for 10 years, based on when it was labeled.
Operational pro	cedure	Admin Office 365		10 años	Descripción para usuarios Editar
					Descriptores de plan de archivos Editar
					Retención Editar 10 años Solo conservar Basado en fecha de la asignación de la etiqueta
					Creada por Admin Office 365



Guía de configuración segura para Office 365

3. Editar etiqueta. En el panel derecho pulsar el botón "Editar etiqueta".

Editar etiqueta	Operational procedure
	Editando Configuración de la etiqueta
Nombre	Retención
Descriptores de plan de archivos	Activado
Configuración de la etiqueta	Cuando esta etiqueta se aplica al contenido Conservar el contenido
	 Conservar el contenido Durante: IQuiere que lo eliminemos después de este tiempo? Climinar el contenido automáticamente. Desencadenar una revisión para eliminación. Nada. Dejar el contenido tal como está. No conservar el contenido. Eliminarlo si tiene una antigüedad superior a años Conservar o eliminar el contenido en función de la fecha de la asignación de la etiqueta Clasificación con etiquetas Use una etiqueta para clasificar el contenido como un "registro"
	 No conservar el contenido. Eliminarlo si tiene una antigüedad superior a años conservar o eliminar el contenido en función de la fecha de la asignación de la etiqueta Clasificación con etiquetas Use una etiqueta para clasificar el contenido como un "registro" Guardar Cancelar

Creación de una etiqueta de retención

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

Seguridad y cumplimiento de Of	fice 365			Q @ ? 🖉	3			
E Clusificación								
Etiquetas de	Etiquetas Directivas de etiquetas							
confidencialidad	Cuando se publican, las etiquetas apaneen en las aplicaciones de los usuarios, como Outlook, SharePoint y OneDrive. Cuando se aplique una etiqueta a un correo electrónico o a un documento (ya sea automaticamente o por parte del us contexisto en consecurso de función de la conferminida que han a desidad. Por elemento autora etiqueta regular de							
Etiquetas de retención	Contrator de Oblis informadio nel socializzation de la registra de							
Tipos de información	+ Crear una etiqueta 🖵 Publicar eti	iquetas 🖉 Aplicar automáticamente una etiqueta 🕓	Actualizar Duscar D		I			
confidencial					I			
Prevención de pérdida de V	Nombre	Autor de creación	Período de retención	Última modificación $^{\smallsetminus}$				
D Administración de	CCN-BORRADO3-1DIA	Admin Office 365	1 día	20 de septiembre de 2019	I			

- 2. Pulsar el botón "Crear una etiqueta".
- 3. Asignar nombre a la etiqueta.



Cree una etiqueta para ayudar a los usuarios a clasificar su contenido.	Asignar un nombre a la etiqueta
	Nombre * ①
Asignar un nombre a la etiqueta	CCN-ETIQUETA-RETENCION1
Descriptores de plan de archivos	Descripción para administradores ①
Configuración de la etiqueta	CCN-ETIQUETA-RETENCION1
Revisar la configuración	Descripción para usuarios ①
	ETIQUETA de retención para PRESUPUESTOS
	Siguiente Cancelar

4. Para aplicación automática y cumplimiento regulatorio.

Cree una etiqueta para ayudar a los usuarios a clasificar su contenido.	Descriptores de plan de archivos ×				
Asignar un nombre a la etiqueta	De acuerdo a las condiciones que indique a continuación, aplicaremos esta etiqueta automáticamente al contenido. Los usuarios verán que la etiqueta aplicada en el contenido que coincida con las condiciones especificadas. 🛈				
	ld. de referencia				
Descriptores de plan de archivos	Introduzca un ld. de referencia o cree uno nuevo 🔹				
	Función empresarial o departamento				
Configuración de la etiqueta	Seleccione una función empresarial o departamento o cree uno nuevo				
	Categoría				
Revisar la configuración	Seleccione una categoría o cree una nueva 🔻				
	Tipo de autoridad				
	Seleccione un tipo de autoridad o cree una nueva				
	Disposición o citación				
	Seleccione una disposición o citación o cree una nueva				
	Atrás Siguiente Cancelar				

Pulsar "Siguiente".



CCN-STIC 885A Guía de configuración segura para Office 365

5. Configurar la etiqueta.



6. Revisar y Crear.

Cree una etiqueta para ayudar a los usuarios a clasificar su contenido.	Revisar la configuración	
	Nombre	<u>Editar</u>
Signar un nombre a la etiqueta	CCN-ETIQUETA-RETENCION1	
Oescriptores de plan de archivos	Descripción para administradores	Editar
	CCN-ETIQUETA-RETENCION1	
Configuración de la etiqueta		
	Descripción para usuarios	Editar
Revisar la configuración	ETIQUETA de retención para PRESUPUESTOS	
	Descriptores de plan de archivos	Editar
	Retención	Editar
	5 años Conservar y eliminar Basado en fecha de la asignación de la etiqueta	
	Atrás Crear esta etiqueta Cancelar	
	Atrás Crear esta etiqueta Cancelar	

Publicar etiquetas

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



1. Elegir las etiquetas.

Publique etiquetas para que los usuarios puedan aplicarlas a su contenido.	Elegir etiquetas para publicar
Elija las etiquetas para publicar	cija ias euquetas que uesea publicar en las aplicaciones de su organizacion para que los usuaños puedan aplicanas a su contenido. Si no ve las etiquetas que desea, podrá crear una nueva.
Publicar para usuarios y grupos	La lista está vacía. Elija las etiquetas para publicar
Asignar un nombre a la directiva	Siguiente Cancelar
Revisar la configuración	
Elegir etiquetas	
+ Agregar — Eliminar	
1 etiqueta agregada	

2. Elegir ubicaciones.

Buscar

CCN-ETIOUETA-RETENCION1

- 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.



Guía de configuración segura para Office 365

Publique etiquetas para que los usuarios puedan aplicarlas a su contenido.	Elegir ubicaciones					
🧭 Elija las etiquetas para publicar	🔿 Todas las u	🔿 Todas las ubicaciones. Incluye el contenido del correo electrónico de Exchange, los grupos de Office 365 y los documentc				
Publicar para usuarios y grupos	de OneDriv Permíteme	de OneDrive y SharePoint. Permíteme elegir ubicaciones específicas.				
Asignar un nombre a la directiva	Estado	Ubicación	Incluir	Excluir		
Revisar la configuración						
		E S Correo electrónico de Exchange	Todo Elegir destinatarios	Ninguno Excluir destinatarios		
		Sitios de SharePoint	Todo Elegir sitios	Ninguno Excluir sitios		
		Cuentas de OneDrive	Todo Elegir cuentas	Ninguno Excluir cuentas		
		O Grupos de Office 365	Todo Elegir grupos	Ninguno Excluir grupos		
	Atrás	Siguiente Cancelar				

3. Dar un nombre a la directiva.

Asignar un nombre a la directiva			
Nombre * 🛈			
CCN-DIRECTIVA-RETENCION1			
Descripción			
CCN-DIRECTIVA-RETENCION1			
Atrás Siguiente Cancelar			



4. Revisar y Publicar.

Publique etiquetas para que los usuarios puedan aplicarlas a su contenido.	Revisar la configuración ×
📀 Elija las etiquetas para publicar	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. Elija las etiquetas para publicar Editar
🤗 Publicar para usuarios y grupos	Se publicará 1 etiqueta (estará disponible) para que los usuarios puedan clasificar su contenido CCN-ETIQUETA-RETENCION1 5 años conservar + suprimir
Asignar un nombre a la directiva	Publicar para usuarios y grupos Editar
Revisar la configuración	Correo electrónico de Exchange Cuentas de OneDrive
	Sitios de SharePoint
	Grupos de Office 365
	Nombre de la directiva Editar
	CCN-DIRECTIVA-RETENCION1
	Descripción Editar
	CCN-DIRECTIVA-RETENCION1
	Atrás Publicar etiquetas Cancelar

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:

Inicio > Etiquetas de	retención		
Etiquetas	Directivas de etiquetas		
Cree directivas de etique información acerca de la:	tas para publicar una o más etiquetas en s directivas de etiquetas	las aplicaciones de sus usuarios, como Outlook, SharePoint y O queta OActualizar Buscar P	neDrive. Después de publicar las etiquetas, los usuarios podrán aplicarlas para proteger su contenido o conservarlo. Más
Nombre		Creada por	Última modificación $^{\smallsetminus}$
	A-RETENCION1	Admin Office 365	27 de agosto de 2019

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].



Guía de configuración segura para Office 365

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 directa 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.

<u>Por ejemplo</u>, 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:

Seguridad y cumplimiento de Office 36	5			۵	ø	?	A3
Nueva directiva DLP	Empezar con una pla	antilla o crear una direc	tiva personalizada				×
Seleccionar la información para proteger	Elija un reglamento del sector para ver comienzo de directiva personalizada d Más información acerca de las plantillas	r las plantillas de directiva DLP que puede lesde el principio. Si necesita proteger cor s de directiva DLP	utilizar para proteger esa informac ntenido con etiquetas, podrá elegirl	ión o cr as más	ee un tarde.		Ì
Asignar un nombre a la directiva	Buscar	Mostrar opciones para Todos los p	aíses o regiones \checkmark				
Elegir ubicaciones	Financial	Custom policy	Custom policy Descripción				
Configuración de la directiva	Medical and health		Create a custom policy from scrat the type of content to protect and protect it.	ch. You I how yo	will choo ou want	ose to	
Revisar la configuración	Privacy Custom						
	U						

3. Asignar nombre y descripción.

ombre		
CCN-DLP-1		
escripción		
CCN-DLP-1		
CCN-DLP-1		

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.



CCN-STIC 885A Guía

Guía de configuración segura para Office 365



O seleccionar ubicaciones específicas:

Elegir ubica	aciones		>
	E S Correo electrónico de Exchange	Todo Elegir grupos de distribución	Ninguno Excluir grupos de distribución
	S Sitios de SharePoint	Todo Elegir sitios	Ninguno Excluir sitios
	Cuentas de OneDrive	Todo Elegir cuentas	Ninguno Excluir cuentas
	T B Mensajes de chat y canal de Teams	Todo Elegir cuentas	Ninguno Excluir cuentas

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.

Personalice el tipo de contenido que desea proteger				
Seleccione "Buscar contenido que incluya" si desea establecer rápidamente una directiva que proteja solo información confidencial o contenido etiquetado. Use las opciones avanzadas para ver más opciones, como la protección de contenido en los mensajes de correo electrónico enviados a dominios específicos, datos adjuntos con determinadas extensiones de archivo y mucho más.				
 Buscar contenido que contenga: ① ① Debe seleccionar al menos un tipo de clasificación. Editar 				
Detectar cuándo se comparte este contenido:				
con usuarios fuera de mi organización 🛩				
🔘 Usar configuración avanzada 🕕				
Atrás Siguiente Cancelar				



Personalice el tipo de contenido que desea proteger

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

+ Nueva regla



Las reglas son las que **aplican los requisitos empresariales en el contenido** de su organización. Una directiva contiene **una o más reglas**,

y cada regla consta de las condiciones y acciones. Para cada regla, cuando se cumplen las condiciones, las **acciones se realizan automáticamente.** Las reglas se ejecutan **secuencialmente**, comenzando por la regla de mayor prioridad de cada directiva.

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

Crear	una regla						×
Nombre	Condiciones	Excepciones	Acciones	Notificaciones al usuario	Reemplazos de usuario	Informes de incidentes	
Opciones Nombre * Escriba u Descripción	Opciones Nombre * Escriba un nombre descriptivo aquí. Descripción						
← Condicio	Escriba una descripción para la regla.						
Aplicarem + Agre	Aplicaremos esta directiva en el contenido que coincida con estas condiciones.						
Excepcion Excepcio	nes						
No aplicar + Agre	No aplicaremos esta regla al contenido que coincida con una de estas excepciones.						
^ Acciones							
Use las acciones para proteger el contenido cuando se cumplan las condiciones.							



Guía de configuración segura para Office 365

△ Notificaciones al usuario	
Use las notificaciones para informar a los usuarios y para enseñarles a usar correctamente la información confidencial.	
Desactivado	
∧ Reemplazos de usuario	
Permita a los usuarios que ven la sugerencia invalidar la directiva y compartir el contenido.	
Desactivado Desa activar las partifecciones de unuario parmites que las unuaries innorma la directiva	
Debe activar las nouncaciones de usuario perinten que los usuarios ignoren la unectiva.	
^ Informes de incidentes	
Utilice este nivel de gravedad en las alertas e informes de administración: Baja 🖌	
Envie una alerta a los administradores cuando se produzca una coincidencia con una regla. Desactivado	
Use los informes de incidentes de correo electrónico para que se le envíe una notificación cuando se produzca una coincidencia con una directiva. Desactivado	
∧ Opciones	
Detener el procesamiento de reglas y directivas DLP adicionales si coincide con esta regla. No se procesarán las reglas adicionales.	
Establecer el orden en el que se seleccionará la regla para la evaluación Prioridad: 0 v	

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.

△ Condiciones				
Aplicaremos esta directiva en el contenido que coincida con estas condiciones.				
+ Agregar una condición 🗸				
El contenido incluye				
El contenido está compartido				
La dirección IP del remitente es				
No se pudo digitalizar el contenido de los datos adjuntos de correo electrónico				
Cualquier contenido de los datos adjuntos del correo electrónico no completó la digitalización				
Los datos adjuntos están protegidos con contraseña				
El dominio del destinatario es				
El destinatario es				
La extensión de archivo de los datos adjuntos es				
La propiedad del documento es				
Use las notificaciones para miormar a los usuarios y para enseñaries a usar correctamente la miormad	iór			



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. Exceptiones

	^ Excepciones				
No aplicaremos esta regla al contenido que coincida con una de estas excepciones.					
	+ Agregar una excepción -				
~	Excepto si el contenido contiene información confidencial				
	Excepto si el contenido se comparte				
	Excepto si la dirección IP del remitente es				
	Excepto si no se ha podido digitalizar contenido de los datos adjuntos de correo electrónico				

c. Acciones

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





Guía de configuración segura para Office 365

^	Acciones	
	Use las acciones para proteger el contenido cuando se cumplan las condiciones.	
	Restringir el acceso o cifrar 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 est protegiendo. Pero puede elegir quién tiene acceso a los archivos compartidos de SharePoint y OneDrive. También puede decidir si quiere permitir que los usuarios puedan ignorar las restricciones de la directiva.	á
	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)	
	+ Agregar una acción +	

 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.



Guía de configuración segura para Office 365

△ Notificaciones al usuario
Use las notificaciones para informar a los usuarios y para enseñarles a usar correctamente la información confidencial. Nota: Las notificaciones de equipos se mostrarán en el propio cliente de chat.
CO Activado
Notificaciones por correo electrónico
Notificar qué usuario envió, compartió o modificó por última vez el contenido.
O Notificar a estos contactos:
Personalizar el texto del correo electrónico
Sugerencias de directiva
Personalizar el texto de la sugerencia de directiva
b. <u>Reemplazos de usuarios</u>

Permita a los usuarios que ven la sugerencia invalidar la directiva y compartir el contenido.

Desactivado

c. Informes de incidentes

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



evento.

d. <u>Opciones</u>



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].

	Seguridad y cumplimiento de Office 365 Q 🛞 ? 🗛												
		<	Inicio >	Etiquetas de	confidencialidad								
ጨ	Inicio			Etiquetas	Directivas de	etiquetas							
▲	Alertas	~	Las etique se aplique protegerá	etas de confider e una etiqueta (i en función de	ncialidad se utiliza (independienteme la configuración d	an para clasifi ente de si la a que elija. Por	car mensajes de co plica el usuario o s ejemplo, puede cre	orreo electróni e aplica auton ear etiquetas c	co, documentos, si áticamente), el cor ue cifren archivos,	iios y m itenido que agr	ucho má o el sitio reguen m	s. Cuar se narcado	ido ores
ጽ	Permisos		de contenido y que controlen el acceso de los usuarios a sitios específicos. Más información sobre las etiquetas de confidencialidad				bı						
E	Clasificación	^	+ Cre	ar una etiqueta	Publicar	etiquetas	🖱 Actualizar	Buscar	م				
Γ	Etiquetas de		·	+ Nombre	para mostrar	Auto	or de creación	Ú	tima modificación	I			
L	confidencialidad			Personal		Adm	in Office 365	3/	9/19 11:51				^
	Etiquetas de retención			D. 1 /									
	Tipos de información			Public		Adm	in Office 365	3/	9/19 11:51				
	confidencial			General		Adm	in Office 365	3/	9/19 11:51				
6	Prevención de pérdida de datos	\sim		+ Confiden	tial	Adm	in Office 365	3/	9/19 11:51				
G	Administración de registros	~		+ Highly Co	onfidential	Adm	in Office 365	3/	9/19 11:51				
		\sim							စ္ ¿Necesita ayı	ıda?	Com	entarios	× *

- 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 <u>nivel de sensibilidad menor</u> (una etiqueta "General") podría simplemente tener un encabezado o pie de página aplicados, mientras que al contenido con un <u>nivel de sensibilidad mayor</u> (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**".

	Seguridad y cumplimiento de Off	e 365 Q 🛞	?	A
Ĝ ▲	Inicio Alertas	Las etiquetas de confidencialidad se utilizan para clasificar mensajes de correo electrónico, documentos, sitios y mucho más. Cuando se a 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 elja. Por ejemplo, puede crear etiquetas que cifren archivos, que agreguen marcadores de contenido y que controlen los usuarios a sitios específicos. Más información sobre las etiquetas de confidencialidad	plique a el acces	una o de
x ⁹	Permisos			
E	Clasificación ^	Nombre para mostrar Autor de creación Ultima modificación		^
	Etiquetas de	Personal Admin Office 365 3/9/19 11:51		
	confidencialidad	Public Admin Office 365 3/9/19 11:51	•••	

2. Asignar un nombre a la etiqueta.

Nu co	ueva etiqueta de nfidencialidad	Asignar un nombre a la etiqueta
•	Nombre y descripción	La configuración de protección que elija para esta etiqueta se exigirá inmediatamente para los archivos, mensajes de correo electrónico o sitios a los que se aplique. Los archivos etiquetados estarán protegidos dondequiera que se lleven, tanto si están guardados en la nube o como si están descargados en un equipo.
	Cifrado	Nombre de la etiqueta * 🕕
		CCN-Etiqueta-Confidencial1
	Marcado de contenido	
		Información sobre herramientas * 🛈
	Prevención de pérdida de datos en	Información sobre CCN-Etiqueta-Confidencial1
punto d	de conexión	
•	Etiquetado automático	Descripción 🕕
•	Revisar la configuración	Descripción sobre CCN-Etiqueta-Confidencial1
		Siguiente Cancelar

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.

Nueva etiqueta de confidencialidad	Cifrado
Onmbre y descripción	Controle quién puede tener acceso a archivos y mensajes de correo electrónico que tengan esta etiqueta aplicada. Más información sobre la configuración de cifrado
Cifrado	Cifrado Desactivado
Marcado de contenido	Atrás Siguiente Cancelar
Prevención de pérdida de datos en	
punto de conexión	
Etiquetado automático	
Revisar la configuración	

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.

ado	
Cifrado Activado	
¿Asignar permisos ahora o permitir o	que los usuarios decidan?
Asignar permisos ahora	✓
Las opciones de cifrado que elija se aplica a los archivos de Office. El acceso del usuario al contenido exp	rán automáticamente cuando se aplique la etiqueta al correo electrónico y
Nunca	~
Permitir el acceso sin conexión	
Siempre ~	
Conceder permisos a usuarios y grupo	os específicos *
Asignar permisos	
Usuarios y grupos	Permisos
	1

• Pulsar sobre "Asignar permisos".

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

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

Permitir el acceso sin conexión		
Nunca	\sim	



Guía de configuración segura para Office 365

Asignar permisos	\times
Se asignarán permisos para utilizar el contenido con esta etiqueta aplicada solo a los usuarios o grupos que elija. Puede elegir entre los permisos existentes (como copropietario, coautor y revisor) o personalizarlos para satisfacer sus necesidades.	,
+ Agregar a todos los miembros de inquilinos	
+ Agregar usuarios o grupos	
+ Agregar estas direcciones de correo electrónico o dominios	
Seleccione permisos de presente o personalizado	
Coautor VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,OBJMODEL	
Guardar Cancelar	

• 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.

Seleccione permisos de presente o personalizado Elija las acciones que se permitirán para este usuario o grupo.				
Coautor 🗸				
Ver contenido (VIEW)				
Derechos de visualización (VIEWRIGHTSDATA)				
Editar contenido (DOCEDIT)				
Guardar (EDIT)				
Imprimir (PRINT)				
Copiar y extraer contenido (EXTRACT)				
Responder (REPLY)				
Responder a todos (REPLYALL)				
Reenvíar (FORWARD)				
Editar derechos (EDITRIGHTSDATA)				
Exportar contenido (EXPORT)				
Permitir macros (OBJMODEL)				
Control total (OWNER)				
Guardar Cancelar				

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

Pern	itir que los usuarios asignen permisos cuando apliquen la etiqueta $arphi$	
	En Outlook, aplique restricciones equivalentes a la opción No reenviar 🕕	
	En Word, PowerPoint y Excel, pedir a los usuarios que especifiquen permisos ① Solo se admite cuando está instalado el cliente de etiquetado unificado de Azure Information P.	rotectior



<u>Ejemplo</u>: 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.

frado	
trole quién puede tener acceso a archivos y n rmación sobre la configuración de cifrado	nensajes de correo electrónico que tengan esta etiqueta aplicada. Más
Algunas características, como la coauto en SharePoint y OneDrive. ¿A qué carac	oría o eDiscovery, no funcionarán correctamente con archivos cifrados cterísticas afecta?
Cifrado Activado	r que los usuarios decidan?
Asignar permisos ahora	∀
El acceso del usuario al contenido en Un número de días después de que se	aplica la etiqueta 🗸
Días de expiración del contenido	
30	
Permitir el acceso sin conexión	
Nunca \vee	
Conceder permisos a usuarios y gru Asignar permisos	pos específicos *
Usuarios y grupos	Permisos
.onmicrosoft.com	Visualizador ^

4. Marcado de contenido.





CCN-STIC 885A Guía de config

Guía de configuración segura para Office 365

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.

Nu co	ieva etiqueta de nfidencialidad	Prevención de pérdida de datos en punto de conexión ×
0	Nombre y descripción	Actualmente, solo puede configurar las capacidades de DLP de punto de conexión ofrecidas por Windows Information Protection (WIP). La configuración de DLP para las aplicaciones de Office 365 estará disponible pronto. Información sobre la DLP de punto de conexión y las etiquetas de confidencialidad
0	Cifrado	Prevención de pérdida de datos en punto de conexión Desactivado
0	Marcado de contenido	Atrás Siguiente Cancelar
	Prevención de pérdida de datos en	
punto c	le conexión	
•	Etiquetado automático	
•	Revisar la configuración	

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.

Nı co	ieva etiqueta de nfidencialidad	Etiquetado automático ×
0	Nombre y descripción	El etiquetado automático solo se admite en las aplicaciones de Office cuando está instalado el cliente de etiquetado unificado de Azure Information Protection. Cuando detectemos contenido confidencial en el correo electrónico o en los documentos que cumplan las condiciones que elija, podemos aplicar automáticamente esta etiqueta o mostar un mensaje a los usuarios que les recomiende que la aniliquen ellos mismos. Más información sobre el etiquetado automático
0	Cifrado	Etiquetado automático
0	Marcado de contenido	Desactivado
0	Prevención de pérdida de datos en	Atrás Siguiente Cancelar
ounto d	le conexión	
•	Etiquetado automático	
•	Revisar la configuración	

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:



Guía de configuración segura para Office 365

^ Detectar contenido que inclu	ya
El contenido incluve	
Agregar •	
+ Agregar grupo	
+ Agregar una condición +	
Cuando el contenido cumpla con e	stas condiciones

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.

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

<	Inicio > Tipos de información confidencial		CCN-Informacion-Confic	lencial-Tipo1 🛛 🖾
ရှိ Inicio	Los siguientes tipos de información confidencial están disponibles para que los us tipo personalizado que haya creado.	e en sus directivas de seguridad y cumplimiento. Se incluye una amplia colece	✓ Editar ✓ Tipo de prueba	1 Eliminar
≜ Alertas ✓	+ Crear		Bernindte	
д ^R Permisos	Nombre	Editor	CCN-Informacion-Confidencial-Tipo1	Editar
E Clasificación ^	CCN-Informacion-Confidencial-Tipo1	Plain Concepts S.L (CCN)	Expresión regular	Editar
Etiquetas de confidencialidad	ABA Routing Number	Microsoft Corporation	Balahaan alaun	1000
Etiquetas de retención	Argentina National Identity (DNI) Number	Microsoft Corporation	CONFIDENCIAL TOP SECRET	Cartar
Tipos de información	Australia Bank Account Number	Microsoft Corporation	Diccionario (palabras clave grandes)	Editar
confidencial	Australia Driver's License Number	Microsoft Corporation		

↑ Detectar contenido que incluya				
El contenido incluye			×	
Cualquiera de estos \vee				
Tipo de información confidencial	Número de instancias min máx.	Precisión de coincidencia min máx.		
CCN-Informacion-Confidencial-Tipo1	1 cualquiera	60 100	0 ×	
+ Agregar grupo				

Y asignamos este tipo a la *sensitivity labels*.



Guía de configuración segura para Office 365

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".

III Seguridad y cumplimien	o de Office 365	0 0 1
	Inicio > Etiguetas de confidencialidad	CCN-Etiqueta-Confidencial1
\Lambda Inicia	Riquetas Directivas de etiquetas	Z Editor etiqueta R Eliminar etiqueta
Alertas	Las etiquetas de confidencialidad se utilian para clasificar menoges de como electrónico, documentos, stisos y mucho más Cuando se aplique una etiqueta (independentemente de si la aplica el usuario o se aplica autom ejemplo, puede crear etiquetas que ciferen archivos, que agreguem marcadores de contenido y que controllen el acceso de los suarios a sitos específicos. Más información sobre se etiquetas de confidencialidad	
R ^R Permisos	+ Crear una etiqueta 🛛 Publicar etiquetas O Actualizar CON 🛛 🛪	Nombre CCN-Etiqueta-Confidencial1
E Clasificación	Autor de creación Útima model	Nombre para mostrar
Etiquetas de		CCN-Etiqueta-Confidencial1
confidencialidad Etiquetas de retención		Información sobre herramientas Editar Información sobre CCN-Etiqueta-Confidencial1
Tipos de información confidencial		Descripción Editar Descripción sobre CCN-Etiqueta-Confidencial I

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

Nueva directiva de etiqueta de confidencialidad	Elija etiquetas de confidencialidad para publicar	X
Elija las etiquetas para publicar	Cuando se publiquen, las etiquetas que elija aquí estarán disponibles en aplicaciones de Office (Word, Excel, PowerPoint y Outlook), sitios de SharePoint y Teams, y grupos de Office 365 de usuarios específicos.	
Publicar para usuarios y grupos	Publicar estas etiquetas (1 etiquetas) CCN-Etiqueta-Confidencial1	
Configuración de la directiva	Siguiente Cancelar	
Revisar la configuración		

3. Elegir usuarios o grupos.

Nueva directiva de etiqueta de confidencialidad	Publicar estas etiquetas de confidencialidad		
🥏 Elija las etiquetas para publicar	Seleccione a los usuarios o grupos (grupos de seguridad habilitados para correo, lista de distribución, grupo de O365) para quienes se deben publicar las etiquetas.		
Publicar para usuarios y grupos	Publicar en	Incluir	
Configuración de la directiva	۹д۹ Usuarios y grupos	3 usuarios o grupos	
Revisar la configuración		Elegir usuarios o grupos	
	Atrás Siguiente	Cancelar	

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.

Nueva directiva de etiqueta de confidencialidad	Configuración de la directiva	×	
🔗 Elija las etiquetas para publicar	Ahora que ha agregado una configuración de directiva personalizada, es hora de darle un nombre.		
Publicar para usuarios y grupos	CCN-Directiva-Etiqueta-Confidencial1		
Configuración de la directiva	Descripción		
Revisar la configuración	Descripción de CCN-Directiva-Etiqueta-Confidencial1		
	Atrás Siguiente Cancelar		

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.



Guía de configuración segura para Office 365

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.



Guía de configuración segura para Office 365

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].

	Centro de administración	n de Micros	oft 365			Q	٢	?	(
=			Serv	vicios y complementos					
ŵ	Inicio					_			
8	Usuarios	~	+ Imp	plementar un complemento	D Buscar	ΥFi	ltrar	=	
				Nombre 1	Descripción	А	plicacio	ones hos	it
۶٩	Grupos	~	A 33	Aplicaciones integradas	Permitir que los usuarios decidan si las aplicaciones de terceros pueden obtener acceso a su in	forma			
2	Roles		Ô	Aplicaciones y servicios propiedad del usuario	Permitir que los usuarios tengan acceso a las pruebas de Tienda Office y Office 365.				
43	Recursos	~	٥	Autenticación moderna	Activa o desactiva Autenticación moderna para toda la organización.				
	Facturación	~	5	Autenticación multifactor de Azure	Administre la configuración de la autenticación multifactor para los usuarios.				
្ច	Soporte técnico	~	Ţ	Azure Servicios de voz	Permita el uso de los correos electrónicos y los documentos de su organización para mejorar la	a prec			
0	Configuración	~	5	Bookings	Elija si desea permitir Microsoft Bookings y si Bookings puede procesar pagos de los clientes.				
	Dominios		Q	Búsqueda de Microsoft en Bing	Active o desactive el acceso a Búsqueda de Microsoft en Bing para los empleados de su compa	nñía.			
	Búsqueda de Microsoft		İ	Calendario	Permitir que los usuarios compartan sus calendarios con usuarios ajenos a la organización.				
	Servicios y complementos Seguridad y privacidad			Comunicación de Microsoft a los usuarios	Permiten a los usuarios de la organización recibir correo electrónico de Microsoft sobre formac	ión y			
	Perfil de la organización		٥	Conexión de datos de Microsoft Graph	Administrar y actualizar la configuración de Conexión de datos de Microsoft Graph				
	Relaciones con partners		$\overline{1}$	Configuración de descarga de software de Office	Elija si desea que los usuarios instalen Office aplicaciones en sus propios dispositivos.				



5. GLOSARIO Y ABREVIATURAS

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

Término	Definición			
AAD	Azure Active Directory (Directorio Activo de Azure).			
AD DS	<i>Active Directory Domain Services</i> (Servicios de dominio de Directorio Activo).			
AIP	Azure Information Protection.			
Azure AD	Azure Active Directory.			
Azure RMS	Azure Rights Management (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	Cloud Service Provider			
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	Esquema Nacional de Seguridad.			
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 movilio empresarial (EMM) basado en nube que ayuda a los empleado ser productivos mientras mantiene protegidos los da corporativos. Al igual que otros servicios de Azure, Micros Intune está disponible en el portal de Azure. Intune permite: Administrar los dispositivos móviles y los equipos que 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	Office 365.			
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	PowerShell.			
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.			



CCN-STIC 885A Guía de configuración segura para Office 365

6. 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	0						
ор	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: Si No Evidencias Recogidas: Si No	Cumple:					
Op.acc.3	Segregación de funciones y tareas							
	Se ha asignado adecuadamente los roles de administración.	Aplica:	Cumple:					


		🗌 Si	🗌 No	🗌 Si	🗌 No
		Evidencias F	Recogidas:	Observaci	ones:
		🗌 Si	🗌 No		
Op.acc.5	Mecanismo de autenticación	1		1	
	Se ha habilitado <u>Multi-Factor Authentication</u> (MFA) para los usuarios de la organización.	Aplica:		Cumple:	
		🗌 Si	🗌 No	🗖 Si	🗌 No
		Evidencias F	Recogidas:	Observaci	ones:
		🗌 Si	🗌 No		



		Evidencias Recogidas:	Observaciones:
		🗆 Si 🗌 No	
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:	Cumple:
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
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,</i> etc.).	Aplica:	Cumple:



		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	
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:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	
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.	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No



	* Si la organización dispone de <i>Office 365 Advanced Threat Protection</i> (Office 365 ATP).		
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	
op.exp.8	Registro de la actividad de los usuarios		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos.	Aplica:	Cumple:
		🗌 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
op.exp.10	Protección de los registros de actividad		1
		Aplica:	Cumple:



	Se ha securizado la consulta del registro de actividad mediante el establecimiento de los roles adecuados.	🗌 Si 🗌 No	🗌 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
		Evidencias Recogidas:	Observaciones:
		🗌 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:	Cumple:
		🗌 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
mp.info.2	Calificación de la información		
	Se han aplicado políticas de DLPs.	Aplica:	Cumple:
		🗌 Si 🗌 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	



mp.info.2	Calificación de la información		
	Se han aplicado <i>sensitivity labels.</i>	Aplica:	Cumple:
		🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
mp.info.3	Cifrado		
	Se ha aplicado un cifrado especial mediante etiquetas de sensibilidad a sitios de Sharepoint que precisan una protección especial.	Aplica:	Cumple:
	* 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> .	🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🔲 No	



mp.info.6	Limpieza de documentos		
	Se ha eliminado información personal y en general cualquier metadato que pudiera estar asociado a los documentos.	Aplica:	Cumple:
	*Mediante la herramienta Inspector de documentos (característica que se accede desde las propias aplicaciones de Word, Excel, PowerPoint o Visio) o aplicaciones de terceros.	🗌 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	
mp.info.9	Copias de seguridad		1
	Se dispone de planes específicos de copias de seguridad de la información en aquellos servicios en donde se admita.	Aplica:	Cumple:
		🗆 Si 🔲 No	🗌 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗌 Si 🗌 No	



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 sistema de defensa DDoS de Azure.	Aplica:	Cumple:	
		Evidencias Recogidas:	Observaciones:
		🗆 Si 🗌 No	
	Servicios y complementos		
	Se ha controlado los servicios y complementos disponibles para los usuarios.	Aplica:	Cumple:
		🗆 Si 🗌 No	🗆 Si 🗌 No
		Evidencias Recogidas:	Observaciones:
		🗆 Si 🔲 No	