

Guía de configuración segura para Exchange Online



MAYO 2024



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

cpage.mpr.gob.es

Edita:



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

NIPO: 083-19-260-0

Fecha de Edición: mayo de 2024

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1. EXCHANGE ONLINE	4
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA	4
1.2 DEFINICIÓN DEL SERVICIO.....	4
1.3 PREREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL	5
2. DESPLIEGUE DE EXCHANGE ONLINE.....	7
2.1 ADMINISTRADOR – CONFIGURACIÓN INICIAL.....	7
2.2 USUARIO FINAL - PRIMEROS PASOS	8
3. CONFIGURACIÓN DE EXCHANGE ONLINE.....	19
3.1 MARCO OPERACIONAL.....	19
3.1.1 CONTROL DE ACCESO	19
3.1.1.1 IDENTIFICACIÓN.....	19
3.1.1.2 REQUISITOS DE ACCESO	19
3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS	19
3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO	25
3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS)	29
3.1.1.6 MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)	30
3.1.2 EXPLOTACIÓN	30
3.1.2.1 PROTECCION FRENTE A CODIGO DAÑINO.....	30
3.1.2.2 GESTION DE INCIDENTES	32
3.1.2.3 REGISTRO DE LA ACTIVIDAD	32
3.1.3 MONITORIZACION DEL SISTEMA.....	38
3.2 MEDIDAS DE PROTECCIÓN	38
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES.....	38
3.2.2 PROTECCIÓN DE LA INFORMACIÓN	39
3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN	39
3.2.2.2 COPIAS DE SEGURIDAD.....	41
3.2.3 PROTECCIÓN DE LOS SERVICIOS	44
3.2.3.1 PROTECCIÓN DEL CORREO ELECTRÓNICO.....	44
3.2.3.2 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO	81
4. OTRAS CONSIDERACIONES DE SEGURIDAD	82
4.1 TIPOS DE BUZONES	82
4.2 REGLAS DE FLUJO DE CORREO	91
4.3 REGLAS DE ACCESO DE DISPOSITIVO Y CUARENTENA.....	92
4.4 DIRECTIVAS DE BUZON DE CORREO PARA DISPOSITIVOS MOVILES	93
4.5 DIRECTIVA DE USO COMPARTIDO	94
5. GLOSARIO Y ABREVIATURAS	96
6. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD	97

1. EXCHANGE ONLINE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración del servicio Exchange Online cumpliendo con los requisitos necesarios del Esquema Nacional de Seguridad en su categoría ALTA.

Esta guía debe usarse en conjunto con [CCN-STIC-885A - Guía de configuración segura para Office 365], donde se describen generalidades de Office 365 y características comunes a todos los servicios, así como un glosario con los términos y abreviaturas de seguridad utilizadas en estas guías.

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

- Documentación oficial de Microsoft.
- CCN-STIC-884A - Guía de configuración segura para Azure.
- CCN-STIC-885A - Guía de configuración segura para Office 365.
- ENS Real Decreto BOE-A-2010-1330.
- ENS Real Decreto BOE-A-2022-7191.

1.2 DEFINICIÓN DEL SERVICIO

Exchange Online (EXO) es la plataforma de correo electrónico incluida con Office 365, conjunto de aplicaciones y servicios basados en la nube alojados en servidores propiedad de Microsoft y disponibles desde dispositivos con conexión a Internet. Hay que destacar también que Office 365 funciona sobre Microsoft Azure.

Las principales características de Exchange Online son:

- Proporciona al usuario acceso a correo electrónico, calendario, contactos y tareas desde equipos de escritorio, dispositivos móviles y vía web.
- Posibilidad de conexión con cliente Outlook.
- Protección frente a correo no deseado y malware con Exchange Online protection.
- Completamente integrado con Entra ID.
- Los servidores EXO se alojan en Centros de Datos de Microsoft.

Los subservicios de Exchange Online involucrados en esta guía son:

- Archivado de Microsoft Exchange Online. Proporciona funcionalidad de archivado, cumplimiento.
- Protección de Microsoft Exchange Online. Servicio de filtros de emails que ayudan a proteger frente a spam y malware, y permite establecer políticas de salvaguarda de la información.

1.3 PREREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL

Instalación modulo ExchangeOnline

Para conectarse a Exchange Online PowerShell, se necesita descargar y usar el Módulo de PowerShell de Exchange Online. Para instalar el módulo ejecutar el siguiente comando:

```
Install-Module -Name ExchangeOnlineManagement
```

Para más información sobre la instalación de este módulo, ver [Conexión a Exchange Online PowerShell | Microsoft Learn](#).

Conexión modulo ExchangeOnline

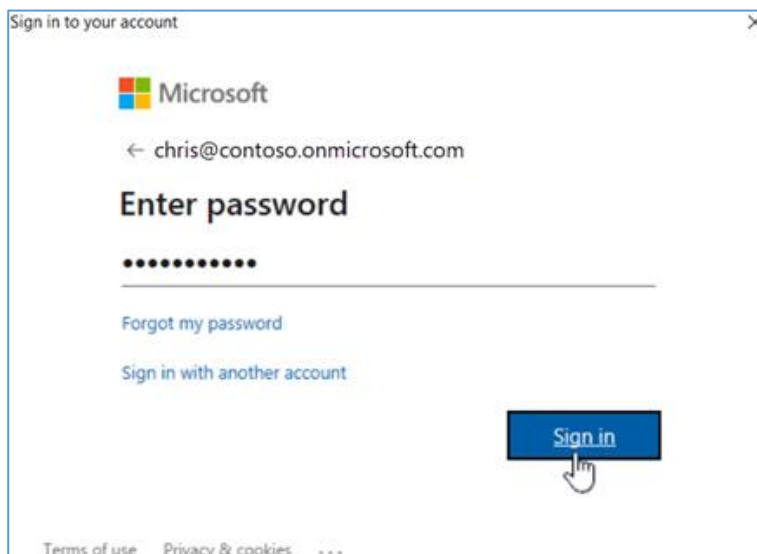
PowerShell de Office 365 permite gestionar y configurar Exchange Online desde la línea de comandos, con un usuario con derechos de administración. Consultar la guía [CCN-STIC-885A -Guía de configuración segura para Office 365].

Para administrar la configuración de Exchange Online desde la línea de comandos desde un equipo local, primero hay que establecer la conexión:

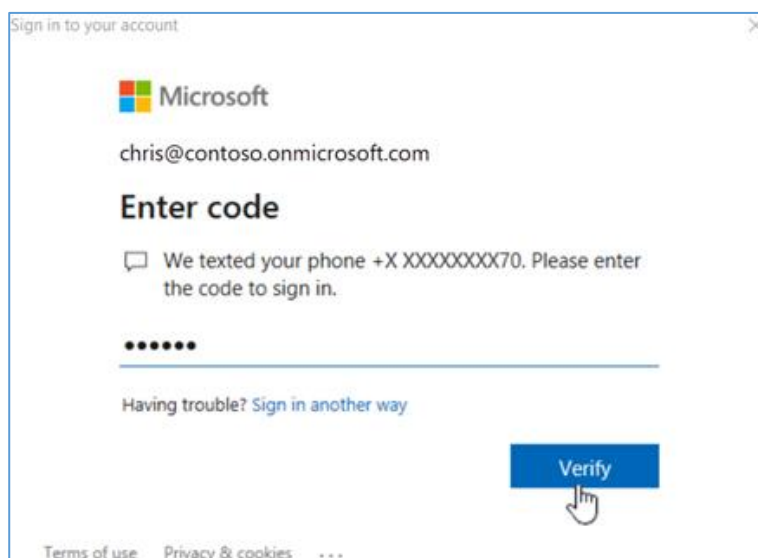
- a) Escribir las credenciales de Office 365.

```
Connect-ExchangeOnline -UserPrincipalName chris@contoso.onmicrosoft.com
```

- b) Proporcionar la configuración de conexión necesaria.



En el caso de tener MFA activado (SMS, código de verificación, notificación push, etc...), se deberá también realizar esta verificación.



- c) Al finalizar no olvidar desconectar la sesión remota.

[Disconnect-ExchangeOnline](#)

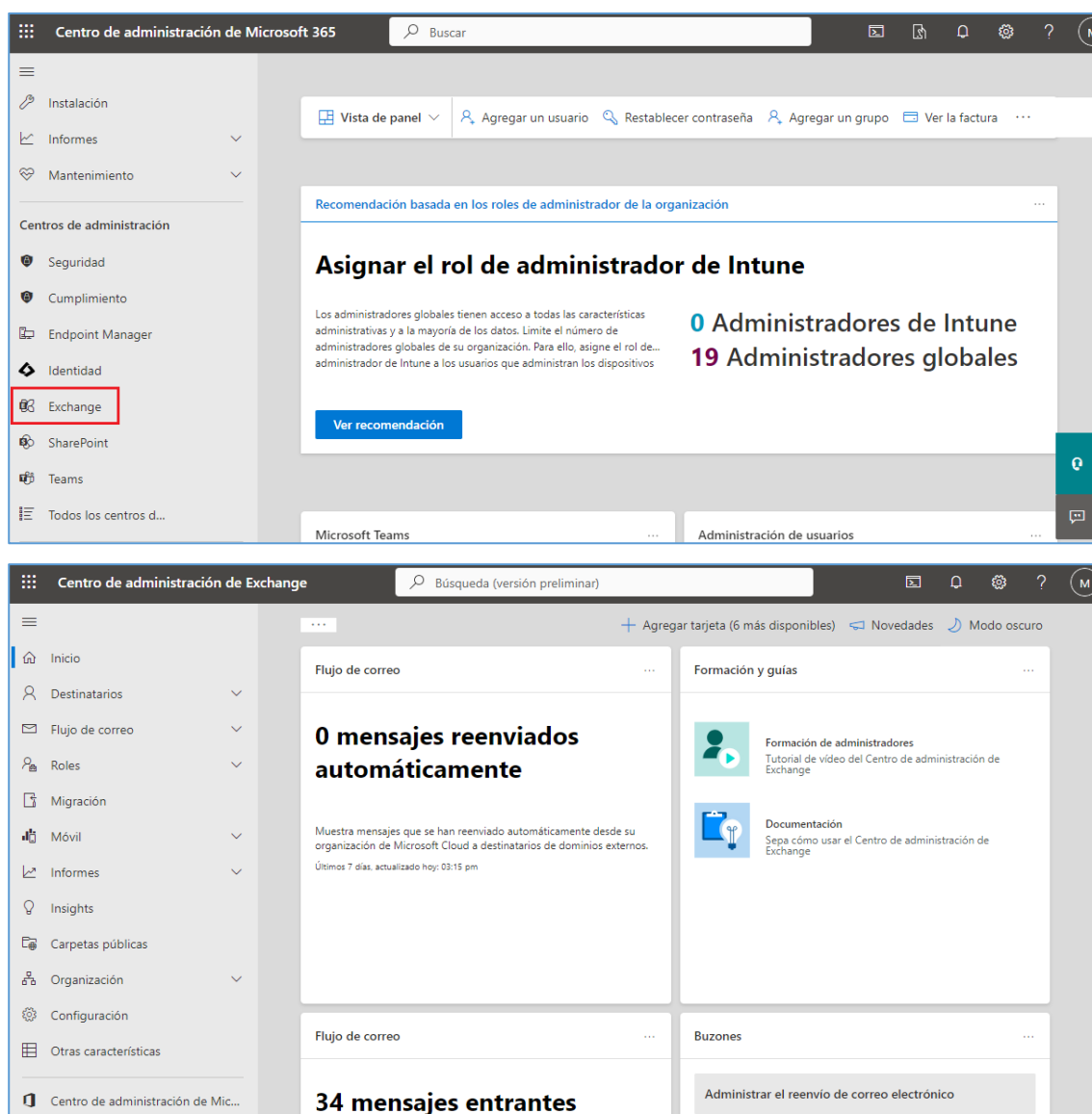
2. DESPLIEGUE DE EXCHANGE ONLINE

Exchange Online no necesita instalación previa en el entorno on-premise del cliente, ya que es un servicio on-line accesible desde internet y alojado en el tenant de Office 365 de la organización. Utiliza la infraestructura de “Nube pública” referida en la guía [823-Cloud Computing].

Exchange Online, así como el conjunto de 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

El usuario administrador podrá acceder al portal de administración de Exchange Online a través del portal de administración de Office 365 (portal.office365.com) o directamente desde la URL “<https://admin.exchange.microsoft.com/#/homepage>”.

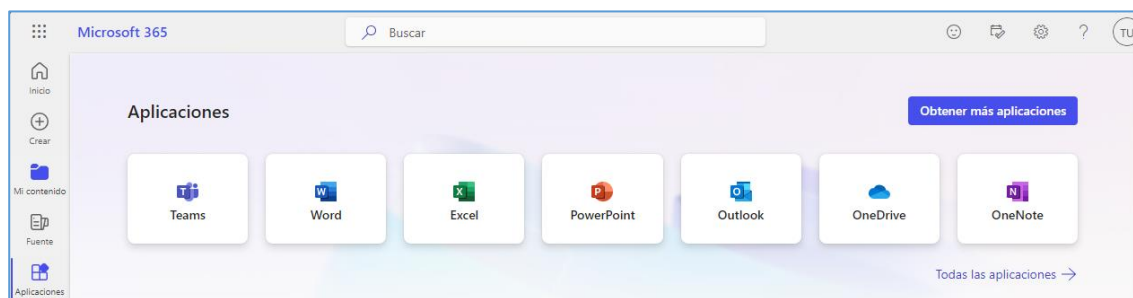


Estas son las características que figuran en el panel de navegación izquierdo.

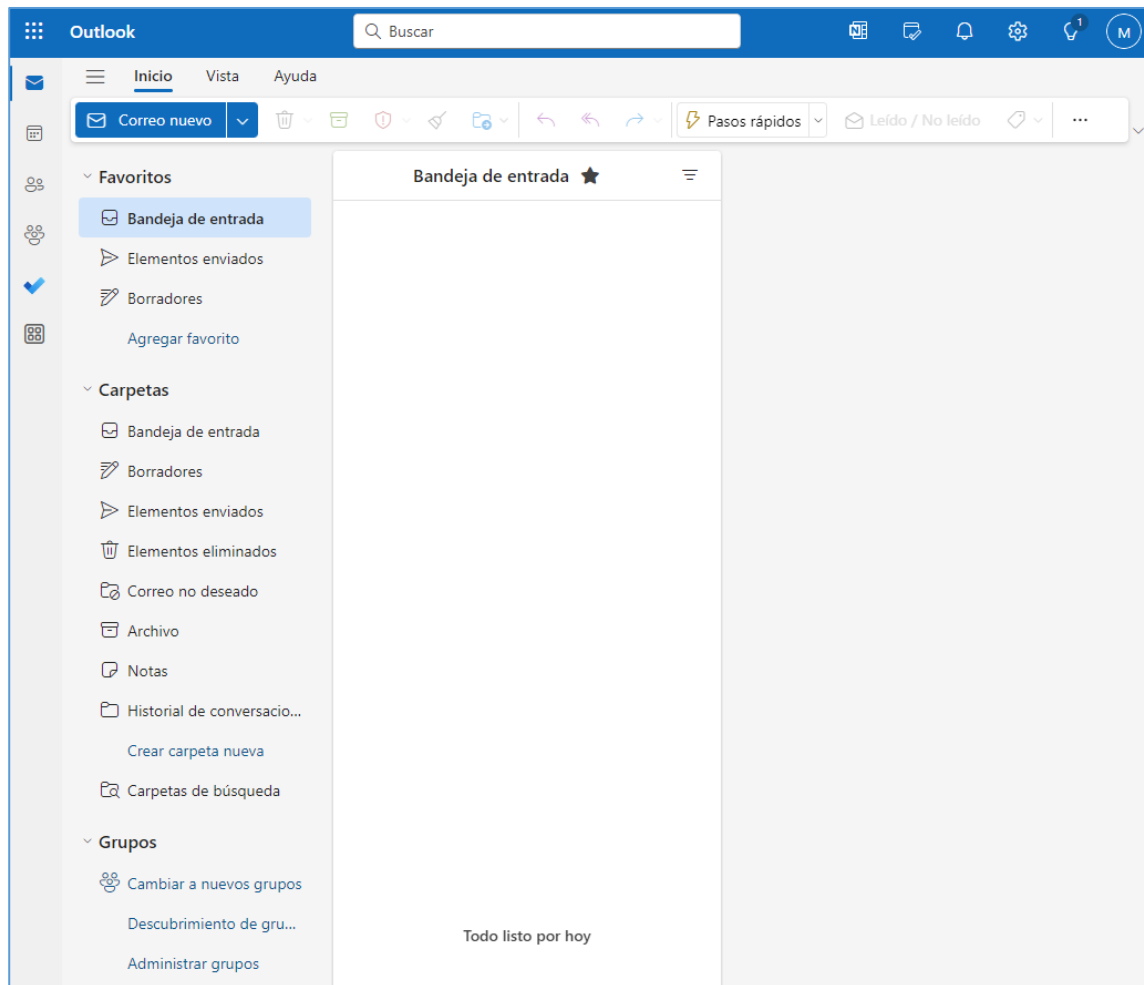
Área	Qué puede hacer aquí
Destinatarios	Ver y administrar los buzones (buzones de usuario y compartidos), grupos, buzones de recursos y contactos.
Flujo de correo	Mensajes de seguimiento; crear reglas; administrar dominios remotos y dominios aceptados; agregar conectores; y administrar alertas y directivas de alertas.
Roles	Administrar roles de administrador.
Migración	Migrar buzones en lotes.
Móvil	Administrar los dispositivos móviles que permiten conectar a la organización. Se puede administrar las directivas de acceso a dispositivos móviles y de buzones de dispositivos móviles.
Informes	Ver informes sobre el flujo de correo y los lotes de migración.
Información	Use las recomendaciones para detectar tendencias o conclusiones y realizar acciones para corregir problemas relacionados con el buzón y el flujo de correo.
Carpetas públicas	Administrar las carpetas públicas y los buzones de correo de las carpetas públicas.
Organización	Administrar el uso compartido de la organización y las aplicaciones para Outlook.

2.2 USUARIO FINAL - PRIMEROS PASOS

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

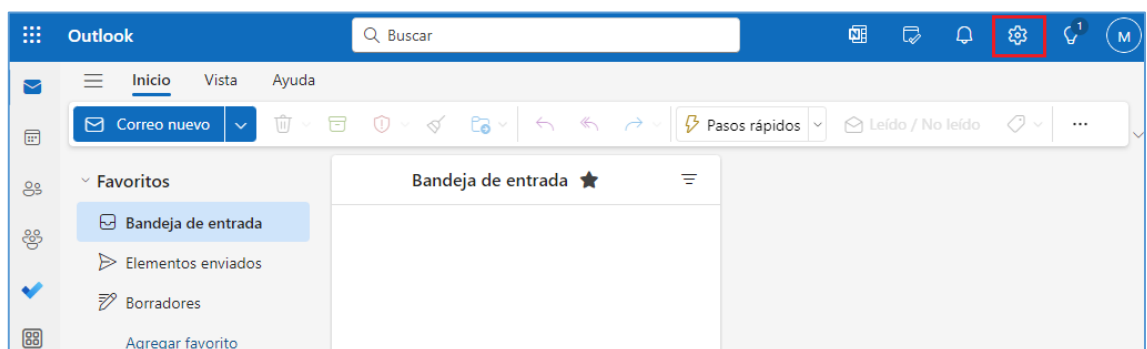


Pulsar en el icono de Outlook para acceder al cliente de correo electrónico.

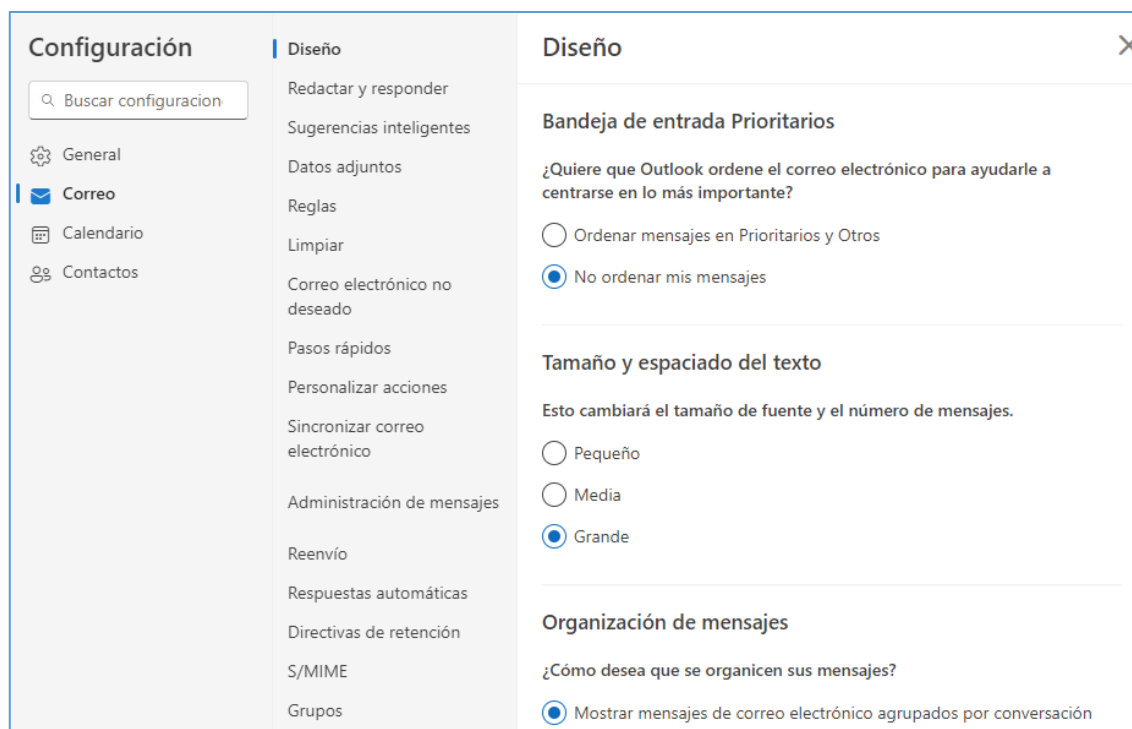


Configuración del entorno

a) Click en el menú de Configuración en el panel superior derecho:



b) Configurar opciones de las distintas categorías:



Configuración

Buscar configuración

General

Correo

Calendario

Contactos

Diseño

Redactar y responder

Sugerencias inteligentes

Datos adjuntos

Reglas

Limpiar

Correo electrónico no deseado

Pasos rápidos

Personalizar acciones

Sincronizar correo electrónico

Administración de mensajes

Reenvío

Respuestas automáticas

Directivas de retención

S/MIME

Grupos

Diseño

Bandeja de entrada Prioritarios

¿Quiere que Outlook ordene el correo electrónico para ayudarle a centrarse en lo más importante?

☐ Ordenar mensajes en Prioritarios y Otros

☒ No ordenar mis mensajes

Tamaño y espaciado del texto

Esto cambiará el tamaño de fuente y el número de mensajes.

☐ Pequeño

☐ Media

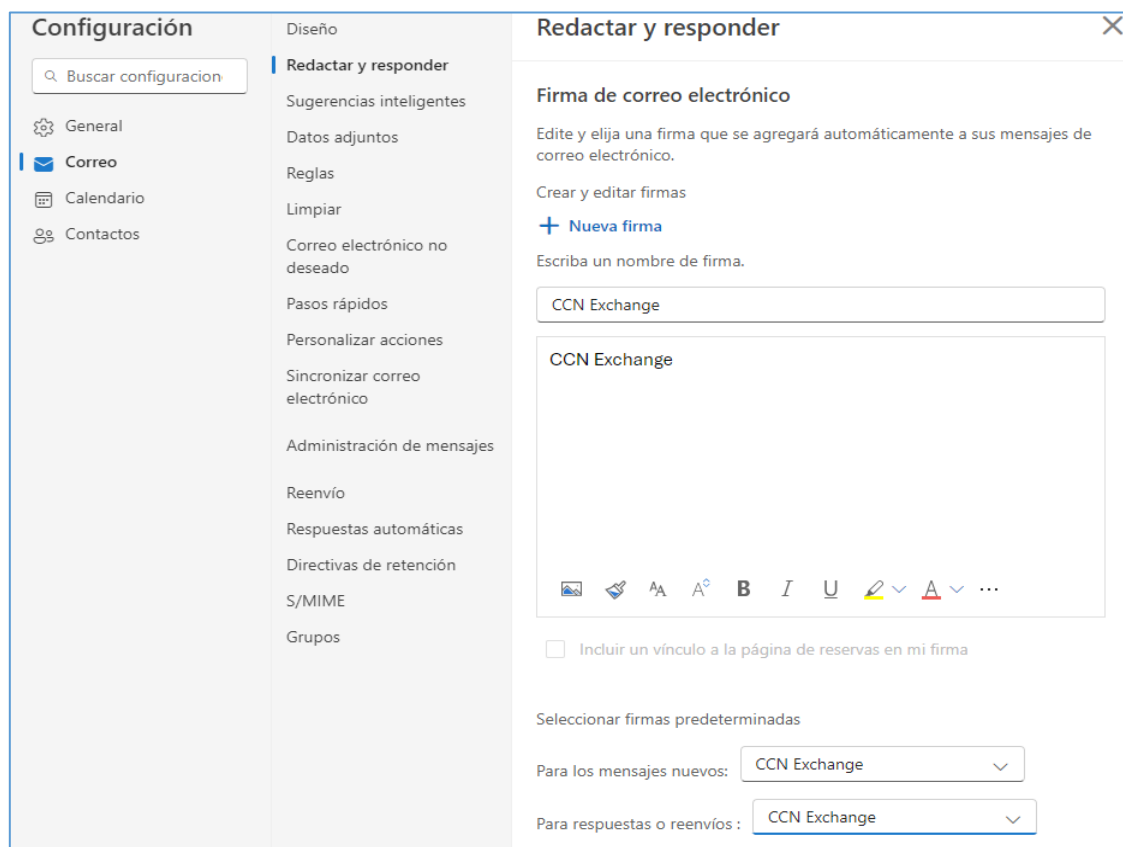
☒ Grande

Organización de mensajes

¿Cómo desea que se organicen sus mensajes?

☒ Mostrar mensajes de correo electrónico agrupados por conversación

- 1) Se recomienda definir una **“firma de correo electrónico”** e incluirla automáticamente en los correos que se redacten. Menú [Correo\Redactar y responder].



Configuración

Buscar configuración

General

Correo

Calendario

Contactos

Diseño

Redactar y responder

Sugerencias inteligentes

Datos adjuntos

Reglas

Limpiar

Correo electrónico no deseado

Pasos rápidos

Personalizar acciones

Sincronizar correo electrónico

Administración de mensajes

Reenvío

Respuestas automáticas

Directivas de retención

S/MIME

Grupos

Redactar y responder

Firma de correo electrónico

Edite y elija una firma que se agregará automáticamente a sus mensajes de correo electrónico.

Crear y editar firmas

[+ Nueva firma](#)

Escriba un nombre de firma.

CCN Exchange

CCN Exchange

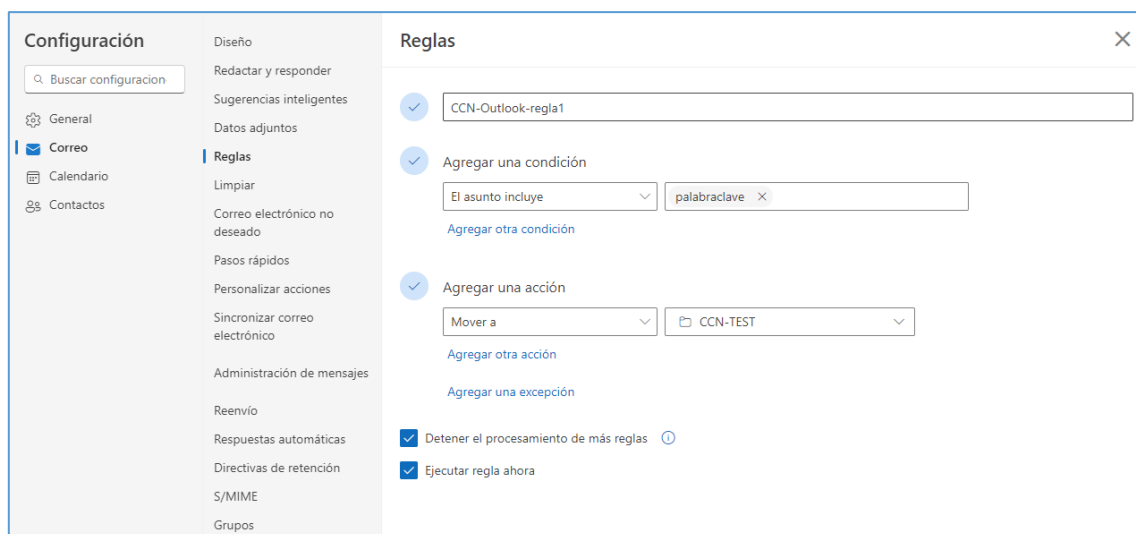
☐ Incluir un vínculo a la página de reservas en mi firma

Seleccionar firmas predeterminadas

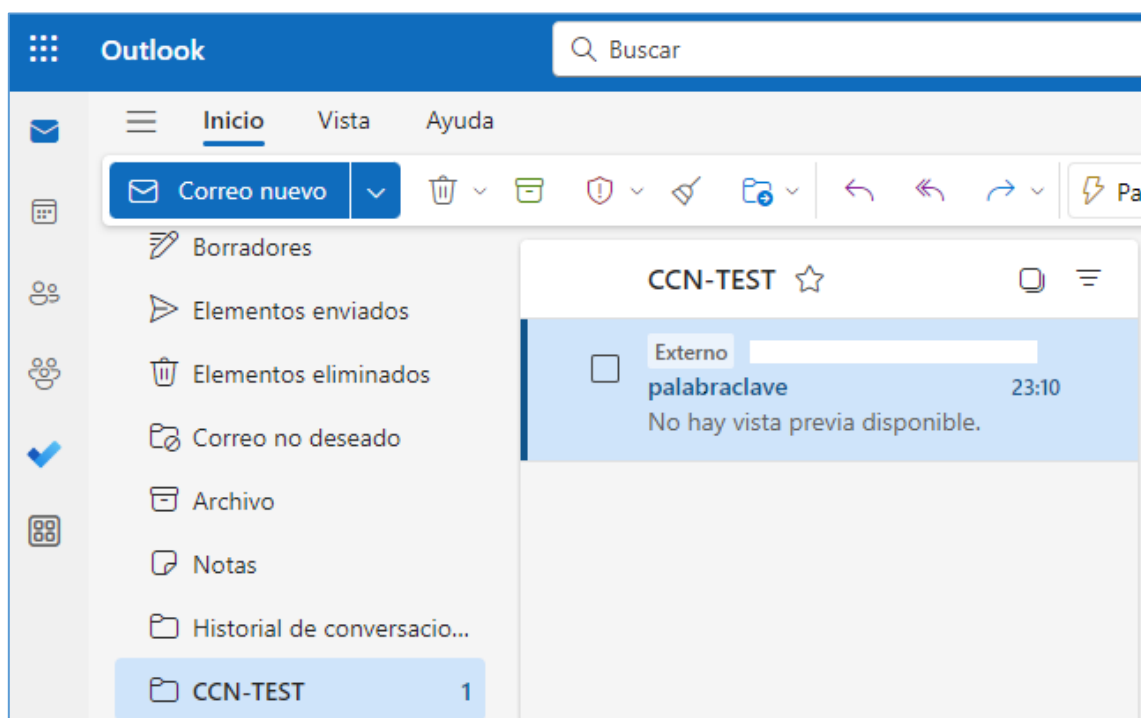
Para los mensajes nuevos: CCN Exchange

Para respuestas o reenvíos: CCN Exchange

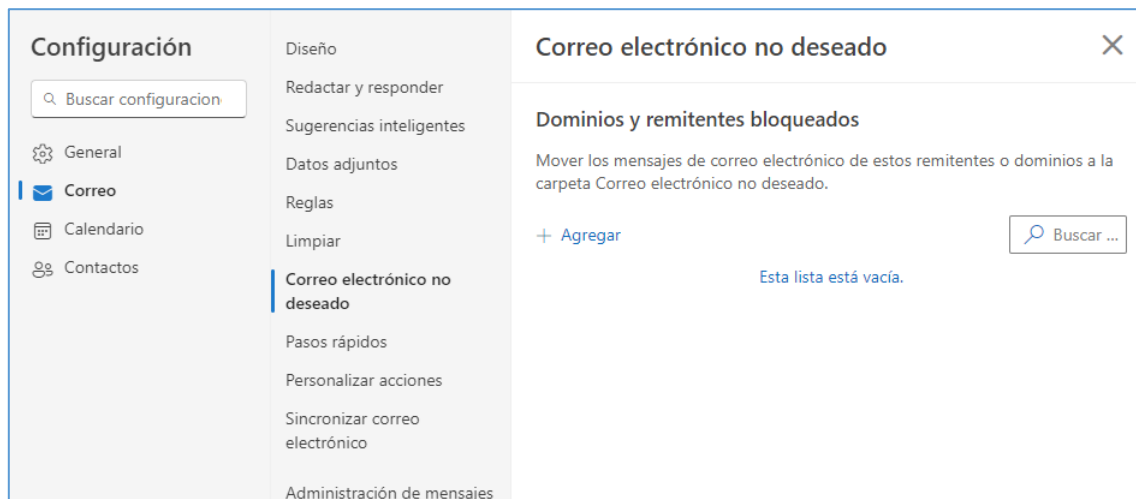
- 2) Aplicar **reglas al correo entrante**. Es posible mover, marcar, categorizar o reenviar un correo entrante en función del contenido. Menú [Correo\Reglas].



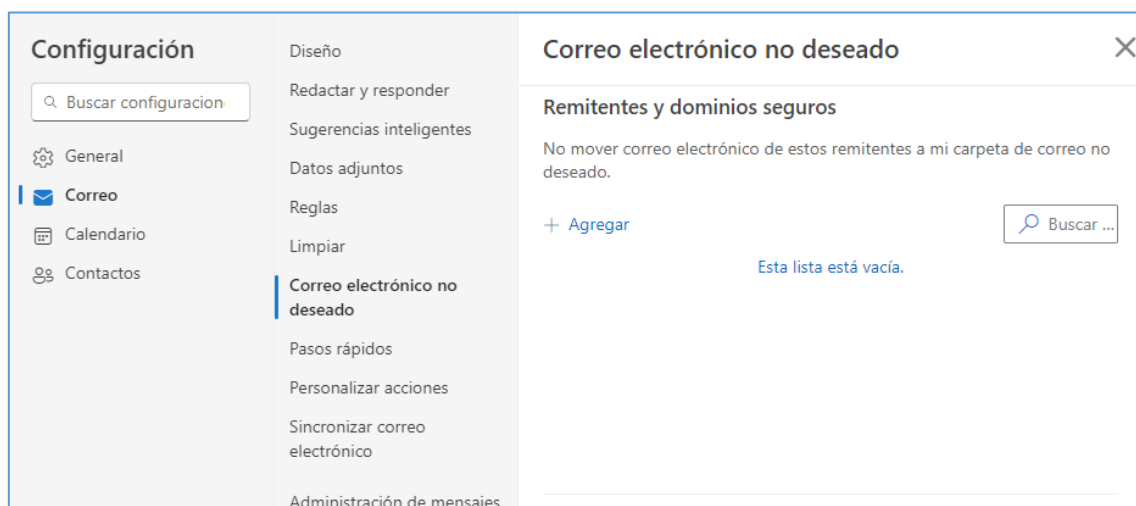
En el ejemplo, al recibir un correo que incluya en el asunto la palabra: *palabraclave*, se moverá a la carpeta CCN-TEST.



- 3) **Correo electrónico no deseado.** Menú [Correo\Correo electrónico no deseado]. Es posible especificar remitentes individuales o dominios de correos no deseados que se moverán automáticamente a la carpeta *Correo electrónico no deseado*.



También se puede establecer una lista de remitentes seguros:



Y establecer una serie de filtros en base a las opciones elegidas:

Filtros

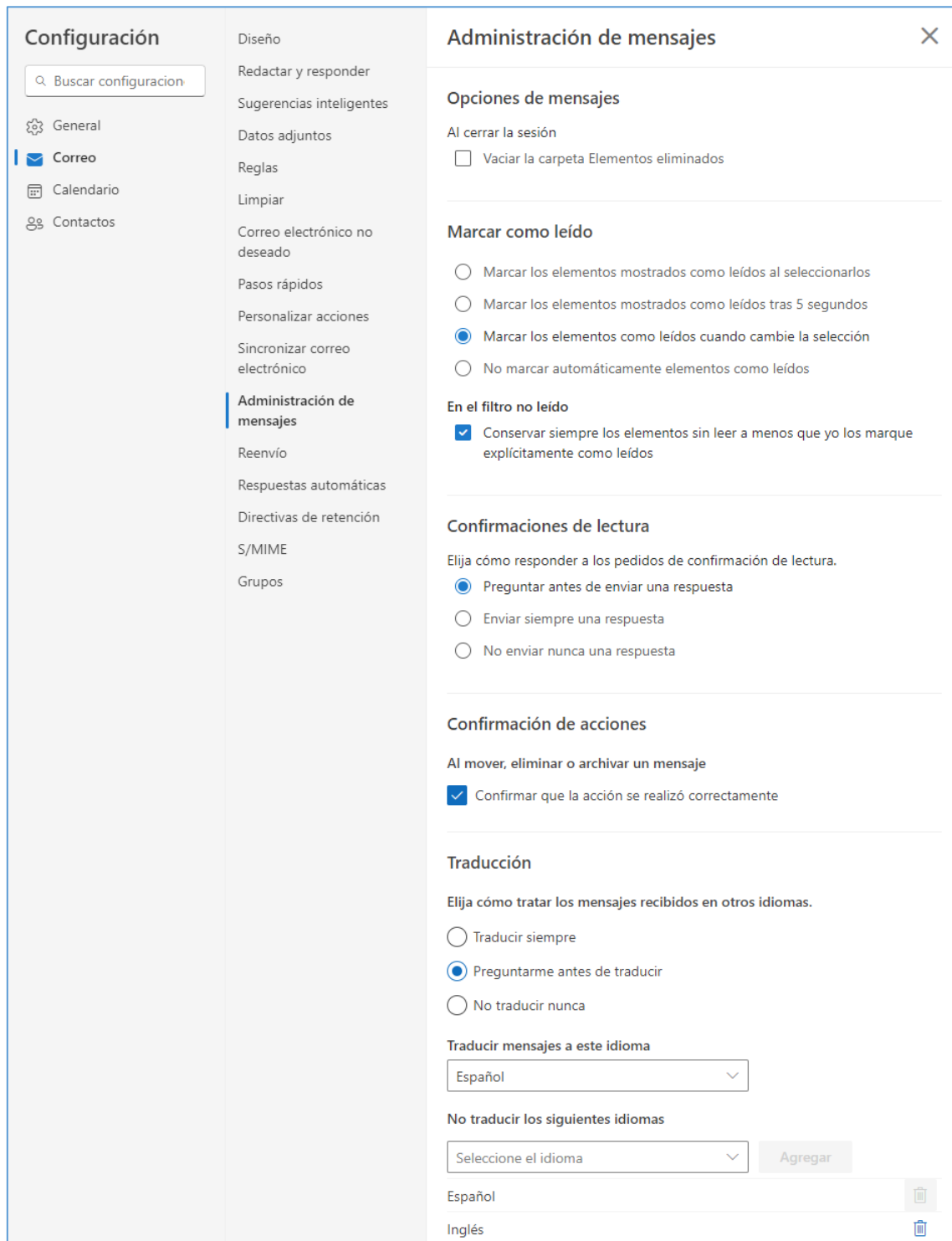
☐ Confiar solo en el correo electrónico procedente de direcciones de mi lista de remitentes y dominios seguros y listas de distribución seguras

☒ Confiar en correo electrónico de mis contactos

Creación de informes

☒ Al informar de phishing o correo no deseado, preguntarme siempre antes de enviar un informe.

- 4) **Administración de mensajes.** Menú [Correo\Administración de mensajes]. Se administran opciones interesantes como Vaciar la carpeta de Elementos eliminados al cerrar la sesión de Outlook, marcas de mensajes leídos, confirmaciones de lectura, confirmación de acciones y traducción.



The screenshot shows the 'Administración de mensajes' (Message Management) configuration window in Outlook. The left sidebar shows the 'Configuración' (Settings) menu with 'Correo' (Mail) selected. The main pane is divided into two sections: 'Administración de mensajes' and 'Traducción'.

Administración de mensajes

Opciones de mensajes

Al cerrar la sesión

☐ Vaciar la carpeta Elementos eliminados

Marcar como leído

☐ Marcar los elementos mostrados como leídos al seleccionarlos

☐ Marcar los elementos mostrados como leídos tras 5 segundos

☒ Marcar los elementos como leídos cuando cambie la selección

☐ No marcar automáticamente elementos como leídos

En el filtro no leído

☒ Conservar siempre los elementos sin leer a menos que yo los marque explícitamente como leídos

Confirmaciones de lectura

Elija cómo responder a los pedidos de confirmación de lectura.

☒ Preguntar antes de enviar una respuesta

☐ Enviar siempre una respuesta

☐ No enviar nunca una respuesta

Confirmación de acciones

Al mover, eliminar o archivar un mensaje

☒ Confirmar que la acción se realizó correctamente

Traducción

Elija cómo tratar los mensajes recibidos en otros idiomas.

☐ Traducir siempre

☒ Preguntarme antes de traducir

☐ No traducir nunca

Traducir mensajes a este idioma

Español

No traducir los siguientes idiomas

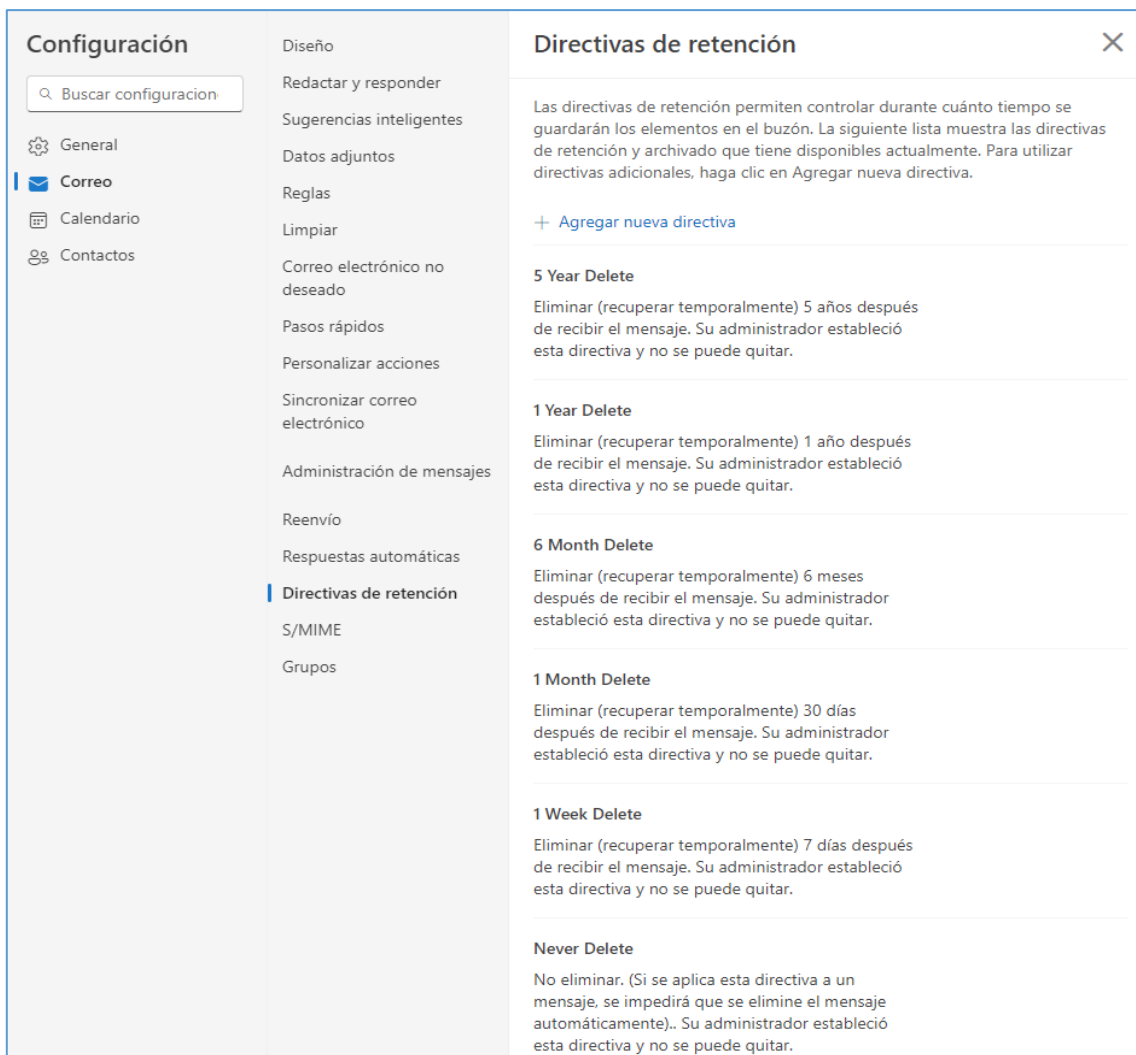
Seleccione el idioma

Agregar

Español

Inglés

- 5) **Directivas de Retención.** Menú [Correo\Directivas de retención]. Estas directivas de retención permiten establecer por cuanto tiempo se conserva el mensaje en el buzón.



Configuración

Buscar configuración

General

Correo

Calendario

Contactos

Diseño

Redactar y responder

Sugerencias inteligentes

Datos adjuntos

Reglas

Limpiar

Correo electrónico no deseado

Pasos rápidos

Personalizar acciones

Sincronizar correo electrónico

Administración de mensajes

Reenvío

Respuestas automáticas

Directivas de retención

S/MIME

Grupos

Directivas de retención

Las directivas de retención permiten controlar durante cuánto tiempo se guardarán los elementos en el buzón. La siguiente lista muestra las directivas de retención y archivado que tiene disponibles actualmente. Para utilizar directivas adicionales, haga clic en Agregar nueva directiva.

+ Agregar nueva directiva

5 Year Delete

Eliminar (recuperar temporalmente) 5 años después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.

1 Year Delete

Eliminar (recuperar temporalmente) 1 año después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.

6 Month Delete

Eliminar (recuperar temporalmente) 6 meses después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.

1 Month Delete

Eliminar (recuperar temporalmente) 30 días después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.

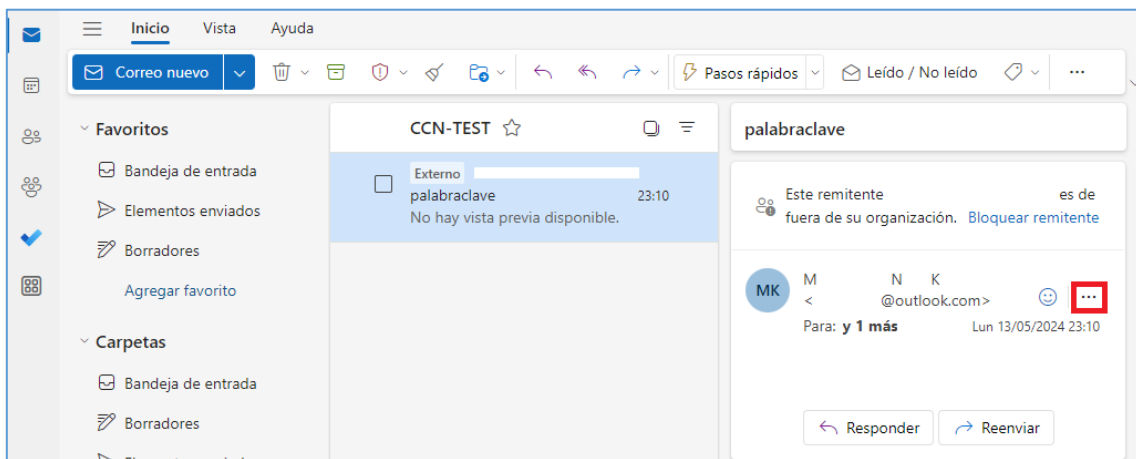
1 Week Delete

Eliminar (recuperar temporalmente) 7 días después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.

Never Delete

No eliminar. (Si se aplica esta directiva a un mensaje, se impedirá que se elimine el mensaje automáticamente). Su administrador estableció esta directiva y no se puede quitar.

Desde la bandeja de mensajes, seleccionando uno de ellos, se podrá aplicar la directiva deseada.



Inicio Vista Ayuda

Correo nuevo

Pasos rápidos

Leído / No leído

Favoritos

Bandeja de entrada

Elementos enviados

Borradores

Agregar favorito

Carpetas

Bandeja de entrada

Borradores

Elementos enviados

CCN-TEST

Externo

palabraclave

No hay vista previa disponible.

23:10

palabraclave

Este remitente es de fuera de su organización. Bloquear remitente

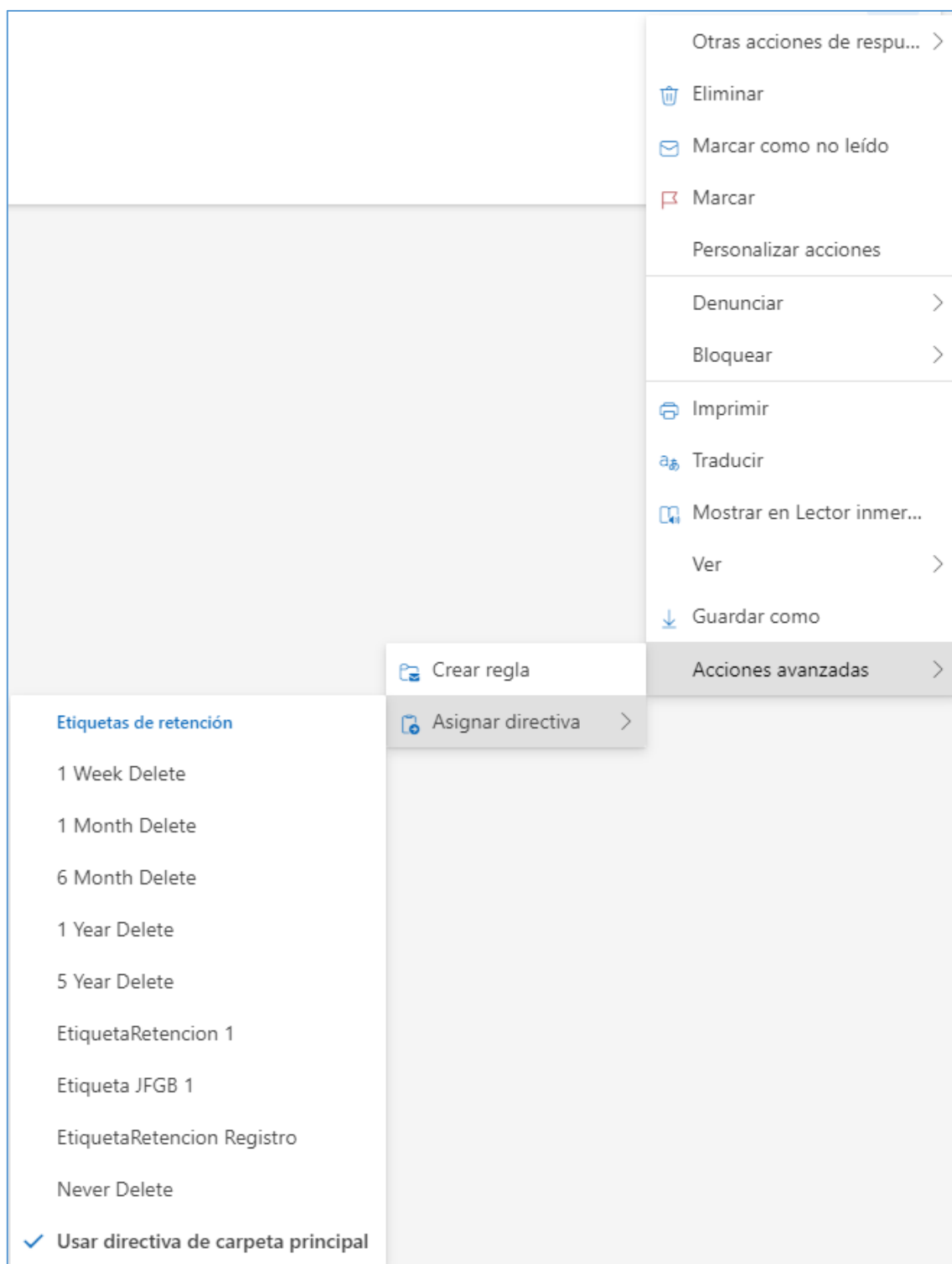
M N K

@outlook.com>

Para: y 1 más

Lun 13/05/2024 23:10

Responder Reenviar



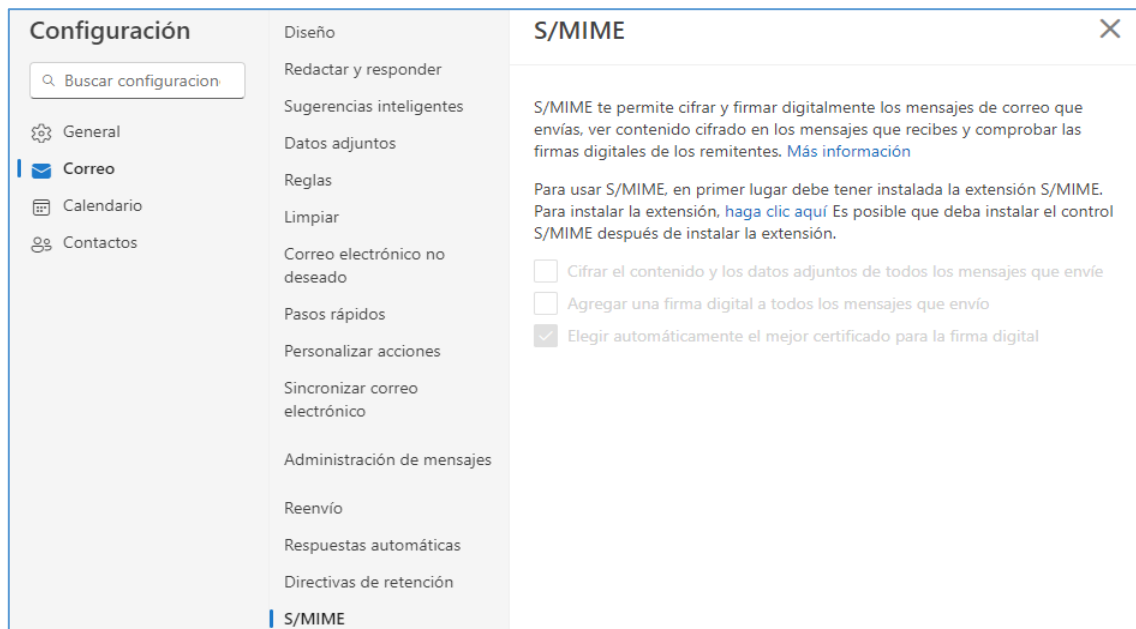
Otras acciones de respu... >

- Eliminar
- Marcar como no leído
- Marcar
- Personalizar acciones
- Denunciar >
- Bloquear >
- Imprimir
- Traducir
- Mostrar en Lector inner...
- Ver >
- Guardar como
- Acciones avanzadas >
- Crear regla
- Asignar directiva >

Etiquetas de retención

- 1 Week Delete
- 1 Month Delete
- 6 Month Delete
- 1 Year Delete
- 5 Year Delete
- EtiquetaRetencion 1
- Etiqueta JFGB 1
- EtiquetaRetencion Registro
- Never Delete
- ✓ Usar directiva de carpeta principal

- 6) **S/MIME**. Menú [Correo\S/MIME]. Permite cifrar y firmar digitalmente los mensajes de correo a enviar, ver contenido en los mensajes recibidos y comprobar las firmas digitales de los remitentes. Una firma digital garantiza a los destinatarios que el mensaje no se ha alterado.



S/MIME es una funcionalidad que el Administrador debe habilitar previamente para que esté disponible. Usar los cmdlets `Get-SmimeConfig` y `set-SmimeConfig` para ver y administrar esta característica en Exchange Online PowerShell. Más información:

[Set-SmimeConfig \(ExchangePowerShell\) | Microsoft Learn](#)

- 7) **Grupos**. Menú [Correo\Grupos]. Se puede seleccionar el envío de una copia de correo electrónico cada vez que se envía un email a un grupo del cual se es miembro.



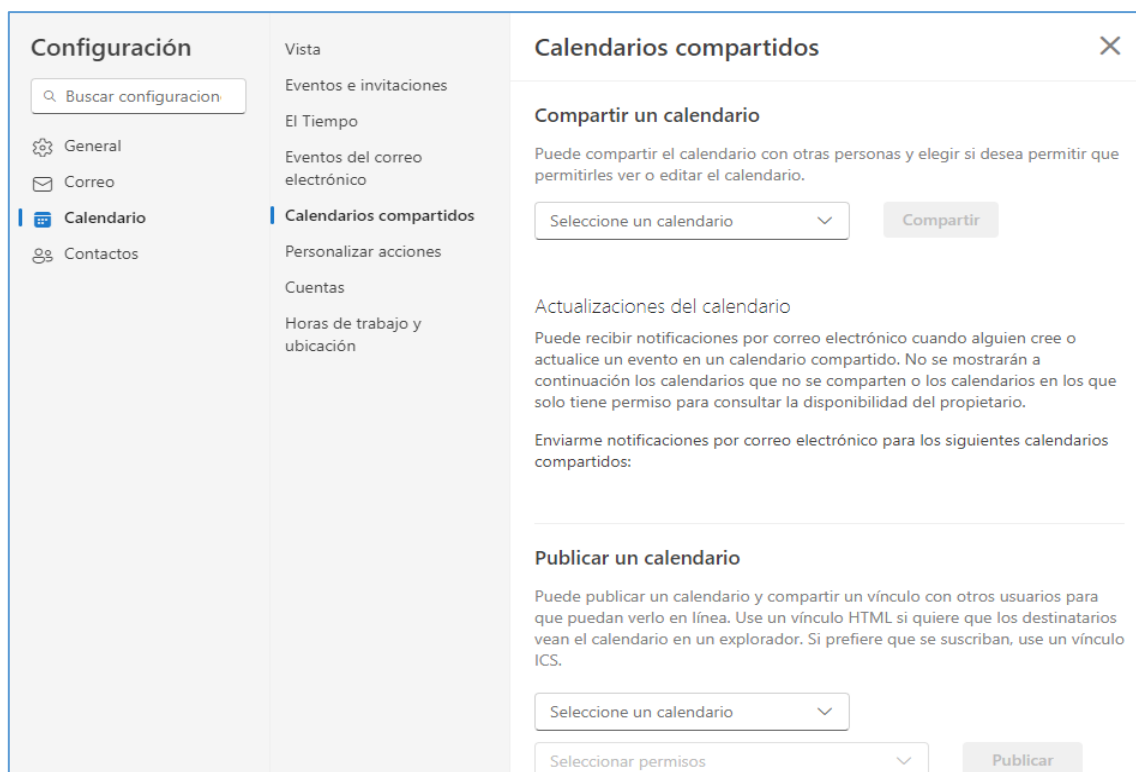
8) **Eventos e invitaciones.** Menú [Calendario\Eventos y notificaciones].

Configuración	Vista	Eventos e invitaciones
Buscar configuración General Correo Calendario Contactos	Eventos e invitaciones El Tiempo Eventos del correo electrónico Calendarios compartidos Personalizar acciones Cuentas Horas de trabajo y ubicación	Eventos que cree Personalice la configuración de los eventos que cree. ☒ Agregar reunión en línea a todos los eventos Elegir un proveedor de reuniones ☒ Microsoft Teams Aviso predeterminado 15 minutos antes ☐ Reducir la duración de todos los eventos Invitaciones de otras personas Controle cómo se administran las invitaciones, las respuestas y las notificaciones. ☒ Eliminar invitaciones que haya actualizado el organizador ☐ Eliminar las notificaciones sobre eventos reenviados Guardar eventos rechazados ☐ Muestra los eventos rechazados en el calendario; se mostrará como libre.

9) **Eventos de correo electrónico.** Menú [Calendario\Eventos de correo electrónico].

Configuración	Vista	Eventos del correo electrónico
Buscar configuración General Correo Calendario Contactos	Eventos e invitaciones El Tiempo Eventos del correo electrónico Calendarios compartidos Personalizar acciones Cuentas Horas de trabajo y ubicación	Outlook puede agregar automáticamente eventos como vuelos de compañías aéreas y otras reservas desde su correo electrónico a su calendario. Puede eliminar los eventos que no quiera en su calendario o usar la siguiente configuración para dejar de agregar eventos desde el correo electrónico. ☒ Marcar eventos como privados en mi calendario para que solo yo los pueda ver Agregar estos eventos del correo electrónico a mi calendario: Entregas de paquete Mostrar los resúmenes de eventos en el correo electrónico solamente Reserva de vuelos Mostrar el resumen de eventos en el correo electrónico y en el calendario Reservas de hoteles Mostrar el resumen de eventos en el correo electrónico y en el calendario Reservas de alquiler de coches Mostrar el resumen de eventos en el correo electrónico y en el calendario Nota: Si desactiva los eventos del correo electrónico, los eventos que ya se han agregado a su calendario no se eliminarán, y sus resúmenes seguirán apareciendo en el correo electrónico.

- 10) **Calendarios compartidos.** Menú [Calendario\Calendarios compartidos].
Permite especificar con quién se comparte el calendario y que permisos tendrá sobre el mismo.



Configuración

Buscar configuración

General

Correo

Calendario

Contactos

Vista

Eventos e invitaciones

El Tiempo

Eventos del correo electrónico

Calendarios compartidos

Personalizar acciones

Cuentas

Horas de trabajo y ubicación

Calendarios compartidos

Compartir un calendario

Puede compartir el calendario con otras personas y elegir si desea permitir que permitan ver o editar el calendario.

Seleccione un calendario

Compartir

Actualizaciones del calendario

Puede recibir notificaciones por correo electrónico cuando alguien cree o actualice un evento en un calendario compartido. No se mostrarán a continuación los calendarios que no se comparten o los calendarios en los que solo tiene permiso para consultar la disponibilidad del propietario.

Enviarme notificaciones por correo electrónico para los siguientes calendarios compartidos:

Publicar un calendario

Puede publicar un calendario y compartir un vínculo con otros usuarios para que puedan verlo en línea. Use un vínculo HTML si quiere que los destinatarios vean el calendario en un explorador. Si prefiere que se suscriban, use un vínculo ICS.

Seleccione un calendario

Seleccionar permisos

Publicar

3. CONFIGURACIÓN DE EXCHANGE ONLINE

A continuación, se abordará la configuración del servicio Exchange Online centrándose en el cumplimiento de los requisitos del Esquema Nacional de Seguridad que aplican exclusivamente a este servicio.

3.1 MARCO OPERACIONAL

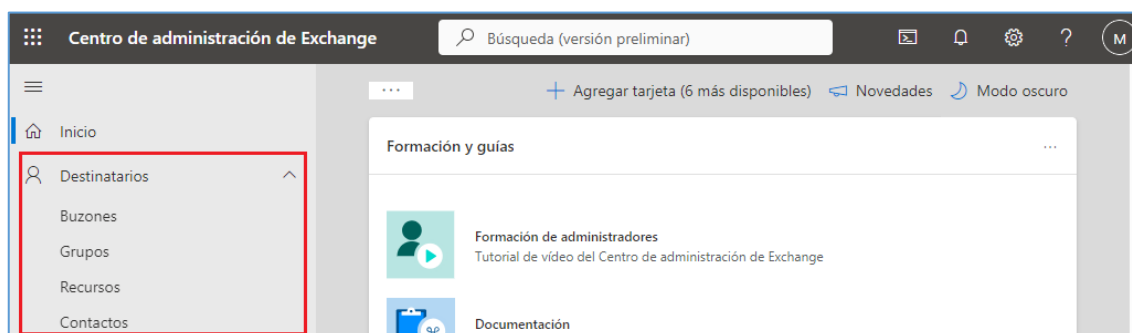
3.1.1 CONTROL DE ACCESO

3.1.1.1 IDENTIFICACIÓN

La gestión de identidades de Exchange Online es común a todas las aplicaciones de la solución Office 365 y se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.1.2 REQUISITOS DE ACCESO

En el Centro de administración de Exchange se pueden visualizar y administrar buzones de correo, grupos, buzones de recursos, contactos, buzones de correo compartidos. Así por ejemplo se podrán establecer permisos para acceder a un buzón compartido, especificando los usuarios delegados capaces de iniciar sesión en el buzón compartido y si se les permite "enviar como" en nombre de dicho buzón. Para ampliar información consultar el apartado [4.1 Tipos de buzones].



3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Exchange Online de Office 365 incluye una amplia variedad de permisos predefinidos, basados en el modelo de permisos Control de acceso basado en roles (RBAC), que permite conceder de forma fácil permisos a los **administradores y usuarios**.

- **Roles de administración:** estos roles contienen permisos que se pueden asignar a los administradores o usuarios especialistas mediante grupos de roles que administran una parte de la organización de Exchange Online, como los destinatarios o la administración de cumplimiento.
- **Roles de usuario final:** estos roles, que se asignan mediante directivas de asignación de roles, permiten a los usuarios administrar aspectos de su

propio buzón y de los grupos de distribución de los que son propietarios. Los roles de usuario final empiezan por el prefijo **My**.

Grupos de roles y directivas de asignación de roles

Los roles de administración conceden permisos para realizar tareas en Exchange Online, pero se necesita un método sencillo para asignar los roles a administradores y usuarios. Exchange Online ofrece las siguientes características para ayudar a hacer las asignaciones:

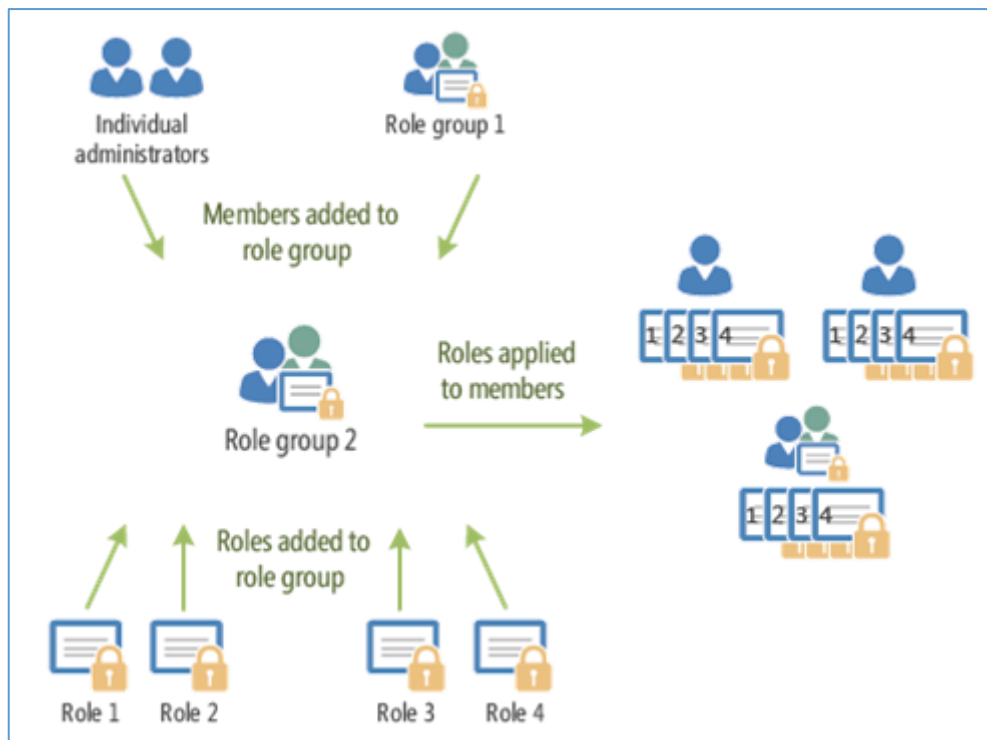
- **Grupos de roles:** los grupos de roles permiten conceder permisos a administradores y usuarios especialistas.
- **Directivas de asignación de roles:** las directivas de asignación de roles permiten conceder permisos a los usuarios finales para cambiar la configuración de su propio buzón o de los grupos de distribución de los que son propietarios.

En las secciones siguientes se muestra más información sobre los grupos de roles y las directivas de asignación de roles.

Grupos de roles

Para que sea más sencillo asignar varios roles a un administrador, Exchange Online incluye grupos de roles. Los grupos de roles suelen abarcar áreas de administración más amplias, como la administración de destinatarios. Solo se usan con roles de administración, es decir, no pueden usarse con roles de usuario final. Los miembros de los grupos de roles pueden ser usuarios de Exchange Online y otros grupos de roles.

En la figura siguiente se ve la relación entre usuarios, grupos de roles y roles.



Exchange Online incluye varios grupos de roles integrados, cada uno de los cuales da permisos para administrar áreas concretas de Exchange Online. Algunos grupos de roles pueden solaparse con otros grupos. En la tabla siguiente se explica el uso de cada uno de los grupos de roles.

Grupo de funciones	Descripción
Administración de cumplimiento	Los miembros pueden configurar y administrar la configuración de cumplimiento en Exchange de acuerdo con sus directivas.
Discovery Management	Los miembros pueden realizar búsquedas de buzones de correo en la organización de Exchange Online para obtener datos que cumplan criterios específicos y también puedan configurar retenciones legales en buzones.
Servicio de asistencia	Los miembros pueden ver y administrar la configuración de destinatarios individuales y ver destinatarios en una organización de Exchange. Los miembros de este grupo de roles solo pueden administrar la configuración que cada usuario puede administrar en su propio buzón.
Administración de higiene	Los miembros pueden administrar las características contra correo no deseado de Exchange, conceder permisos para que los productos antivirus se integren con Exchange y administrar las reglas de flujo de correo.
Administración de la organización	Los miembros tienen acceso administrativo a toda la organización Exchange Online y pueden realizar casi cualquier tarea en Exchange Online.
Recipient Management	Los miembros tienen acceso administrativo para crear o modificar Exchange Online destinatarios dentro de la organización Exchange Online.
Records Management	Los miembros pueden configurar características de cumplimiento, como etiquetas de directiva de retención, clasificaciones de mensajes y reglas de flujo de correo.
Administrador de seguridad	La pertenencia a este grupo de roles se sincroniza entre servicios y se administra de forma centralizada. No puede administrar este grupo de roles en Exchange Online. Puede agregar miembros a este grupo de roles agregando usuarios al rol de administrador de seguridad de Microsoft Entra en el Centro de administración de Microsoft 365.
Lector de seguridad	La pertenencia a este grupo de roles se sincroniza entre servicios y se administra de forma centralizada. No puede administrar este grupo de roles en Exchange Online.
UM Management	Los miembros pueden administrar las características y la configuración de mensajería unificada (UM) de Exchange.
Administración de la organización de solo visualización	Los miembros pueden ver las propiedades de cualquier objeto de la organización Exchange Online.

Estos grupos de roles se muestran en el Centro de Administración de Exchange, menú [permisos].

- Acceder al Centro de Administración de Exchange como se describe en el apartado [2.1. Administrador – configuración inicial].
- En el menú de la izquierda seleccionar la opción [Roles\Roles de administrador].

Roles	Grupo de roles ↑	Descripción
Roles de administrador	Addresslist	
Roles de usuario	AddresslistViewOnly	
Directivas de Outlook Web App	Communication Compliance	Viewer of communication compliance that can access the available reports and widgets.
Migración	Communication Compliance Adminis...	Investigators of insider risk management that can triage alerts, investigate and action on cases as well as explore content.
Móvil	Compliance Administrator	Perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.
Informes	Compliance Management	This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.
Insights	ComplianceAdmins_707264093	Members of this management role group can perform Outlook.com support Partners tier 9 activities.
Carpets públicas	Discovery Management	Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.
Organización	ExchangeServiceAdmins_-263732468	Membership in this role group is synchronized across services and managed centrally. This role group is not manageable through Microsoft Exchange. Members of this role group include Exchange-Online service administrators only. By default, this group may not be assigned any roles. However, it will be a member of the Organization Management role group and will inherit the capabilities of that role group.
Configuración	GlobalReaders_-927977443	View reports, alerts, and settings of security and compliance features.
Otras características	Help Desk	Members of this management role group can view and manage the configuration for individual recipients and view recipients in an Exchange organization. Members of this role group can only manage the configuration each user can manage on his or her own mailbox. Additional permissions can be added by assigning additional management roles to this role group.
Centro de administración de Mic...		

Crear nuevos grupos de roles

- Desde [Roles/Roles de administrador], pulsar el botón “Agregar grupos de roles” para crear un nuevo rol de administrador.

Roles de administrador

Los grupos de roles de administrador conceden permiso a los usuarios para ver datos, completar tareas y usar los cmdlets de PowerShell en el Centro de administración de Exchange. Conceda a los usuarios solo el acceso que necesiten mediante la asignación del rol menos permisivo. [Más información sobre la administración de grupos de roles](#)

 Agregar grupo de roles
 36 elementos



b) Asignar nombre, descripción y el ámbito.

Roles de administrador > Agregar grupo de roles

Datos básicos

Permiso

Administradores

Revisar y finalizar

Configurar los datos básicos

Para empezar, rellene información básica acerca del grupo de funciones que está creando.

Nombre *

Descripción

Ámbito de escritura ①

c) Seleccionar los permisos que tendrá el grupo de roles.

Roles de administrador > Agregar grupo de roles

☒ Datos básicos

Permiso

Administradores

Revisar y finalizar

Agregar permisos

Seleccione los roles que se van a agregar al grupo de roles de CCN-Grupo-Roles1. Las funciones definen el ámbito de las tareas que los miembros asignados a este grupo de roles tienen permiso para administrar.

80 elementos

☐	Rol ↑	Descripción	Ámbito de destinari...	Ámbito de configuraci...
☐	Address List (View-Only)		Organization	OrganizationConfig
☐	Address Lists	This role enables administrators to manage address lists, global address lists, and offline address lists in an organization.	Organization	OrganizationConfig
☐	Application Calendars.Read	Allows the app to read events of all calendars without a signed-in user	Organization	None
☐	Application Calendars.Rea...	Allows the app to create, read, update, and delete events of all calendars without a signed-in user	Organization	None
☐	Application Contacts.Read	Allows the app to read all contacts in all mailboxes without a signed-in user.	Organization	None

Volver **Siguiente** Cancelar

- d) Seleccionar los usuarios que serán miembros de este grupo.

Roles de administrador > Agregar grupo de roles

✓ Datos básicos

✓ Permiso

● Administradores

✓ Revisar y finalizar

Asignar administradores

Seleccione los usuarios que desea asignar a este grupo de roles. Tendrán permisos para administrar los roles que asignó en el paso anterior.

Miembros

Buscar por nombre o por dirección de correo electrónico

ccn-user

×

- e) Revisar y finalizar.

Roles de administrador > Agregar grupo de roles

✓ Datos básicos

✓ Permiso

✓ Administradores

● Revisar y finalizar

Revisar el grupo de roles y finalizar

Le recomendamos dar a conocer a los miembros del grupo de roles cómo les afectarán estos cambios.

Datos básicos
Nombre: CCN-Grupo-Roles1
Descripción: CCN-Grupo-Roles1
Ámbito de escritura: Default
[Editar los datos básicos](#)

Permisos
Address Lists, Application Calendars.Read, Application Calendars.ReadWrite
[Editar permisos](#)

Administradores
[Editar administradores](#)

Modificación de grupos de roles

- a) Click en el nombre del Rol y se abrirá un menú donde se puede cambiar la descripción, miembros y los permisos.



Permisos de Exchange Online en Office 365

Al crear un usuario en Office 365, se pueden asignar varios roles de administración, algunos de los cuales conceden al usuario permisos de administración en Exchange Online. Consultar guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Directivas de asignación de roles

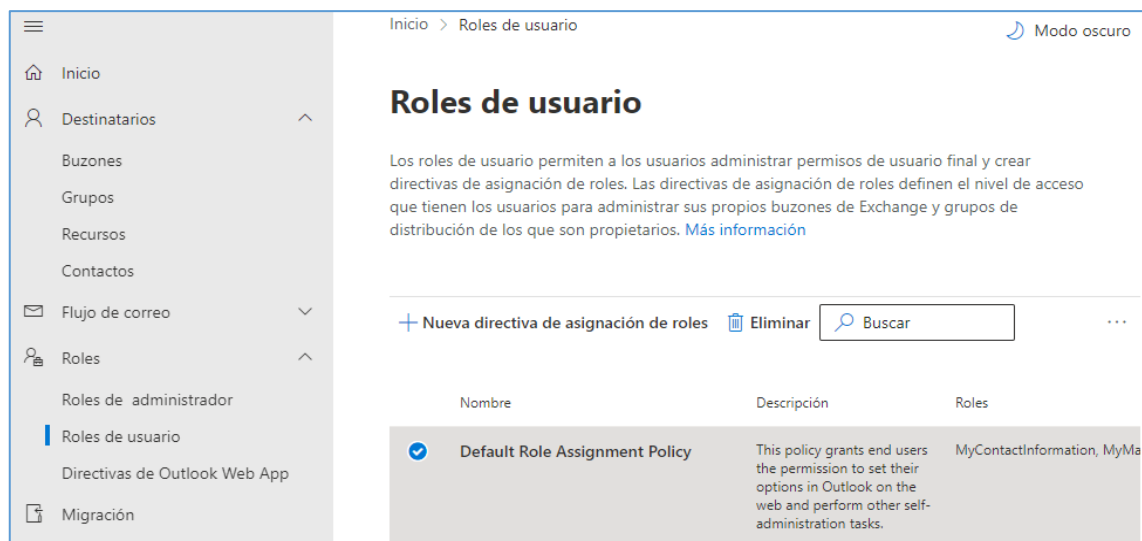
Exchange Online ofrece directivas de asignación de roles que permiten controlar las opciones que los usuarios pueden configurar en sus propios buzones y en los grupos de distribución que tienen. Estas opciones incluyen el nombre para mostrar, la información de contacto, la configuración del correo de voz y la pertenencia a grupos de distribución.

La organización de Exchange Online puede tener varias directivas de asignación de roles que ofrecen distintos niveles de permisos para los diversos tipos de usuarios de las organizaciones. Una de las directivas de asignación de roles de la organización se marca como predeterminada.

Estas directivas de asignación de roles se muestran en el Centro de Administración de Exchange, menú [Roles].

- a) Acceder al Centro de Administración de Exchange como se describe en el apartado [2.1. Administrador – configuración inicial].

b) En el menú de la izquierda seleccionar la opción [Roles\Roles de usuarios].



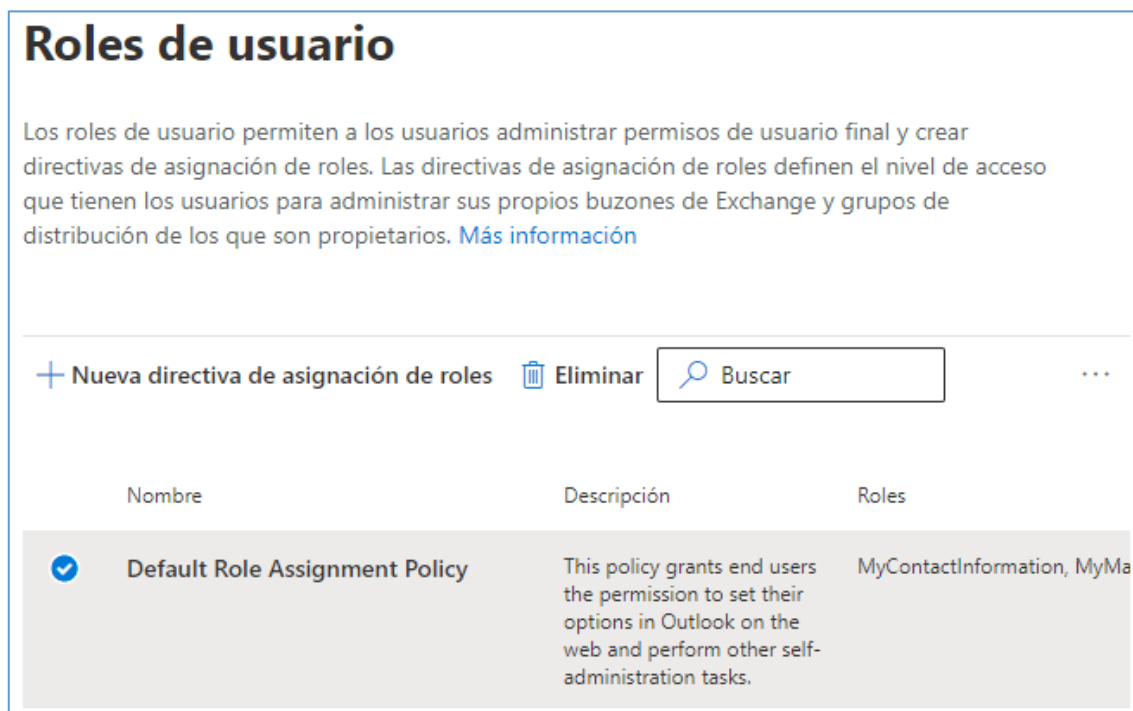
Por defecto está definida la directiva “Default Role Assignment Policy”, con las siguientes características:

Rol	Descripción
MyContactInformation	Permite a los usuarios modificar su información de contacto, incluida la dirección y los números de teléfono.
MyProfileInformation	Permite modificar el nombre, la inicial intermedia, el apellido y el nombre para mostrar en la GAL.
MyDistributionGroups	Crear nuevos grupos de distribución, eliminar los grupos de su propiedad, modificar los grupos de su propiedad y administre la pertenencia a grupos para los grupos de su propiedad.
MyDistributionGroup Membership	Unirse o dejar grupos de distribución existentes (si el grupo está configurado para permitir que los miembros se unan o abandonen el grupo).
My Custom Apps	Instalar aplicaciones personalizadas.
My Marketplace Apps	Instalar aplicaciones del Marketplace
My ReadWriteMailbox Apps	Instalar aplicaciones con permisos ReadWriteMailbox.
MyBaseOptions	Permite a los usuarios ver y modificar la configuración básica de su propio buzón y las configuraciones asociadas.
MyMailSubscriptions	Permite a los usuarios ver y modificar la configuración de su suscripción de correo electrónico, como el formato de mensaje y los valores predeterminados del protocolo.
MyRetentionPolicies	Permite a los usuarios agregar etiquetas personales que no forman parte de su directiva de retención asignada.
MyTextMessaging	Este rol permite que los usuarios creen, vean y modifiquen

	su configuración de mensajería de texto.
MyVoiceMail	Este rol permite que los usuarios vean y modifiquen su configuración de correo de voz.

Crear directivas de asignación de roles

- a) Desde [Roles/Roles de usuario], pulsar el botón “Nueva directiva de asignación de roles” para crear un nuevo rol de usuario.



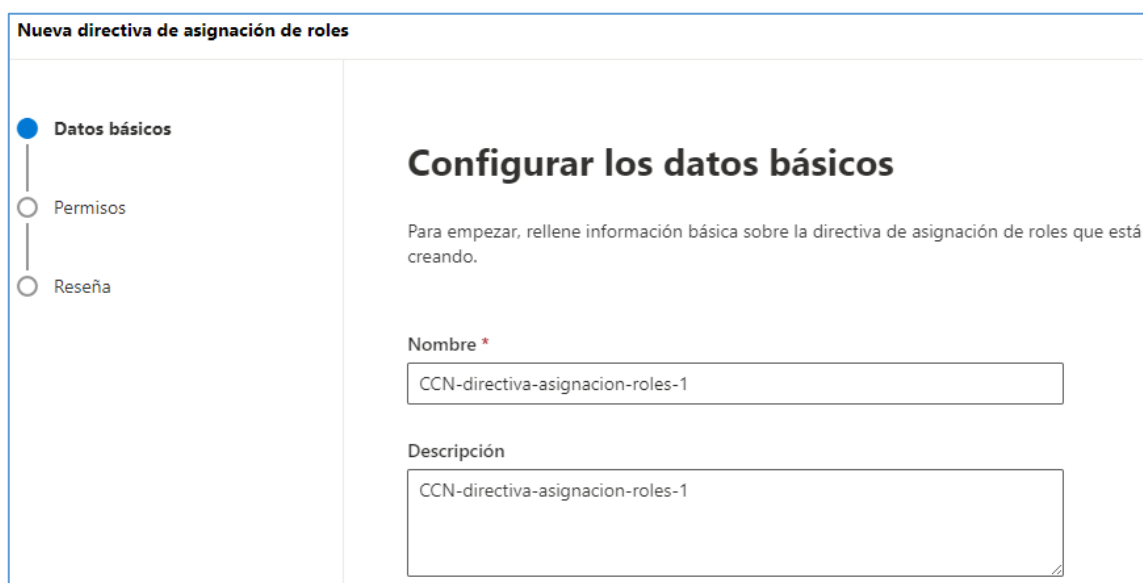
Roles de usuario

Los roles de usuario permiten a los usuarios administrar permisos de usuario final y crear directivas de asignación de roles. Las directivas de asignación de roles definen el nivel de acceso que tienen los usuarios para administrar sus propios buzones de Exchange y grupos de distribución de los que son propietarios. [Más información](#)

+ Nueva directiva de asignación de roles Eliminar Buscar ...

Nombre	Descripción	Roles
✓ Default Role Assignment Policy	This policy grants end users the permission to set their options in Outlook on the web and perform other self-administration tasks.	MyContactInformation, MyMa

- b) Asignamos un nombre y descripción.



Nueva directiva de asignación de roles

Datos básicos

Permisos

Reseña

Configurar los datos básicos

Para empezar, rellene información básica sobre la directiva de asignación de roles que está creando.

Nombre *

CCN-directiva-asignacion-roles-1

Descripción

CCN-directiva-asignacion-roles-1

c) Seleccionar los permisos que tendrá la directiva.

Nueva directiva de asignación de roles

☒ Datos básicos

☒ **Permisos**

☐ Reseña

Agregar permisos

Seleccione los permisos para los usuarios a los que se asigna esta directiva

Información de contacto

☒ MyContactInformation ⓘ

☐ MyAddressInformation

☒ MyMobileInformation

☒ MyPersonalInformation

Información del perfil

☒ MyProfileInformation ⓘ

☒ MyDisplayName

☒ MyName

Grupos de distribución

☐ MyDistributionGroups ⓘ

Pertenencias a grupos de distribución

☐ MyDistributionGroupMembership ⓘ

Otros roles

☐ My Custom Apps ⓘ

☐ My Marketplace Apps ⓘ

☐ My ReadWriteMailbox Apps ⓘ

☐ MyBaseOptions ⓘ

☐ MyMailSubscriptions ⓘ

☐ MyMailboxDelegation ⓘ

☐ MyRetentionPolicies ⓘ

☐ MyTextMessaging ⓘ

☐ MyVoiceMail ⓘ

d) Revisar y finalizar.

Nueva directiva de asignación de roles

☒ Datos básicos

☒ Permisos

☐ Reseña

Revisar la directiva de asignación de roles y finalizar

Datos básicos

Nombre : CCN-directiva-asignacion-roles-1

Descripción : CCN-directiva-asignacion-roles-1

Permisos

MyContactInformation MyProfileInformation

Modificar directivas de asignación de roles

a) Click en el nombre de la directiva y se abrirá un menú donde se puede cambiar la descripción y los permisos.

Inicio > Roles de usuario

Roles de usuario

Los roles de usuario permiten a los usuarios administrar permisos de usuario final y crear directivas de asignación de roles. Las directivas de asignación de roles definen el nivel de acceso que los usuarios para administrar sus propios buzones de Exchange y grupos de distribución de correo electrónico. [Más información](#)

+ Nueva directiva de asignación de roles Eliminar Actualizar

Nombre	Descripción
Default Role Assignment Policy	This policy grants end users the permission to manage their own mailboxes and perform other self-administration tasks.
☒ CCN-directiva-asignacion-roles-1	CCN-directiva-asignacion-roles-1

CCN-directiva-asignacion-roles-1

Nombre

CCN-directiva-asignacion-roles-1

Descripción

CCN-directiva-asignacion-roles-1

[Administrar la configuración general](#)

Permisos

[Administrar permisos](#)

3.1.1.5 MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Información sobre políticas de contraseñas, autenticación MFA y otros aspectos relacionados con la autenticación se muestra en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Simplemente reseñar que la autenticación moderna está habilitada de forma predeterminada en Exchange Online.

Autenticación moderna en Exchange Online

La autenticación moderna en Exchange Online habilita las características de autenticación como la autenticación multifactor (MFA), tarjetas inteligentes, autenticación basada en certificados (CBA) y proveedores de identidades SAML de

terceros. La autenticación moderna se basa en la Biblioteca de autenticación de Active Directory (ADAL) y OAuth 2.0.

Nota: No es recomendable hacer uso de autenticación básica, salvo que técnicamente no esté admitido otro modelo de autenticación. La autenticación básica transmite continuamente la combinación usuario y contraseña, mientras que la autenticación moderna está basada en un token de acceso.

3.1.1.6 MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

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

3.1.2 EXPLOTACIÓN

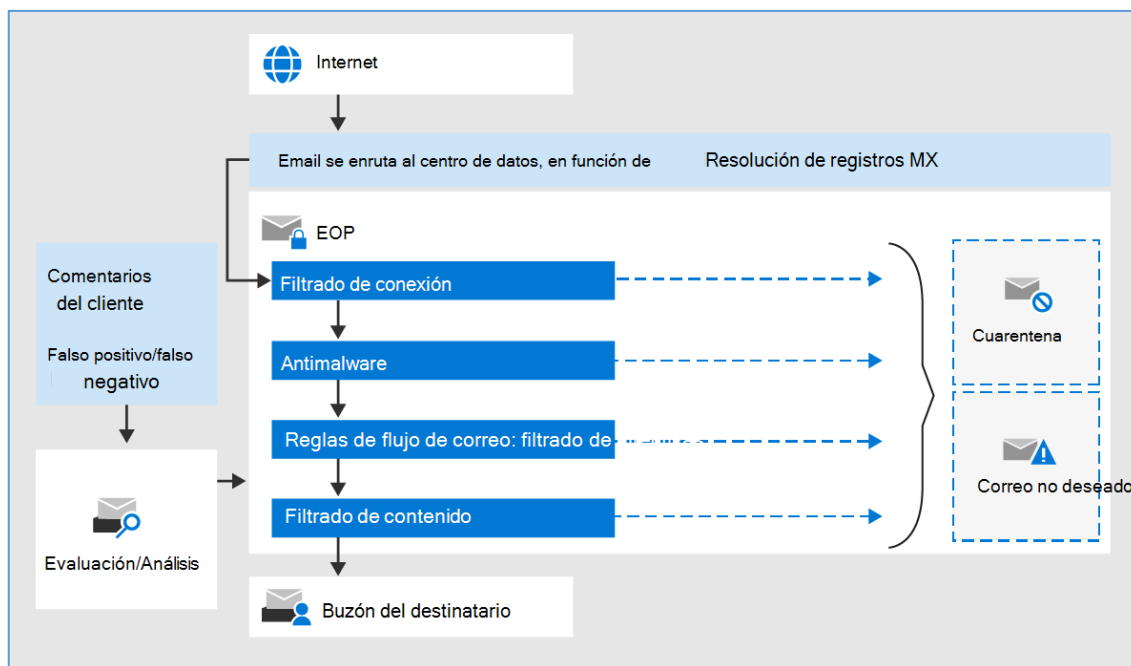
Exchange Online siempre estará actualizado. Es decir, el servicio es mantenido permanentemente por Microsoft, encargándose de las actualizaciones y parches, así como de establecer los mecanismos de detección y protección ante amenazas.

3.1.2.1 PROTECCION FRENTE A CODIGO DAÑINO

Office 365 incluye una variedad de características de protección contra amenazas. Las características de protección contra amenazas se incluyen en todas las suscripciones de Office 365, sin embargo, algunas suscripciones incluyen características más avanzadas, como por ejemplo Datos adjuntos seguros y Vínculos seguros.

Cómo funciona EOP

Exchange Online Protection (EOP) es un servicio de filtro de correo electrónico basado en nube que ayuda a proteger la organización contra correo no deseado y malware. Exchange Online Protection se incluye en Exchange Online y en cualquier plan de Office 365 que englobe Exchange Online.



- Cuando un mensaje entrante llega a EOP, pasa inicialmente a través del filtrado de conexiones, que comprueba la reputación del remitente. La mayoría del correo no deseado se detiene en este momento y EOP lo rechaza.
- A continuación, se inspecciona el mensaje en busca de malware. Si se encuentra malware en el mensaje o en los datos adjuntos de un mensaje, este se envía a cuarentena. De manera predeterminada, solo los administradores pueden ver e interactuar con mensajes en cuarentena de malware. Sin embargo, los administradores pueden crear y usar directivas de cuarentena para especificar qué usuarios pueden acceder a los mensajes en cuarentena.
- El mensaje continúa a través del filtrado de directivas, donde se evalúa con respecto a las reglas de flujo de correo (también conocidas como reglas de transporte) que haya creado. Por ejemplo, una regla puede enviar una notificación a un administrador cuando llega un mensaje de un remitente específico.
- El mensaje pasa por el filtrado de contenido (antispam y contra la suplantación de identidad) donde los mensajes dañinos se identifican como correo no deseado, spam de alta confianza, phishing, suplantación de identidad de alta confianza o en masa (directivas contra correo no deseado) o suplantación de identidad (configuración de suplantación de identidad en directivas anti-phishing). Se puede configurar la acción para realizar el mensaje en función del veredicto de filtrado (cuarentena, traslado a la carpeta de Email no deseado, etc.) y lo que los usuarios pueden hacer a los mensajes en cuarentena mediante directivas de cuarentena.

Se entrega a los destinatarios un mensaje que pasa correctamente todas estas capas de protección.

Para obtener más información, vea [Orden y prioridad de la protección por correo electrónico - Microsoft Defender for Office 365 | Microsoft Learn](#).

Nota: O365 ha unificado todas las soluciones en <https://security.microsoft.com/threatpolicy>.

Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] y el apartado [3.2.4.1 Protección de correo electrónico] de la presente guía.

ZAP (Zero-hour auto purge)

En las organizaciones de Microsoft 365 con buzones de Exchange Online, la purga automática de cero horas (ZAP) es una característica de protección en Exchange Online Protection (EOP) que detecta y neutraliza de forma retroactiva mensajes malintencionados de phishing, spam o malware que ya se han entregado a Exchange Online buzones.

ZAP está disponible con la protección de Exchange Online predeterminada que se incluye con cualquier suscripción a Office 365 que contenga buzones de correo de Exchange Online.

Las firmas de spam y malware en el servicio se actualizan diariamente en tiempo real. Sin embargo, los usuarios todavía pueden recibir mensajes malintencionados. Por ejemplo:

- Malware de Zero-Day que era indetectable durante el flujo de correo.
- Contenido que se arma después de ser entregado a los usuarios.

ZAP soluciona estos problemas supervisando continuamente las actualizaciones de firmas de malware y correo no deseado en el servicio, y es perfecta para los usuarios. ZAP busca y realiza una acción automatizada en los mensajes que ya están en el buzón de un usuario. La búsqueda de ZAP se limita a las últimas 48 horas de correo electrónico entregado. No se notifica a los usuarios si ZAP detecta y mueve un mensaje.

3.1.2.2 GESTION DE INCIDENTES

Ver apartado [3.1.2.1 Protección frente a código dañino] de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] donde se explica cómo acceder a los informes de “Administración de Amenazas”.

3.1.2.3 REGISTRO DE LA ACTIVIDAD

Para configurar el registro de actividad del servicio de Exchange, será necesario hacer uso de la funcionalidad de Auditoría disponible a través del Centro de Seguridad de Office 365. Más información en este mismo apartado de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

El registro de auditoría de buzones está activado de forma predeterminada en todas las organizaciones. Esto significa que ciertas acciones realizadas por los propietarios, delegados y administradores del buzón de correo se registran automáticamente. Los

registros de auditoría de buzón correspondientes están disponibles para que los administradores busquen en el registro de auditoría del buzón.

En la tabla siguiente se describen las acciones de buzón que están disponibles en el registro de auditoría de buzones de correo para buzones de usuario y buzones compartidos:

Acción buzón	Descripción
AddFolderPermissions	Aunque este valor se acepta como una acción de buzón de correo, ya se incluye en la acción UpdateFolderPermissions y no se audita por separado. En otras palabras, no use este valor.
ApplyRecord	Un elemento se etiqueta como un registro.
Copy	Se ha copiado un mensaje a otra carpeta.
Crear	Se creó un elemento en la carpeta Calendario, Contactos, Borrador, Notas o Tareas del buzón (por ejemplo, se crea una nueva convocatoria de reunión). No se audita la creación, el envío ni la recepción de un mensaje. Además, no se audita la creación de una carpeta de buzón de correo.
FolderBind	Se tuvo acceso a una carpeta de buzón de correo. Esta acción también se registra cuando el administrador o un delegado abren el buzón de correo. Nota: Se consolidan los registros de auditoría de las acciones de enlace de carpeta realizadas por los delegados. Se genera un registro de auditoría para el acceso a carpetas individuales en un período de 24 horas.
HardDelete	Un mensaje se purgó de la carpeta Elementos recuperables.
MailboxLogin	El usuario ha iniciado sesión en su buzón de correo.
MailItemsAccessed	Nota: Este valor solo está disponible para los usuarios con licencias E5/A5/G5. Se produce cuando los clientes y protocolos de correo acceden a los datos de correo.
MessageBind	Nota: Este valor solo está disponible para los usuarios <i>sin</i> licencias E5/A5/G5. Un administrador ha visto un mensaje en el panel de vista previa o lo ha abierto.
ModifyFolderPermissions	Aunque este valor se acepta como una acción de buzón de correo, ya se incluye en la acción UpdateFolderPermissions y no se audita por separado. En otras palabras, no use este valor.
Move	Se ha movido un mensaje a otra carpeta.

MoveToDeletedItems	Un mensaje se ha eliminado y movido a la carpeta Elementos eliminados.
RecordDelete	Un elemento etiquetado como registro se eliminó temporalmente (se movió a la carpeta Elementos recuperables). Los elementos etiquetados como registros no se pueden eliminar permanentemente (purgados de la carpeta Elementos recuperables).
RemoveFolderPermissions	Aunque este valor se acepta como una acción de buzón de correo, ya se incluye en la acción UpdateFolderPermissions y no se audita por separado. En otras palabras, no use este valor.
SearchQueryInitiated	Nota: Este valor solo está disponible para los usuarios con licencias E5/A5/G5. Una persona usa Outlook (Windows, Mac, iOS, Android o Outlook en la Web) o la aplicación Correo para Windows 10 para buscar elementos en un buzón.
Send	Nota: Este valor solo está disponible para los usuarios con licencias E5/A5/G5. El usuario envía un mensaje de correo electrónico, responde a un mensaje de correo electrónico o reenvía un mensaje de correo electrónico.
SendAs	Un mensaje se ha enviado con el permiso Enviar como. Este permiso permite a otro usuario enviar el mensaje como si procediera del propietario del buzón.
SendOnBehalf	Un mensaje se ha enviado con el permiso SendOnBehalf. Este permiso permite que otro usuario envíe el mensaje en nombre del propietario del buzón. El mensaje indica al destinatario a nombre de quién se ha enviado el mensaje y quién lo ha enviado realmente.
SoftDelete	Un mensaje se ha eliminado de manera permanente o se ha eliminado de la carpeta Elementos eliminados. Los elementos eliminados de forma temporal se mueven a la carpeta Elementos recuperables.
Actualizar	Se ha cambiado un mensaje o cualquiera de sus propiedades.
UpdateCalendarDelegation	Se asignó una delegación de calendario a un buzón de correo. La delegación de calendario otorga a otra persona en la misma organización permisos para administrar el calendario del propietario del buzón.
UpdateFolderPermissions	Un permiso de la carpeta se ha cambiado. Los permisos de carpeta controlan qué usuarios de su organización pueden tener acceso las carpetas de un buzón de correo y los mensajes que contienen.

UpdateInboxRules	Se agregó, quitó o cambió una regla de bandeja de entrada. Las reglas de bandeja de entrada procesan los mensajes en la Bandeja de entrada del usuario en función de las condiciones. Las acciones especifican qué hacer en los mensajes que coinciden con las condiciones de la regla. Por ejemplo, mueva el mensaje a una carpeta especificada o elimine el mensaje.
------------------	--

Comprobar que la auditoría de buzones de correo está activada

[Get-OrganizationConfig](#) | [Format-List AuditDisabled](#)

El valor *false* indica que la auditoría de buzones de correo está habilitada de forma predeterminada para la organización.

Activar auditoría de buzones compartidos

En caso de que se encuentre desactivada, seguir los siguientes pasos:

- Iniciar una sesión remota de PowerShell como se describe en el apartado [1.3 Prerequisitos para el despliegue mediante PowerShell].
- Activar la auditoría del buzón.

[Set-Mailbox "Buzon compartido CCN1" -AuditEnabled \\$true](#)

Las acciones auditadas para delegados sobre un buzón compartido se muestran con el siguiente comando:

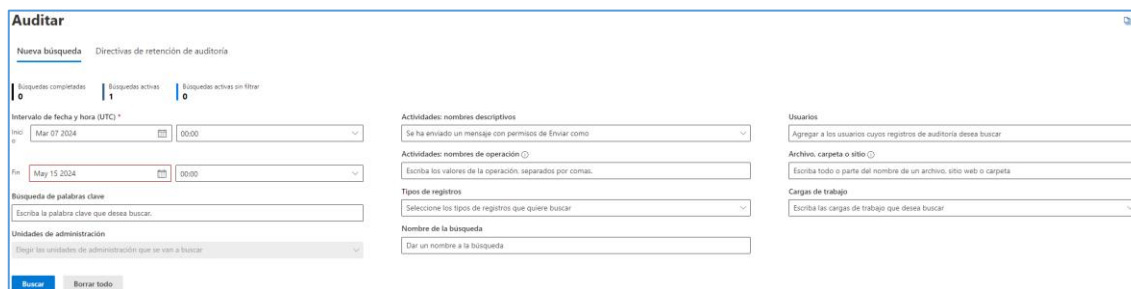
[Get-Mailbox "Buzon compartido CCN1" | Select-Object -ExpandProperty AuditDelegate](#)

Respecto al registro de auditoría en lo relativo a buzones de Exchange, a continuación, se destacan algunos ejemplos concretos de búsquedas interesantes:

Búsquedas relacionadas con buzones compartidos

Ejemplo: “Detectar si un usuario delegado ha enviado un correo en nombre de un buzón compartido”.

- Desde el Centro de seguridad de Office 365 menú [Sistema/Auditar].
- En actividades seleccionar “Se ha enviado un mensaje con permisos de Enviar como”.
- Seleccionar rangos de fecha y pulsar el botón “Buscar”.



- d) Una vez terminada la búsqueda, hacer click encima y se mostraran los resultados.

Auditar

[Obtener información sobre la auditoría](#)

Nueva búsqueda

Directivas de retención de auditoría

Búsquedas completadas

1

Búsquedas activas

0

Búsquedas activas sin filtrar

0

Intervalo de fecha y hora (UTC) *

Inicio

May 21 2024

00:00

Fin

May 22 2024

00:00

Búsqueda de palabras clave

Escriba la palabra clave que desea buscar.

Unidades de administración

Elegir las unidades de administración que se van a buscar

Actividades: nombres descriptivos

Elegir qué actividades buscar

Actividades: nombres de operación

Escriba los valores de la operación, separados por comas.

Tipos de registros

Seleccione los tipos de registros que quiere buscar

Nombre de la búsqueda

Dar un nombre a la búsqueda

Usuarios

Agregar a los usuarios cuyos registros de auditoría desea buscar

Archivo, carpeta o sitio

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

Cargas de trabajo

Escriba las cargas de trabajo que desea buscar

Buscar

Borrar todo

Copiar esta búsqueda

Eliminar

Actualizar

1 elemento

Nombre de la búsqueda

Estado de...

Progr...

Tiemp...

Resultados tot...

Hora de cre...

Búsqueda realizada por

☐ CCN-Auditar

Completado 100% 5m, 17s 1 22 de may. de 202...

Fecha (UTC) ↓	Dirección IP ↓	Usuario ↓	Tipo de registro ↓	Actividad ↓	Elemento ↓	Unidades de a... ↓	Detalles ↓
21 de may. de 2024 12:50	89.46.	azir@p	ExchangeItem	Se ha enviado un ...			

- e) Hacer click encima del registro y se podrá ver los detalles de este.

Detalles

Detalles

Fecha (UTC)
2024-05-21T12:50:35

Dirección IP
89.46.

Usuarios
10032

Actividad
SendAs

Elemento

Detalles

Unidades de administración

CreationTime
2024-05-21T12:50:35

Id

Operation
SendAs

OrganizationId

RecordType
2

ResultStatus
Succeeded

UserKey

UserType
0

Version
1

Workload
Exchange

ClientIP
89.46.

Otros tipos de búsquedas

Otras acciones para auditar de buzones se muestran en la siguiente lista:

Nombre descriptivo

Elementos de buzón a los que se ha accedido
Permisos de buzón de delegado agregados
Se ha agregado o quitado un usuario con acceso delegado a la carpeta calendario
Se agregaron permisos a la carpeta
Mensajes copiados a otra carpeta
Elementos del buzón creado
Nueva regla de bandeja de entrada creada en la aplicación web de Outlook
Mensajes eliminados de la carpeta elementos eliminados
Mensaje etiquetado como un registro
Mensajes movidos a otra carpeta
Mensajes movidos a la carpeta Elementos eliminados
Permiso de carpeta modificada
Regla de bandeja de entrada modificada de la aplicación web de Outlook
Mensajes que se han purgado del buzón
Permisos de buzón de delegado quitados
Permisos quitados de la carpeta
Enviar mensaje
Mensaje enviado mediante los permisos de Enviar como
Mensaje enviado mediante los permisos en nombre de
Reglas de la bandeja de entrada actualizadas desde el cliente de Outlook
Mensaje actualizado
Usuario que ha iniciado sesión en un buzón
Etiquetar mensaje como un registro

3.1.3 MONITORIZACION DEL SISTEMA

Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] para ver los distintos mecanismos de monitorización del servicio.

Conviene destacar que, a nivel de configuración de directivas de alertas, existen muchas actividades relacionadas con Exchange. Algunas directivas de alerta predeterminadas están disponibles si la organización tiene la suscripción complementaria correspondiente además de una suscripción a E1 o E3.

Para obtener más información de las alertas predeterminadas disponibles, ver el enlace [Directivas de alertas de Microsoft 365 | Microsoft Learn](#).

3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

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

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

Todas las comunicaciones de Office 365 están cifradas.

3.2.2 PROTECCIÓN DE LA INFORMACIÓN

3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN

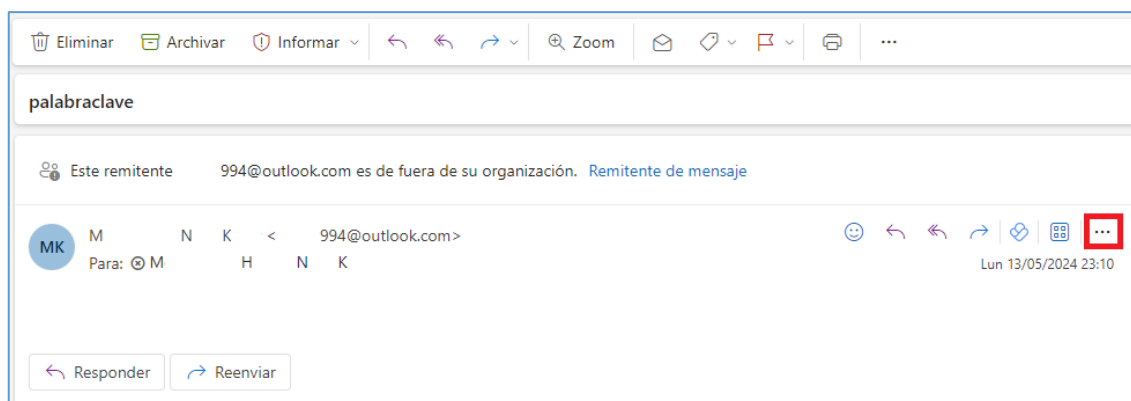
Office 365 cuenta con diversos mecanismos para calificar la información, como se explican en el apartado [3.2.3.1 Calificación de la información] de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]. A continuación, se describen varios desde el punto de vista de Exchange Online.

ETIQUETAS DE RETENCIÓN

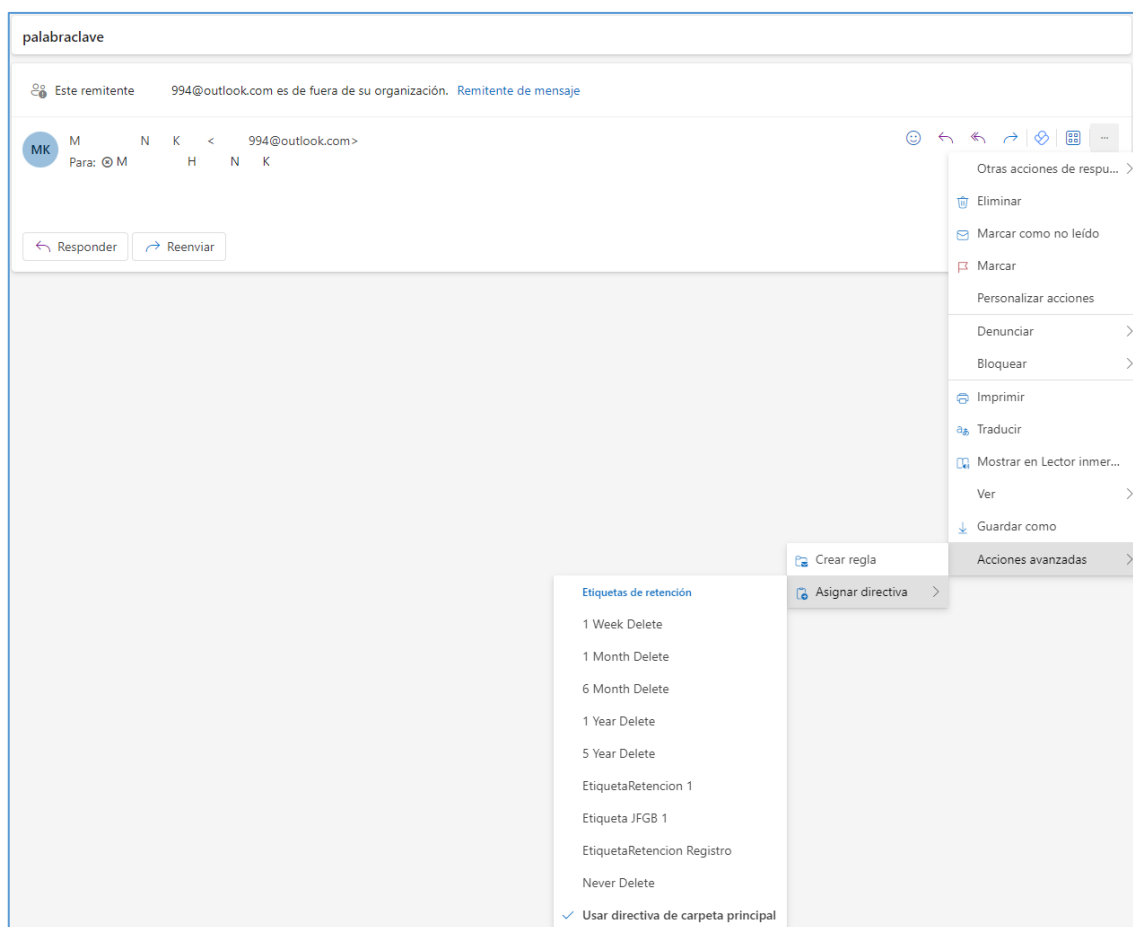
Las etiquetas de retención se usan para aplicar la configuración de retención a carpetas y elementos individuales, como mensajes de correo electrónico y correo de voz. Estas configuraciones especifican el tiempo que permanece un mensaje en un buzón de correo y la acción que se debe llevar a cabo cuando el mensaje llega a la antigüedad de retención especificada. Cuando el mensaje alcanza la antigüedad de retención, se elimina o se mueve al buzón Archivo local del usuario.

Más información sobre la creación de etiquetas de retención en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

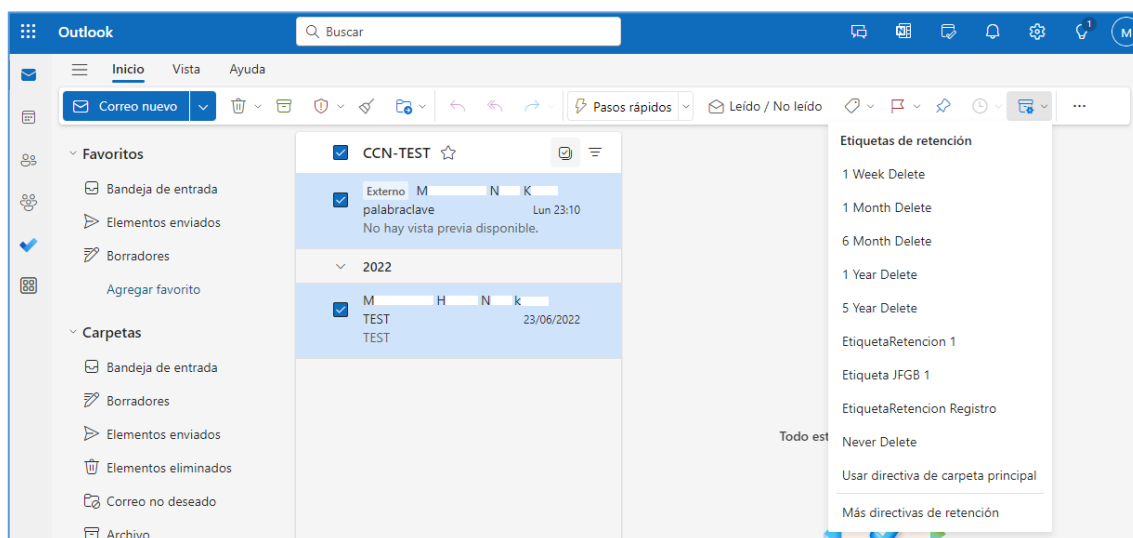
- Para aplicar una directiva de retención en un elemento, pulsar en el icono “Más acciones”.



- A continuación, pulsar sobre el ítem [Acciones avanzadas\Asignar directivas] y seleccionar dentro de “etiquetas” la etiqueta de retención correspondiente.



Es posible seleccionar varios elementos en la carpeta y aplicar la directiva en “masa”:

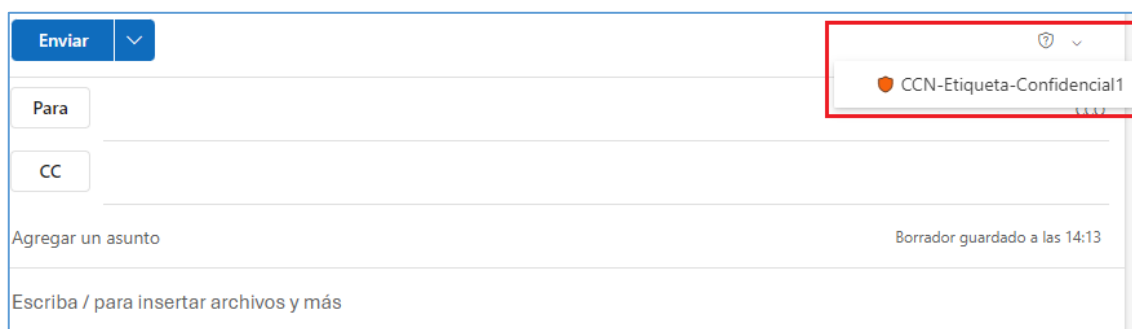


O365 SENSITIVITY LABELS

Los usuarios necesitan colaborar con otros usuarios, tanto dentro como fuera de la organización. Esto significa que el contenido ya no permanece detrás de un firewall: se mueve por todas partes, pasando por dispositivos, aplicaciones y servicios. Y cuando se mueve, se requiere que sea de una forma segura y protegida que cumpla las directivas de cumplimiento de la organización. Con las etiquetas de sensibilidad, se puede clasificar y ayudar a proteger el contenido sensible, sin poner impedimentos a la productividad y la capacidad de colaboración de los usuarios.

Más información sobre la creación de sensitivity labels en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Para aplicar una “Sensitivity label” basta con acceder al menú [sensibilidad] del elemento y aplicar la etiqueta correspondiente:



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.

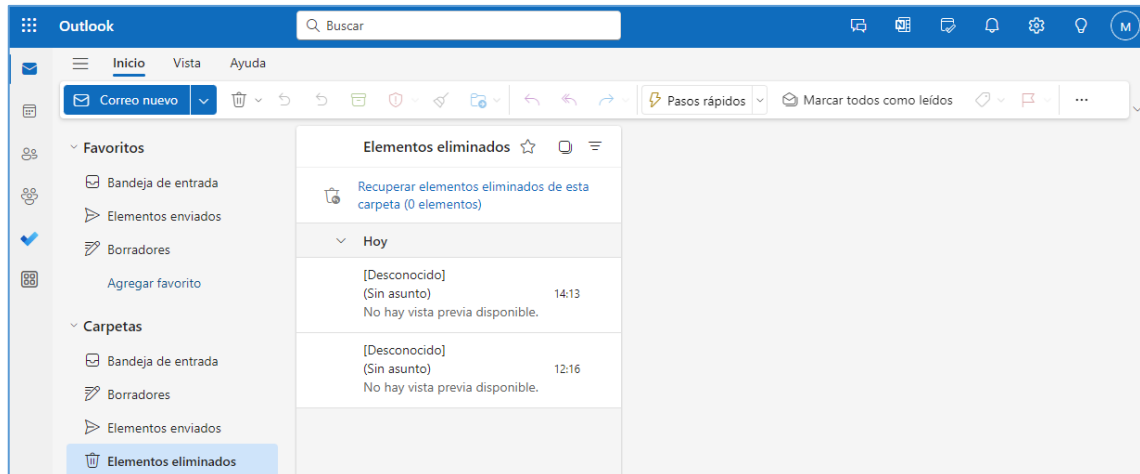
Más información sobre la creación de DLPs en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.2.2.2 COPIAS DE SEGURIDAD

Office 365 tienen un servicio de copia de seguridad muy básico y limitado en el tiempo.

Ofrece protección en caso de error en el hardware o en el software. Para ello, Office 365 crea automáticamente una copia de seguridad de todos los emails enviados y recibidos, replicando buzónes de correo de Exchange online en varias bases de datos en centros de datos de Microsoft independientes.

Por otro lado, en caso de que se elimine por error algún elemento, éste queda almacenado en una carpeta “Elementos eliminados” de Outlook.



Cuando se borra un elemento de la carpeta de “Elementos eliminados” pasa a la carpeta de “Elementos recuperables”.

El período de retención de elementos eliminados predeterminado para Exchange Online es de 14 días. Puede modificar este período para los buzones de correo hasta un máximo de 30 días usando PowerShell.

Por ejemplo, para cambiar el período de retención de un buzón a 30 días:

```
Set-Mailbox -Identity "Buzon CCN1" -RetainDeletedItemsFor 30
```

Para cambiar el de todos los buzones de usuario:

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -RetainDeletedItemsFor 30
```

En el caso de los correos eliminados por accidente, pasados 14 días resulta imposible recuperar el archivo manualmente y, 30 días después, ni siquiera el soporte técnico de Office 365 garantiza poder conseguirlo. Del mismo modo, cuando se elimina una cuenta, los administradores tienen 30 días para solicitar la restauración del buzón de archivo. Transcurrido este período, la recuperación ya no es posible.

Single Item recovery

Se puede usar Exchange Online PowerShell para habilitar o deshabilitar la recuperación de elementos individuales (*single item recovery*) en un buzón. En Exchange Online, *single item recovery* está habilitado de forma predeterminada cuando se crea un nuevo buzón. Así los mensajes que son borrados permanentemente (purgados) por el usuario se retienen en la carpeta de “elementos recuperables” del buzón de correo hasta que expire el período de retención del elemento eliminado. Esto permite al administrador recuperar los mensajes purgados por el usuario antes de que expire el período de retención de elementos eliminados.

Ejemplo: habilitar single item recovery en el buzón “Buzon CCN1”.

```
Set-Mailbox -Identity "Buzon CCN1" -SingleItemRecoveryEnabled $true
```

Copias de seguridad realizadas por los usuarios en Outlook

En Exchange Online, la mejor forma de proporcionar una copia de seguridad para los usuarios es el archivado de Exchange Online. No se recomienda usar Outlook para hacer copias de seguridad de los datos en archivos PST debido a la pérdida de detectabilidad y control del contenido. Consultar información de cómo se crean los archive mailbox en el apartado [4.1 Tipos de buzones].

Retención por juicio

Se puede colocar un buzón en suspensión por juicio para conservar todo el contenido del buzón, incluidos los elementos eliminados y las versiones originales de los elementos modificados. Al colocar un buzón de usuario en suspensión por juicio, también se conserva el contenido del buzón de archivo del usuario (si está habilitado). Al crear una suspensión, puede especificar una duración de suspensión (también denominada suspensión basada en tiempo) para que los elementos eliminados y modificados se conserven durante un período especificado y, a continuación, se eliminen permanentemente del buzón. O bien, se puede conservar el contenido indefinidamente (lo que se denomina suspensión infinita) o hasta que se quite la suspensión por litigio. Si se especifica un período de duración de retención, se calcula a partir de la fecha en que se recibe un mensaje o se crea un elemento de buzón.

Esto es lo que sucede al crear una suspensión por litigio.

- Los elementos eliminados permanentemente por el usuario se conservan en la carpeta Elementos recuperables del buzón del usuario mientras dure la suspensión.
- Los elementos purgados de la carpeta Elementos recuperables por el usuario se conservan mientras dure la suspensión.
- La cuota de almacenamiento para la carpeta Elementos recuperables aumenta de 30 GB a 110 GB.
- Los elementos de los buzones principal y de archivo del usuario se conservan.

Crear una suspensión por litigio ejecutando el siguiente comando:

```
Set-Mailbox <username> -LitigationHoldEnabled $true
```

El comando anterior conserva los elementos indefinidamente porque no se especifica la duración de la suspensión. Para crear una suspensión basada en el tiempo, use el siguiente comando:

```
Set-Mailbox <username> -LitigationHoldEnabled $true -LitigationHoldDuration  
<number of days>
```

Para más información de cómo funciona la retención por juicio ver [Crear una retención por juicio](#).

3.2.3 PROTECCIÓN DE LOS SERVICIOS

3.2.3.1 PROTECCIÓN DEL CORREO ELECTRÓNICO

Office 365 incluye una variedad de características de protección contra amenazas.

EXCHANGE ONLINE PROTECTION (EOP)

Exchange Online Protection (EOP) es el servicio de filtrado basado en la nube que protege a su organización contra correo no deseado, malware, suplantación de identidad (phishing) y otras amenazas de correo electrónico. EOP se incluye en todas las organizaciones de Microsoft 365 que tienen Exchange Online buzones.

Los mensajes de correo electrónico se protegen automáticamente contra correo no deseado y malware. Los administradores no necesitan configurar ni mantener las tecnologías de filtrado, que están habilitadas de forma predeterminada. Sin embargo, pueden realizar personalizaciones de filtrado específicas de la empresa en el centro de seguridad de Office365.

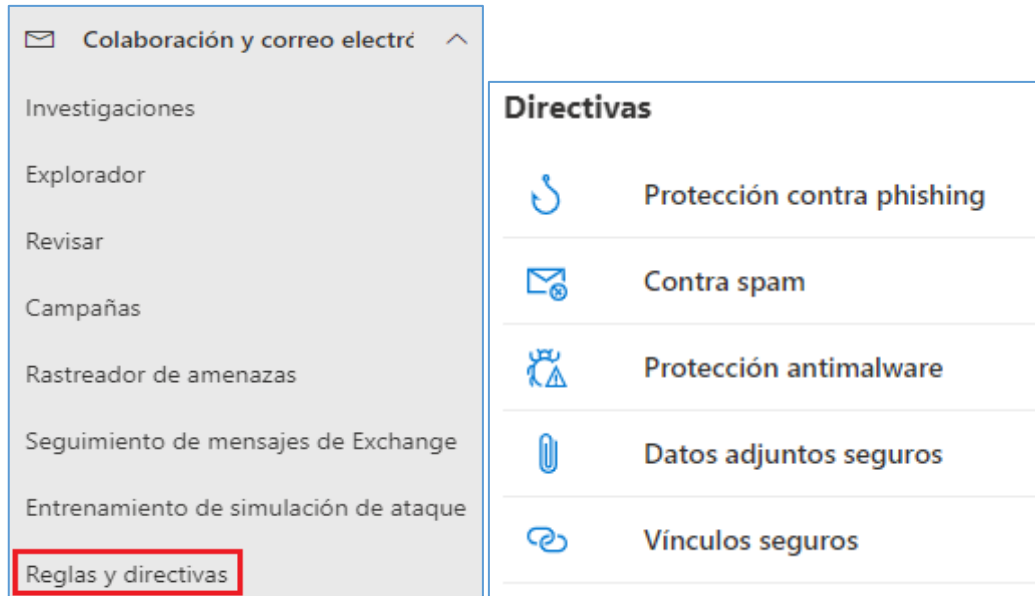
A continuación, se detallan las acciones que pueden realizarse en este sentido a través del Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas].

Filtro de malware

Gracias al uso de varios motores antimalware, EOP ofrece una protección de varias capas diseñadas para detectar todo el malware conocido. Los mensajes que se transportan a través del servicio se analizan en busca de malware (virus, spyware y Ransomware). Si se detecta malware, se puede rechazar el mensaje con un NDR o enviarlo a la cuarentena. También se pueden enviar notificaciones a los remitentes o administradores cuando un mensaje infectado se rechaza y no se entrega.

El filtrado de malware se habilita automáticamente en toda la organización mediante la directiva antimalware predeterminada. Un administrador puede ver y editar, pero no eliminar, la directiva antimalware predeterminada para que se adapte mejor a las necesidades de la organización. Para disfrutar de una mayor granularidad, también se pueden crear directivas personalizadas de filtro de malware y aplicarlas a usuarios, grupos o dominios específicos de la organización. Las directivas personalizadas siempre tienen prioridad frente a las predeterminadas.

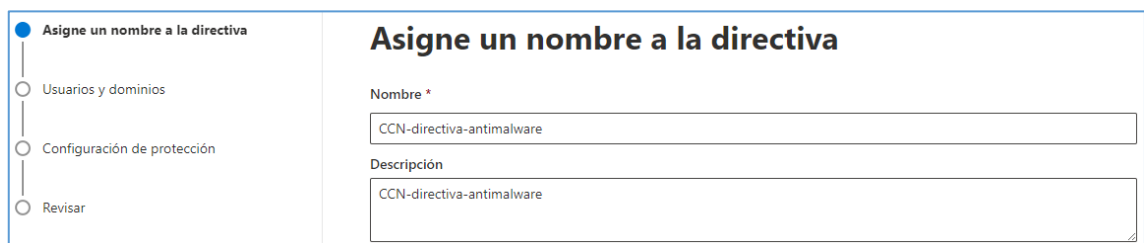
- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Protección antimalware]. Si no hay directivas personalizadas sólo mostrará la directiva predeterminada "Default".



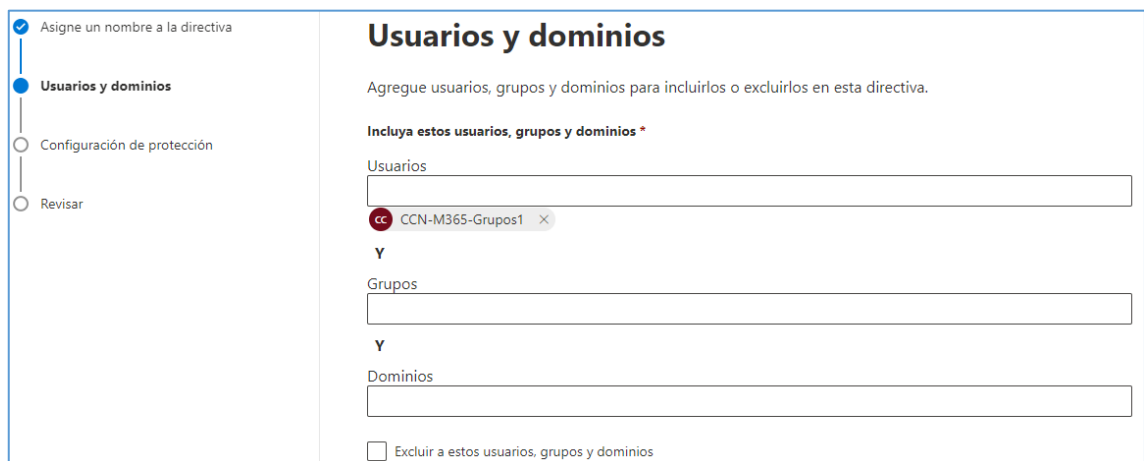
- b) Para crear una directiva personalizada pulsar el botón “Crear”.



- c) Nombre y descripción.



- d) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.



e) Configuración de protección.

Reglas y directivas > Directivas de amenazas > Crear una nueva directiva antimalware

✓ Asigne un nombre a la directiva

✓ Usuarios y dominios

● Configuración de protección

○ Revisar

Configuración de protección

Establecer la configuración para esta directiva antimalware

Configuración de protección

☒ Habilitar el filtro de datos adjuntos comunes ⓘ
 .ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com y 43 otros tipos de archivos
[Seleccionar tipos de archivo](#)

Cuando se encuentran estos tipos de archivo

☒ Rechazar el mensaje con un informe de no entrega (NDR) ⓘ
☐ Poner en cuarentena el mensaje

☒ Habilitar la purga automática contra malware (recomendado) ⓘ

Directiva de cuarentena

AdminOnlyAccessPolicy

Se omitirá el permiso para liberar mensajes en cuarentena para los mensajes con malware detectado y, en su lugar, revertiremos a la solicitud de liberación.

Notificación

Notificaciones del administrador

☐ Notificar a un administrador sobre mensajes no entregados de remitentes internos
☐ Notificar a un administrador sobre mensajes no entregados de remitentes externos

Personalizar notificaciones

☐ Usar texto de notificación personalizado ⓘ

- 1) **Habilitar el filtro de datos adjuntos comunes:** Los tipos de archivos especificados se identifican automáticamente como malware en mensajes de correo electrónico. Aparte de las extensiones predeterminadas especificadas, también podemos añadir personalizadas haciendo click en “Seleccionar tipos de archivo”.
- 2) **Cuando se encuentran estos tipos de archivo:** Seleccionar que acción realizar cuando se detecte malware.
- 3) **Habilitar la purga automática contra malware (recomendado):** ZAP de malware pone en cuarentena los mensajes que contienen malware después de que los mensajes se hayan entregado a los buzones de Exchange Online
- 4) **Directiva de cuarentena:** Si se seleccionó la opción “Poner en cuarentena el mensaje”, entonces se puede elegir que directiva de cuarentena aplicar.
- 5) **Notificaciones del administrador:** Seleccionar esta opción si se quiere enviar notificaciones a los administradores de los correos no entregados.

Notificación**Notificaciones del administrador**☒ Notificar a un administrador sobre mensajes no entregados de remitentes internos

Dirección de correo electrónico del administrador *

Admin-CCN@ .com

☒ Notificar a un administrador sobre mensajes no entregados de remitentes externos

Dirección de correo electrónico del administrador *

Admin-CCN@ .com

6) Personalizar notificaciones:

Añadir nombre y dirección del remitente.

Personalizar notificaciones☒ Usar texto de notificación personalizado ⓘ

Nombre del remitente *

Admin-CCN

Dirección del remitente *

Admin-CCN@ .com

Personalizar las notificaciones de los mensajes de remitentes internos

Asunto *

CCN - Mensaje de remitente interno no entregado

Mensaje *

Su mensaje no ha podido ser entregado.

Personalizar las notificaciones de los mensajes de remitentes externos

Asunto *

CCN - Mensaje de remitente externo no entregado

Mensaje *

Su mensaje no ha podido ser entregado.

7) Revisar y crear:

Reglas y directivas > Directivas de amenazas > Crear una nueva directiva antimalware

✓ Asigne un nombre a la directiva

✓ Usuarios y dominios

✓ Configuración de protección

● Revisar

Revisar

Nombre de la directiva
CCN-directiva-antimalware
[Editar](#)

Descripción
CCN-directiva-antimalware
[Editar](#)

Usuarios y dominios

Usuarios incluidos
CCN-M365-Grupos1@ .onmicrosoft.com
[Editar](#)

Filtro de conexión

Para asegurarse que el correo electrónico que envían personas de confianza no se bloquea, se puede usar la directiva de filtro de conexión para crear una lista de direcciones IP permitidas, también conocida como lista de remitentes seguros. También se puede crear una lista de remitentes bloqueados, que es una lista de direcciones IP, normalmente de spammers conocidos, de las que nunca se quiere recibir mensajes de correo electrónico.

Los mensajes de correo electrónico enviados desde una dirección IP de la lista de IP bloqueadas se rechazan, no se marcan como correo no deseado y no se produce ningún filtro adicional.

La configuración de la directiva de filtro de conexión se aplica únicamente a los mensajes entrantes.

- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Contra spam], una vez dentro hacer click en la directiva con nombre “**Directiva de filtro de conexión (predeterminado)**”.

Reglas y directivas > Directivas de amenazas > Directivas de correo electrónico no deseado

Directivas de correo electrónico no deseado

Utilice esta página para configurar directivas que se incluyen en la protección contra correo no deseado. Estas directivas incluyen el filtrado de conexión, el de correo no deseado y el de correo no deseado de salida. [Más información](#)

+ Crear directiva Actualizar 1 elemento

Nombre	Estado	Prioridad	Tipo
☐ Directiva de filtro de conexión (predeterminado)	● Siempre activada	La más baja	

- b) Desde el siguiente menú se podrá editar la directiva. Click en “Editar directiva de filtro de conexión”.



Directiva de filtro de conexión (predeterminado)

● Siempre activada | Prioridad La más baja

Descripción

-

[Edite la descripción](#)

Filtrado de conexión

Lista de direcciones IP permitidas

Lista de direcciones IP bloqueadas

Lista segura

● Activado

[Editar directiva de filtro de conexión](#)

- c) Agregar las IP que se quieren permitir o bloquear.





Directiva de filtro de conexión (predeterminado)

● Siempre activada | Prioridad La más baja

Always allow messages from the following IP addresses or address range:

Always block messages from the following IP addresses or address range:

☒ Turn on safe list

- **Lista de direcciones IP permitidas:** omite el filtrado de correo no deseado para todos los mensajes entrantes de las direcciones IP de origen o intervalos de direcciones IP especificados. Todos los mensajes entrantes se examinan en busca de malware y suplantación de identidad de alta confianza.
- **Lista de direcciones IP bloqueadas:** bloquea todos los mensajes entrantes de las direcciones IP de origen o intervalos de direcciones IP especificados. Los mensajes entrantes se rechazan, no se marcan como correo no deseado y no se produce ningún otro filtrado.
- **Lista segura:** la lista segura de la directiva de filtro de conexión es una lista de permitidos dinámica que no requiere ninguna configuración de cliente. Microsoft identifica estos orígenes de correo electrónico de confianza de suscripciones a varias listas de terceros. Habilitado o deshabilitado el uso de la lista segura; no se puede configurar los servidores de la lista. El filtrado de correo no deseado se omite en los mensajes entrantes de los servidores de correo electrónico de la lista segura.

Nota: Para obtener más información, consultar [Crear listas de remitentes seguros](#) y [Crear listas de remitentes bloqueados](#).

No se admiten los intervalos IPv6.

Los mensajes de orígenes bloqueados en la lista de direcciones IP bloqueadas no están disponibles en el seguimiento de mensajes.

Las direcciones IP deben especificarse con el formato nnn.nnn.nnn.nnn, donde nnn es un número entre 0 y 255. También puede especificar rangos CIDR con el formato nnn.nnn.nnn.nnn/rr, donde rr es un número entre 24 y 32.

Admite un máximo de 1273 entradas, aunque para especificar muchas direcciones IP recomendamos el uso de PowerShell con el siguiente comando:

```
Set-HostedConnectionFilterPolicy "Default" -IPAllowList @{"Add"="192.168.2.10","192.169.3.0/24","192.168.4.1-192.168.4.5"; Remove="192.168.1.10"}
```

Filtro de Contra Spam (Entrante)

La configuración del filtro de correo no deseado incluye seleccionar la acción que se realizará cuando se identifiquen mensajes como correo no deseado. La configuración de la directiva de filtro de correo no deseado **se aplica solo a los mensajes entrantes**. Hay dos tipos:

- **Predeterminada:** se usa para configurar el filtro de correo no deseado para toda la organización. No se puede cambiar el nombre de esta directiva y siempre está activada.
- **Personalizada:** pueden aplicarse a usuarios, grupos o dominios específicos de la organización. Las directivas personalizadas siempre tienen prioridad sobre la predeterminada.

Si no hay directivas personalizadas sólo mostrarán las directivas predeterminadas:

- Directiva de entrada de correo no deseado (predeterminado)
- Directiva de filtro de conexión (predeterminado)
- Directiva de salida de correo electrónico no deseado (predeterminado)

a) Para crear políticas de spam acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Directivas de amenazas/Directivas/Contra spam].

Reglas y directivas > Directivas de amenazas > Directivas de correo electrónico no deseado

Directivas de correo electrónico no deseado

Utilice esta página para configurar directivas que se incluyen en la protección contra correo no deseado. Estas directivas incluyen el filtrado de conexión, el de correo no deseado y el de correo no deseado de salida. [Más información](#)

+ Crear directiva Actualizar 3 elementos Directiva

Nombre	Estado	Prioridad	Tipo
☐ Directiva de entrada de correo n...	● Siempre activada	La más baja	
☐ Directiva de filtro de conexión (p...	● Siempre activada	La más baja	
☐ Directiva de salida de correo elec...	● Siempre activada	La más baja	

b) Click en **+ Crear directiva**, entonces hacer click en **Inbound**.

c) Asignar un nombre y descripción a la directiva.

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

Asigne un nombre a la directiva

Agregue un nombre y una descripción para su directiva contra el correo no deseado.

Nombre *

CCN-Spam-Entrante

Descripción

CCN-Spam-Entrante

- **Asigne un nombre a la directiva**
- Usuarios, grupos y dominios
- Umbral de correo electrónico en masa y propiedades de correo no deseado
- Acciones
- Lista de bloqueados y admitidos
- Revisar

- d) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

✓ Asigne un nombre a la directiva

● **Usuarios, grupos y dominios**

○ Umbral de correo electrónico en masa y propiedades de correo no deseado

○ Acciones

○ Lista de bloqueados y admitidos

○ Revisar

Usuarios, grupos y dominios

Agregue usuarios, grupos y dominios para incluirlos o excluirlos en esta directiva.

Incluya estos usuarios, grupos y dominios *

Usuarios

CC

CCN-M365-Grupos1

×

Y

Grupos

Y

Dominios

☐ Excluir a estos usuarios, grupos y dominios

Umbral de correo electrónico en masa y propiedades de correo no deseado

- e) **Umbral de correo electrónico en masa:** El BCL puede ser de 1 a 9. Un valor bajo indica correo electrónico masivo benigno (boletines, anuncios en los que se ha registrado, correo masivo de remitentes válidos conocidos, etc.). Un valor superior indica que el mensaje masivo es 'malo' (probablemente no deseado y más bien del tipo spam).

Establezca el umbral y las propiedades contra el correo electrónico no deseado en masa para esta directiva.

Umbral de correo electrónico en masa ⓘ

7 (Predeterminado)

Un mayor umbral de correo electrónico masivo significa que se enviará más correo electrónico masivo

Los umbrales de BCL se describen en la tabla siguiente.

BCL	Descripción
0	El mensaje no es de un remitente de correo masivo.
1, 2, 3	El mensaje proviene de un remitente de correo masivo que genera pocas quejas.
4, 5, 6, 7	El mensaje proviene de un remitente de correo masivo que genera un número mixto de quejas.
8, 9	El mensaje procede de un remitente masivo que genera un gran número de quejas.

f) **Incrementar puntuación de correo no deseado:**

Las siguientes configuraciones de ASF (Advanced Spam Filter) dan como resultado un aumento en la puntuación de correo no deseado y, por lo tanto, una mayor probabilidad de que se marque como spam con un nivel de confianza de correo no deseado (SCL) de 5 o 6, que corresponde a un veredicto de filtro de correo no deseado y a la acción correspondiente en las directivas contra correo no deseado. No todos los mensajes que coincidan con las siguientes condiciones de ASF se marcan como correo no deseado.

Propiedades de correo no deseado

✓ **Incrementar puntuación de correo no deseado**

Especifica si desea aumentar la calificación de correo no deseado para los mensajes que incluyan estos tipos de vínculos o de direcciones URL.

Vínculos de imagen a sitios remotos

Desactivado ▼

Dirección IP numérica en dirección URL

Desactivado ▼

URL de redireccionamiento a otro puerto

Desactivado ▼

Enlaces a sitios web .biz o .info

Desactivado ▼

- **Vínculos de imagen a sitios remotos:** Los mensajes que contienen vínculos de etiqueta HTML a sitios remotos (por ejemplo, mediante http) se marcan como correo no deseado.
- **Dirección IP numérica en dirección URL:** Los mensajes que contienen direcciones URL basadas en números (normalmente, direcciones IP) se marcan como correo no deseado.
- **URL de redireccionamiento a otro puerto:** Los mensajes que contienen hipervínculos que redirigen a puertos TCP distintos de 80 (HTTP), 8080 (HTTP alternativo) o 443 (HTTPS) se marcan como correo no deseado.
- **Enlaces a sitios web .biz o .info:** Los mensajes que contienen .biz o .info vínculos en el cuerpo del mensaje se marcan como correo no deseado.

g) **Marcar como correo no deseado:**

Especifica si desea marcar los mensajes que incluyan estas propiedades como correo no deseado.

Mensajes vacíos

Desactivado ▼

Etiquetas insertadas en HTML

Desactivado ▼

JavaScript o VBScript en HTML

Desactivado ▼

Etiquetas Form en HTML

Desactivado ▼

Etiquetas Frame o iFrame en HTML

Desactivado ▼

Errores web en HTML

Desactivado ▼

Etiquetas de objeto en HTML

Desactivado ▼

Palabras no permitidas ⓘ

Desactivado ▼

Registro SPF: error no recuperable ⓘ

Desactivado ▼

Filtrado de id. del remitente: error no recuperable ⓘ

Desactivado ▼

Devolución de correo no enviado ⓘ

Desactivado ▼

Contiene idiomas específicos

Desactivado ▼

De estos países o regiones

Desactivado ▼

La siguiente configuración de Marcar como ASF de correo no deseado establece la SCL de los mensajes detectados en 9, que corresponde a un veredicto de filtro de correo no deseado de alta confianza y a la acción correspondiente en las directivas contra correo no deseado.

- **Mensajes vacíos:** Los mensajes sin asunto, sin contenido en el cuerpo del mensaje y sin datos adjuntos se marcan como correo no deseado de alta confianza.
- **Etiquetas incrustadas en HTML:** Los mensajes que contienen <embed> etiquetas HTML se marcan como spam de alta confianza. Esta etiqueta permite insertar diferentes tipos de documentos en un documento HTML (por ejemplo, sonidos, vídeos o imágenes).
- **JavaScript o VBScript en HTML:** Los mensajes que usan JavaScript o Visual Basic Script Edition en HTML se marcan como correo no deseado de alta confianza. Estos lenguajes de scripting se usan en los mensajes de correo electrónico para hacer que se produzcan acciones específicas automáticamente.
- **Etiquetas de formulario en HTML:** Los mensajes que contienen <form> etiquetas HTML se marcan como spam de alta confianza. Esta etiqueta se usa para crear formularios de sitio web. Los anuncios en correo electrónico a menudo incluyen esa etiqueta con el fin de solicitar información del destinatario.
- **Etiquetas frame o iframe en HTML:** Los mensajes que contienen <frame> o <iframe> etiquetas HTML se marcan como spam de alta confianza. Estas etiquetas se usan en mensajes de correo electrónico para dar formato a la página para mostrar texto o gráficos.
- **Errores web en HTML:** Un error web (también conocido como baliza web) es un elemento gráfico (a menudo tan pequeño como un píxel por un píxel) que se usa en los mensajes de correo electrónico para determinar si el destinatario lee el mensaje. Los mensajes que contienen errores web se marcan como spam de alta confianza. Los boletines de noticias legítimos pueden usar errores web, aunque muchos consideran esto una invasión de privacidad.
- **Etiquetas de objeto en HTML:** Los mensajes que contienen <object> etiquetas HTML se marcan como spam de alta confianza. Esta etiqueta permite que los complementos o aplicaciones se ejecuten en una ventana HTML.
- **Palabras no permitidas:** Microsoft mantiene una lista dinámica pero no modificable de palabras asociadas a mensajes potencialmente ofensivos. Los mensajes que contienen palabras de la lista de palabras confidenciales en el asunto o el cuerpo del mensaje se marcan como correo no deseado de alta confianza.

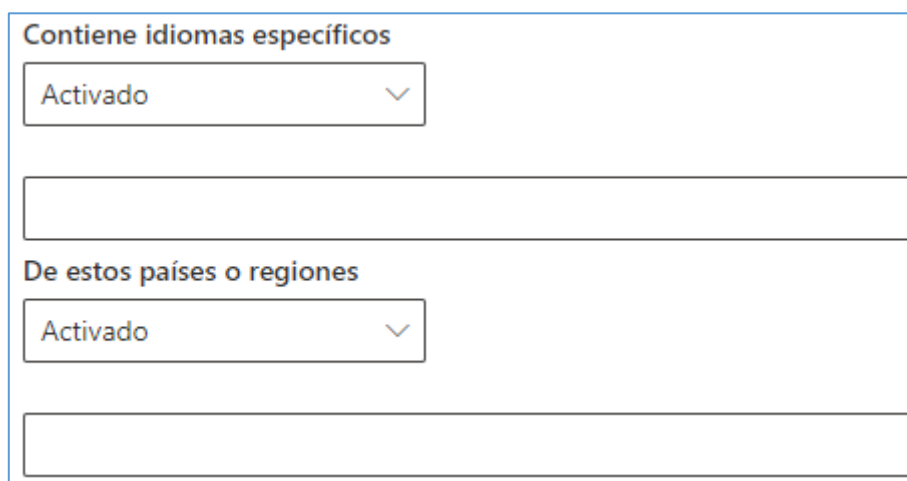
- **Registro SPF: error no recuperable:** Los mensajes enviados desde una dirección IP que no se especifica en el registro SPF Sender Policy Framework (SPF) en DNS para el dominio de correo electrónico de origen se marcan como correo no deseado de alta confianza. El modo de prueba no está disponible para esta configuración.

La siguiente configuración de Marcar como ASF de correo no deseado establece la SCL de los mensajes detectados en 6, que corresponde a un veredicto de filtro de correo no deseado y a la acción correspondiente en las directivas contra correo no deseado.

- **Error de filtrado de identificador de remitente:** El mensaje no ha superado la comprobación de identificación de la combinación SPF y remitente, la cual ayuda a proteger contra los encabezados de los mensajes que contengan remitentes falsos.
- **Devolución de correo no enviado:** Cuando esta configuración está habilitada, cualquier mensaje que coincida con las características de rebote del informe de no entrega (NDR) se marcará como spam. No es necesario habilitar esta configuración si su organización usa Exchange Online Protection para enviar correo saliente.

La configuración Contiene idiomas específicos y De estos países no forma parte de ASF.

- **Contiene idiomas específicos:** Si se activa, aparecerá un cuadro en donde hay que escribir el nombre del idioma.
- **De estos países o regiones:** Si se activa, aparecerá un cuadro en donde hay que escribir el nombre del país o región.



Contiene idiomas específicos

Activado

De estos países o regiones

Activado

- h) **Modo de prueba:** En las configuraciones indicadas en el punto anterior, aparte de las opciones de *Activar* y *Desactivar* esta la opción de *Prueba*. Si se activa la opción de Prueba, se puede decidir qué hacer en el caso de haya coincidencia.

Modo de prueba

Configure las opciones de modo Prueba para cuando se produce una coincidencia para una opción avanzada habilitada para pruebas.

- ☒ Ninguno
- ☐ Agregar texto de encabezado X predeterminado
- ☐ Enviar mensaje CCO

Acciones

- i) **Acciones del mensaje:** Seleccione la acción que se va a realizar en los mensajes en función de los veredictos de filtrado de correo no deseado:

- Correo no deseado
- Correo no deseado de confianza alta
- Phishing
- Suplantación de identidad de alta confianza
- Se completó o superó el nivel de quejas masivas (BCL)

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

☒ Asigne un nombre a la directiva

☒ Usuarios, grupos y dominios

☒ Umbral de correo electrónico en masa y propiedades de correo no deseado

☒ **Acciones**

☐ Lista de bloqueados y admitidos

☐ Revisar

Acciones

Configure sus acciones para esta directiva

Acciones en mensajes

Correo no deseado

Mover el mensaje a la carpeta Correo electrónico no deseado

Correo no deseado de confianza alta

Mover el mensaje a la carpeta Correo electrónico no deseado

Phishing

Mensaje en cuarentena

Seleccionar directiva de cuarentena

DefaultFullAccessPolicy

Suplantación de identidad de alta confianza

Mensaje en cuarentena

Se omitirá el permiso para liberar mensajes en cuarentena para los mensajes detectados como phishing de alta confianza. El permiso revertirá a la solicitud de liberación en su lugar.

Seleccionar directiva de cuarentena

AdminOnlyAccessPolicy

Se completó o superó el nivel de quejas masivas (BCL)

Mover el mensaje a la carpeta Correo electrónico no deseado

- j) **Mensajes dentro de la organización sobre los que tomar medidas:** Controla si el filtrado de correo no deseado y las acciones de veredicto correspondientes se aplican a los mensajes internos (mensajes enviados entre los usuarios de la organización). Los valores disponibles son los siguientes:

- Valor predeterminado: este es el valor predeterminado. Este valor es el mismo que al seleccionar Mensajes de suplantación de identidad de alta confianza.
- Ninguna
- Mensajes de suplantación de identidad de alta confianza
- Suplantación de identidad (phishing) y mensajes de suplantación de identidad (phishing) de alta confianza
- Todos los mensajes de suplantación de identidad (phishing) y correo no deseado de alta confianza
- Todos los mensajes de suplantación de identidad y correo no deseado

Mensajes dentro de la organización sobre los que tomar medidas

Ninguno

- k) **Conservar el spam en cuarentena durante esta cantidad de días:** En esta opción se especifica cuánto tiempo debe mantenerse el mensaje en cuarentena si ha seleccionado Mensaje en cuarentena como la acción para un veredicto de filtrado de correo no deseado. Una vez expirado el período de tiempo, el mensaje se elimina y no se puede recuperar. Los valores válidos están comprendidos entre 1 y 30 días.

Conservar el spam en cuarentena durante esta cantidad de días

15

- l) **Agregar este texto de encabezado X:** Este cuadro es obligatorio y solo está disponible si se ha seleccionado Agregar encabezado X en las opciones anteriores. La longitud máxima es de 255 caracteres y el valor no puede contener espacios o dos puntos (:).

Agregar este texto de encabezado X

- m) **Anteponer la línea de asunto con este texto:** Este cuadro es obligatorio y solo está disponible si se ha seleccionado Anteponer la línea de asunto con este texto en las opciones anteriores.

Anteponer la línea de asunto con este texto

- n) **Redirigir a esta dirección de correo electrónico:** Este cuadro es obligatorio y solo está disponible si se ha seleccionado Redirigir el mensaje a dirección de correo electrónico en las opciones anteriores.

Redirigir a esta dirección de correo electrónico

- o) **Sugerencias de seguridad:** Una pancarta codificada en color de Outlook que avisará a los destinatarios de los mensajes que pueden ser perjudiciales.

Sugerencias de seguridad

☒ Habilitar sugerencias de seguridad para el spam ⓘ

- p) **Purga automática (ZAP):** Detecta y neutraliza retroactivamente mensajes de phishing, correo no deseado o malware que ya se han entregado en los buzones de Exchange Online.

Purga automática (ZAP)

☒ Habilitar purga automática (ZAP) ⓘ

☒ Habilitar para mensajes de suplantación de identidad (phishing)

☒ Habilitar para mensajes de correo no deseado

Lista de bloqueados y admitidos

Añadir los remitentes o dominios a permitir o bloquear.

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

☒ Asigne un nombre a la directiva

☒ Usuarios, grupos y dominios

☒ Umbral de correo electrónico en masa y propiedades de correo no deseado

☒ Acciones

☒ **Lista de bloqueados y admitidos**

☐ Revisar

Lista de bloqueados y admitidos

Elegir qué usuarios, grupos y dominios permitir o bloquear en esta directiva. Nota: Las entradas permitidas que configure aquí no se aplican a los mensajes marcados como suplantación de identidad de alta confianza.

Permitido

Remitentes (0)
Entregar siempre los mensajes de estos remitentes
[Administrar 0 remitente\(s\)](#)

Dominios (0)
Entregar mensajes siempre de estos dominios
[Mostrar dominios](#)

Bloqueado

Remitentes (0)
Marcar siempre los mensajes de estos remitentes como spam
[Administrar 0 remitente\(s\)](#)

Dominios (0)
Marcar siempre los mensajes de estos dominios como spam
[Bloquear dominios](#)

Nota:

La funcionalidad de estas listas se ha reemplazado en gran medida por la [lista de permitidos o bloqueados de inquilinos](#). Para obtener información importante, consulte [Permitir y bloquear la lista en directivas contra correo no deseado](#).

No agregar dominios que posea la organización ni dominios populares (por ejemplo, microsoft.com) a la lista de dominios permitidos. Eso se considera una acción de riesgo alto, ya que crea oportunidades para que los remitentes dudosos le envíen correo que, de lo contrario, se filtraría.

Revisar

q) **Revisar** la configuración antes de crear la directiva.

Filtro de Contra Spam (Salida)

a) Para crear políticas de spam acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Contra spam].

Reglas y directivas > Directivas de amenazas > Directivas de correo electrónico no deseado

Directivas de correo electrónico no deseado

Utilice esta página para configurar directivas que se incluyen en la protección contra correo no deseado. Estas directivas incluyen el filtrado de conexión, el de correo no deseado y el de correo no deseado de salida. [Más información](#)

+ Crear directiva ▾ Actualizar 3 elementos X ≡ ▾

Nombre	Estado	Prioridad	Tipo
☐ Directiva de entrada de correo n...	● Siempre activada	La más baja	
☐ Directiva de filtro de conexión (p...	● Siempre activada	La más baja	
☐ Directiva de salida de correo elec...	● Siempre activada	La más baja	

- b) Click en **+ Crear directiva ▾**, entonces hacer click en **Outbound**.
- c) Asignar un nombre y descripción a la directiva.

Reglas y directivas > Directivas de amenazas > Create anti-spam outbound policy

● **Asigne un nombre a la directiva**

○ Usuarios, grupos y dominios

○ Configuración de protección saliente

○ Revisar

Asigne un nombre a la directiva

Agregue un nombre y una descripción para su directiva contra el correo no deseado.

Nombre *

Descripción

- d) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.

✓ **Asigne un nombre a la directiva**

● **Usuarios, grupos y dominios**

○ Configuración de protección saliente

○ Revisar

Usuarios, grupos y dominios

Agregue usuarios, grupos y dominios para incluirlos o excluirlos en esta directiva.

Incluya estos usuarios, grupos y dominios *

Usuarios

CCN-M365-Grupos1 X

Y

Grupos

Y

Dominios

☐ Excluir a estos usuarios, grupos y dominios

e) **Secciones de límites de mensajes:** la configuración de esta sección configura los límites para los mensajes de correo electrónico salientes de Exchange Online buzones:

- **Establecer un límite de mensajes externos:** el número máximo de destinatarios externos por hora. El valor máximo permitido es 10000.
- **Establecer un límite de mensajes interno:** el número máximo de destinatarios internos por hora. El valor máximo permitido es 10000.
- **Establecer un límite de mensajes diario:** el número total máximo de destinatarios por día. El valor máximo permitido es 10000.

Reglas y directivas > Directivas de amenazas > Create anti-spam outbound policy

☒ Asigne un nombre a la directiva

☒ Usuarios, grupos y dominios

☒ **Configuración de protección saliente**

☐ Revisar

Configuración de protección

Establezca la configuración de correo no deseado saliente para esta directiva.

Límites de mensaje

Establecer un límite de mensajes externos

Establecer un límite de mensajes internos

Establecer un límite de mensajes diarios

f) **Restricción impuesta a los usuarios que llegarán al límite de mensajes:** Desde esta confirmación se pueda indicar la acción a ejecutar si se superase cualquiera de los límites indicados en el punto anterior:

- Restringir al usuario el envío de correo hasta el día siguiente.
- Impedir que el usuario envíe correo.
- Sin acción, solo alerta: se envían las notificaciones Email.

Restricción impuesta a los usuarios que llegarán al límite de mensajes

Restringir al usuario el envío de correo hasta el siguiente día

Restringir al usuario el envío de correo hasta el siguiente día

Restringir al usuario el envío de correo

Ninguna acción, solo alerta

g) **Reglas de reenvío:** Controla el reenvío automático de correo electrónico Exchange Online buzones a destinatarios externos.

- **Automático:** controlado por el sistema: este es el valor predeterminado. Este valor es lo mismo que Desactivado. Cuando se introdujo originalmente este valor, era equivalente a On. Con el tiempo, gracias a los principios de seguridad de forma predeterminada, el efecto de este valor se cambió finalmente a Desactivado para todos los clientes.
- **Activado:** la directiva no deshabilita el reenvío automático de correo electrónico externo.
- **Desactivado:** la directiva deshabilita todo el reenvío automático de correo electrónico externo.

Reglas de reenvío

Reglas de reenvío automático

Automático: controlado por el sistema

Automático: controlado por el sistema

Desactivado: el reenvío está deshabilitado

Activado: el reenvío está habilitado

h) **Notificaciones:** Esta sección es para configurar destinatarios adicionales que deben recibir copias y notificaciones de mensajes de correo electrónico salientes sospechosos:

- **Enviar una copia de mensajes salientes sospechosos o mensajes que superen estos límites a estos usuarios y grupos:** Esta configuración agrega los destinatarios especificados al campo CCO de mensajes salientes sospechosos.

Nota: Esta configuración solo funciona en la directiva de correo no deseado saliente predeterminada. No funciona en las directivas de correo no deseado de salida personalizadas.

- **Notifique a estos usuarios y grupos si un remitente está bloqueado debido al envío de correo no deseado de salida.**

Nota: Esta configuración está en desuso en las directivas de correo no deseado saliente, ya que la directiva de alerta predetermina denominada **User restricted from sending email** ya envía notificaciones a los miembros del grupo TenantAdmins (Global admins).

Notificaciones

- ☐ Enviar una copia de mensajes salientes sospechosos o mensajes que superen estos límites a estos usuarios y grupos
- ☐ Notifique a estos usuarios y grupos si un remitente está bloqueado debido al envío de correo no deseado de salida

i) Revisar y finalizar:

Reglas y directivas > Directivas de amenazas > Create anti-spam outbound policy

✓ Asigne un nombre a la directiva

✓ Usuarios, grupos y dominios

✓ Configuración de protección saliente

● **Revisar**

Revisar

Nombre de la directiva
CCN-Spam-Salida
[Editar nombre](#)

Descripción
CCN-Spam-Salida
[Edite la descripción](#)

Usuarios, grupos y dominios

Usuarios incluidos
CCN-M365-Grupos1@ .onmicrosoft.com
[Editar usuarios, grupos y dominios](#)

Configuración de protección

Restringir el envío a destinatarios externos (por hora)
100

Restringir el envío a destinatarios internos (por hora)
100

Límite máximo de destinatarios por día
100

Acción de exceso de límite
Restringir al usuario el envío de correo hasta el siguiente día

Reenvío automático
Automático: controlado por el sistema

Enviar una copia de mensajes salientes sospechosos o mensajes que superen estos límites a estos usuarios y grupos
● Desactivado

Notifique a estos usuarios y grupos si un remitente está bloqueado debido al envío de correo no deseado de salida
● Desactivado
[Edite la configuración de protección](#)

Directivas de cuarentena

Crear directivas

En Exchange Online Protection (EOP) y Microsoft Defender para Office 365, las directivas de cuarentena permiten a los administradores definir la experiencia del usuario para los mensajes en cuarentena:

- Qué usuarios pueden hacer con sus propios mensajes en cuarentena (mensajes donde son destinatarios) en función de por qué se puso en cuarentena el mensaje.
- Si los usuarios reciben notificaciones periódicas (cada cuatro horas, diarias o semanales) sobre sus mensajes en cuarentena a través de notificaciones de cuarentena.

Para crear directivas de cuarentena, seguir los siguientes pasos:

- Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Directivas de cuarentena], Si no hay directivas personalizadas sólo mostrará las directivas predeterminadas.

Directiva de cuarentena

Utilice esta página para configurar la forma en que se administran los mensajes en la cuarentena de Office 365. También puede configurar cómo los usuarios finales y administradores pueden ver y administrar los mensajes en cuarentena. [Obtenga más información sobre la directiva de cuarentena](#)

+ Agregar directiva personalizada
 Actualizar
 Exportar
 Configuración global
 3 elementos

Nombre de la directiva	Última actualización
☐ DefaultFullAccessPolicy	
☐ AdminOnlyAccessPolicy	
☐ DefaultFullAccessWithNotificationPolicy	

- Click en el botón **+ Agregar directiva personalizada**.
- Asignar un nombre a la directiva.

● Nombre de la directiva

○ Acceso a mensajes de destinatario

○ Notificación de cuarentena

○ Resumen

Nombre de la directiva

Nombre de la directiva *

d) Definir el tipo de acceso a los mensajes en cuarentena.

- **Acceso limitado:** Los usuarios pueden ver los mensajes en cuarentena, pero no pueden liberarlos, para hacer esto, deberán solicitarlo desde el mismo panel de cuarentena.

☒ Nombre de la directiva ☒ Acceso a mensajes de destinatario ☒ Notificación de cuarentena ☐ Resumen	Acceso a mensajes de destinatario Especifique el acceso que quiere que tengan los destinatarios cuando se aplique esta directiva de cuarentena a un mensaje. Más información sobre el acceso de destinatarios a los mensajes Acceso a mensajes de destinatario * ☒ Acceso limitado Los destinatarios pueden ver los mensajes en cuarentena, pero no pueden liberar mensajes del estado de cuarentena ☐ Establecer acceso específico (avanzado) Especifique exactamente lo que los destinatarios pueden hacer con los mensajes en cuarentena Con acceso limitado el destinatario obtendrá una vista previa del mensaje, solicitará la liberación del mensaje, lo eliminará y bloqueará al remitente Con acceso limitado el destinatario no liberará el mensaje
--	---

- **Establecer acceso específico (avanzado):** Especificar exactamente lo que los destinatarios pueden hacer con los mensajes en cuarentena.

Preferencia de acción de liberación:

- En blanco: los usuarios no pueden liberar ni solicitar la liberación de sus mensajes de la cuarentena. Este es el valor predeterminado.
- Permitir que los destinatarios soliciten que un mensaje se libere de la cuarentena.
- Permitir que los destinatarios liberen un mensaje de la cuarentena.

Seleccione las preferencias de acción de liberación

▼

Permitir que los destinatarios soliciten que un mensaje se libere de la cuarentena

 Permitir que los destinatarios liberen un mensaje de la cuarentena

Acciones adicionales que los destinatarios pueden realizar en mensajes en cuarentena:

☐ Eliminar

☐ Vista previa

☐ Bloquear remitente

- e) **Notificación de cuarentena:** Si se quiere que el usuario reciba una notificación cuando un mensaje donde es el destinatario, habilitar la siguiente opción.

☒ Nombre de la directiva ☒ Acceso a mensajes de destinatario ☒ Notificación de cuarentena ☐ Resumen	Notificación de cuarentena ☒ Habilitar
---	--

- f) **Resumen:** Revisar configuración antes de crear la directiva.

☒ Nombre de la directiva ☒ Acceso a mensajes de destinatario ☒ Notificación de cuarentena ☒ Resumen	Revisar directiva Nombre de la etiqueta Nombre CCN-Cuarentena Editar Acceso al mensaje de usuario El destinatario puede: - solicitud para liberar el mensaje de la cuarentena - bloquear remitente - eliminar el mensaje - obtener una vista previa del mensaje Editar Notificación de cuarentena Habilitado Sí Editar
--	--

Personalizar notificaciones

Se puede personalizar las notificaciones de correo electrónico que se envían a los destinatarios que reciben el mensaje de cuarentena. Para hacerlo:

- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Directivas de cuarentena.

b) Click en el botón  Configuración global.

c) Desde el siguiente menú podremos personalizar las notificaciones.

Configuración de notificación de cuarentena

Personalizar las notificaciones de correo electrónico que se envían a los destinatarios que reciben el mensaje de cuarentena.

Nombre para mostrar del remitente

Tenga en cuenta que el nombre para mostrar del remitente se invalidará si se usa una dirección de remitente activa con un nombre para mostrar existente

Especificar la dirección del remitente

Escriba una dirección de remitente del dominio de la organización.

Asunto

Aviso de declinación de responsabilidades

Elegir idioma

English_USA 

Agregar

Haga clic en el idioma para mostrar los valores configurados previamente

☐ Usar el logotipo de mi empresa
Reemplazar el logotipo de Microsoft con el logotipo de la empresa

Parece que no ha cargado el logotipo de su empresa, cargue el logotipo de la empresa en el centro de administración siguiendo las instrucciones que se indican en [esta documentación](#)

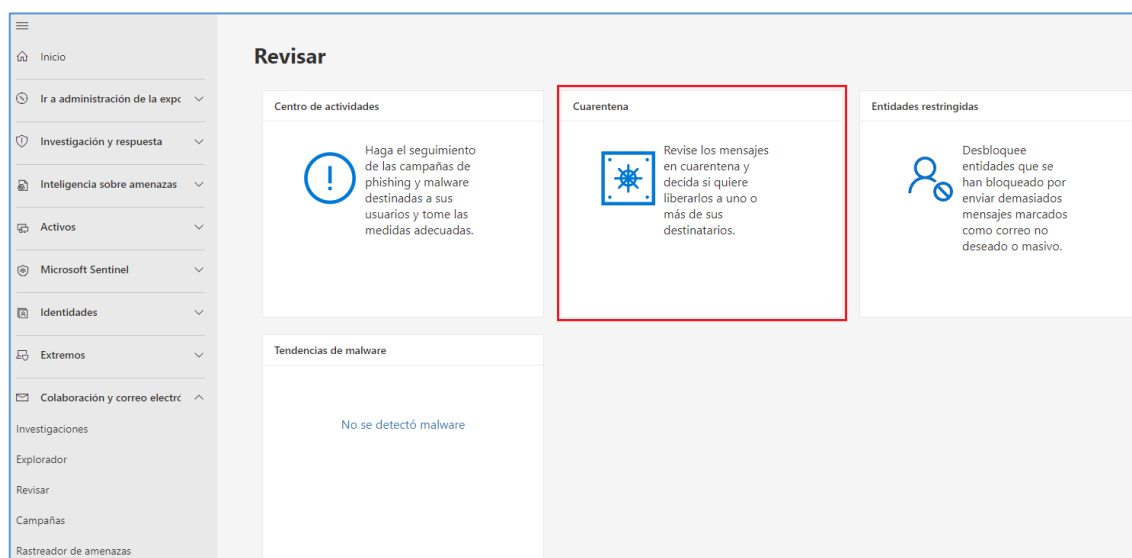
Enviar notificaciones de correo no deseado para el usuario final

Diariamente 

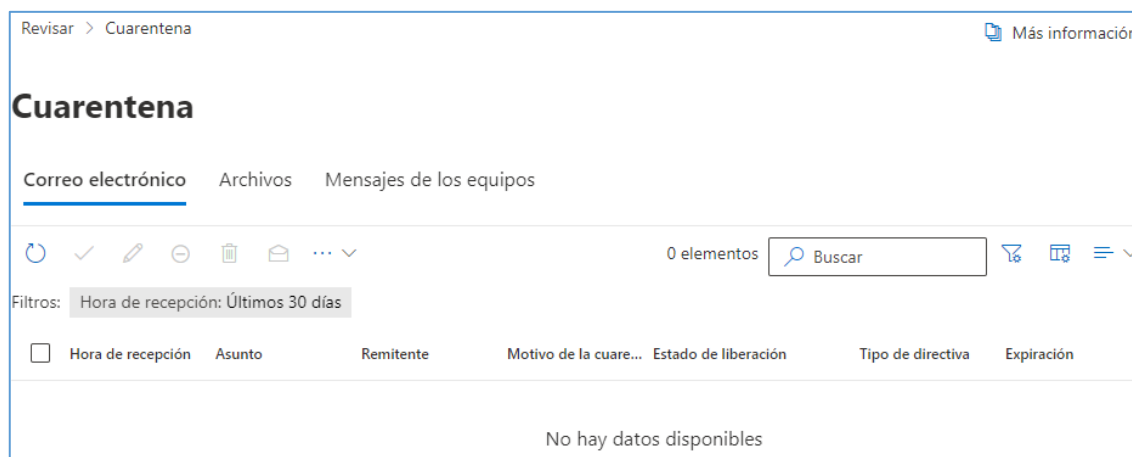
Revisar mensajes en cuarentena

Conviene revisar los elementos en cuarentena. Se pueden liberar uno o más mensajes para los usuarios seleccionados o para todos los usuarios. Si un elemento se detectó incorrectamente como correo no deseado, también se puede informar de un falso positivo.

- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico\Revisar].



También podemos acceder a través de la URL <https://security.microsoft.com/quarantine>.



DKIM

DKIM (DomainKeys Identified Mail) es un proceso de autenticación que puede ayudar a proteger tanto a los remitentes como a los destinatarios de correos electrónicos falsificados y de suplantación de identidad.

Se deben agregar firmas DKIM a los dominios de la organización para que los destinatarios sepan que los mensajes de correo electrónico proceden realmente de usuarios de la organización y que no se han modificado una vez enviados.

Office 365 configura automáticamente DKIM para los dominios "onmicrosoft.com" iniciales. Eso significa que no es necesario hacer nada para configurar DKIM para ningún nombre de dominio inicial.

- a) Acceder al Centro de administración de Exchange, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Configuración de autenticación de correo electrónico].

Reglas y directivas > Directivas de amenazas > Configuración de autenticación de correo electrónico

Configuración de autenticación de correo electrónico

ARC DKIM

DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) es un proceso de autenticación que puede ayudarle a proteger tanto a los remitentes como a los destinatarios de los correos electrónicos falsificados y de phishing. Agregue firmas DKIM a sus dominios para que los destinatarios sepan que los mensajes de correo electrónico proceden realmente de usuarios de su organización y que no se han modificado una vez enviados. [Más información sobre DKIM](#)

 Exportar
  Actualizar
 2 elementos  

Nombre	Dominio aceptado	Tipo de dominio
☐ .mail.onmicrosoft.com	.mail.onmicrosoft.com	Autoritativo
☐ .onmicrosoft.com (dominio de firma predeterminado)	.onmicrosoft.com	Autoritativo

- b) Hacer click en el dominio que se quiere activar DKIM, luego activar la opción **Firmar mensajes para este dominio con firmas de DKIM**.

Firmar mensajes para este dominio con firmas de DKIM

☐ Deshabilitado

Estado

No se están aplicando las firmas de DKIM para este dominio.

Protección contra phishing

Cada organización en Office 365 tiene una política anti-phishing predeterminada que se aplica a todos los usuarios. Se puede crear múltiples políticas anti-phishing personalizadas que puede abarcar a usuarios, grupos o dominios específicos dentro de la organización. Las políticas personalizadas que se creen tienen prioridad sobre la política predeterminada. Agregar, editar y eliminar las políticas anti-phishing se realizan desde el Centro de seguridad de Office 365.

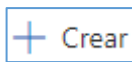
- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Protección contra phishing].

Protección contra phishing

De forma predeterminada, Microsoft 365 incluye características integradas que ayudan a proteger a los usuarios de ataques de phishing. Configure directivas de protección contra suplantación de identidad (anti-phishing) para aumentar esta protección. Por ejemplo, puede refinar la configuración para detectar y prevenir mejor los ataques de suplantación de identidad y suplantación electrónica. La directiva predeterminada se aplica a todos los usuarios dentro de la organización. Puede crear directivas personalizadas de mayor prioridad para usuarios, grupos o dominios específicos. [Más información sobre las directivas de protección contra suplantación de identidad \(anti-phishing\)](#)

💡 0 dominios y usuarios suplantados en los últimos 7 días. Ver suplantaciones			
+ Crear ↓ Exportar ↻ Actualizar 1 elemento Default ✕ Filtrar ≡			
☐ Nombre	Estado	Prioridad	Última modificación
☐ Office365 AntiPhish Default (predeterminado)	● Siempre activada	La más baja	13 de ago. de 2021

b) Pulsar el botón



c) Asignar un nombre y descripción a la directiva.

Nombre de la directiva

Usuarios, grupos y dominios

Umbral de suplantación de identidad y protección

Acciones

Revisar

Nombre de la directiva

Agregue un nombre y una descripción para su directiva de protección contra suplantación de identidad (anti-phishing).

Nombre * ⓘ

Descripción

d) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.

☒ Nombre de la directiva

Usuarios, grupos y dominios

Umbral de suplantación de identidad y protección

Acciones

Revisar

Usuarios, grupos y dominios

Agregue usuarios, grupos y dominios para incluirlos o excluirlos en esta directiva.

Incluya estos usuarios, grupos y dominios *

Usuarios

Y

Grupos

Y

Dominios

☐ Excluir a estos usuarios, grupos y dominios

Umbral de suplantación de identidad y protección

- e) **Umbral de correo electrónico de phishing:** Este umbral controla el nivel de confidencialidad para aplicar modelos de aprendizaje automático a los mensajes para determinar un veredicto de suplantación de identidad (phishing).
- **1 - Estándar:** este es el valor predeterminado. La gravedad de la acción que se realiza en el mensaje depende del grado de confianza de que el mensaje es phishing (confianza baja, media, alta o muy alta). Por ejemplo, los mensajes que se identifican como phishing con un alto grado de confianza tienen las acciones más severas aplicadas, mientras que los mensajes que se identifican como phishing con un bajo grado de confianza tienen acciones menos severas aplicadas.
 - **2 - Agresivo:** Los mensajes que se identifican como phishing con un alto grado de confianza se tratan como si fueran identificados con un alto grado de confianza.
 - **3 - Más agresivo:** los mensajes que se identifican como phishing con un grado medio o alto de confianza se tratan como si se identificaran con un grado de confianza muy alto.
 - **4 - Más agresivo:** los mensajes que se identifican como phishing con un bajo, medio o alto grado de confianza se tratan como si se identificaran con un grado muy alto de confianza.

Reglas y directivas > Directivas de amenazas > Crear una directiva nueva contra el phishing

✓

Nombre de la directiva

✓

Usuarios, grupos y dominios

●

Umbral de suplantación de identidad y protección

○

Acciones

○

Revisar

Umbral de suplantación de identidad y protección

Establezca los umbrales de phishing y las protecciones de suplantación y suplantación electrónica deseadas para esta directiva. [Obtener más información](#)

Umbral de correo electrónico de phishing ⓘ

1 - Estándar

Este es el valor por defecto. La gravedad de la acción que se realiza sobre el mensaje depende del grado de confianza en que el mensaje es de suplantación de identidad (confianza baja, media, alta o muy alta).

- f) **Habilitar usuarios que deben protegerse:** Agregar hasta 350 usuarios internos y externos que quiera proteger de la suplantación por parte de atacantes. Se recomienda agregar los usuarios con roles clave en la organización.

 **Habilitar usuarios que deben protegerse (0/350)** ⓘ

Habilitar la protección de usuarios para hasta 350 remitentes internos y externos.

[Más información sobre cómo agregar usuarios a la protección contra la suplantación](#)

[Administrar 0 remitente\(s\)](#)

g) **Habilitar dominios para proteger:**

En la mayoría de los casos es suficiente con activar el check “Incluir dominios de mi propiedad”.

☒ **Habilitar dominios para proteger (0)**

Habilitar la protección del usuario para estos dominios de remitentes internos y externos

☐ Incluir dominios de mi propiedad ⓘ
[Ver mis dominios](#)

☐ Incluir dominios personalizados ⓘ
[Administrar 0 dominios personalizados](#)

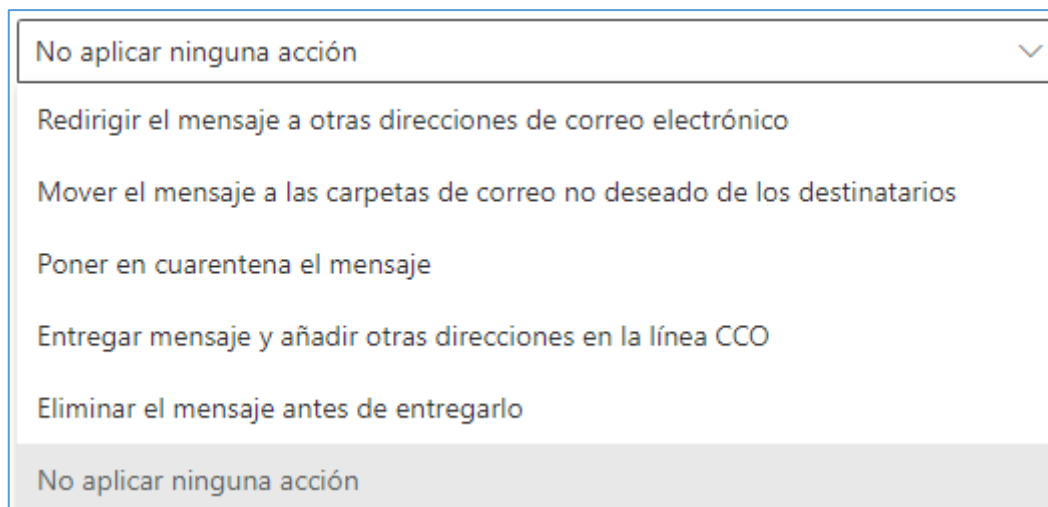
h) **Agregar dominios y remitentes de confianza:** Agregar remitentes y dominios de confianza para que no se marquen como un ataque basado en la suplantación de identidad.

- **Habilitar la inteligencia de buzones:** Permite una inteligencia artificial (IA) que determina los patrones de correo electrónico del usuario con sus contactos frecuentes para identificar posibles intentos de suplantación.
- **Habilitar la inteligencia para protección contra la suplantación de identidad (recomendado):** Permite mejorar los resultados de la suplantación de identidad basándose en el mapa de remitentes individual de cada usuario y permite definir acciones específicas sobre los mensajes suplantados

i) **Habilitar la inteligencia contra la suplantación de identidad (recomendado):** Permite decidir cómo filtrar el correo electrónico de remitentes de dominios suplantados. Para controlar qué remitentes tienen permiso para suplantar sus dominios o los dominios externos, usar la configuración de inteligencia ante la suplantación de identidad en la [página de suplantación con la lista Permitir o bloquear espacios empresariales](#).

Acciones

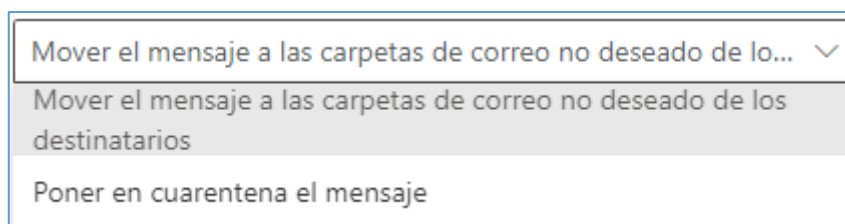
- j) **Si se detecta un mensaje como suplantación de usuario:** Seleccionar una acción si el correo electrónico lo envía un usuario o dominio suplantados:



- k) **Respetar la directiva de registros DMARC cuando el mensaje se detecta como suplantación de identidad:** Esta configuración se activa al respetar la directiva DMARC del remitente para errores explícitos de autenticación por correo electrónico. Cuando se selecciona esta configuración, están disponibles las siguientes opciones:

- Si el mensaje se detecta como suplantación de identidad y la directiva DMARC se establece como p=quarantine: las acciones disponibles son:
 - i. Poner en cuarentena el mensaje
 - ii. Mover el mensaje a las carpetas de Email no deseado de los destinatarios
- Si el mensaje se detecta como suplantación de identidad y la directiva DMARC se establece como p=reject: Las acciones disponibles son:
 - i. Poner en cuarentena el mensaje
 - ii. Rechazar el mensaje

- l) **Si el mensaje se detecta como suplantación de identidad por la inteligencia de suplantación de identidad:** Las opciones disponibles son:



m) **Sugerencias e indicadores de seguridad:** Las sugerencias de seguridad son mensajes de advertencia que se muestran a los destinatarios al abrir mensajes de correo electrónico sospechosos.

- **Mostrar la sugerencia de seguridad del primer contacto (recomendado):** Esta sugerencia se muestra a los destinatarios al recibir por primera vez un mensaje del remitente, o bien no reciben de forma habitual mensajes del remitente.
- **Mostrar el consejo de seguridad sobre la suplantación de identidad del usuario:** Esta sugerencia se muestra a los destinatarios en los mensajes en los que la dirección de correo electrónico del remitente esté incluida en la protección contra la suplantación del usuario.

Texto de sugerencia: "Este remitente es similar a alguien que le ha enviado anteriormente un correo electrónico, pero puede no ser esa persona".

- **Mostrar suplantación de dominio:** Esta sugerencia se muestra a los destinatarios de los mensajes en los que el dominio de correo electrónico del remitente esté incluido en la protección contra la suplantación de dominio.

Texto de sugerencia: "Puede que este remitente esté suplantando un dominio asociado con su organización".

- **Mostrar caracteres inusuales de suplantación de identidad consejo de seguridad:** Esta sugerencia se muestra a los destinatarios de los mensajes donde el nombre o la dirección de correo electrónico del remitente contenga caracteres que no suelen usarse juntos (por ejemplo, una mezcla de símbolos matemáticos y texto normal o una mezcla de letras mayúsculas y minúsculas).

Sugerencia de ejemplo: La dirección de correo electrónico MARY@CoNToso.CoM incluye letras o números inesperados. Le recomendamos no interactuar con este mensaje.

- **Mostrar (?) para los remitentes no autenticados para la suplantación:** Esto ayuda a los usuarios a distinguir si el remitente es realmente quien dice ser mediante una señal visual. Más información sobre remitentes sospechosos en Outlook. Habilite si quiere aplicar un símbolo "?" en la tarjeta de remitente de Outlook si el remitente no supera las comprobaciones de autenticación.
- **Mostrar la etiqueta "vía":** Elija si desea aplicar una etiqueta "vía" en Outlook (p. ej., chris@contoso.com vía fabrikham.com).

Sugerencias e indicadores de seguridad ⓘ

☒
 Mostrar la sugerencia de seguridad del primer contacto (recomendado) ⓘ

☒
 Mostrar el consejo de seguridad sobre la suplantación de identidad del usuario ⓘ

☒
 Mostrar suplantación de dominio ⓘ

☒
 Mostrar caracteres inusuales de suplantación de identidad consejo de seguridad ⓘ

☒
 Mostrar (?) para los remitentes no autenticados para la suplantación ⓘ

☒
 Mostrar la etiqueta "vía". ⓘ

n) **Revisar:** Comprobar la configuración de la directa antes de crearla.

Datos adjuntos seguros

Datos adjuntos seguros en Microsoft Defender para Office 365 proporciona una capa adicional de protección para los datos adjuntos de correo electrónico que ya han sido examinados por la protección contra malware en Exchange Online Protection (EOP). En concreto, Los datos adjuntos seguros usan un entorno virtual para comprobar los datos adjuntos en los mensajes de correo electrónico antes de que se entreguen a los destinatarios (un proceso conocido como detonación).

a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Protección contra phishing].

Reglas y directivas > Directivas de amenazas > Datos adjuntos seguros

Datos adjuntos seguros

Configure una directiva de datos adjuntos seguros para usuarios o grupos específicos con el objetivo de ayudar a impedir que los usuarios abran o compartan archivos adjuntos de correo electrónico con contenido malintencionado. [Más información sobre los datos adjuntos seguros para el correo electrónico](#)

+ Crear ↓ Exportar ↻ Actualizar 📄 Informes ⚙ Configuración global 0 elementos 🔍 . × ≡

☐ Nombre	Estado	Prioridad
No hay datos disponibles		

b) Para editar la configuración global de **Datos adjuntos seguros**, hacer click en el botón  **Configuración global**.

Configuración global

Use esta página para proteger a su organización del contenido malintencionado que haya en los datos adjuntos de correo electrónico y en los archivos de SharePoint, OneDrive y Microsoft Teams.

Proteger archivos de SharePoint, OneDrive y Microsoft Teams

Si un archivo de cualquier biblioteca de SharePoint, OneDrive o Microsoft Teams se identifica como malintencionado, Archivos adjuntos seguros evitará que los usuarios lo abran o lo descarguen. [Más información](#)

Activar Defender para Office 365 para SharePoint, OneDrive y Microsoft Teams

☒

Ayude a los usuarios a permanecer seguros al confiar en un archivo para que se abra desde una vista protegida externa en las aplicaciones de Office.

Para que un usuario tenga permiso para confiar en un archivo abierto en una versión compatible de Office, Microsoft Defender para punto de conexión comprobará el archivo en cuestión. [Obtenga más información sobre Documentos seguros.](#)

Active Documentos seguros para los clientes de Office. Solo disponible con una licencia de Microsoft 365 E5 o Seguridad de Microsoft 365 E5. [Obtenga más información sobre cómo trata Microsoft sus datos.](#)

☒

Permitir que los usuarios hagan clic en la Vista protegida, incluso si Documentos seguros ha identificado el archivo como malintencionado

☐

Guardar **Cancelar**

- c) Para crear una directiva de **Datos adjuntos seguros**, hacer click en el botón

[+ Crear](#)

- d) Asignar un nombre y descripción a la directiva.

☒ Asigne un nombre a la directiva

☐ Usuarios y dominios

☐ Configuración

☐ Revisar

Asigne un nombre a la directiva

Nombre *

CCN-DatosAdjuntosSeguros

Descripción

CCN-DatosAdjuntosSeguros

- e) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.

Reglas y directivas > Directivas de amenazas > Crear directiva de datos adjuntos seguros

☒ Asigne un nombre a la directiva

☒ **Usuarios y dominios**

☐ Configuración

☐ Revisar

Usuarios y dominios

Incluya estos usuarios, grupos y dominios

Usuarios

 CCN-M365-Grupos1 

Y

Grupos

Y

Dominios

☐ Excluir a estos usuarios, grupos y dominios

- f) **Respuesta al malware desconocido en datos adjuntos seguros:** Seleccionar la acción para realizar cuando se detecte malware desconocido en los datos adjuntos.

Respuesta al malware desconocido en datos adjuntos seguros

Selecciona la acción para realizar cuando se detecte malware desconocido en los datos adjuntos. [Más información](#)

Advertencia

- Las acciones **Supervisar** y **Bloquear** pueden causar un retraso significativo en la entrega del mensaje. [Más información](#)
- La Entrega dinámica** solo está disponible para los destinatarios con buzones alojados.
- Para **Bloquear** o **Entrega dinámica**, los mensajes con archivos adjuntos detectados se ponen en cuarentena y solo los puede liberar un administrador.

☒ **Desactivado:** Datos adjuntos seguros no examinará los datos adjuntos seguros.

☐ **Monitor:** entrega el mensaje si se detecta malware y realiza un seguimiento de los resultados del análisis.

☐ **Bloquear:** bloquear mensajes actuales y futuros, y datos adjuntos con malware detectado.

☐ **Entrega dinámica (vista previa de mensajes):** Entrega inmediata del mensaje sin datos adjuntos. Vuelva a adjuntar los archivos una vez completado el examen.

- g) **Directiva de cuarentena:** Seleccionamos la directiva de cuarentena que se aplicara a los mensajes que están en cuarentena por datos adjuntos seguros (bloqueo o entrega dinámica).

AdminOnlyAccessPolicy

Se omitirá el permiso para liberar mensajes en cuarentena para los mensajes con malware detectado y, en su lugar, revertiremos a la solicitud de liberación.

- h) **Redirigir mensajes con datos adjuntos detectados:** Habilitar la redirección y especificar cuenta de correo electrónico para notificación.

Nota: Las opciones de *Contiene idiomas específicos* y *De estos países o regiones* no forman parte de ASF.

Redirigir mensajes con datos adjuntos detectados

Habilitar redirección solo admite la acción Supervisar. [Más información](#)

☒ Habilitar redirección ⓘ

Enviar mensajes que contengan datos adjuntos supervisados a la dirección de correo electrónico especificada.

ccn-O365@ccn.onmicrosoft.com

- i) **Revisar:** Comprobar la configuración de la directiva antes de crearla.

Vínculos seguros

Los vínculos seguros ayudan a evitar que los usuarios sigan vínculos en correos electrónicos y documentos que van a sitios web considerados malintencionados. Desde esta página se configuran directivas que determinan cómo todos los usuarios de la organización, o solo algunos determinados, interactúan con vínculos seguros.

- a) Acceder al Centro de seguridad de Office365, menú [Colaboración y correo electrónico/Reglas y directivas/Directivas de amenazas/Vínculos seguros].

Reglas y directivas > Directivas de amenazas > Vínculos seguros

Vínculos seguros

Vínculos seguros ayuda a evitar que los usuarios sigan vínculos en correos electrónicos y documentos que van a sitios web considerados malintencionados. Utilice esta página para configurar directivas que determinan cómo todos los usuarios de su organización, o solo algunos determinados, interactúan con Vínculos seguros. [Más información sobre Vínculos seguros](#)

+ Crear ↓ Exportar ↺ Actualizar 📄 Informes

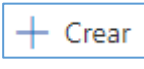
0 elementos 🔍 . ✕ ≡ ▾

☐ Nombre ▾

Estado ▾

Prioridad ▾

No hay datos disponibles

- b) Para crear una directiva, hacer click en el botón .
- c) Asignar un nombre y descripción a la directiva.

- **Asigne un nombre a la directiva**
- Usuarios y dominios
- Configuración de protección de direcciones URL y clics
- Notificación
- Revisar

Asigne un nombre a la directiva

Agregue un nombre y una descripción para su directiva de enlaces seguros.

Nombre *

Descripción

- d) Añadir los usuarios, grupos o dominios a los que se le aplicara esta directiva, también podemos excluir.

- ✓ **Asigne un nombre a la directiva**
- **Usuarios y dominios**
- Configuración de protección de direcciones URL y clics
- Notificación
- Revisar

Usuarios y dominios

Agregue usuarios, grupos y dominios para incluirlos o excluirlos en esta directiva.

Incluya estos usuarios, grupos y dominios

Usuarios

CCN-M365-Grupos1

Y

Grupos

Y

Dominios

☐ Excluir a estos usuarios, grupos y dominios

- e) Configuración de protección de direcciones URL y clics.

- Correo electrónico:

Correo electrónico

- ✓ **Activado:** Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en el correo electrónico. Las direcciones URL se reescriben de forma predeterminada.
- ✓ **Aplicar vínculos seguros a los mensajes de correo electrónico enviados dentro de la organización**
- ✓ **Aplicar un análisis de URL en tiempo real para vínculos sospechosos y vínculos que apuntan a archivos**
- ✓ **Espere a que el análisis de URL se complete antes de entregar el mensaje.**
- ✓ **No vuelva a escribir las direcciones URL; realice las comprobaciones solo a través de la API de vínculos seguros.**

No vuelva a escribir las siguientes URL en el correo electrónico (0)

[Administrar 0 dirección URL](#)

- Teams:

- ☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en Microsoft Teams. Las direcciones URL no se reescriben.

- Aplicaciones de Office 365:

- ☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en aplicaciones de Microsoft Office. Las direcciones URL no se reescriben.

- Configuración de protección de clics:

- ☒ Realizar un seguimiento de los clics de usuario
- ☒ Permitir que los usuarios hagan clic en la dirección URL original
- ☒ Mostrar la personalización de marca de la organización en las notificaciones y las páginas de advertencia

- f) **Notificación:** Seleccionar si se quiere enviar un texto de notificación predeterminado o enviar un texto personalizado.

Notificación

¿Cómo quiere que sus usuarios reciban las notificaciones?

☒ Utilizar el texto de notificación predeterminado

☐ Usar texto de notificación personalizado

- g) **Revisar:** Comprobar la configuración de la directa antes de crearla.

3.2.3.2 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 TIPOS DE BUZONES

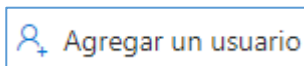
Existen varios tipos de buzones en Exchange, a continuación, se explica en qué consisten y más adelante se verá cómo se crean y administran.

- **Buzón de usuario (user mailbox).** Es el buzón de usuario tradicional para que los usuarios puedan enviar y recibir correo.
- **Buzón de archivo (archive mailbox).** El buzón de archivo funciona como buzón auxiliar de uno primario proporcionando a los usuarios más espacio de almacenamiento de buzones. El archive mailbox puede ser una buena opción para sustituir o reducir el uso de PSTs en la red. En español se encuentra con diversos nombres: archivo local, histórico en línea, buzón de archivo, etc.
- **Buzón de recursos (resource mailbox).** El buzón de recurso es un tipo de buzón especial que representa una sala o equipamiento. La idea es que estos puedan ser incluidos dentro de un meeting y automatizar o facilitar la reserva de estos recursos.
- **Buzón compartido (shared mailbox).** El buzón compartido está orientado a escenarios donde necesitamos un buzón tipo “genérico”. Es decir, un buzón que va a ser gestionado por múltiples personas. Este tipo de buzones no tienen contraseña y solamente se puede acceder a este a través de permisos.
- **Buzón de carpeta pública (public folder mailbox).** Es un tipo de buzón especial “PublicFolder” donde se almacena tanto jerarquía como contenido de estas carpetas públicas (lo que se podría distribuir en varios buzones).
- **Buzón remoto (remote mailbox).** Este buzón se utiliza en una organización híbrida donde existen buzones alojados On premises (local) y otros en Office 365. Cuando se crea un remote mailbox se configura un usuario habilitado para correo con un buzón en la nube asociado.

Crear buzón de usuario (User mailbox)

- a) Los buzones de usuario no se pueden crear desde el panel de administración de Exchange, estos se deben crear desde el portal de Office365. Acceder al Centro de administración de Office365, menú [Usuarios/Usuarios activos].

- b) Hacer click en el botón



- c) Rellenar el formulario.

● Información básica

○ Licencias de producto

○ Configuración opcional

○ Finalizar

Configurar la información básica

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

Nombre

Apellidos

Nombre para mostrar *

Nombre de usuario *

Dominios

@ .onmicrosoft.com

☒ Crear una contraseña de manera automática

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

☐ Enviar contraseña por correo electrónico al finalizar

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

Asignar licencias de producto

Asigne las licencias que desea que tenga este usuario.

Seleccione la ubicación *

España

Licencias (1) *

☒ Asignar una licencia de producto al usuario

☒ **Microsoft 365 Empresa Estándar**

 19 de 25 licencias disponibles

☐ Crear usuario sin licencia de producto (no se recomienda)

Es posible que tengan acceso limitado o que no tengan acceso a Microsoft 365 hasta que asigne una licencia de producto.

Aplicaciones (37)

Mostrar aplicaciones para:

Todas las licencias

☒ Seleccionar todo

Administración de dispositivos móviles para Office 365

☐ Microsoft 365 Empresa Estándar

Esta aplicación se asigna a nivel de organización. No se puede asignar por usuario.

☒ **Aplicaciones de Microsoft 365 para negocios**

 Microsoft 365 Empresa Estándar

☒ **Avatares para Teams**

 Microsoft 365 Empresa Estándar

☒ **Avatares para Teams (adicional)**

 Microsoft 365 Empresa Estándar

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

Configuración opcional

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

Roles (Usuario: sin acceso de administración)

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

[Más información sobre roles de administración](#)

☒ Usuario (sin acceso al centro de administración)

☐ Acceso al centro de administración

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

☐ Administrador de Exchange 

☐ Administrador de SharePoint 

☐ Administrador de Teams 

☐ Administrador de soporte técnico de servicio 

☐ Administrador de usuarios 

f) Añadimos información del usuario, si es necesario.

Información del perfil 

Puesto

Departamento

Oficina

Teléfono de la oficina **Número de fax**

- g) Una vez creado el usuario aparece el siguiente mensaje.



CCN-O365 agregado a los usuarios activos

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

Detalles del usuario

Nombre para mostrar: CCN-O365

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

Contraseña: ***** [Mostrar](#)

Buzón de archivo local (archive mailbox)

- Acceder al [Centro de administración de Exchange](#), luego acceder al menú [Destinatarios/Buzones].
- Hacer click en la cuenta que se quiere activar el buzón de archivado.
- Click en Administrar el archivo del buzón.



User mailbox

 Ocultar buzón  Reenvío de correo electrónico ...

General Organización Delegación Buzón **Otros**

Atributos personalizados

[Atributos personalizados](#)

Respuestas automáticas

[Administrar respuestas automáticas](#)

Convertir en buzón compartido

[Convertir en buzón compartido](#)

Archivo del buzón

Habilitado

[Administrar el archivo del buzón](#)

Sugerencia de correo

Desactivada

[Administrar información sobre correo](#)

Miembro de

[Pertenencia al grupo](#)

Recuperar elementos eliminados

[Recuperar elementos eliminados](#)

Suspensión per litigio

[Administrar suspensión por litigio](#)

Límite de destinatarios

[Establecer límite de destinatarios](#)

- d) Habilitamos la opción de archivado.

Administrar el archivo del buzón

Estado del archivo del buzón ☐ Deshabilitado

- e) Para ver los detalles del archivado, en el mismo menú del punto anterior los podemos ver una vez activado.

Administrar el archivo del buzón

Estado del archivo del buzón ☒ Habilitado

Uso de archivo

El uso del archivo muestra el límite de almacenamiento de archivo y el uso actual.
[Más información](#)

El archivo de ampliación automática está usando 0.00 GB.

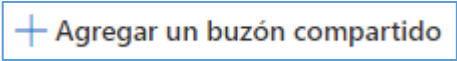
 Almacenamiento adicional es una característica premium que requiere una licencia de Exchange Online Plan 2 o Archivado de Exchange Online para habilitarla para cada buzón de usuario. [Más información](#)

Nombre 

In-Place Archive - CCN

Buzón compartido (*shared mailbox*)

Es importante activar la “Auditoría de buzones compartidos” para permitir la trazabilidad en estos buzones, como se describe más adelante en este mismo apartado.

- a) Acceder al [Centro de administración de Exchange](#), luego acceder al menú [Destinatarios/Buzones].
- b) Click en el botón .
- c) Completar el formulario.

Agregar un buzón de correo compartido

El correo electrónico puede enviarse a y desde el nombre y la dirección de correo del buzón compartido, en lugar de una persona. Después de crear el buzón compartido, puede agregar miembros que puedan leer y responder al correo.

Nombre para mostrar *

Dirección de correo electrónico *

@



Alias

Editar un buzón compartido

- Acceder al [Centro de administración de Exchange](#), luego acceder al menú [Destinatarios/Buzones].
- Doble clic sobre el nombre del buzón compartido.
- Editar las propiedades del buzón.



CCN-Shared

 Shared mailbox

 Ocultar buzón
  Reenvío de correo electrónico
 ...

[General](#)
[Organización](#)
[Delegación](#)
[Buzón](#)
[Otros](#)

Información de contacto

Nombre	Apellidos
Nombre para mostrar	Alias
CCN-Shared	CCN-Shared
Id. de usuario	Teléfono móvil
CCN-Shared@.onmicrosoft.com	

[Administrar información de contacto](#)

Ocultar de la lista global de direcciones (LGD) No Administrar la ocultación de LGD	Direcciones de correo CCN-Shared@.com Administrar los tipos de direcciones de correo electrónico
--	---

Uso del buzón: 0.01 MB/49.5 GB  0.00 % de uso Último inicio de sesión: El buzón aún no ha iniciado sesión Más información acerca del uso del buzón	Aplicaciones de correo electrónico y dispositivos móviles Configuración predeterminada de Outlook en la web, IMAP, POP3, MAPI aplicada Administrar la configuración de las aplicaciones de correo electrónico Administrar dispositivos móviles
--	--

d) **Permisos de:**

- **Enviar como:** Si se quiere permitir al delegado enviar un correo electrónico desde este buzón compartido hay que añadir su nombre a la lista “Enviar como”. Desde la perspectiva del destinatario, el correo es enviado por este buzón compartido.

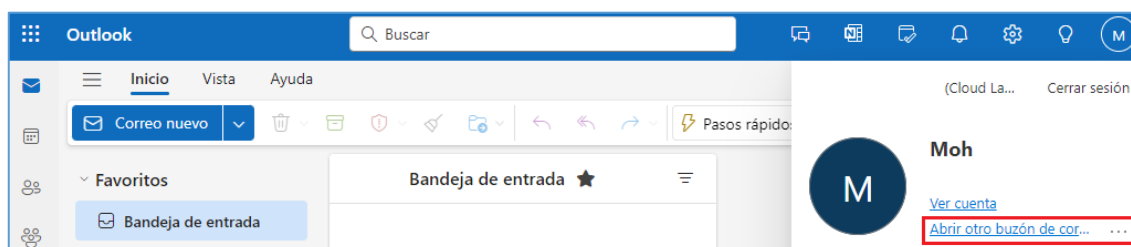
- **Lectura y administración (acceso total):** El permiso Acceso completo le permite a un delegado abrir el buzón compartido y comportarse como el propietario del buzón de correo.



Gestionar el buzón compartido en Outlook

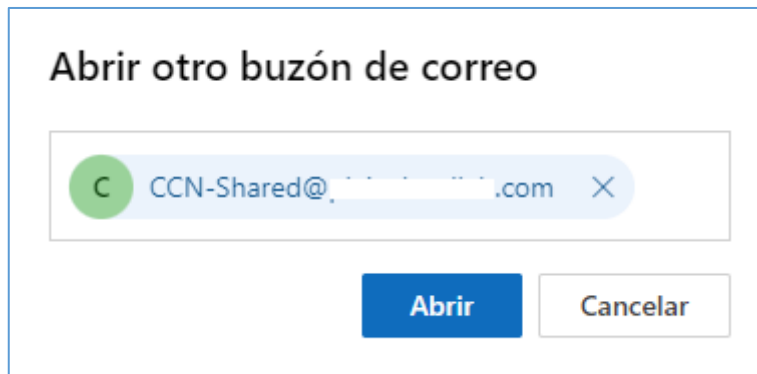
Un usuario delegado puede gestionar correos en nombre del buzón compartido de la siguiente forma:

- Entrar en la web de Outlook, y pulsar en el icono de administración de cuentas de usuario en el panel superior derecho.

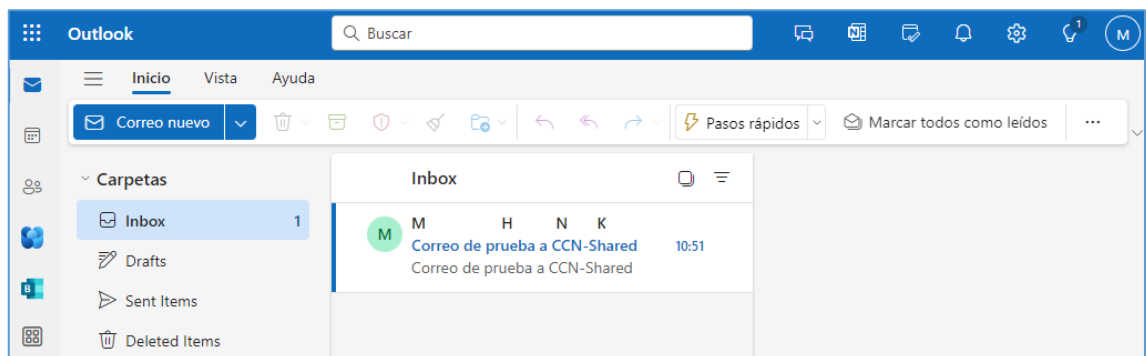


- Clic en "Abrir otro buzón de correo".

c) Introducir nombre del buzón compartido.



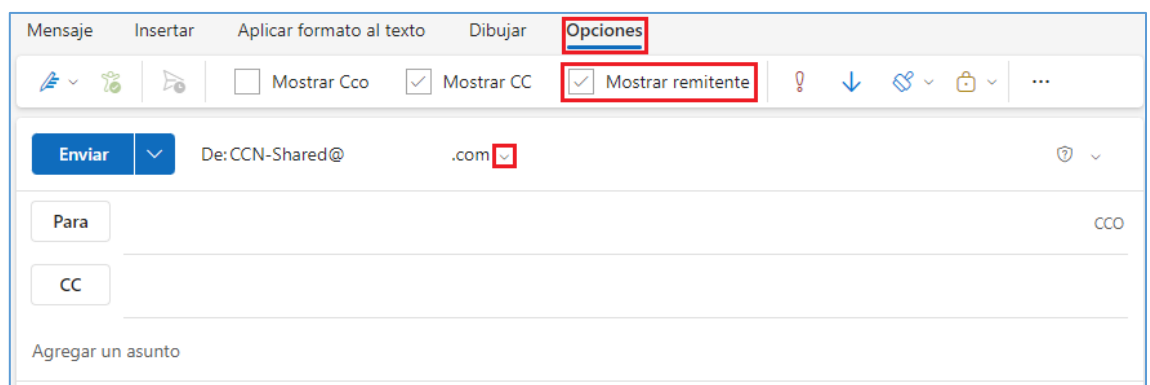
d) Se abre Outlook con todos los elementos del buzón compartido.



Ahora se podrá enviar correos, leer los recibidos, etc.

Otra forma de enviar un correo en nombre de un buzón compartido sin abandonar el panel del usuario delegado es:

- 1) Abrir Outlook con la identidad del usuario delegado.
- 2) Elegir "Nuevo correo".
- 3) Si no aparece el campo "De" en la parte superior del mensaje, en opciones elegir "Mostrar remitente"



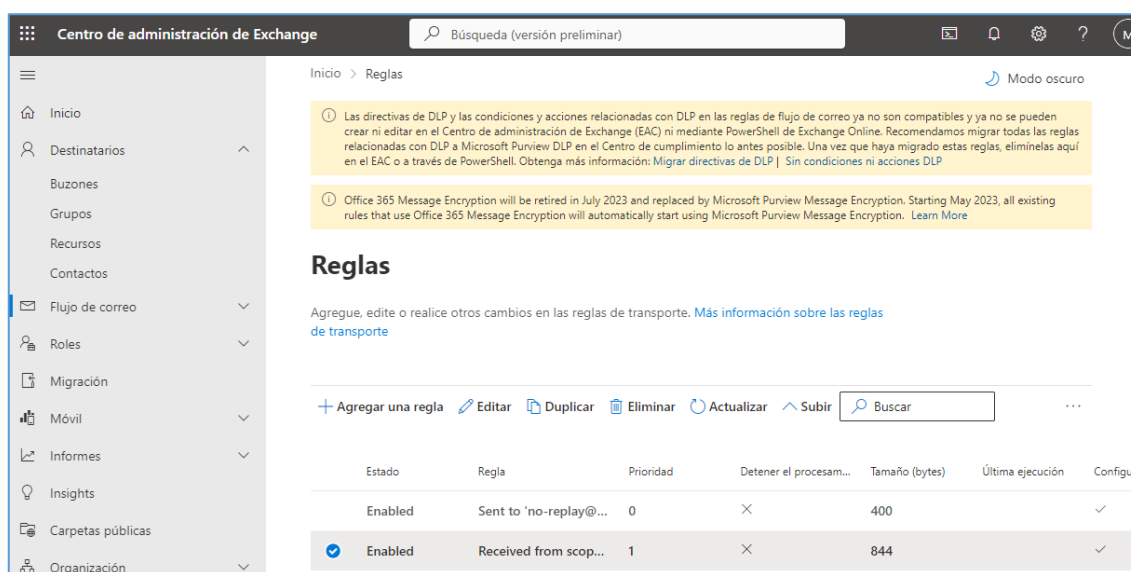
Gestionar el buzón compartido en Outlook

Ver apartado [3.1.2.2 Registro de actividad].

4.2 REGLAS DE FLUJO DE CORREO

Las reglas de flujo de correo (también conocidas como reglas de transporte) sirven para identificar y realizar acciones en mensajes que fluyen a través de la organización de Exchange Online. Las reglas de flujo de correo son similares a las reglas de la Bandeja de entrada que hay disponibles en Outlook y en Outlook en la web. La diferencia principal radica en que las reglas de flujo de correo actúan en los mensajes mientras se encuentran en tránsito y no después de que se entreguen al buzón de correo.

Se acceden desde el Centro de administración de Exchange, menú [Flujo de correo/Reglas].



- **Condiciones:** Identificar los mensajes a los que se van a aplicar las acciones. Algunas condiciones examinan campos de encabezado del mensaje (por ejemplo, los campos Para, De o CC). Otras examinan propiedades del mensaje (por ejemplo, el asunto, el cuerpo, los datos adjuntos, el tamaño del mensaje o la clasificación del mensaje). La mayoría de las condiciones exigen que se especifique un operador de comparación (por ejemplo, es igual a, no es igual a o contiene) y un valor de coincidencia.
- **Excepciones:** opcionalmente, identificar los mensajes a los que no deben aplicarse las acciones. Los mismos identificadores de mensaje que están disponibles en las condiciones están también disponibles en las excepciones. Las excepciones invalidan las condiciones e impiden que se apliquen las acciones de regla a un mensaje, aunque este cumpla todas las condiciones configuradas.
- **Acciones:** especificar qué hacer con los mensajes que coincidan con las condiciones de la regla y que no coincidan con ninguna de las excepciones. Existen numerosas acciones disponibles, como, por ejemplo, rechazar, eliminar o redirigir mensajes; agregar más destinatarios; agregar prefijos al

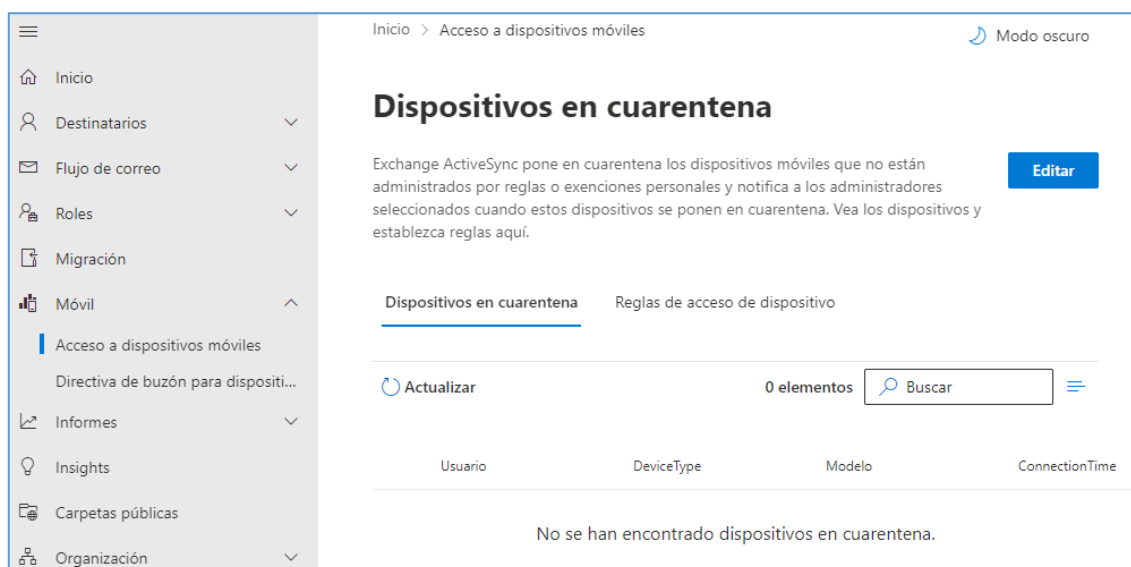
asunto del mensaje; o insertar avisos de declinación de responsabilidades en el cuerpo del mensaje.

- **Propiedades:** especificar otras opciones de configuración de reglas que no sean condiciones, excepciones o acciones, por ejemplo, cuándo se debe aplicar la regla, si se debe aplicar o probar la regla y el período de tiempo en el que la regla está activa.

4.3 REGLAS DE ACCESO DE DISPOSITIVO Y CUARENTENA

Se pueden usar muchos clientes diferentes para obtener acceso a la información de un buzón de correo de Exchange Online. Estos clientes incluyen programas de escritorio como Microsoft Outlook, Outlook en la web (anteriormente conocido como Outlook Web App) y clientes móviles, como teléfonos, tabletas y otros dispositivos móviles.

- a) Desde el Centro de administración de Exchange, menú [Móvil\Acceso de dispositivo móviles]:



Inicio > Acceso a dispositivos móviles

Modo oscuro

Dispositivos en cuarentena

Exchange ActiveSync pone en cuarentena los dispositivos móviles que no están administrados por reglas o exenciones personales y notifica a los administradores seleccionados cuando estos dispositivos se ponen en cuarentena. Vea los dispositivos y establezca reglas aquí.

Editar

Dispositivos en cuarentena Reglas de acceso de dispositivo

Actualizar 0 elementos Buscar

Usuario	DeviceType	Modelo	ConnectionTime
No se han encontrado dispositivos en cuarentena.			

- b) Pulsar el botón

Editar

Configuración de acceso de Exchange ActiveSync

Configuración de la conexión

Cuando dispositivos móviles de la familia o modelo seleccionados intentan conectarse:

- ☐ Permitir acceso
- ☐ Bloquear acceso
- ☒ Cuarentena: permitirme decidir si bloquearlo o permitirlo más tarde

Mensajes de correo de notificación de cuarentena

Selecciona los administradores que recibirán mensajes de correo cuando se ponga en cuarentena un dispositivo móvil.

Buscar nombre o correo electrónico

Texto que se incluirá en los mensajes enviados a los usuarios que tengan dispositivos móviles en cuarentena, bloqueados o en proceso de ser identificados:

Nota: Se recomienda establecer el valor “Cuarentena” o “Bloquear acceso” para dispositivos que no están administrados por una regla o una exención personal.

4.4 DIRECTIVAS DE BUZON DE CORREO PARA DISPOSITIVOS MOVILES

En Microsoft 365 o Office 365, puede crear directivas de buzón de dispositivo móvil para aplicar un conjunto común de directivas o configuración de seguridad a una colección de usuarios. Se crea una directiva de buzón de dispositivo móvil predeterminada en cada organización de Microsoft 365 o Office 365.

Puede usar las directivas de buzones de dispositivos móviles para administrar diferentes parámetros de configuración. Por ejemplo, los siguientes:

- Solicitar una contraseña.
- Especificar la longitud mínima de la contraseña.
- Permitir un PIN numérico o requerir caracteres especiales en la contraseña.
- Designar el tiempo que puede permanecer inactivo un dispositivo antes de solicitar al usuario que vuelva a escribir la contraseña.

- Borrar un dispositivo tras un número específico de intentos de contraseña erróneos.

Desde el Centro de administración de Exchange, menú [Móvil\Directiva de buzón para dispositivos móviles]:



Inicio > Directiva de buzón para dispositivos móviles

Directiva de buzón para dispositivos móviles

Puede crear directivas de buzón de dispositivos móviles para aplicar un conjunto común de directivas o configuraciones de seguridad a una colección de usuarios. Se crea una directiva de buzón de dispositivo móvil predeterminada para cada organización. [Más información sobre las directivas de buzón de dispositivo](#)

+ Nuevo Editar Eliminar Actualizar 1 elemento 1 selected Buscar

Nombre	Modificado	Contraseña
Default	8/17/2020 12:52:24 PM	Opcional

4.5 DIRECTIVA DE USO COMPARTIDO

Es posible que las personas de la organización quieran compartir calendarios con asociados de empresa individuales, amigos o familiares. Las directivas de uso compartido controlan el modo en que los usuarios comparten sus calendarios con otras personas de la organización.

a) Se accede desde el Centro de administración de Exchange, menú [Organización\uso compartido].

- Uso compartido de la organización:



Inicio > Uso compartido

Uso compartido

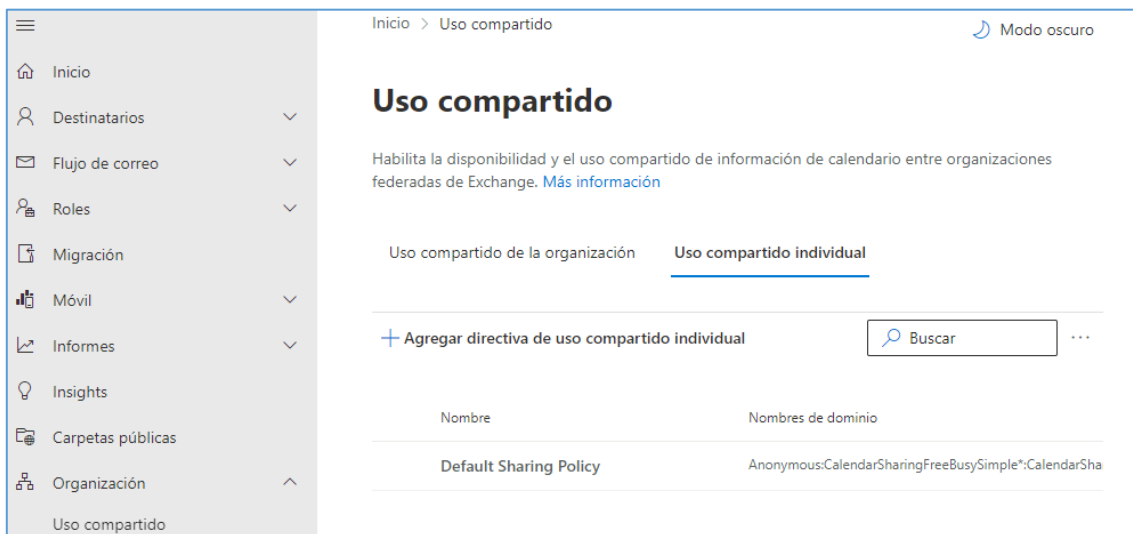
Habilita la disponibilidad y el uso compartido de información de calendario entre organizaciones federadas de Exchange. [Más información](#)

Uso compartido de la organización Uso compartido individual

+ Agregar relación de organización Actualizar 1 elemento Buscar

Nombre	Nombres de dominio
O365 to On-premises - 7080683c	

- Uso compartido individual:



Inicio > Uso compartido Modo oscuro

Uso compartido

Habilita la disponibilidad y el uso compartido de información de calendario entre organizaciones federadas de Exchange. [Más información](#)

Uso compartido de la organización **Uso compartido individual**

+ Agregar directiva de uso compartido individual

Nombre	Nombres de dominio
Default Sharing Policy	Anonymous:CalendarSharingFreeBusySimple*;CalendarSha

5. GLOSARIO Y ABREVIATURAS

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

Término	Definición
ASF	<i>Advanced Spam Filtering</i> . Filtro de correo no deseado avanzado.
CNAME	Un CNAME o registro de <i>Canonical Name</i> es un tipo de registro que puede encontrarse en un DNS y que permite al usuario especificar el alias de un nombre de dominio.
DKIM	<i>DomainKeys Identified Mail</i> . Es un proceso de autenticación que puede ayudar a proteger tanto a los remitentes como a los destinatarios de correos electrónicos falsificados y de suplantación de identidad.
Mailbox	Buzón de correo electrónico.
Outlook on the Web	Es lo que antes se conocía como Outlook Web App (OWA). Incluye un cliente de correo electrónico basado en la web, una herramienta de calendario, un administrador de contactos y un administrador de tareas.
Phishing	<i>Suplantación de identidad</i> . Ataque que se caracteriza por intentar adquirir información sensible de forma fraudulenta.
PST	Son archivos de datos de Outlook (.pst), que se guardan en el PC, y contienen mensajes y otros elementos de Outlook.
Recipient	En una organización de Exchange, se refiere a personas y recursos. Un <i>recipient</i> es un objeto con email habilitado en AD y al cual Microsoft Exchange puede entregar o enrutar mensajes.

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		Estado
op	Marco Operacional		
op.acc	Control de Acceso		
op.acc.1	Identificación Se ha configurado el uso de cuentas y la asignación de licencias a usuarios. Siguiendo las recomendaciones de Office 365 basada en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]	Aplica:	Cumple:
		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas:	Observaciones:
		☐ Si ☐ No	
op.acc.2	Requisitos de Acceso Se han comprobado los permisos de acceso a buzones compartidos de igual modo la configuración del tipo de buzón.	Aplica:	Cumple:
		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas:	Observaciones:
		☐ Si ☐ No	

op.acc.3	Segregación de funciones y tareas Se ha asignado adecuadamente los <i>roles</i> y <i>grupos de roles</i> de Exchange Online.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.acc.4	Proceso de gestión de derechos de acceso Se han creado y/o editado <u>directivas de asignación de roles</u> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.acc.5 y op.acc.6	Mecanismo de autenticación Se ha bloqueado el acceso a aplicaciones que no usan la autenticación moderna. Siguiendo las recomendaciones del apartado 3.1.1.5 Mecanismos de autenticación de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

op.exp	Explotacion		
op.exp.8	Registro de la actividad		
	Se ha activado el registro de auditoría.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.8	Registro de la actividad		
	Se ha comprobado que la auditoría de buzones compartidos se encuentra activada.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.mon	Monitorización del sistema		
	Se han configurado alertas en el <i>Centro de Seguridad de Office 365</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ 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 etiquetas de retención.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.2	Calificación de la información		
	Se han aplicado <i>sensitivity labels</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	Copias de seguridad		
	Se ha aplicado la <i>retención por juicio</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	Copias de seguridad		
	Se controla el uso de <i>Single Item Recovery</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	Copias de seguridad		
	Se han realizado copias con el archivado de Exchange.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info	Reglas de flujo de correo		
	Se han creado reglas de flujo de correo para la organización de Exchange	Aplica:	Cumple:

	Online.	☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s	Protección de los servicios		
mp.s.1	Protección de correo electrónico		
	Se han aplicado filtros de malware.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		
	Se han aplicado filtros de conexión.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		

	Se han aplicado filtros de <i>correo no deseado tanto entrantes como salientes</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		
	Se han creado directivas de cuarentena.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		
	Se han revisado los correos en <i>cuarentena</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		

	Se ha configurado el proceso de autenticación DKIM.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección contra phishing		
	Se ha configurado políticas de anti-phishing ATP.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		
	Se ha configurado políticas de Datos adjuntos seguros.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.1	Protección de correo electrónico		
	Se ha configurado políticas de vinculos seguros.	Aplica:	Cumple:

		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s.4	Protección frente a la denegación de servicio		
	Se ha tenido en cuenta la información detallada en la guía [CCN-STIC-884A - Guía de configuración segura para Azure] sobre el <i>sistema de defensa DDoS de Azure</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
	OTRAS CONSIDERACIONES DE SEGURIDAD		
	ActiveSync		
	Se ha configurado ActiveSync para dispositivos móviles.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
	Directivas de buzón de correo para dispositivos móviles		

	Se han creado directivas de buzón de correo para dispositivos móviles.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
	Directivas de uso compartido		
	Se han creado directivas de uso compartido.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

