

2023-02-17



HORNETSECURITY

365 TOTAL PROTECTION

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Contents

Convenciones lingüísticas y símbolos en la documentación.....	4
Acerca de 365 Total Protection.....	6
Incorporación de un cliente nuevo como partner.....	8
Crear un enlace de incorporación.....	8
Añadir clientes de 365 Total Protection a Control Panel.....	9
Instalar 365 Total Protection.....	10
Configurar 365 Total Backup.....	14
Actualización a 365 Total Protection como cliente.....	25
Actualizar a 365 Total Protection.....	25
Convenciones lingüísticas y símbolos en la documentación.....	41
Acerca de la migración de buzones de correo.....	43
Limitaciones de la migración de buzones de correo.....	45
Requisitos para la migración de buzones de correo.....	46
Requisitos para buzones de correo.....	47
Crear un grupo de roles en un servidor Exchange.....	48
Crear un grupo de roles en Microsoft 365.....	53
Conceder derechos de lectura y administración de buzones de correo en Microsoft 365.....	57
Conceder permisos de lectura y administración de buzones de correo en Microsoft 365 mediante PowerShell.....	60
Permitir el acceso a los servicios web de Exchange.....	60
Desactivar la limitación de los servicios web de Exchange.....	63
Migración de datos de buzones de correo.....	65
Validar un entorno.....	66
Descartar la validación de un entorno.....	71
Migrar buzones de correo.....	73
Finalizar la migración de buzones de correo.....	82
Configurar 365 Total Backup.....	83
Configuración de los servicios de Microsoft.....	95
Configuración básica.....	95

Grundlegende Configuración.....	95
Configuración avanzada.....	108
Configuración avanzada.....	108
Adquirir 365 Total Protection.....	110
Visualización de las cantidades de buzones de correo, licencias y dominios.....	111
Administración de buzones de correo.....	112
Administración de grupos en Control Panel.....	113
Sincronizar grupos de Microsoft 365 en Control Panel.....	113
Interacción de 365 Total Protection con otros servicios.....	116
Email Encryption.....	116
Activar Continuity Service (solo para 365 Total Protection Enterprise).....	117
Atributos sincronizados desde Azure Active Directory.....	119
Retirada tras el periodo de prueba o baja.....	121
Eliminar o desactivar el conector.....	121
Eliminar clientes.....	122
Índice.....	125



Convenciones lingüísticas y símbolos en la documentación

Aclaración sobre el género empleado

Para mejorar la legibilidad, en esta documentación se emplea el masculino genérico. Cabe señalar aquí que el uso exclusivo de la forma masculina debe entenderse como independiente del género.

Símbolos utilizados

Los siguientes símbolos se utilizan para identificar mejor los pasos relevantes dentro de los capítulos dedicados a instrucciones:

Símbolo	Significado	Explicación
	Requisito	Condición que debe cumplirse antes del siguiente paso.
	Resultado intermedio	Resultado alcanzado provisionalmente tras un paso concreto.
	Resultado final	Resultado alcanzado una vez finalizada la secuencia de pasos de un capítulo de instrucciones.

Advertencias e indicaciones de seguridad

Las advertencias e indicaciones de seguridad se emplean para informar al usuario sobre riesgos residuales y peligros, así como sobre el procedimiento a emplear para evitarlos. En esta documentación se emplean las siguientes advertencias e indicaciones de seguridad:

Símbolo	Significado	Explicación
	NOTA	Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores.
	CONSEJO	Indicación sobre opciones de configuración.
	IMPORTANTE	Advertencias con información sobre limitaciones u opciones de configuración importantes del servicio.



Símbolo	Significado	Explicación
	ATENCIÓN	Advertencia sobre costes adicionales que pueden surgir al contratar servicios.
	ADVERTENCIA	Advertencia sobre una posible pérdida de datos.
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.



Acerca de 365 Total Protection

Nuestro servicio 365 Total Protection se dirige a clientes de Microsoft 365 y protege sus correos y datos en Microsoft 365. 365 Total Protection se ha desarrollado especialmente para Microsoft 365 y está perfectamente integrado con dicho entorno.

365 Total Protection está disponible en las versiones Business, Enterprise y Enterprise Backup. Estas versiones se diferencian entre sí en diversas funciones.

- Todas las versiones protegen los correos electrónicos y datos mediante el filtrado de archivos adjuntos (véase [Acerca de Content Control](#)), reglas de filtrado de correo personalizadas (véase [Acerca de Compliance Filter](#)) y ajustes relativos al cifrado de correos (véase [Email Encryption](#)).
- Las versiones Enterprise y Enterprise Backup permiten además archivar correos conforme a las exigencias legales (véase [Archiving](#)), ofrecen mecanismos de análisis para la detección de amenazas complejas (véase [Estructura y funcionamiento de ATP](#)) y mantienen el tráfico de correo electrónico funcionando en caso de avería del servidor de correo del cliente (véase [Sobre Continuity Service](#)). Adicionalmente, estas versiones permiten a los administradores eliminar correos ya entregados de los buzones de correo de Microsoft 365 (véase [Tipos de buzón de correo](#)) de sus usuarios (véase [Ex Post Deletion](#)), si, por ejemplo, se determina con posterioridad que un correo supone una amenaza.
- La versión Enterprise Backup permite además copiar y restaurar datos del inquilino de Microsoft 365 y de los terminales con Windows de un cliente (véase [Acerca de 365 Total Backup](#)).

Tras configurar 365 Total Protection para un cliente, los dominios, grupos y usuarios del cliente en Control Panel se sincronizarán con los de su organización de Microsoft 365. Posteriormente, dichos dominios, grupos y usuarios se sincronizarán periódicamente con Microsoft 365.

Los administradores a nivel de partner pueden configurar directamente 365 Total Protection para un nuevo cliente durante la incorporación (véase [Incorporación de un cliente nuevo como partner](#) en la página 8). Nuestros clientes preexistentes pueden efectuar por sí mismos la actualización a 365 Total Protection (véase [Actualización a 365 Total Protection como cliente](#) en la página 25).



Nota:

Los clientes preexistentes que actualicen a la versión Enterprise o Enterprise Backup y hayan empleado anteriormente un servidor Exchange local pueden migrar datos de buzones de correo de su servidor Exchange local a su inquilino de Microsoft 365 durante la actualización (véase [Acerca de la migración de buzones de correo](#) en la página 43). Esto facilita la transición de los clientes a Microsoft 365.



Una vez configurado 365 Total Protection comienza una fase de prueba de 14 días. Para poder seguir empleando 365 Total Protection después de la fase de prueba, el cliente deberá adquirir el servicio (véase [Adquirir 365 Total Protection](#) en la página 110).



Incorporación de un cliente nuevo como partner

Con 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) los partners pueden efectuar una configuración automática para clientes con cuenta de Microsoft 365. Todos los dominios y usuarios creados en Microsoft 365 se añaden automáticamente y se muestran en Control Panel.



Nota:

Los miembros de grupos de Microsoft 365 también se pueden sincronizar en Control Panel. Para sincronizar miembros de grupos, los administradores a nivel de cliente deben crear grupos con los mismos nombres en Control Panel. Para más información, véase [Administración de grupos en Control Panel](#) en la página 113.

Los administradores a nivel de partner tienen dos opciones para configurar clientes: Un administrador a nivel de partner o bien envía un enlace de incorporación al cliente (véase [Crear un enlace de incorporación](#) en la página 8) para que éste efectúe la configuración por sí mismo, o bien inicia sesión en Microsoft con los datos de acceso de administrador del cliente y efectúa allí el proceso de incorporación (véase [Añadir clientes de 365 Total Protection a Control Panel](#) en la página 9). Cuando un administrador a nivel de cliente haya iniciado la incorporación de un cliente, el administrador puede configurar 365 Total Protection para el cliente (véase [Instalar 365 Total Protection](#) en la página 10). Si se ha seleccionado la versión 365 Total Protection Enterprise Backup, el administrador a nivel de partner también puede configurar 365 Total Backup para el cliente para copiar los datos de su inquilino de Microsoft 365.

A continuación es preciso realizar algunos ajustes de DNS en los dominios para derivar el tráfico de correo electrónico.

Crear un enlace de incorporación

Puede crear un enlace de incorporación para sus clientes con el que éstos podrán efectuar por sí mismos la configuración de nuestros servicios. El enlace dirige a un formulario de incorporación de 365 Total Protection. Puede compartir este enlace de incorporación con sus clientes para que éstos puedan efectuar por sí mismos la configuración de 365 Total Protection (véase [Instalar 365 Total Protection](#) en la página 10). El enlace puede emplearse varias veces.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee crear el nuevo cliente.
3. Vaya a **365 Total Protection > 365 Total Protection**.



4. En **Su dirección de incorporación**, seleccione una versión de 365 Total Protection para sus clientes. Tiene las siguientes opciones:

- **Dejar sin seleccionar**
- **Business**
- **Enterprise**
- **Enterprise Backup**



Se crea un enlace unívoco.

5. Haga clic en  para copiar el enlace al portapapeles.



El enlace de incorporación ha sido creado.

Añadir clientes de 365 Total Protection a Control Panel

Si dispone de datos de acceso de administrador al entorno de Microsoft 365 (véase [Acerca de 365 Total Protection](#) en la página 6), puede añadir un nuevo cliente de 365 Total Protection directamente a través de Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner bajo el cual desee crear un nuevo cliente de 365 Total Protection.



Figura 1: Seleccionar un partner en la selección de ámbitos

3. Vaya a **365 Total Protection > 365 Total Protection**.



4. Seleccione una versión de 365 Total Protection para el nuevo cliente.



Figura 2: Seleccionar versión



Se muestra el formulario de incorporación.



Se ha iniciado la incorporación de un nuevo cliente de 365 Total Protection.

A continuación puede configurar 365 Total Protection para el cliente (véase [Instalar 365 Total Protection](#) en la página 10).

Instalar 365 Total Protection

Puede configurar 365 Total Protection.



Ha abierto el formulario de incorporación de 365 Total Protection (véase [Añadir clientes de 365 Total Protection a Control Panel](#) en la página 9).

Una vez abierto el formulario de incorporación de 365 Total Protection, puede configurar dicho servicio (véase [Acerca de 365 Total Protection](#) en la página 6).



1.



Importante:

El campo **Nombre mostrado en Control Panel (dominio)** es para indicar el dominio principal del cliente, y no su dominio .onmicrosoft. Este dominio se mostrará en Control Panel.

Introduzca sus datos de contacto en el formulario de incorporación.



Nota:

Estos datos de contacto sirven para que podamos ponernos en contacto con usted en caso de dificultades.

INCORPORACIÓN A 365 TOTAL PROTECTION

Nombre mostrado en Control Panel (dominio)
ejemplo.com

 Empresa
Ejemplo

Título Nombre Apellidos
D. John Doe

Correo electrónico Teléfono
doe@ejemplo.com 123456

Protección de datos
 Acepto que Hornetsecurity o un partner certificado procese mis datos y se ponga en contacto conmigo conforme a la [política de privacidad](#).

IT Security News
 Me gustaría recibir las IT Security News regularmente.

 Iniciar ahora

Figura 3: Introducir datos de contacto

2. Marque la casilla bajo **Protección de datos**.
3. Opcional: Si desea recibir nuestras IT Security News, marque la casilla **Me gustaría recibir las IT Security News regularmente**.



4.

Atención:

Una vez activado 365 Total Protection, comenzará un periodo de prueba gratuito de 14 días. Para poder seguir empleando 365 Total Protection después de la fase de prueba, el cliente deberá adquirir el servicio (véase [Adquirir 365 Total Protection](#) en la página 110).

Haga clic en **Iniciar ahora** para iniciar el proceso de configuración.



Se abre la página de inicio de sesión de Microsoft.

5. Inicie sesión en Microsoft 365 con sus datos de acceso de administrador.

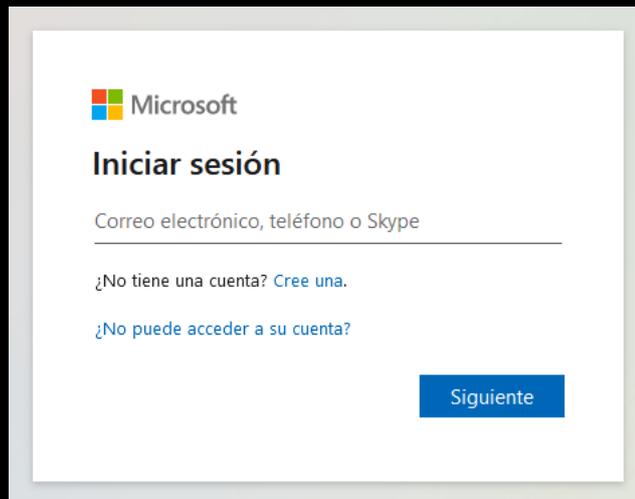


Figura 4: Introducir el nombre de usuario de Microsoft

Nota:

A continuación, en la sincronización, solo se transmiten dominios y buzones de correo. No se realizan cambios en la configuración de Microsoft. Los grupos también se sincronizan con Microsoft 365 si un cliente ha creado manualmente grupos con los mismos nombres en Control Panel (véase [Administración de grupos en Control Panel](#) en la página 113).



6. Conceda los permisos necesarios para conectar nuestros servicios con Microsoft.

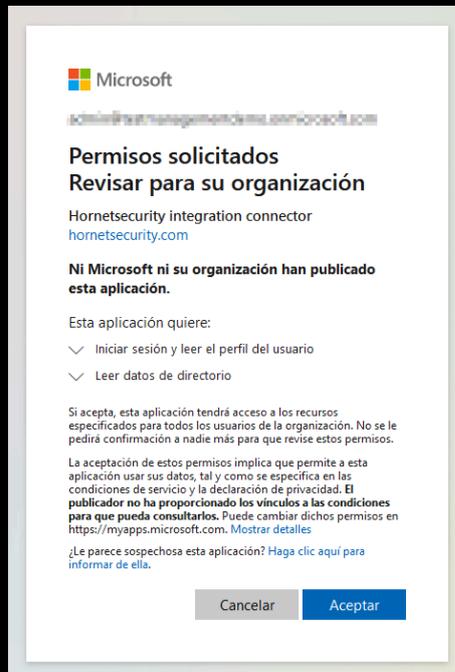


Figura 5: Conceder los permisos



Los dominios y buzones de correo de Microsoft 365 se crean en Control Panel. Los dominios se añaden al módulo **Configuración de cliente > Dominios** (véase **Dominios**). Al principio, los dominios se muestran con el estado **No verificado** en la columna **Verificado**. Al cabo de unos minutos se comprueba si es posible verificarlos (véase **Verificación de dominios**).



Los dominios y buzones de correo se han creado en Control Panel. A partir de ahora, el administrador de la organización de Microsoft 365 del cliente puede iniciar sesión en Control Panel con sus datos de acceso de Microsoft 365 y configurar los servicios.

Tras la sincronización deberá configurar los servicios de Microsoft (véase **Configuración de los servicios de Microsoft** en la página 95) para poder disfrutar al completo de nuestros servicios.

Si ha seleccionado 365 Total Protection Enterprise Backup, también debe configurar 365 Total Backup (véase **Configurar 365 Total Backup** en la página 14) para copiar los datos del inquilino de Microsoft 365 del cliente.



Configurar 365 Total Backup



Ha configurado 365 Total Protection Enterprise Backup para un cliente (véase [Instalar 365 Total Protection](#) en la página 10).

El servicio 365 Total Protection Enterprise Backup combina los servicios 365 Total Protection Enterprise y 365 Total Backup (véase [Acerca de 365 Total Protection](#) en la página 6). Una vez haya configurado 365 Total Protection Enterprise Backup para un cliente, puede configurar 365 Total Backup para el mismo. Este procedimiento le permite configurar 365 Total Backup conforme a la configuración por defecto. En este caso se realizan copias de seguridad de todos los buzones de correo de Microsoft 365, archivos almacenados en cuentas de empresa de OneDrive y en bibliotecas de documentos de SharePoint, así como chats de usuarios y grupos de Teams del inquilino del cliente.



Nota:

Los administradores a nivel de cliente o partner pueden configurar 365 Total Backup con otros ajustes abriendo 365 Total Backup desde el módulo **Copia de seguridad > 365 Total Backup** (véase [Iniciar 365 Total Backup](#)).

Con 365 Total Backup también se pueden realizar copias de seguridad de terminales con Windows. Pero los terminales no se incluyen en la configuración por defecto.

Solo los administradores a nivel de partner pueden configurar copias de seguridad de terminales. Para ello, los administradores a nivel de partner pueden abrir 365 Total Backup desde el módulo **Copia de seguridad > 365 Total Backup**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio del cliente en la selección de ámbitos.



3. Vaya a **365 Total Protection > 365 Total Protection**.



Se muestra el estado de la configuración de 365 Total Protection Enterprise Backup.

Estado de la configuración 365 Total Protection Enterprise Backup

SE HA CONECTADO MICROSOFT 365.

21 buzones de correo | 20 licencias ⓘ | 2 dominios

Ajustar la configuración de DNS de sus dominios

La configuración de DNS de al menos un dominio sincronizado no se ha ajustado o es incorrecta. Siga las instrucciones del manual para ajustar correctamente la configuración de DNS.

Configurar 365 Total Backup

Haga clic en "Configurar ahora" para conceder los permisos necesarios para hacer copias de seguridad de su inquilino de Microsoft 365.

Configurar el tráfico de correo electrónico saliente

Es necesario que configure su tráfico de correo electrónico saliente. Las instrucciones se incluyen en nuestro manual.

Figura 6: Estado de la configuración

4. En **Configurar 365 Total Backup**, haga clic en **Configurar ahora**.



La página de configuración de 365 Total Backup se abre en una nueva pestaña. Los datos del cliente ya están introducidos.



Nota:

La página utiliza el idioma elegido para el partner del cliente en Control Panel (véase [Ajustar zona horaria e idioma por defecto](#)).



5. Haga clic en **Continuar**.

Figura 7: Comprobar los datos



Se abre una ventana con un resumen de los pasos de configuración.



6. Haga clic en el paso 1.

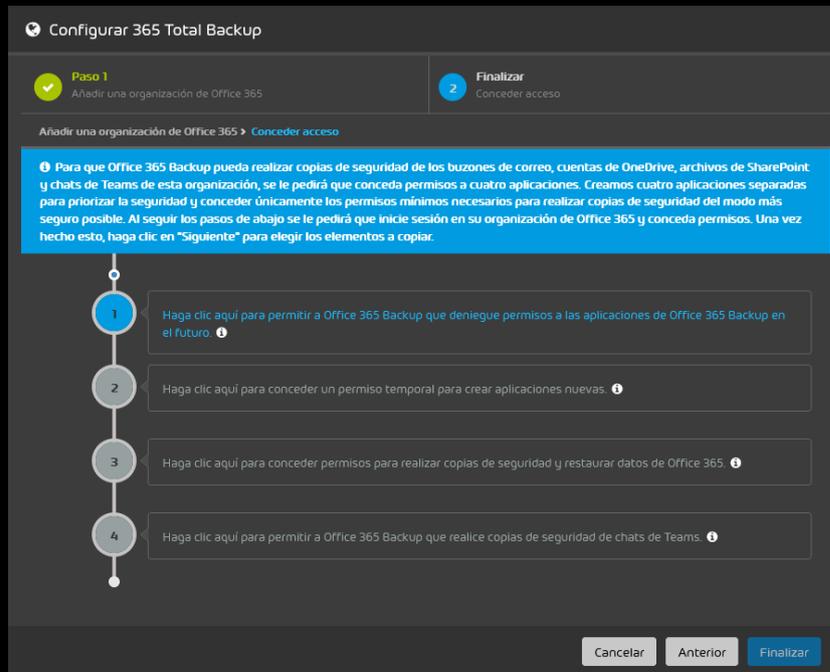


Figura 8: Realizar el paso 1



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

7. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



8. Conceda los permisos solicitados.

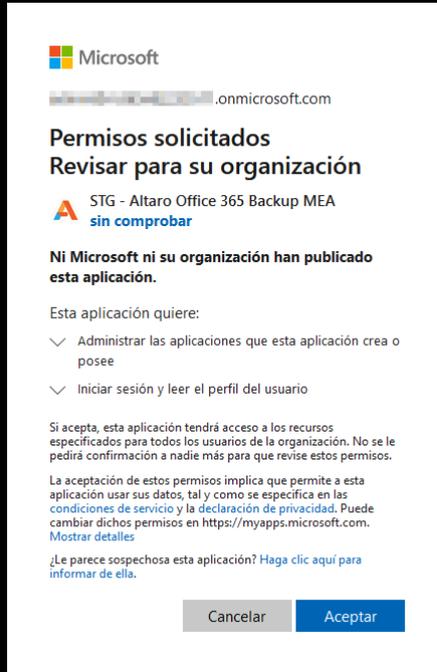


Figura 9: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.



Figura 10: Ventana de confirmación

9. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



10. Haga clic en el paso 2.

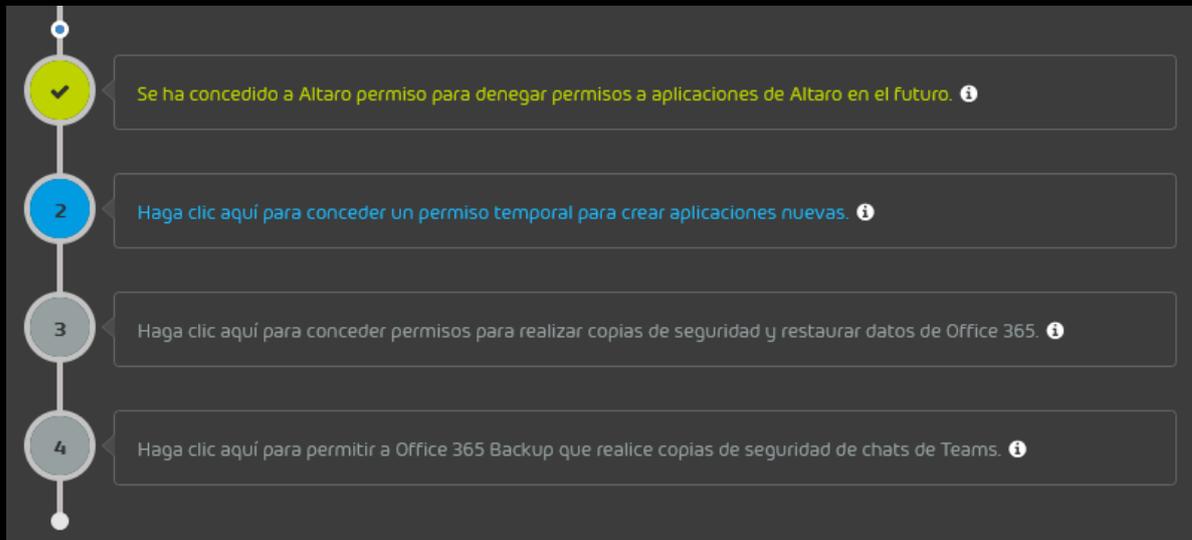


Figura 11: Realizar el paso 2



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

11. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



365 Total Backup obtiene acceso al inquilino del cliente. Se muestra un mensaje de confirmación.



Figura 12: Ventana de confirmación

12. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



13. Haga clic en el paso 3.

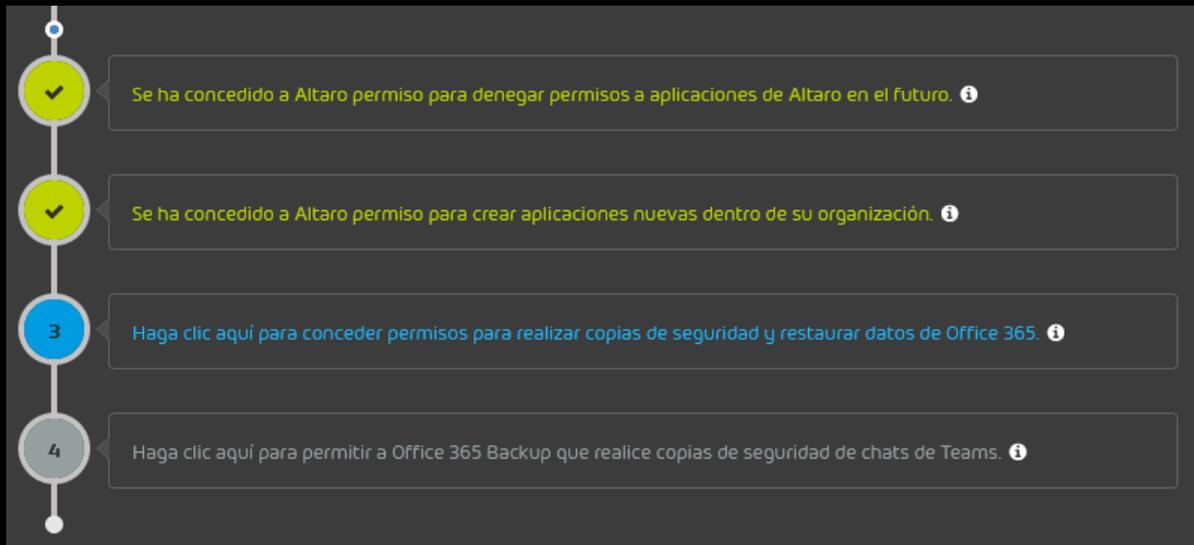


Figura 13: Realizar el paso 3



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

14. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



15. Conceda los permisos solicitados.

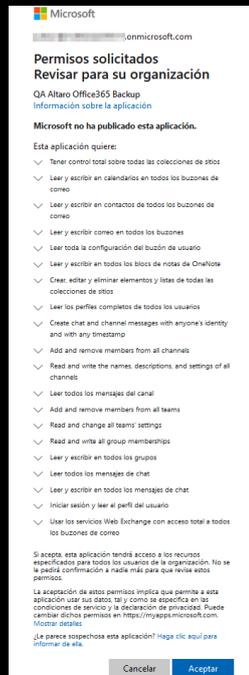


Figura 14: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.

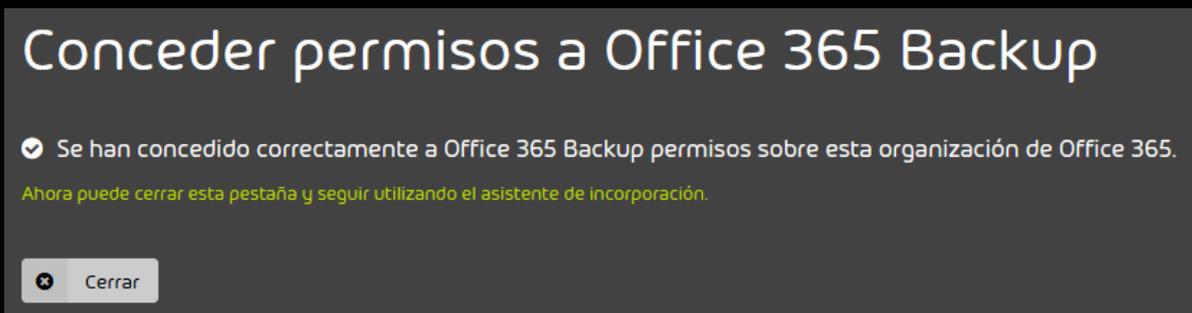


Figura 15: Ventana de confirmación



16. Haga clic en el paso 4.

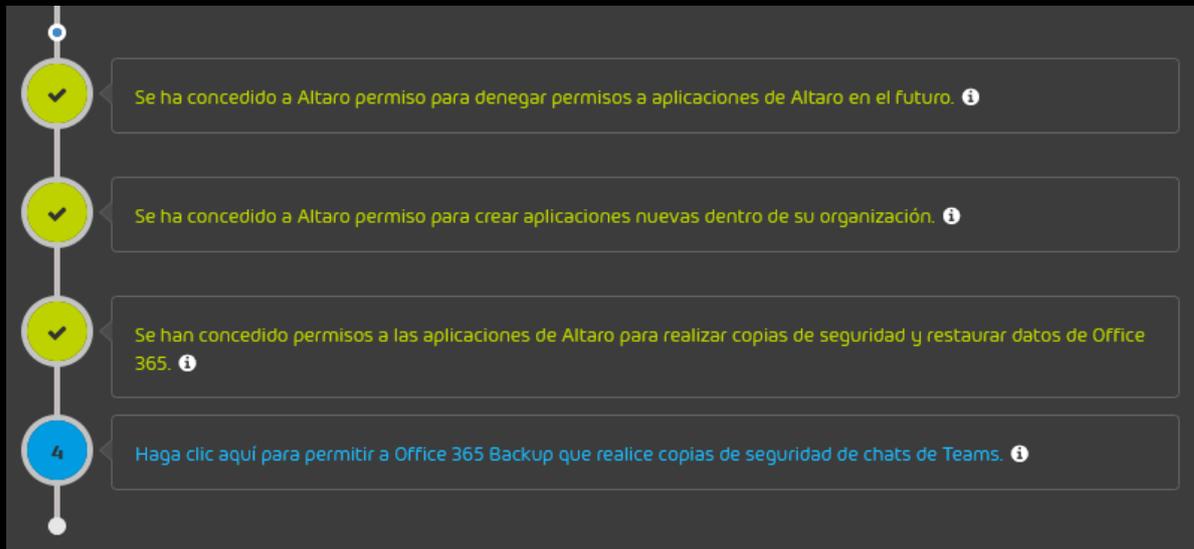


Figura 16: Realizar el paso 4



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

17. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



18. Conceda los permisos solicitados.

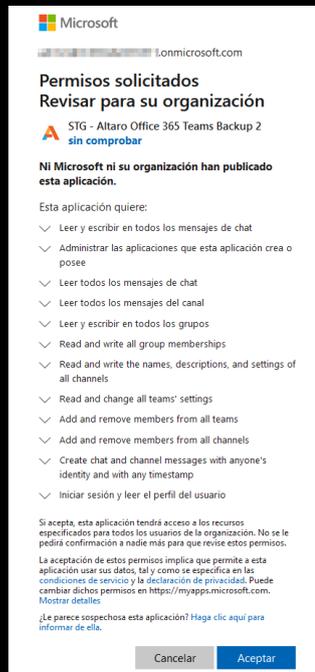


Figura 17: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.



Figura 18: Ventana de confirmación

19. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



20. Haga clic en **Finalizar**.

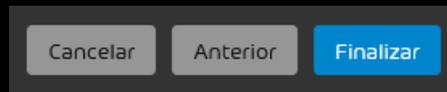


Figura 19: Finalizar la configuración



La pestaña se cierra. La configuración de 365 Total Backup se da por finalizada en el módulo **365 Total Protection > 365 Total Protection** de Control Panel.



Figura 20: Estado de la configuración de 365 Total Backup



365 Total Backup se ha configurado.



Actualización a 365 Total Protection como cliente

Si un cliente que ya utiliza nuestros servicios dispone de un inquilino de Microsoft 365, puede actualizarse a 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) por sí mismo en Control Panel (véase [Actualizar a 365 Total Protection](#) en la página 25).

Los clientes que se actualicen a la versión Enterprise o Enterprise Backup y hayan empleado anteriormente un servidor Exchange local pueden migrar datos de buzones de correo de sus servidores Exchange locales a sus inquilinos de Microsoft 365 durante la actualización (véase [Acerca de la migración de buzones de correo](#) en la página 43). Esto facilita a los clientes su transición a Microsoft 365.

Durante la actualización a 365 Total Protection, Control Panel adopta automáticamente todos los dominios y buzones de correos creados en Control Panel.

Actualizar a 365 Total Protection



Usted dispone de un inquilino de Microsoft 365 y utiliza nuestros servicios.

Como cliente nuestro puede usted actualizar nuestros servicios a 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **365 Total Protection > 365 Total Protection**.



4.

! **Importante:**

Al actualizar nuestros servicios a 365 Total Protection, los buzones de correo y los dominios se sincronizan con Microsoft 365 en Control Panel. Nuevos buzones de correo se añaden a Control Panel y los buzones de correo existentes se actualizan según la configuración en Microsoft 365.

! **Importante:**

La actualización no puede efectuarse si ha elegido la opción **Spam and Malware Protection** como entorno primario en el módulo **POP3/IMAP** (véase [Configurar el entorno primario](#)).

! **Importante:**

La opción **Enterprise Backup** solo se puede seleccionar si el partner ha activado 365 Total Backup (véase [Activar 365 Total Backup](#)).

Haga clic en la versión de 365 Total Protection a la que desee actualizar nuestros servicios. Tiene las siguientes opciones:

- **Business**
- **Enterprise**
- **Enterprise Backup**

i **Nota:**

Para más información sobre las versiones, véase [Acerca de 365 Total Protection](#) en la página 6.



Figura 21: Seleccionar versión





Si la autenticación multifactor está habilitada para el dominio en Control Panel (véase [Habilitar la autenticación multifactor](#)), se muestra un mensaje sobre la autenticación multifactor. De lo contrario, se muestra un mensaje de advertencia.

5.



Importante:

La actualización a 365 Total Protection solo puede efectuarse con la autenticación multifactor desactivada en Control Panel. Después de la actualización a 365 Total Protection, los usuarios del inquilino de Microsoft 365 inician sesión en Control Panel con sus datos de acceso de Microsoft 365 y se aplican las directivas de autenticación del inquilino (véase [Habilitar la autenticación multifactor](#)).

Si se muestra un mensaje sobre la autenticación multifactor, haga clic en **Confirmar**.

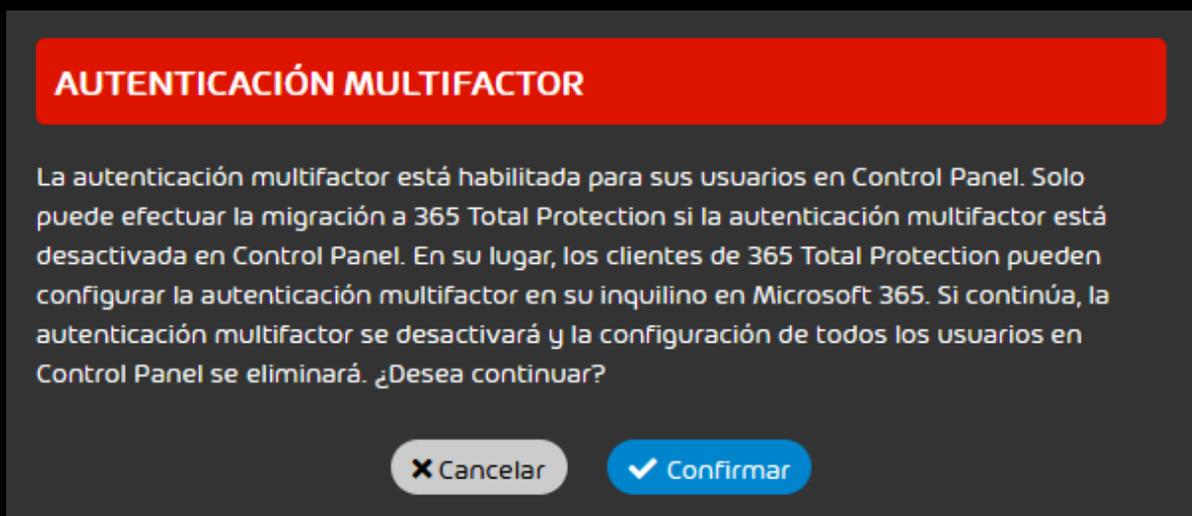


Figura 22: Desactivar la autenticación multifactor



La autenticación multifactor se desactiva para los usuarios del dominio. Para los usuarios que ya tenían configurada la autenticación multifactor, se elimina la configuración. Se muestra un mensaje de advertencia.



6. Para iniciar la actualización a 365 Total Protection, haga clic en **Confirmar**.

MIGRACIÓN A 365 TOTAL PROTECTION

Está a punto de efectuar la migración a 365 Total Protection. Los buzones de correo del entorno primario que no se administren en Microsoft 365 se asignarán al entorno secundario seleccionado.

A partir de ahora, los correos electrónicos de estos buzones de correo se enrutarán al servidor de destino del entorno secundario. Si este servidor de destino es distinto al entorno primario, el enrutamiento de correo electrónico puede fallar.

Durante la migración a 365 Total Protection, los buzones de correo y los dominios en Control Panel se sincronizarán con Microsoft 365. Nuevos buzones de correo se añadirán a Control Panel y los buzones de correo existentes se actualizarán según la configuración en Microsoft 365.

Figura 23: Confirmar



7.

! **Importante:**

Los clientes no pueden utilizar al mismo tiempo 365 Total Protection y conexiones LDAP en Control Panel. Si el cliente tiene conexiones LDAP activas o buzones LDAP (véase [Conexión mediante LDAP](#)), las conexiones LDAP se desactivarán y todos los buzones LDAP se convertirán en buzones de correo normales. Los usuarios y grupos dejarán de sincronizarse con el servicio de directorio mediante LDAP. Los ajustes del cliente en la pestaña **Conexión LDAP** del módulo **Dashboard de servicios** seguirán almacenados en segundo plano, pero no se mostrarán mientras que el cliente utilice 365 Total Protection.

Si el cliente cancela la actualización a 365 Total Protection o rescinde su contrato de 365 Total Protection y desea volver a emplear sus conexiones LDAP, los administradores a nivel de cliente pueden volver a activarlas (véase [Activar la conexión mediante LDAP](#)). Los buzones de correo que se sincronicen con el servicio de directorio volverán a convertirse en buzones LDAP en un plazo de 24 horas.

Para desactivar sus conexiones LDAP activas y convertir sus buzones LDAP en buzones de correo normales, haga clic en **Confirmar**.

DESACTIVAR LA CONEXIÓN LDAP

Su dominio tiene una conexión LDAP activada o buzones de correo LDAP. 365 Total Protection solo puede emplearse sin conexión LDAP ni buzones de correo LDAP. Si continúa, la conexión LDAP se desactivará y todos los buzones de correo LDAP se convertirán en buzones de correo normales en Control Panel. Si decide reactivar la conexión LDAP más adelante, dichos buzones de correo volverán a convertirse en buzones de correo LDAP en un plazo de 24 horas. ¿Desea continuar?

X Cancelar

✓ Confirmar

Figura 24: Desactivar la conexión mediante LDAP

Se muestra el primer paso para la configuración de 365 Total Protection.



8. Seleccione si, tras la actualización, los buzones de correo del entorno primario que no se administren en el inquilino de Microsoft 365 del cliente deben asignarse a un entorno secundario existente o a un entorno secundario nuevo.



Nota:

Después de la actualización a 365 Total Protection, solo los buzones de correo de Microsoft 365 del inquilino del cliente pueden estar asignados al entorno primario. Por tanto, otros buzones de correo que ya existan en Control Panel y que estén actualmente asignados al entorno primario deben asignarse a un entorno secundario en su lugar. Estos buzones de correo pueden asignarse a un entorno secundario existente o un entorno secundario nuevo.

Si aún no existe ningún entorno secundario para el cliente, la opción **Entorno existente** se oculta.

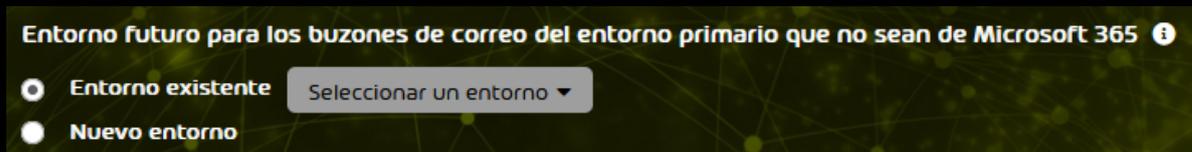


Figura 25: Seleccionar un entorno para buzones ajenos a Microsoft 365 en el entorno primario



Si se ha seleccionado la segunda opción, se muestra un formulario para crear un entorno secundario.

9. Si ha seleccionado la opción **Entorno existente**, seleccione un entorno secundario en el menú desplegable **Seleccionar un entorno**.



Nota:

Si existe solo un entorno secundario para el cliente, éste ya está seleccionado.



10. Si ha seleccionado la opción **Nuevo entorno**, cree un entorno secundario en el formulario.

Nuevo entorno

Individual POP3/IMAP Hornet.email

Nombre del entorno en Control Panel

Dirección del servidor de destino ⓘ

✕ Cancelar ✓ Añadir

Figura 26: Crear un entorno



Nota:

Para más información sobre cómo crear entornos secundarios, véase [Crear un entorno secundario](#).

11. Haga clic en **Continuar**.



Se muestra el siguiente paso de la configuración de 365 Total Protection.



12. Opcional: Si desea habilitar la migración de buzones de correo, marque la casilla **Habilitar la migración de buzones**.



Nota:

La migración de buzones de correo facilita a los clientes su transición de un servidor Exchange local a Microsoft 365. Durante la actualización a 365 Total Protection, los clientes pueden transmitir los datos de sus buzones de correo en un servidor Exchange local a su inquilino de Microsoft 365. Para más información, véase [Acerca de la migración de buzones de correo](#) en la página 43.



Nota:

La migración de buzones de correo solo está disponible en las versiones Enterprise y Enterprise Backup de 365 Total Protection. En la versión Business, esta casilla está deshabilitada.



Figura 27: Habilitar la migración de buzones de correo

13. Haga clic en **Continuar**.



Si se ha marcado la casilla **Habilitar la migración de buzones** se mostrará una ventana de confirmación. De lo contrario se mostrará el siguiente paso de la configuración de 365 Total Protection.



14. Si se muestra una ventana de confirmación, haga clic en **Confirmar**.

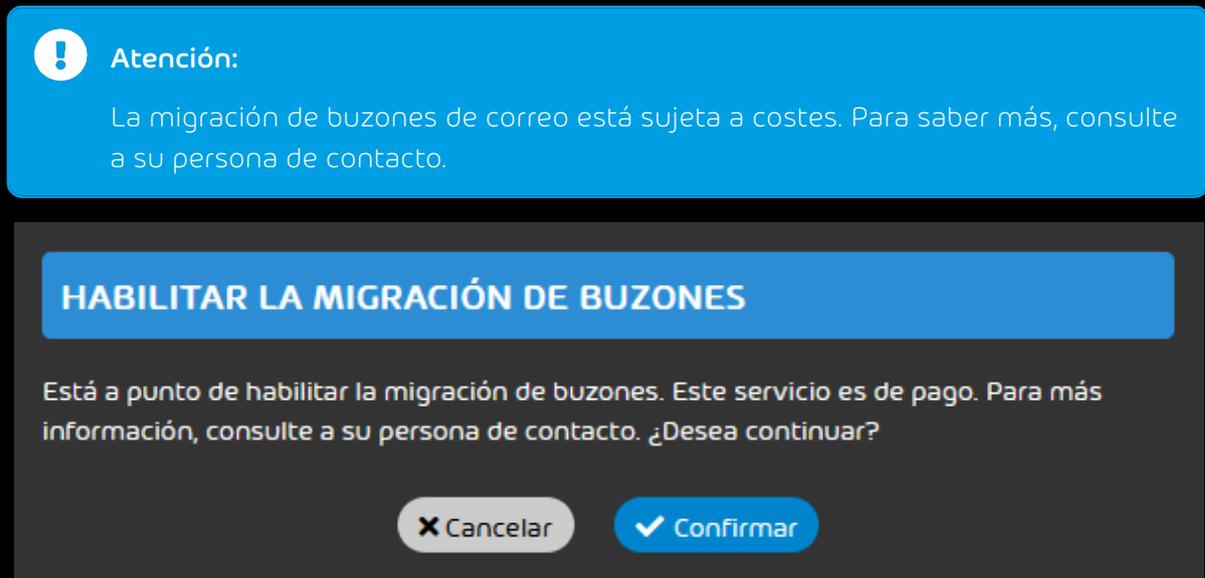


Figura 28: Confirmar la habilitación de la migración de buzones de correo



La migración de buzones de correo se habilita. Tan pronto como el cliente inicie la actualización a 365 Total Protection podrá transferir los datos de sus buzones de correo de un servidor Exchange local a su inquilino de Microsoft 365.

Se muestra el siguiente paso de la configuración de 365 Total Protection.



15. Seleccione el entorno a asignar a los buzones de Microsoft 365 ya disponibles en Control Panel y asignados actualmente a un entorno secundario. Accione el interruptor de la opción deseada.



Nota:

Después de la actualización a 365 Total Protection, el inquilino de Microsoft 365 del cliente se define como entorno primario (véase [Configuración del entorno primario](#)). Los buzones de correo de Microsoft 365 que se añadan a Control Panel después de la actualización a 365 Total Protection se asignan automáticamente al entorno primario durante la sincronización con Microsoft 365.

Las opciones afectan a los buzones de correo de Microsoft 365 que ya existan en Control Panel antes de la actualización y que estén asignados a un entorno secundario. Estos buzones de correo de Microsoft 365 pueden asignarse al entorno primario o permanecer en su entorno actual después de la actualización. Independientemente de si realmente existen buzones de correo de este tipo en Control Panel, es necesario elegir una opción para el cliente.



Nota:

Si se ha habilitado la migración de buzones de correo, no es posible modificar este ajuste. Si en Control Panel hay buzones de correo del inquilino de Microsoft 365 del cliente que se encuentren actualmente asignados a un entorno secundario, dichos buzones se asignarán al nuevo entorno primario tras la actualización a 365 Total Protection.

Entorno futuro para los buzones de Microsoft 365 de entornos secundarios ⓘ

- Mover los buzones de Microsoft 365 de los entornos secundarios al nuevo entorno primario
- Dejar los buzones de Microsoft 365 en su entorno secundario actual

Figura 29: Seleccionar un entorno para buzones de Microsoft 365 en entornos secundarios.

16. Haga clic en **Continuar**.



Se muestra un formulario.



17. Introduzca sus datos de contacto en el formulario.

Nota:

Estos datos de contacto sirven para que podamos ponernos en contacto con usted en caso de dificultades.

INCORPORACIÓN

 **Empresa**

Título **Nombre** **Apellidos**

Correo electrónico **Teléfono**

IT Security News
 Me gustaría recibir las IT Security News regularmente.

 **Migrar ahora**

Figura 30: Introducir datos de contacto

18. Si desea recibir nuestras IT Security News, marque la casilla **Deseo recibir las IT Security News regularmente.**

- 19.

Atención:

Una vez activado 365 Total Protection, comenzará un periodo de prueba gratuito de 14 días. Para poder seguir empleando 365 Total Protection después de la fase de prueba, el cliente deberá adquirir el servicio (véase [Adquirir 365 Total Protection](#) en la página 110).

Para iniciar la actualización, haga clic en **Migrar ahora**.



Se abre la página de inicio de sesión de Microsoft 365.



20. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365 del cliente.

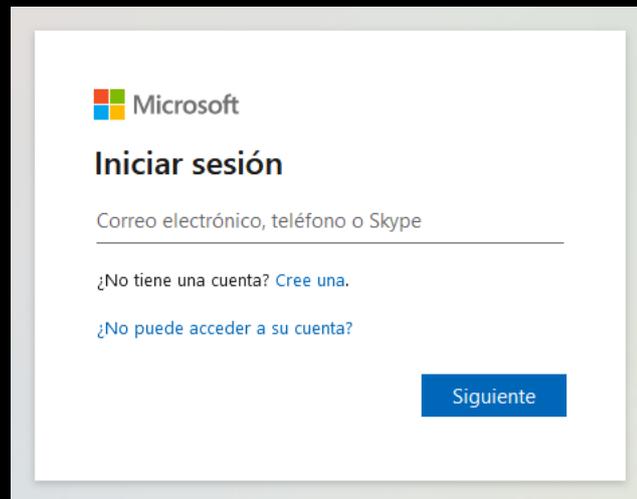


Figura 31: Iniciar sesión



21. Para sincronizar nuestros servicios con Microsoft 365, conceda los permisos solicitados.

Nota:

Durante la sincronización se transmiten dominios y buzones de correo de Microsoft 365 a Control Panel. La configuración de Microsoft no se modifica.

Si existen grupos en Control Panel que tengan el mismo nombre que grupos en Microsoft 365, la pertenencia de los buzones de correo de Microsoft 365 a estos grupos también se sincronizará en Control Panel (véase [Administración de grupos en Control Panel](#) en la página 113 y [Sincronizar grupos de Microsoft 365 en Control Panel](#) en la página 113).



Figura 32: Conceder los permisos



22. Si ha habilitado la migración de buzones (véase el paso 12 en la página 32), conceda los permisos solicitados.



Nota:

Estos permisos nos permiten acceder a los buzones de correo del inquilino de Microsoft 365 y solo son necesarios para efectuar la migración de buzones. Recomendamos eliminar los permisos de la aplicación Hornetsecurity Mailbox Migration del inquilino de Microsoft 365 del cliente tras la actualización a 365 Total Protection.

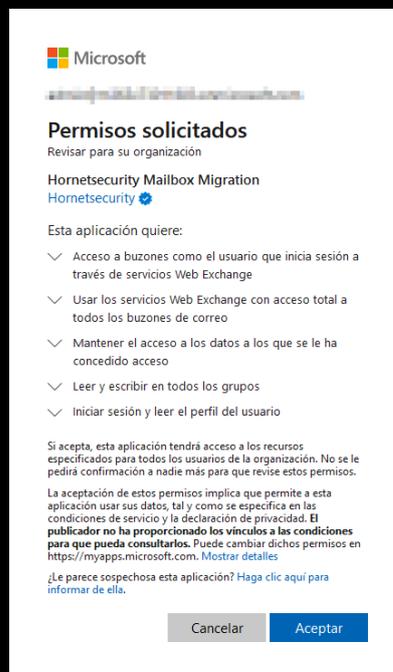


Figura 33: Conceder permisos para la migración de buzones



Si se ha habilitado la migración de buzones de correo (véase 12 en la página 32), la actualización a 365 Total Protection se interrumpirá para que el cliente pueda transferir los datos de los buzones de correo de su servidor Exchange local a su inquilino de Microsoft 365 (véase **Acerca de la migración de buzones de correo** en la página 43). La actualización a 365 Total Protection solo se efectuará una vez los administradores hayan finalizado la migración de buzones de correo.

Si no se ha habilitado la migración de buzones de correo, la actualización a 365 Total Protection se efectuará inmediatamente. En cuanto la actualización haya finalizado



correctamente se mostrará la cantidad de dominios y buzones de correo sincronizados. Los dominios y buzones de correo de Microsoft 365 se han creado bajo el cliente en Control Panel. Los dominios se añaden al módulo **Configuración de cliente > Dominios** (véase **Dominios**). Al principio, los dominios se muestran con el estado **No verificado** en



la columna **Verificado**. Al cabo de unos minutos se comprueba si es posible verificarlos (véase **Verificación de dominios**).



Nota:

Durante la actualización se ejecutan diversas operaciones, tales como la creación o modificación de entornos, direcciones de correo electrónico, dominios y buzones de correo. Dichas operaciones se documentan en el módulo **Registro de auditorías 2.0** (véase **Registro de auditorías 2.0**).

Estado de la configuración 365 Total Protection Enterprise

SE HA CONECTADO MICROSOFT 365.

3 buzones de correo | 2 licencias | 2 dominios

Ajustar la configuración de DNS de sus dominios
La configuración de DNS de al menos un dominio sincronizado no se ha ajustado o es incorrecta. Siga las instrucciones del manual para ajustar correctamente la configuración de DNS.
Configurar ahora

Configurar el tráfico de correo electrónico saliente
Es necesario que configure su tráfico de correo electrónico saliente. Las instrucciones se incluyen en nuestro manual.
Configurar automáticamente

Instalación de Hornetsecurity Outlook Add-in
Puede instalar automáticamente Hornetsecurity Outlook Add-in en las aplicaciones Outlook de sus usuarios. Tras la instalación, sus usuarios podrán ejecutar varias funciones de Control Panel directamente desde sus aplicaciones de Outlook.
Instalar

Estatus del contrato: Preparación de prueba

Figura 34: Actualización correcta



Importante:

Si la actualización falla, se indicará la razón. Una vez subsanado el error, es posible volver a iniciar la actualización.



Estado de la configuración 365 Total Protection Enterprise LA SINCRONIZACIÓN HA FALLADO.

Estado de sincronización:	
Esperar permisos de Microsoft	✓
Comprobaciones previas	✗
Migración	⊙
Obtener dominios	⊙
Obtener diferencia	⊙
Obtener administradores	⊙
Obtener usuarios	⊙
Escribir dominios	⊙
Escribir usuarios	⊙
Escribir configuración	⊙

✗ La IP de destino y el nombre de host de destino deben estar definidos en Spam and Malware Protection.

Figura 35: Actualización fallida



Los dominios y buzones de correo de Microsoft 365 se han transferido a 365 Total Protection. Los dominios y buzones de correo se han creado en Control Panel. A partir de este momento puede iniciar sesión en Control Panel con sus datos de acceso a Microsoft 365 y configurar los servicios.

Para aprovechar al máximo nuestros servicios, ajuste la configuración de los dominios sincronizados (véase [Configuración de los servicios de Microsoft](#) en la página 95) y configure el tráfico de correo electrónico saliente.

Si ha seleccionado 365 Total Protection Enterprise Backup, también debe configurar 365 Total Backup (véase [Configurar 365 Total Backup](#) en la página 83) para copiar los datos de su inquilino de Microsoft 365.

Convenciones lingüísticas y símbolos en la documentación

Aclaración sobre el género empleado

Para mejorar la legibilidad, en esta documentación se emplea el masculino genérico. Cabe señalar aquí que el uso exclusivo de la forma masculina debe entenderse como independiente del género.



Símbolos utilizados

Los siguientes símbolos se utilizan para identificar mejor los pasos relevantes dentro de los capítulos dedicados a instrucciones:

Símbolo	Significado	Explicación
	Requisito	Condición que debe cumplirse antes del siguiente paso.
	Resultado intermedio	Resultado alcanzado provisionalmente tras un paso concreto.
	Resultado final	Resultado alcanzado una vez finalizada la secuencia de pasos de un capítulo de instrucciones.

Advertencias e indicaciones de seguridad

Las advertencias e indicaciones de seguridad se emplean para informar al usuario sobre riesgos residuales y peligros, así como sobre el procedimiento a emplear para evitarlos. En esta documentación se emplean las siguientes advertencias e indicaciones de seguridad:

Símbolo	Significado	Explicación
	NOTA	Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores.
	CONSEJO	Indicación sobre opciones de configuración.
	IMPORTANTE	Advertencias con información sobre limitaciones u opciones de configuración importantes del servicio.
	ATENCIÓN	Advertencia sobre costes adicionales que pueden surgir al contratar servicios.
	ADVERTENCIA	Advertencia sobre una posible pérdida de datos.



Símbolo	Significado	Explicación
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.

Acerca de la migración de buzones de correo

Nos gustaría hacer más sencillo el cambio a Microsoft 365 para aquéllos de nuestros clientes que han utilizado hasta ahora un servidor Exchange local. Por tanto, a los clientes que se pasen a 365 Total Protection Enterprise o Enterprise Backup (véase [Actualización a 365 Total Protection como cliente](#)) les ofrecemos la opción de transferir los datos de los buzones de correo de sus servidores Exchange locales a su inquilino de Microsoft 365.



Nota:

La migración de buzones es compatible con servidores Exchange a partir de la versión 2007.

Durante la migración de buzones se transfieren los siguientes datos:

- Correos con sus archivos adjuntos
- Contactos
- Calendarios
- Tareas
- Notas



Nota:

Si es posible, las marcas de los correos (p. ej., "leído", "no leído", "importante") también se mantienen en el inquilino de Microsoft 365.



Nota:

No es posible migrar los siguientes datos de buzones de correo:

- Carpetas públicas
- Archivos
- Diarios
- Configuraciones de usuarios
- Listas de distribución
- Permisos sobre buzones



Nota:

Para más información sobre otras limitaciones de la migración de buzones, véase [Limitaciones de la migración de buzones de correo](#) en la página 45.

Los administradores a nivel de partner y cliente pueden habilitar la migración de buzones de correo durante la actualización del cliente a 365 Total Protection (véase [Actualizar a 365 Total Protection](#)). Si la migración de buzones se habilita, la actualización se pausa para que los administradores puedan transferir los datos de todos los buzones de correo deseados desde un servidor Exchange local al inquilino de Microsoft 365 del cliente.



Atención:

La migración de buzones de correo conlleva costes adicionales conforme a la lista de precios.

Sin embargo, antes de la migración de buzones de correo deben cumplirse determinados requisitos en el servidor Exchange, en el inquilino de Microsoft 365 y en Control Panel (véase [Requisitos para la migración de buzones de correo](#) en la página 46). Una vez realizados los preparativos, los administradores pueden efectuar la migración de datos de buzones de correo desde Control Panel (véase [Migración de datos de buzones de correo](#) en la página 65).



Nota:

Las migraciones de correo pueden tardar varios días. No es posible dar estimaciones precisas, pues la duración depende de los siguientes factores:

- Cantidad y tamaño de los buzones de correo implicados
- Carga total de migraciones de buzones de correo en la lista de espera

Los administradores son informados por correo electrónico sobre cambios en el estado de las migraciones. Además, los administradores pueden consultar el estado en todo momento en el módulo **365 Total Protection > 365 Total Protection**. Durante la migración de buzones es posible emplear Control Panel como de costumbre.

En cuanto los administradores hayan finalizado la migración de buzones de correo, continuará la actualización a 365 Total Protection.

Limitaciones de la migración de buzones de correo

La migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43) tiene limitaciones. Estas limitaciones afectan a los datos que pueden transmitirse. A continuación se exponen dichas limitaciones.

Limitaciones causadas por los servicios web de Exchange (EWS)

Las restricciones de EWS limitan en Microsoft los recursos de servidores que pueden consumir un usuario o una aplicación. Esto tiene por objeto garantizar la fiabilidad y el tiempo de servicio de los servidores. Para la migración de buzones de correo, esto implica las siguientes limitaciones:

- El propietario de un buzón de correo se convierte en el organizador de todas sus citas en el inquilino de Microsoft 365.
- No es posible migrar el estado de participación en citas ("aceptada" o "rechazada").
- Durante la migración de buzones de correo se intenta resolver las direcciones internas de sistema (p.#j., direcciones X500) y sustituirlas por una dirección de correo electrónico válida. Si este proceso falla, las direcciones no se transmiten al servidor de Microsoft 365.
- Durante la migración de buzones de correo se filtran registros inválidos (p.#j., URLs inválidos en campos de páginas web) que serían rechazados por el inquilino de Microsoft 365.



Limitaciones causadas por el servidor Exchange local

Dependiendo de la versión del servidor Exchange local, pueden producirse las siguientes limitaciones:

- Si un correo supera el límite de datos del inquilino de Microsoft 365, dicho correo no se transmite. En tal caso, el usuario recibe una notificación.
- Los correos con un tamaño mayor a 64 MB no se transmiten.
- El volumen de datos máximo por buzón de correo no debe superar los 50 GB.
- La representación de determinados mensajes de correo (p.#j., formatos MIME especiales) en el inquilino de Microsoft 365 difiere de su representación en el servidor Exchange local.
- La asignación de propiedades de elementos está limitada (p.#j., por falta de compatibilidad con el inquilino de Microsoft 365).
- La asignación de carpetas compartidas está limitada.

Requisitos para la migración de buzones de correo

Antes de la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43) deben cumplirse determinados requisitos en el servidor Exchange local, en el inquilino de Microsoft 365 y en Control Panel. Solo entonces podrán los administradores a nivel de cliente efectuar la migración de buzones de correo desde Control Panel (véase [Migración de datos de buzones de correo](#) en la página 65).

Ya que durante la migración de buzones de correo solo se transmiten datos entre buzones de correo existentes, dichos buzones de correo deben estar ya disponibles en el servidor Exchange local, en el inquilino de Microsoft 365 y en Control Panel (véase [Requisitos para buzones de correo](#) en la página 47).

En el servidor Exchange local debe cumplirse un requisito adicional. Como durante la migración de buzones de correo accedemos a los buzones de correo por migrar con los datos de acceso de un administrador en el servidor Exchange local, dicho administrador del servidor Exchange local debe tener derecho a iniciar sesión en los buzones de correo de los usuarios. Por tanto, es preciso asignar el rol **ApplicationImpersonation** a dicho administrador (véase [Crear un grupo de roles en un servidor Exchange](#) en la página 48).

También en el inquilino de Microsoft 365 deben cumplirse requisitos adicionales. Por tanto, al igual que al administrador del servidor Exchange local, es preciso asignar el rol **ApplicationImpersonation** al administrador del inquilino de Microsoft 365 (véase [Crear un grupo de roles en Microsoft 365](#) en la página 53). Para acelerar la validación de entornos (véase [Validar un entorno](#) en la página 66) durante la migración de buzones de correo, puede



conceder al administrador del inquilino de Microsoft 365 derechos de lectura y administración sobre los buzones de correo cuyos datos se vayan a transferir. Puede conceder al administrador acceso, bien a buzones de correo individuales mediante Exchange Admin Center (véase [Conceder derechos de lectura y administración de buzones de correo en Microsoft 365](#) en la página 57) o bien a todos los buzones de correo del inquilino de Microsoft 365 con PowerShell (véase [Conceder permisos de lectura y administración de buzones de correo en Microsoft 365 mediante PowerShell](#) en la página 60). Ya que para acceder a los buzones de correo en el inquilino de Microsoft 365 se emplean los servicios web de Exchange, es preciso realizar también preparativos en los servicios web de Exchange. Para que sea posible acceder a los buzones de correo a través de los servicios web de Exchange, es preciso permitir el acceso a los servicios web de Exchange (véase [Permitir el acceso a los servicios web de Exchange](#) en la página 60). También es preciso desactivar la limitación de los servicios web de Exchange (véase [Desactivar la limitación de los servicios web de Exchange](#) en la página 63) para que los datos puedan transferirse con mayor ancho de banda.

Requisitos para buzones de correo

Durante la migración de buzones (véase [Acerca de la migración de buzones de correo](#) en la página 43) se transmiten datos del servidor Exchange local de un cliente a su inquilino de Microsoft 365 a través de Control Panel. Sin embargo, durante el proceso no se crean buzones de correo nuevos. Por tanto, antes de la migración de buzones de correo, el cliente debe asegurarse de que los buzones de correo a migrar ya existan en los siguientes sistemas:

- Servidor Exchange local
- Inquilino de Microsoft 365
- Control Panel



Importante:

Para que sea posible relacionar entre sí los buzones de correo en los diversos sistemas, las direcciones de correo electrónico de los mismos deben ser idénticas hasta la arroba (@). Los dominios deben ser diferentes en el servidor Exchange local y el inquilino de Microsoft 365, ya que los buzones de correo están asignados a servidores distintos.

Para añadir varios buzones de correo al inquilino de Microsoft 365 a la vez, los administradores del cliente pueden primero exportar los buzones de correo del servidor Exchange local y después importarlos en formato CSV en el inquilino de Microsoft 365.

Para añadir los buzones de correo a Control Panel, los administradores a nivel de cliente pueden sincronizar los buzones de correo en Control Panel con el servidor Exchange local mediante una conexión LDAP (véase [Conexión mediante LDAP](#)), importarlos desde un archivo CSV (véase



Importar buzones de correo desde un archivo CSV) o añadirlos manualmente a Control Panel (véase [Añadir un buzón de correo](#)).

Crear un grupo de roles en un servidor Exchange



Los buzones de correo cuyos datos se han de transferir están disponibles en el servidor Exchange local (véase [Requisitos para buzones de correo](#) en la página 47). Es usted administrador del servidor Exchange local del cliente.

La migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43) requiere el acceso al servidor Exchange local del cliente. Para ello se emplean los datos de acceso de un administrador del servidor Exchange local. Como durante la migración de buzones de correo es preciso leer los datos de todos los buzones de correo a migrar, el administrador debe tener derecho a iniciar sesión en dichos buzones de correo. Para conceder al administrador dicho derecho debe usted crear un grupo de roles en el servidor Exchange local. Mediante dicho grupo de roles puede usted conceder al administrador los derechos del rol **ApplicationImpersonation**.

1. Abra el Centro de administración de Exchange de su servidor de Exchange en su navegador.



Nota:

Por defecto, el Centro de administración de Exchange está disponible en la dirección **https://<nombre-de-dominio>/ecp**. El comodín **<nombre-de-dominio>** debe reemplazarse por la dirección absoluta del servidor Exchange local en el sistema de nombres de dominio.

2. Inicie sesión en el Centro de administración de Exchange con sus datos de acceso de administrador del servidor Exchange local.
3. Vaya a **permisos**.
4. Seleccione la pestaña **roles de administrador**.



- Haga clic en el símbolo de suma.

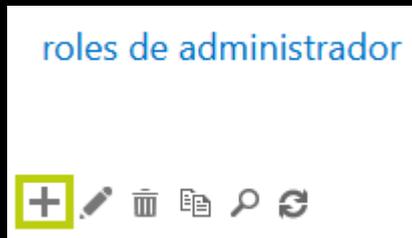


Figura 36: Añadir rol de administrador



Se muestra la ventana **nuevo grupo de roles**.

nuevo grupo de roles

*Nombre:

Descripción:

Ámbito de escritura: Predeterminado

Unidad organizativa:

Roles:

Miembros:

Guardar Cancelar

Figura 37: nuevo grupo de roles

- Introduzca un nombre para el nuevo grupo de roles en el campo **Nombre**. Puede elegir el nombre libremente.
- Opcional: Introduzca una descripción del grupo de roles en el campo **Descripción**.



8. En **Roles**, haga clic en el icono de suma.

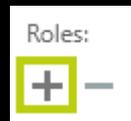


Figura 38: Añadir rol



Se muestra la ventana **Seleccionar una función**.

9. Seleccione el rol **ApplicationImpersonation** en la lista.



Nota:

El rol **ApplicationImpersonation** da derecho al administrador a iniciar sesión en el servidor Exchange local en nombre de otros buzones de correo.

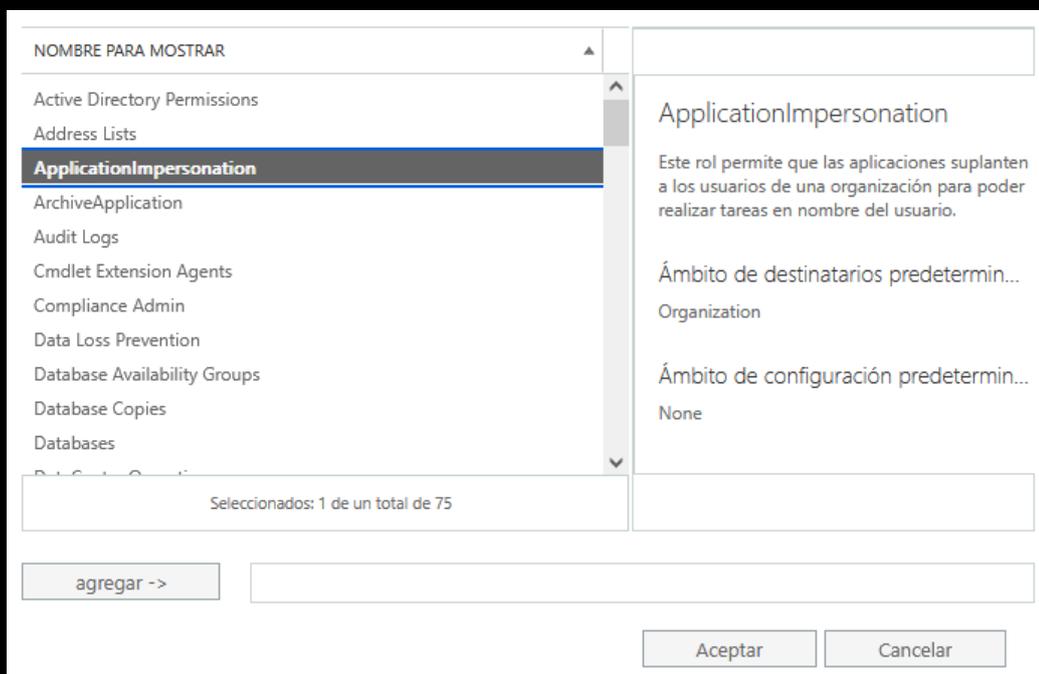


Figura 39: Seleccionar ApplicationImpersonation



10. Haga clic en **agregar**.



El rol se selecciona.



Figura 40: Rol seleccionado

11. Haga clic en **Aceptar**.



La ventana **Seleccionar una función** se cierra. El rol **ApplicationImpersonation** se muestra bajo **Roles** en la ventana **nuevo grupo de roles**.

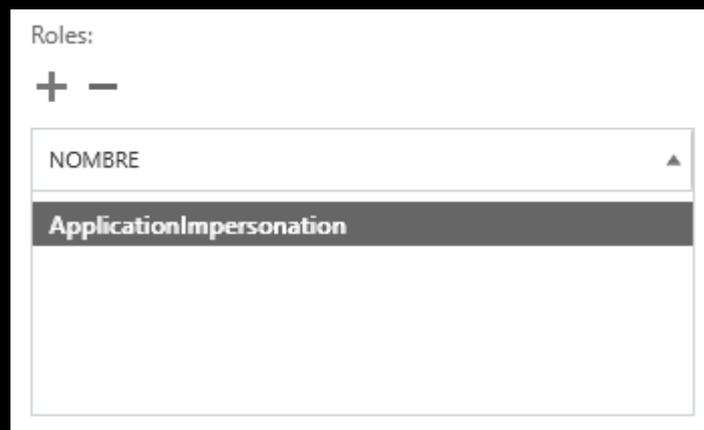


Figura 41: Rol añadido

12. En **Miembros**, haga clic en el icono de suma.



Figura 42: Añadir miembros



Se abre la pantalla **Seleccionar miembros**.

13. En la lista de la ventana **Seleccionar miembros**, seleccione el administrador con cuyos datos de acceso para el servidor Exchange local se vaya a realizar la migración de buzones



de correo en Control Panel (véase [Migración de datos de buzones de correo](#) en la página 65).

NOMBRE	NOMBRE PARA MOSTRAR
Adele Vance	Adele Vance
Administrator	Administrator
Alex Wilber	Alex Wilber
Allan Deyoung	Allan Deyoung
Christie Cline	Christie Cline

Figura 43: Seleccionar el administrador

14. Haga clic en **agregar**.



El administrador se selecciona.

agregar -> Administrator[quitar];

Figura 44: Administrador seleccionado

15. Haga clic en **Aceptar**.



La ventana **Seleccionar miembros** se cierra. El administrador seleccionado se muestra en la ventana **nuevo grupo de roles** bajo **Miembros**.

Miembros:

+ -

NOMBRE	NOMBRE PARA MOSTRAR
Administrator	Administrator

Figura 45: Administrador añadido



16. Haga clic en **Guardar**.



La ventana **nuevo grupo de roles** se cierra. El grupo de roles se añade a la pestaña **roles de administrador** bajo **permisos** en el Centro de administración de Exchange. A partir de ahora, el administrador tiene derecho a iniciar sesión en todos los buzones de correo del servidor Exchange local.



Se han concedido a un administrador los derechos del rol **ApplicationImpersonation** en el servidor Exchange local del cliente.

Crear un grupo de roles en Microsoft 365



Los buzones de correo cuyos datos se han de transferir están disponibles en el inquilino de Microsoft 365 (véase **Requisitos para buzones de correo** en la página 47). Es usted administrador del inquilino de Microsoft 365.

La migración de buzones de correo (véase **Acerca de la migración de buzones de correo** en la página 43) requiere el acceso al inquilino de Microsoft 365 del cliente. Para ello se emplean los datos de acceso de un administrador del inquilino de Microsoft 365. Como durante la migración de buzones de correo es preciso acceder a todos los buzones de correo del inquilino de Microsoft 365, el administrador debe tener derecho a iniciar sesión en dichos buzones de correo. Para conceder al administrador dicho derecho debe usted crear un grupo de roles en el inquilino de Microsoft 365. Mediante dicho grupo de roles puede usted conceder al administrador los derechos del rol **ApplicationImpersonation**.

1. Abra la página web **admin.exchange.microsoft.com**.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Roles > Roles de administrador**.



- Haga clic en **Agregar grupo de roles**.



Figura 46: Añadir grupo de roles



Se muestra la página **Configurar los datos básicos**.

Configurar los datos básicos

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

Nombre *

Ejemplo: Administración de cumplimiento del departamento de TI

Descripción

Escriba una descripción para que otros administradores conozcan el propósito de este grupo de roles.

Ámbito de escritura ⓘ

Default

Figura 47: Configurar los datos básicos

- Introduzca un nombre para el nuevo grupo de roles en el campo **Nombre**. Puede elegir el nombre libremente.
- Opcional: Introduzca una descripción del grupo de roles en el campo **Descripción**.
- Haga clic en **Siguiente**.



Se muestra la página **Agregar permisos**.



8. Seleccione el rol **ApplicationImpersonation** en la lista de roles.

<input type="checkbox"/>	ApplicationImpersonation	This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.	Organization	None
--------------------------	---------------------------------	---	--------------	------

Figura 48: Seleccionar ApplicationImpersonation

9. Haga clic en **Siguiente**.



Se muestra la página **Asignar administradores**.

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

Figura 49: Siguiente

10. En el campo **Miembros**, introduzca el nombre o la dirección de correo electrónico del administrador cuyos datos de acceso se vayan a emplear en la migración de buzones de correo y seleccione dicho administrador.



11. Haga clic en **Siguiente**.



Se muestra la página **Revisar el grupo de roles 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: ApplicationImpersonation
Descripción:
Ámbito de escritura: Default
[Editar los datos básicos](#)

Permisos
ApplicationImpersonation
[Editar permisos](#)

Administradores
admin
[Editar administradores](#)

Figura 50: Página Revisar el grupo de roles y finalizar

12. Haga clic en **Agregar grupo de roles**.



El grupo de roles se crea. La creación puede tardar hasta 1 minuto. Una vez creado el grupo de roles, se muestra un mensaje de éxito.

Status

✔ Se ha agregado el ApplicationImpersonation grupo de roles.

Características relacionadas
[Ver este grupo de roles](#)
[Agregar otro grupo de roles](#)

Figura 51: Mensaje de éxito



13. Haga clic en **Listo**.



El mensaje de éxito se cierra. El módulo **Roles > Roles de administrador** vuelve a mostrarse. El nuevo grupo de roles se muestra en la lista de grupos de roles.



Se han concedido a un administrador los derechos del rol **ApplicationImpersonation** en el inquilino de Microsoft 365 del cliente.

Conceder derechos de lectura y administración de buzones de correo en Microsoft 365



Los buzones de correo a los cuales se vayan a migrar datos están disponibles en el inquilino de Microsoft 365 del cliente (véase **Requisitos para buzones de correo** en la página 47). Es usted administrador del inquilino de Microsoft 365.

Para agilizar la validación de entornos (véase **Validar un entorno** en la página 66) necesaria durante la migración de buzones de correo (véase **Acerca de la migración de buzones de correo** en la página 43), puede usted conceder permisos de lectura y administración de los buzones de correo a migrar al administrador cuyos datos de acceso al inquilino de Microsoft 365 del cliente vayan a emplearse para la migración de buzones de correos. Así, el administrador obtiene acceso directo a los buzones de correo.



Nota:

Durante la validación de entornos (véase **Validar un entorno** en la página 66) para la migración de buzones se comprueba, en primer lugar, si es posible acceder directamente a los buzones de correo a migrar con los datos de acceso del administrador. Si no es posible acceder a ellos directamente, se utiliza el rol **ApplicationImpersonation** (véase **Crear un grupo de roles en Microsoft 365** en la página 53) para efectuar el acceso en su lugar. Esto provoca que la validación tarde más.

Para la migración de buzones recomendamos validar en primer lugar un entorno con pocos buzones de correo y conceder al administrador del inquilino de Microsoft 365 acceso directo a dichos buzones de correo. De este modo, la validación se realizará rápidamente y el administrador podrá familiarizarse con el proceso.



Nota:

En el Centro de administración de Microsoft solo es posible conceder al administrador el derecho de acceso directo a buzones de correo individuales. Solo PowerShell permite conceder al administrador acceso directo a todos los buzones de correo a la vez (véase [Conceder permisos de lectura y administración de buzones de correo en Microsoft 365 mediante PowerShell](#) en la página 60).

1. Abra la página web **admin.microsoft.com**.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Usuarios > Usuarios activos**.



Se muestra una lista con todos los usuarios activos del inquilino de Microsoft 365.

4. En la lista, haga clic en el nombre para mostrar de un usuario a cuyo buzón de correo se vayan a transmitir posteriormente datos del servidor Exchange local del cliente.



En el lado derecho de la ventana se muestra información sobre el usuario.

5. Seleccione la pestaña **Correo**.

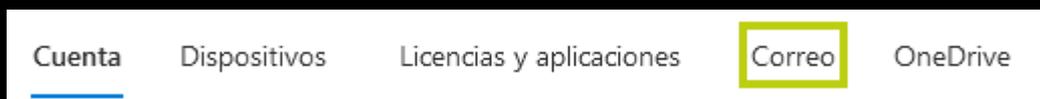


Figura 52: Seleccionar la pestaña Correo

6. En **Permisos del buzón**, haga clic en **Permisos de lectura y administración**.

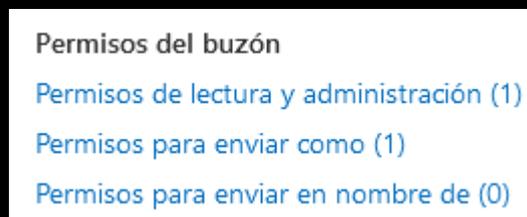


Figura 53: Seleccionar permisos



Se muestra la página **Permisos de lectura y administración**.



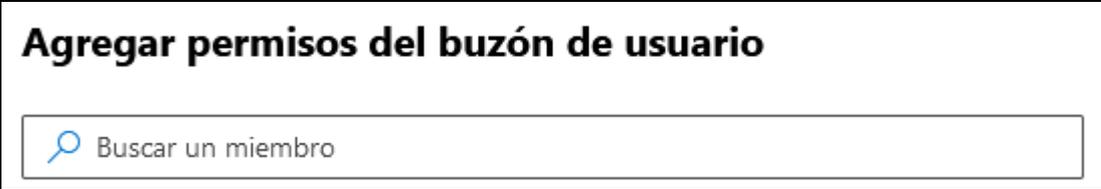
- Haga clic en **Agregar permisos**.



Figura 54: Añadir permisos



Se muestra la página **Agregar permisos del buzón de usuario**.



Agregar permisos del buzón de usuario

Buscar un miembro

Figura 55: Página Agregar permisos del buzón de usuario

- Busque el administrador cuyos datos de acceso al inquilino de Microsoft 365 se vayan a emplear posteriormente en la migración de buzones de correo y seleccione dicho administrador.
- Haga clic en **Agregar**.



Vuelve a mostrarse la página **Permisos de lectura y administración**. El administrador se muestra en la lista de permisos. Se conceden al administrador permisos de lectura y administración sobre el buzón de correo. Los cambios pueden tardar hasta 1 hora en hacerse efectivos.

- Haga clic en el aspa de la esquina superior derecha de la página.



La página se cierra. El módulo **Usuarios > Usuarios activos** vuelve a mostrarse.

- Repita los pasos **4** en la página 58 a **10** en la página 59 para todos los buzones de correo a los que vayan a transmitirse posteriormente datos del servidor Exchange local del cliente.



Se han concedido a un administrador permisos de lectura y administración sobre buzones de correo del inquilino de Microsoft 365 del cliente.



Conceder permisos de lectura y administración de buzones de correo en Microsoft 365 mediante PowerShell



Los buzones de correo a los cuales se vayan a migrar datos están disponibles en el inquilino de Microsoft 365 del cliente (véase [Requisitos para buzones de correo](#) en la página 47). Es usted administrador del inquilino de Microsoft 365.

Para agilizar la validación de entornos (véase [Validar un entorno](#) en la página 66) necesaria durante la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43), puede usted conceder permisos de lectura y administración de los buzones de correo a migrar al administrador cuyos datos de acceso al inquilino de Microsoft 365 del cliente vayan a emplearse para la migración de buzones de correos. Así, el administrador obtiene acceso directo a los buzones de correo. En lugar de conceder al administrador acceso a buzones de correo individuales (véase [Conceder derechos de lectura y administración de buzones de correo en Microsoft 365](#) en la página 57), puede usted concederle acceso a todos los buzones de correo del inquilino de Microsoft 365 al mismo tiempo con PowerShell.

1. Abra la PowerShell de su inquilino de Microsoft 365.
2. Ejecute la siguiente orden sustituyendo el comodín **<dirección de correo del administrador>** por la dirección de correo del administrador al cual se desee conceder permisos de lectura y administración sobre todos los buzones de correo del inquilino de Microsoft 365:

```
get-mailbox | add-mailboxpermission -User <dirección de correo del administrador> - AccessRights FullAccess
```



El administrador obtiene permisos de escritura y administración sobre todos los buzones de correo del inquilino de Microsoft 365. En la PowerShell se enumeran los usuarios a los cuales tiene pleno acceso el administrador.



Se han concedido a un administrador permisos de lectura y administración sobre todos los buzones de correo del inquilino de Microsoft 365 del cliente.

Permitir el acceso a los servicios web de Exchange



Es usted administrador del inquilino de Microsoft 365 del cliente.



Durante la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43) debemos acceder a los datos de los buzones de correo del inquilino de Microsoft 365 del cliente. Para acceder a ellos empleamos los servicios web de Exchange. Por tanto, debe usted permitir el acceso a los servicios web de Exchange del inquilino de Microsoft 365.

1. Abra la página web aad.portal.azure.com.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Centro de administración de Azure Active Directory**.

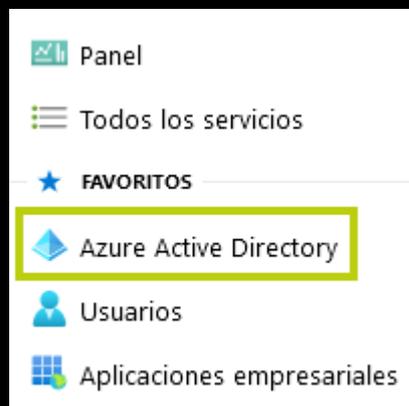


Figura 56: Abrir Azure Active Directory



4. En **Administrar**, haga clic en **Propiedades**.

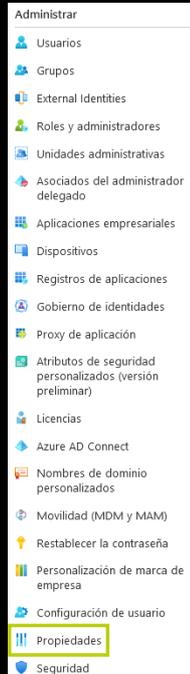


Figura 57: Abrir los ajustes



- Haga clic en el enlace **Administrar valores predeterminados de seguridad** en la parte inferior de la página.

[Administrar valores predeterminados de seguridad](#)

Figura 58: Abrir los valores predeterminados de seguridad



Se muestra la página **Habilitar valores predeterminados de seguridad**.

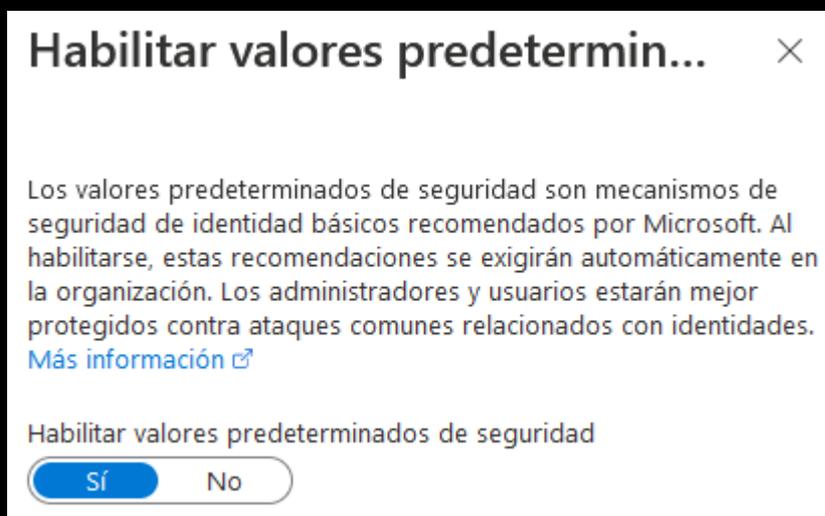


Figura 59: Valores de seguridad

- Haga clic en **No**.
- Haga clic en **Guardar**.



Los cambios se guardan.



Se ha permitido el acceso a los servicios web de Exchange.

Desactivar la limitación de los servicios web de Exchange



Es usted administrador del inquilino de Microsoft 365 del cliente.

Para poder migrar datos al inquilino de Microsoft 365 del cliente con mayor ancho de banda durante la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#))



en la página 43) debe usted desactivar temporalmente la limitación de los servicios web de Exchange.

1. Abra la página web admin.microsoft.com.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Introduzca el siguiente texto en el campo de introducción de datos: **EWS Throttling**.
4. Haga clic en **Ejecutar pruebas**.

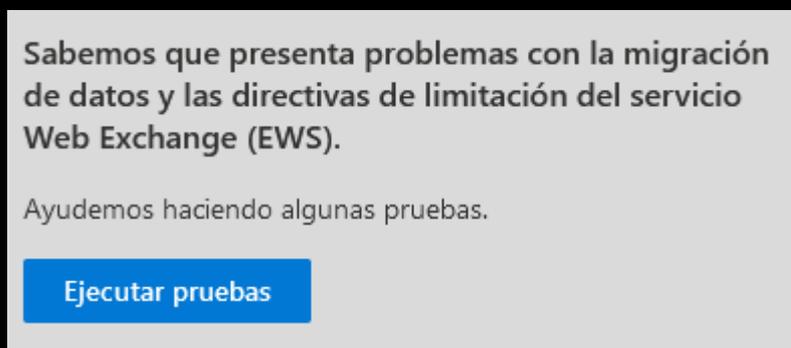


Figura 60: Realizar pruebas



Las pruebas se realizan. Si los servicios web de Exchange están limitados, se muestra el siguiente texto.

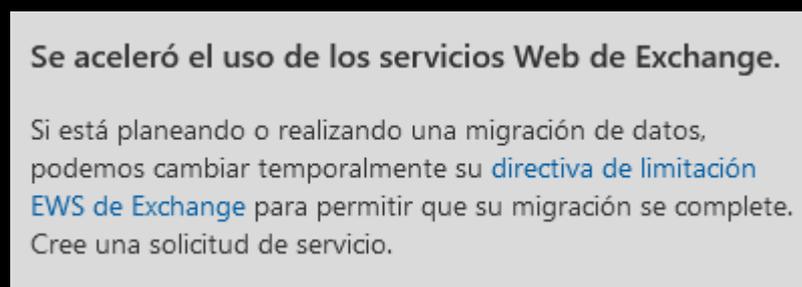


Figura 61: Limitación activa

5. Envíe una solicitud de soporte técnico a Microsoft para eliminar la limitación de los servicios web de Exchange durante 30 días.



El soporte técnico de Microsoft desactiva la limitación de los servicios web de Exchange.



Se ha desactivado temporalmente la limitación de los servicios web de Exchange.



Migración de datos de buzones de correo

Durante una actualización a 365 Total Protection Enterprise o Enterprise Backup (véase [Actualizar a 365 Total Protection](#)), los administradores a nivel de partner y cliente pueden transferir datos de buzones de correo de un servidor Exchange local al inquilino de Microsoft 365 del cliente (véase [Acerca de la migración de buzones de correo](#) en la página 43).



Importante:

Para que los administradores puedan efectuar la migración de buzones de correo en Control Panel, deben cumplirse determinados requisitos en el servidor Exchange local, en el inquilino de Microsoft 365 y en Control Panel (véase [Requisitos para la migración de buzones de correo](#) en la página 46).



Nota:

Las migraciones de correo pueden tardar varios días. No es posible dar estimaciones precisas, pues la duración depende de los siguientes factores:

- Cantidad y tamaño de los buzones de correo implicados
- Carga total de migraciones de buzones de correo en la lista de espera

Los administradores son informados por correo electrónico sobre cambios en el estado de las migraciones. Además, los administradores pueden consultar el estado en todo momento en el módulo **365 Total Protection > 365 Total Protection**. Durante la migración de buzones es posible emplear Control Panel como de costumbre.

Para migrar datos de buzones de correo, los administradores deben realizar varios pasos en Control Panel. En primer lugar, los administradores deben validar el entorno de los buzones de correo cuyos datos deseen transferir al inquilino de Microsoft 365 del cliente (véase [Validar un entorno](#) en la página 66). Con la validación nos aseguramos de que sea posible acceder al servidor Exchange local y al inquilino de Microsoft 365.



Nota:

Los administradores pueden validar varios entornos. Así es posible transferir datos de buzones de correo de diversos servidores Exchange al inquilino de Microsoft 365 del cliente.



Después de validar un entorno, el administrador puede seleccionar uno o varios buzones de correo del mismo y migrar sus datos (véase **Migrar buzones de correo** en la página 73).

! Importante:

Los administradores solo pueden migrar buzones de correo de entornos que hayan validado ellos mismos.

Una vez transmitidos los datos de todos los buzones de correo deseados al inquilino de Microsoft 365 del cliente, los administradores pueden finalizar la migración de buzones de correo (véase **Finalizar la migración de buzones de correo** en la página 82). A continuación, la actualización a 365 Total Protection continuará automáticamente (véase **Actualizar a 365 Total Protection**).

! Importante:

La migración de buzones de correo solo puede realizarse una vez. Una vez finalizada la migración de buzones de correo ya no es posible migrar más datos de buzones de correo.

Validar un entorno



Ha iniciado la actualización a 365 Protection Enterprise o Enterprise Backup y habilitado la migración de buzones de correo (véase **Actualizar a 365 Total Protection**). Ha realizado los preparativos necesarios para la migración de buzones de correo en el servidor Exchange, en el inquilino de Microsoft 365 y en Control Panel (véase **Requisitos para la migración de buzones de correo** en la página 46). Ha añadido buzones de correo al entorno que desea validar (véase **Entornos secundarios**).

Durante una actualización a 365 Total Protection Enterprise o Enterprise Backup (véase **Actualizar a 365 Total Protection**) puede usted transmitir datos de buzones de correo de un servidor Exchange local al inquilino de Microsoft 365 del cliente (véase **Acerca de la migración de buzones de correo** en la página 43). Para migrar datos de buzones de correo (véase **Migración de datos de buzones de correo** en la página 65) es necesario acceder al servidor Exchange local y al inquilino de Microsoft 365. Por tanto, antes de migrar datos de buzones de correo (véase **Migrar buzones de correo** en la página 73) debe usted validar el entorno (véase **Entornos secundarios**) al que estén asignados los buzones de correo del servidor Exchange local en Control Panel. Para hacerlo debe usted introducir los datos de acceso del servidor Exchange local. Con la validación nos aseguramos de que sea posible acceder al servidor Exchange local.



Nota:

Los administradores pueden validar varios entornos. Así es posible transferir datos de buzones de correo de diversos servidores Exchange al inquilino de Microsoft 365 del cliente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee validar un entorno.
3. Vaya a **365 Total Protection > 365 Total Protection**.



En el módulo se muestra la página **Migración de buzones**.



4.

**PRECAUCIÓN:**

Si los datos de acceso del servidor Exchange local introducidos se vuelven inválidos durante la migración de buzones de correo, no podrán transferirse más datos desde el servidor Exchange local hasta el inquilino de Microsoft 365. Esto puede provocar que los datos de los buzones de correo queden incompletos en el inquilino de Microsoft 365. Para que los datos de buzones de correo se transmitan al completo, no modifique los datos de acceso del servidor Exchange local antes de que haya finalizado la migración de buzones de correo (véase [Finalizar la migración de buzones de correo](#) en la página 82).

Cumplimente el formulario **Servidor de Exchange local** de la columna **Validación de entorno**.

SERVIDOR DE EXCHANGE LOCAL**Entorno**

Entorno primario ▾

Dirección IP o nombre de host**Correo electrónico de administrador****Contraseña de administrador****Figura 62: Rellenar el formulario**

- En el menú desplegable **Entorno**, seleccione entorno de los buzones de correo cuyos datos desee migrar.
- Introduzca la dirección IP o el nombre de host del servidor Exchange local en que se encuentran los datos de los buzones de correo en el campo **Dirección IP o nombre de host**.
- Introduzca la dirección de correo electrónico de un administrador del servidor Exchange local en el campo **Correo electrónico de administrador**.
- Introduzca la contraseña de un administrador del servidor Exchange local en el campo **Contraseña de administrador**.



- Haga clic en **Validar entorno**.

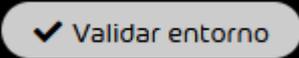


Figura 63: Validar el entorno



El entorno se añade a la lista de la columna **Entornos validados**. El entorno se valida. En cuanto esté listo el resultado de la validación, se le asignará al entorno dentro de la lista.



Si la lista contiene al menos un entorno validado correctamente, se habilitará el botón **Seleccionar buzones a migrar** bajo la misma.

i Nota:

La lista de la columna **Entornos validados** no se actualiza automáticamente. Los administradores pueden recargar la lista haciendo clic en el botón **Actualizar**.

i Nota:

Durante la validación comprobamos que sea posible acceder al servidor Exchange local y al inquilino de Microsoft 365. También comprobamos de modo aleatorio si el administrador del servidor Exchange local y del inquilino de Microsoft 365 tiene acceso a los buzones de correo asignados al entorno en Control Panel.

ENVIRONNEMENTS VALIDÉS: i

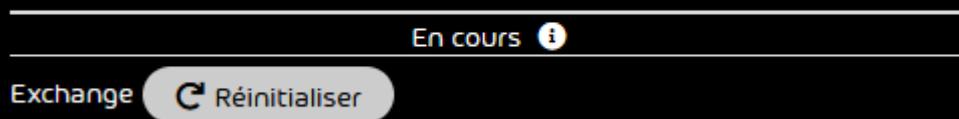


Figura 64: Validación en curso

ENTORNOS VALIDADOS: i

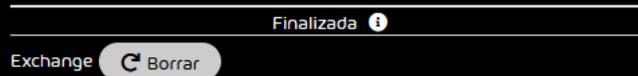


Figura 65: Validación correcta

ENTORNOS VALIDADOS: i



Figura 66: Validación fallida



Nota:

Si la validación fallase, se mostrará información sobre la causa haciendo clic en el botón de los tres puntos. Para reintentar la validación, es preciso descartarla antes (véase [Descartar la validación de un entorno](#) en la página 71).



Se ha validado el entorno.



Importante:

Los datos de acceso del servidor Exchange local y del inquilino de Microsoft 365 no deben modificarse hasta que haya finalizado la migración de los datos de buzones de correo de este entorno.

A continuación puede transferir los datos de buzones de correo del servidor Exchange local al inquilino de Microsoft 365 del cliente (véase [Migrar buzones de correo](#) en la página 73).

Descartar la validación de un entorno



Ha validado un entorno (véase [Validar un entorno](#) en la página 66). Actualmente no se está realizando ninguna migración de buzones de correo de dicho entorno (véase [Migrar buzones de correo](#) en la página 73).

Puede descartar la validación de un entorno para la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43). Descartar la validación es útil en caso de que se hayan modificado los datos de acceso al servidor Exchange local o al inquilino de Microsoft 365 desde que se realizó la validación o de que la validación haya fallado. Después de resolver los posibles errores en el servidor Exchange local, en el inquilino de Microsoft 365 o en Control Panel que hayan provocado el fallo de la validación y de descartar la validación, puede volver a validar el entorno.



Nota:

En el módulo **365 Total Protection > 365 Total Protection**, cada administrador solo ve las validaciones que él mismo ha efectuado. Por tanto, el administrador solo puede descartar sus propias validaciones.



Importante:

Mientras no se haya validado un entorno para un administrador, éste no podrá migrar datos de los buzones de correo de dicho entorno (véase [Migrar buzones de correo](#) en la página 73).



Importante:

Solo es posible descartar la validación de entornos para los que no se estén efectuando actualmente migraciones de buzones de correo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee descartar la validación de un entorno.
3. Vaya a **365 Total Protection > 365 Total Protection**.
4. En la fila de la columna **Entornos validados** correspondiente al entorno cuya validación desee descartar, haga clic en **Borrar**.

Exchange  

Figura 67: Descartar la validación



Se muestra una ventana de confirmación.



- Haga clic en **Aceptar**.

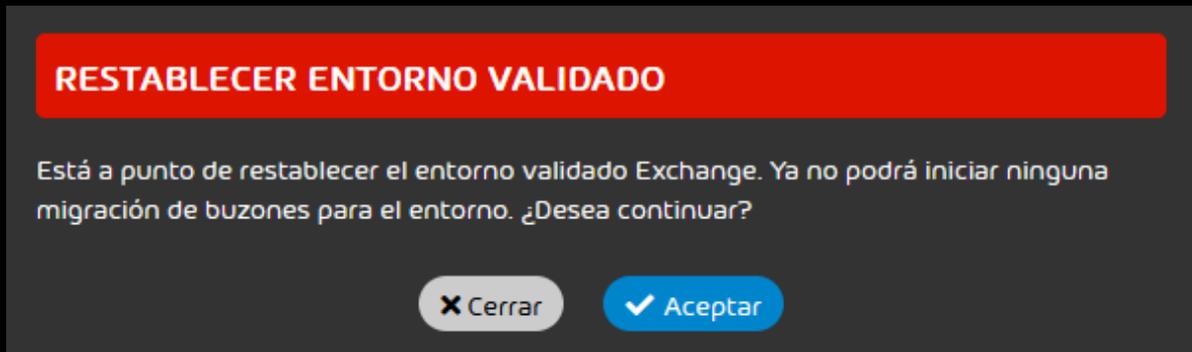


Figura 68: Confirmar el descarte de la validación



Se descarta la validación del entorno. El entorno se elimina de la lista de la columna **Entornos validados**.

A continuación puede validar de nuevo el entorno (véase [Validar un entorno](#) en la página 66).

Migrar buzones de correo



Ha realizado los preparativos necesarios para la migración de buzones de correo en el servidor Exchange, en el inquilino de Microsoft 365 y en Control Panel (véase [Requisitos para la migración de buzones de correo](#) en la página 46). Ha validado el entorno de los buzones de correo cuyos datos desea migrar (véase [Validar un entorno](#) en la página 66).

Con la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43) puede usted migrar los datos de buzones de correo de entornos validados (véase [Validar un entorno](#) en la página 66). En el módulo **Configuración de cliente** > **Buzones** puede usted seleccionar uno o varios buzones de correo para la migración.



Nota:

Solo es posible migrar datos de buzones de correo de los tipos **Buzón LDAP** y **Buzón de correo** (véase [Tipos de buzón de correo](#)).



Nota:

La primera vez que se realice una migración, recomendamos seleccionar pocos buzones de correo para familiarizarse con el proceso.

Siempre es recomendable migrar los datos de los buzones de correo de un entorno en grupos de entre 50 y 100 buzones.



Nota:

Una migración de buzones de correo puede tardar varias horas o días. No es posible hacer predicciones precisas, pues la duración depende de los siguientes factores:

- Cantidad y tamaño de los buzones de correo implicados
- Carga total de migraciones de buzones de correo en la lista de espera

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del cliente cuyos datos de buzones de correo desee migrar.
3. Vaya a **Configuración de cliente > Buzones**.



Nota:

Como alternativa, los administradores pueden navegar hasta el módulo **Configuración de cliente > Buzones** haciendo clic en el botón **Seleccionar buzones a migrar** del módulo **365 Total Protection > 365 Total Protection**.

4. Filtre los buzones de correo mostrados como desee (véase **Buzones de correo**).



Nota:

También es posible filtrar los buzones de correo por el estado de la migración de buzones de correo.



5. Si desea migrar los datos de todos los buzones de correo mostrados, proceda del siguiente modo:
- Haga clic en **Migrar todos los buzones a Microsoft 365**.



Figura 69: Migrar todos los buzones de correo mostrados



Se muestra una ventana de confirmación.

- Haga clic en **Aceptar**.



Figura 70: Confirmar la migración de todos los buzones de correo mostrados



La ventana se cierra.

Si se puede iniciar la migración de los buzones de correo, se muestra un mensaje de éxito.

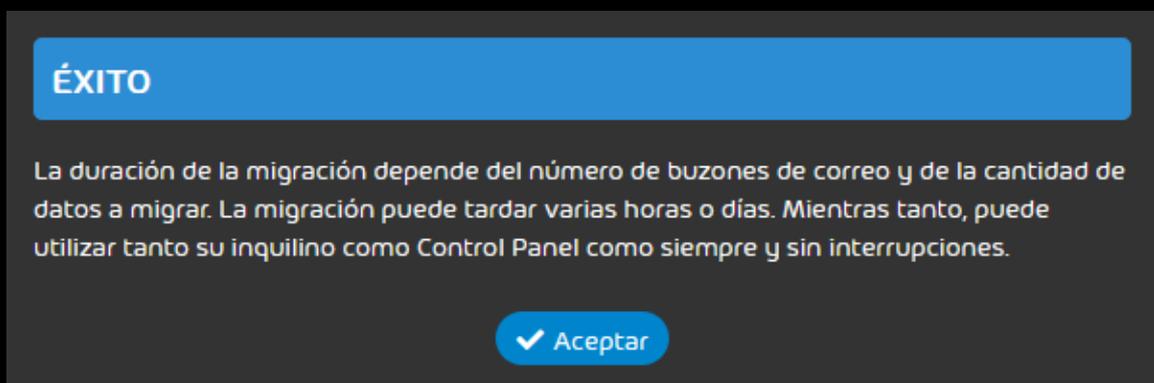


Figura 71: Mensaje de éxito



Si no se puede iniciar la migración para todos los buzones de correo seleccionado, se muestra un mensaje de error o un mensaje de advertencia. En tal caso, la migración tampoco se inicia para el resto de buzones de correo.



Nota:

Un mensaje de error puede mostrarse, por ejemplo, si uno de los buzones de correo seleccionados ya se está migrando, ya que solo es posible realizar una migración por buzón de correo.

Un mensaje de advertencia puede mostrarse, por ejemplo, si el entorno de uno de los buzones de correo seleccionados aún no ha sido validado por el administrador activo. En tal caso, el administrador deberá validar antes el entorno (véase [Validar un entorno](#) en la página 66).



Para al menos un buzón de correo seleccionado, una migración ya está en curso.

Figura 72: Mensaje de error

VALIDACIÓN DE ENTORNO NECESARIA

Los siguientes entornos aún no se han validado:

- Entorno primario

Antes de poder migrar datos de buzones de correo de estos entornos, debe validar los entornos en el módulo "365 Total Protection".

X Cerrar

Ir a la validación >

Figura 73: Mensaje de advertencia por entornos sin validar



6. Si solo desea migrar los datos de una selección de buzones de correo, proceda del siguiente modo:

a) Haga clic en .



En la lista de buzones de correo se muestra una columna con casillas.

b) Marque las casillas de los buzones de correo cuyos datos desee migrar.

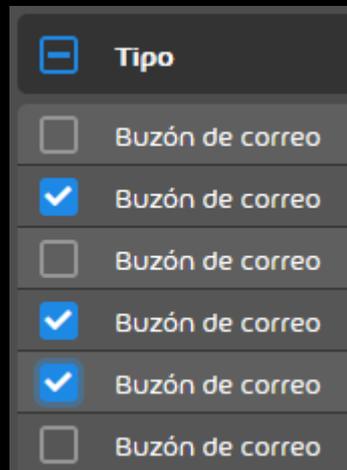


Figura 74: Seleccionar buzones de correo



El botón **Migrar buzones seleccionados a Microsoft 365** se habilita.

c) Haga clic en **Migrar buzones seleccionados a Microsoft 365**.



Figura 75: Migrar buzones de correo seleccionados



Se muestra una ventana de confirmación.

d) Haga clic en **Aceptar**.

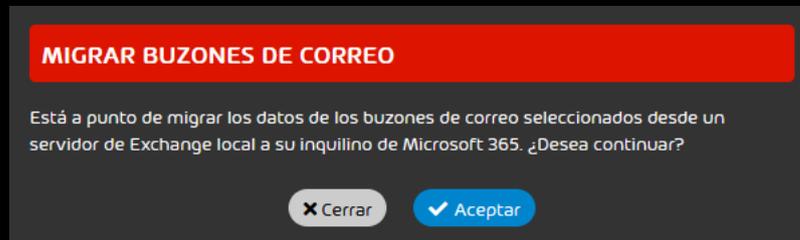


Figura 76: Confirmar la migración de los buzones de correo seleccionados



La ventana se cierra.

Si se puede iniciar la migración de los buzones de correo, se muestra un mensaje de éxito.

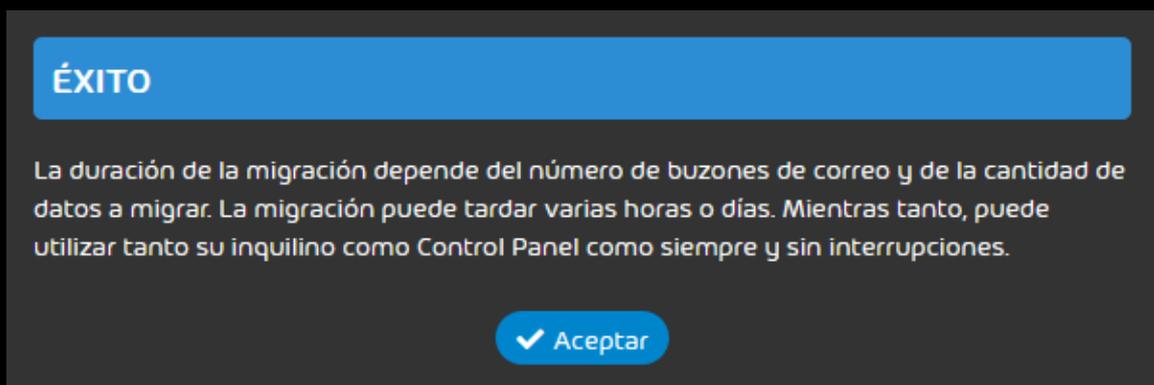


Figura 77: Mensaje de éxito

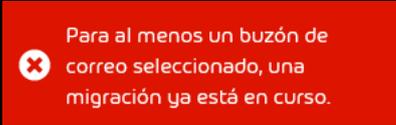
Si no se puede iniciar la migración para todos los buzones de correo seleccionado, se muestra un mensaje de error o un mensaje de advertencia. En tal caso, la migración tampoco se inicia para el resto de buzones de correo.



Nota:

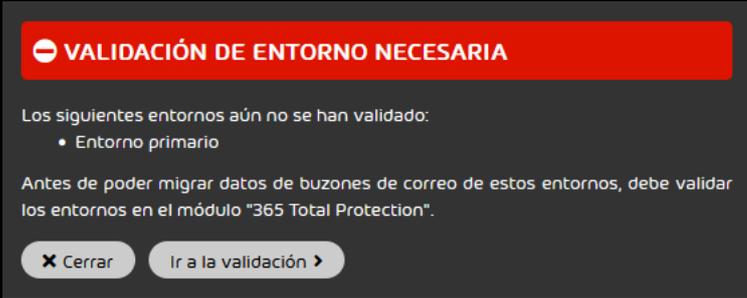
Un mensaje de error puede mostrarse, por ejemplo, si uno de los buzones de correo seleccionados ya se está migrando, ya que solo es posible realizar una migración por buzón de correo.

Un mensaje de advertencia puede mostrarse, por ejemplo, si el entorno de uno de los buzones de correo seleccionados aún no ha sido validado por el administrador activo. En tal caso, el administrador deberá validar antes el entorno (véase [Validar un entorno](#) en la página 66).



Para al menos un buzón de correo seleccionado, una migración ya está en curso.

Figura 78: Mensaje de error



VALIDACIÓN DE ENTORNO NECESARIA

Los siguientes entornos aún no se han validado:

- Entorno primario

Antes de poder migrar datos de buzones de correo de estos entornos, debe validar los entornos en el módulo "365 Total Protection".

[✕ Cerrar](#) [Ir a la validación >](#)

Figura 79: Mensaje de advertencia por entornos sin validar

7. Si se muestra un mensaje de éxito, haga clic en **Aceptar**.



8. Vaya a **365 Total Protection > 365 Total Protection**.



La nueva tarea de migración se muestra en la columna **Migraciones en curso**. Si los buzones de correo de varios entornos se han seleccionado para la migración, en lugar de una sola tarea se crean tareas individuales para cada entorno.

 **Nota:**

La migración se compone de las siguientes fases:

- **en cola:** La tarea de migración se encuentra en la lista de espera y aún no ha comenzado.
- **procesando:** La tarea de migración ha empezado a procesarse.
- **migrando:** Los datos de los buzones de correo se transfieren del servidor Exchange local al inquilino de Microsoft 365.
- **listos para redirección:** La migración de los datos de buzones de correo ha finalizado. Una vez alcanzado este estado, el administrador tiene 14 días para redirigir los buzones de correo migrados en Control Panel (véase el paso 9 en la página 80).
- **redirigiendo:** El administrador ha efectuado la redirección de los buzones de correo migrados. Como entorno de los buzones de correo migrados ya no se emplea el servidor local de Exchange, sino el inquilino de Microsoft 365. Así, nuestros servidores dirigen ahora el tráfico de los buzones de correo migrados al inquilino de Microsoft 365.

Si se produce un fallo durante la migración, ésta se pausará y se pondrá en estado **en pausa**. En tal caso, el administrador deberá intervenir en la migración.

 **Nota:**

Haciendo clic en el botón  junto a la tarea de migración se descarga el registro de la migración. El registro contiene información sobre los buzones de correo migrados y posibles errores.

9. Una vez la tarea de migración haya alcanzado el estado **listos para redirección**, haga clic en el botón  junto a la tarea de migración.



Se muestra una ventana de confirmación.



10. Haga clic en **Iniciar la redirección**.

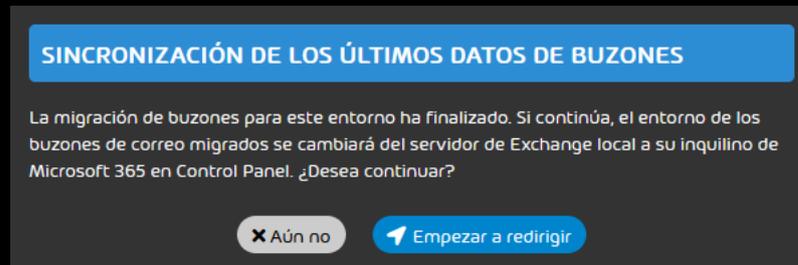


Figura 80: Confirmar la redirección



Como entorno de los buzones de correo migrados ya no se emplea el servidor local Exchange local, sino el inquilino de Microsoft 365. Si la redirección se realiza en un plazo de 14 días tras la migración de los datos de buzones de correo, los datos de los buzones de correo migrados que se hayan modificado entretanto en el servidor Exchange local se sincronizan en el inquilino de Microsoft 365.

! Importante:

Al cabo de 14 días ya no será posible sincronizar automáticamente los datos de buzones de correo actuales del servidor Exchange local con el inquilino de Microsoft 365.

La tarea de migración finaliza y se marca con una marca de verificación verde. Una vez finalizadas todas las tareas de migración, el botón **Finalizar migración de buzones** de la columna **Migraciones en curso** se habilita.

2 buzones de correo
Exchange

redirección en curso
2 / 2 migrados



Figura 81: Tarea de migración finalizada



A continuación puede transmitir los datos de buzones de correo de un servidor Exchange local al inquilino de Microsoft 365 del cliente.

Una vez finalizadas todas las tareas de migración puede finalizar la migración de buzones de correo (véase **Finalizar la migración de buzones de correo** en la página 82).



Finalizar la migración de buzones de correo

 Ha migrado los datos de todos los buzones de correo deseados (véase [Migrar buzones de correo](#) en la página 73).

Una vez finalizadas todas las tareas de migración (véase [Migrar buzones de correo](#) en la página 73) puede finalizar la migración de buzones de correo (véase [Acerca de la migración de buzones de correo](#) en la página 43). A continuación, la actualización del cliente a 365 Total Protection se reanuda automáticamente (véase [Actualizar a 365 Total Protection](#)). Solo una vez finalizada la actualización a 365 Total Protection se sincronizarán en Control Panel los buzones de correo, grupos y dominios del inquilino de Microsoft 365 del cliente.



Importante:

Una vez finalizada la migración de buzones de correo no será posible migrar más datos de buzones de correo. Por tanto, asegúrese de haber migrado los datos de todos los buzones de correo deseados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee finalizar la migración de buzones de correo.
3. Vaya a **365 Total Protection > 365 Total Protection**.
4. En la columna **Migraciones en curso**, haga clic en **Finalizar migración de buzones**.



Nota:

Este botón solo está habilitado si han finalizado todas las tareas de migración de buzones de correo de la columna **Migraciones en curso**.

 Finalizar migración de buzones

Figura 82: Finalizar la migración de buzones de correo



Se muestra una ventana de confirmación.



- Haga clic en **Finalizar migración de buzones**.



Figura 83: Confirmar la finalización de la migración de buzones de correo



La migración de buzones de correo finaliza. A continuación, continúa la actualización del cliente a 365 Total Protection (véase [Actualizar a 365 Total Protection](#)).



La migración de buzones de correo ha finalizado.

Configurar 365 Total Backup



Ha migrado a 365 Total Protection Enterprise Backup (véase [Actualizar a 365 Total Protection](#) en la página 25).

El servicio 365 Total Protection Enterprise Backup combina los servicios 365 Total Protection Enterprise y 365 Total Backup (véase [Acerca de 365 Total Protection](#) en la página 6). Una vez haya migrado a 365 Total Protection Enterprise Backup como cliente, puede configurar 365 Total Backup. Este procedimiento le permite configurar 365 Total Backup conforme a la configuración por defecto. En este caso se realizan copias de seguridad de todos los buzones de correo de Microsoft 365, archivos almacenados en cuentas de empresa de OneDrive y en bibliotecas de documentos de SharePoint, así como chats de usuarios y grupos de Teams de su inquilino.



Nota:

Los administradores a nivel de cliente o partner pueden configurar 365 Total Backup con otros ajustes abriendo 365 Total Backup desde el módulo **Copia de seguridad > 365 Total Backup** (véase [Iniciar 365 Total Backup](#)).

Con 365 Total Backup también se pueden realizar copias de seguridad de terminales con Windows. Pero los terminales no se incluyen en la configuración por defecto.

Solo los administradores a nivel de partner pueden configurar copias de seguridad de terminales. Para ello, los administradores a nivel de partner pueden abrir 365 Total Backup desde el módulo **Copia de seguridad > 365 Total Backup**.



Importante:

Los administradores a nivel de cliente solo pueden configurar 365 Total Backup si su partner les ha concedido acceso a 365 Total Backup (véase [Conceder acceso a 365 Total Backup](#)). De lo contrario, solo los administradores a nivel de partner pueden configurar 365 Total Backup para el cliente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione su dominio en la selección de ámbitos.



3. Vaya a **365 Total Protection > 365 Total Protection**.



Se muestra el estado de la configuración de 365 Total Protection Enterprise Backup.

Estado de la configuración 365 Total Protection Enterprise Backup

SE HA CONECTADO MICROSOFT 365.

21 buzones de correo | 20 licencias ⓘ | 2 dominios

Ajustar la configuración de DNS de sus dominios
La configuración de DNS de al menos un dominio sincronizado no se ha ajustado o es incorrecta. Siga las instrucciones del manual para ajustar correctamente la configuración de DNS.
[Configurar ahora](#)

Configurar 365 Total Backup
Haga clic en "Configurar ahora" para conceder los permisos necesarios para hacer copias de seguridad de su inquilino de Microsoft 365.
[Configurar ahora](#)

Configurar el tráfico de correo electrónico saliente
Es necesario que configure su tráfico de correo electrónico saliente. Las instrucciones se incluyen en nuestro [manual](#).
[Configurar automáticamente](#)

Figura 84: Estado de la configuración

4. En **Configurar 365 Total Backup**, haga clic en **Configurar ahora**.



La página de configuración de 365 Total Backup se abre en una nueva pestaña. Los datos del cliente ya están introducidos.



Nota:

La página utiliza el idioma elegido para el partner del cliente en Control Panel (véase [Ajustar zona horaria e idioma por defecto](#)).



5. Haga clic en **Continuar**.

Figura 85: Comprobar los datos



Se abre una ventana con un resumen de los pasos de configuración.



6. Haga clic en el paso 1.

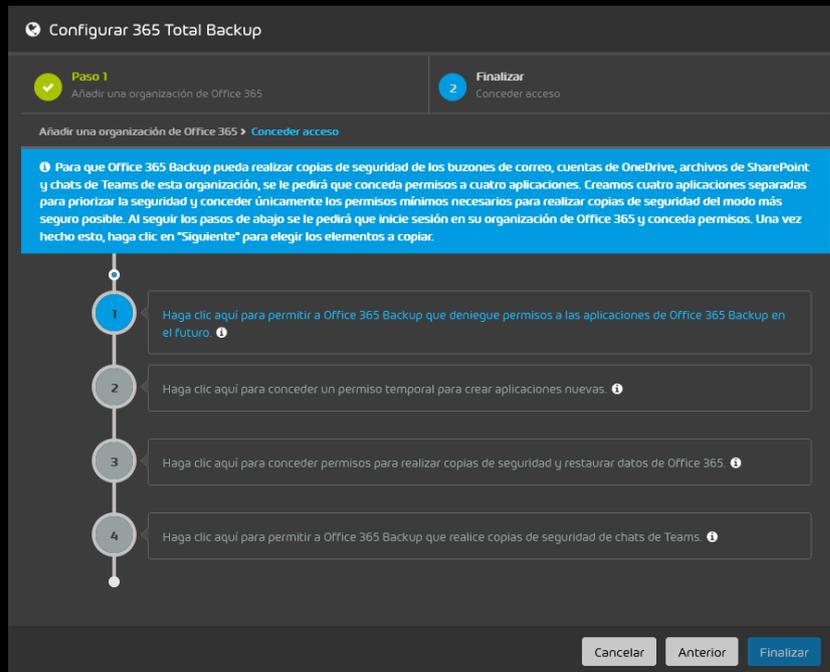


Figura 86: Realizar el paso 1



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

7. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



8. Conceda los permisos solicitados.

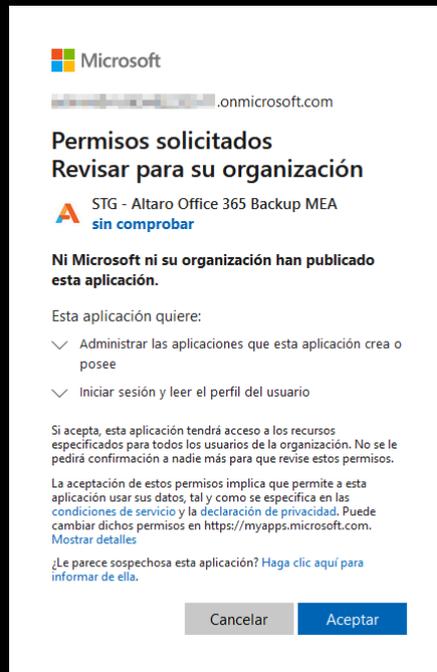


Figura 87: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.



Figura 88: Ventana de confirmación

9. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



10. Haga clic en el paso 2.

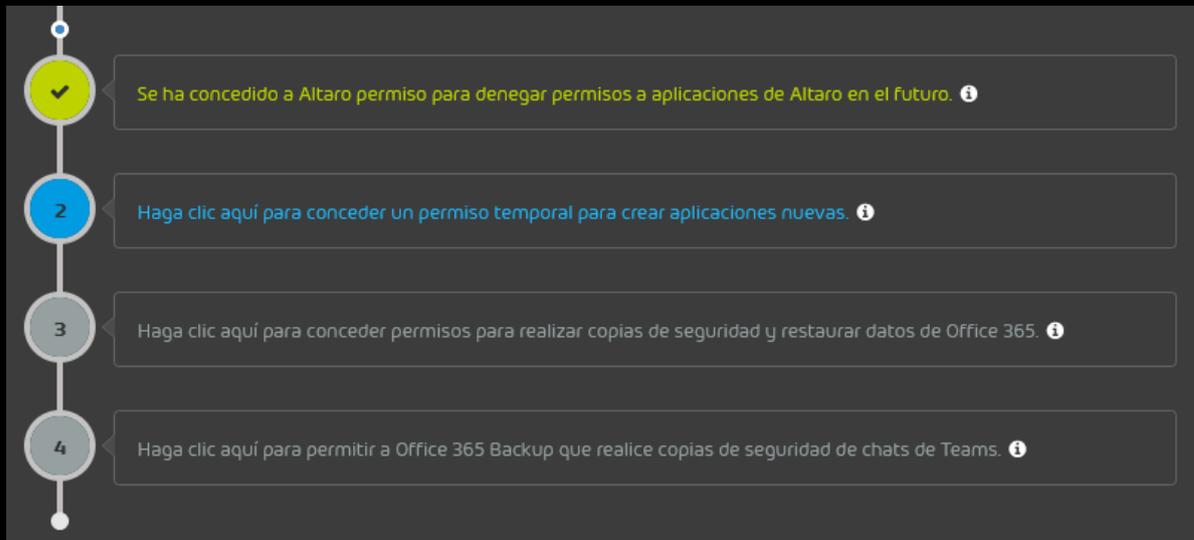


Figura 89: Realizar el paso 2



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

11. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



365 Total Backup obtiene acceso al inquilino del cliente. Se muestra un mensaje de confirmación.

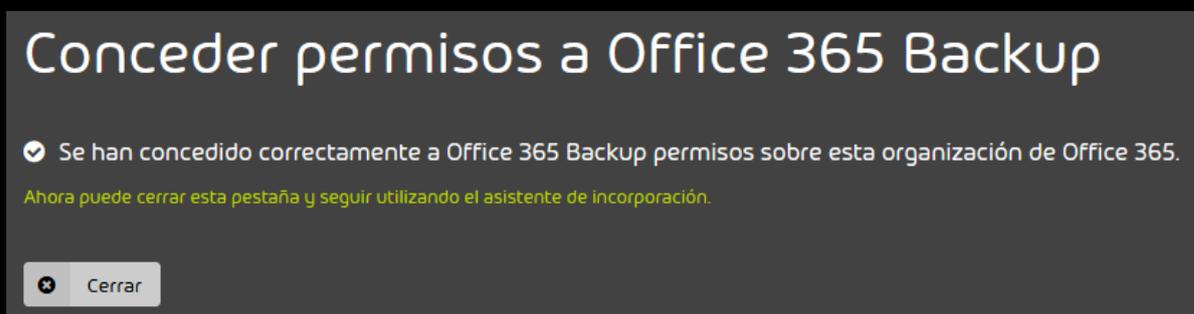


Figura 90: Ventana de confirmación

12. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



13. Haga clic en el paso 3.

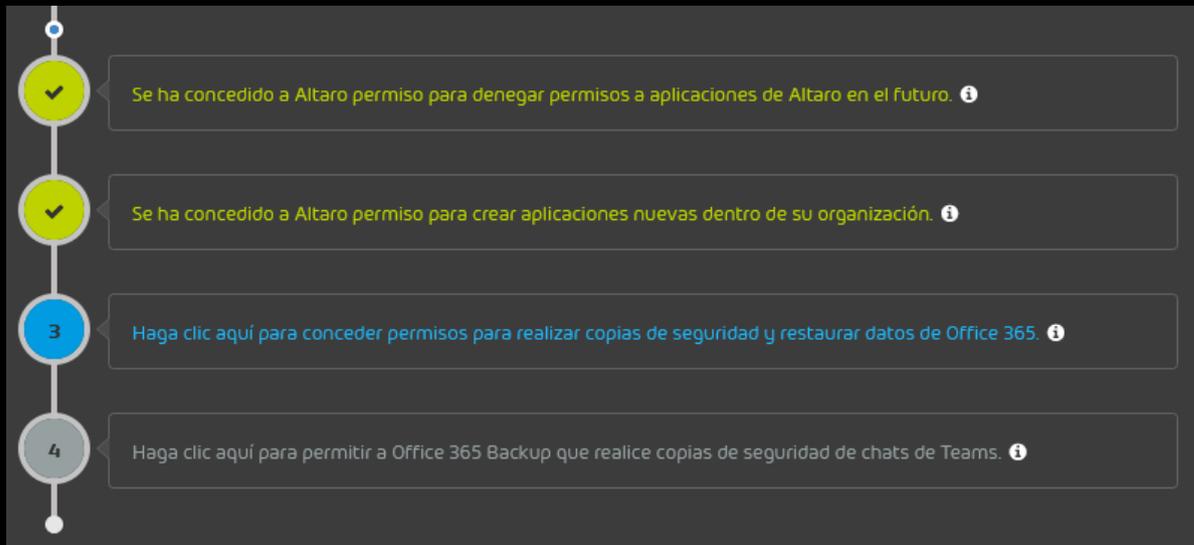


Figura 91: Realizar el paso 3



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

14. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



15. Conceda los permisos solicitados.

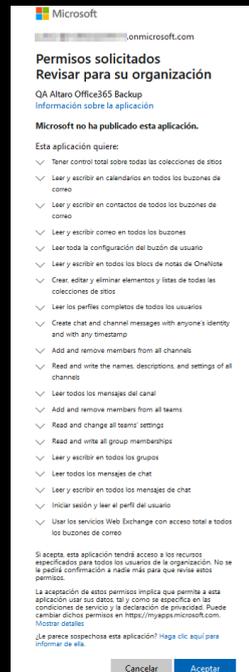


Figura 92: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.

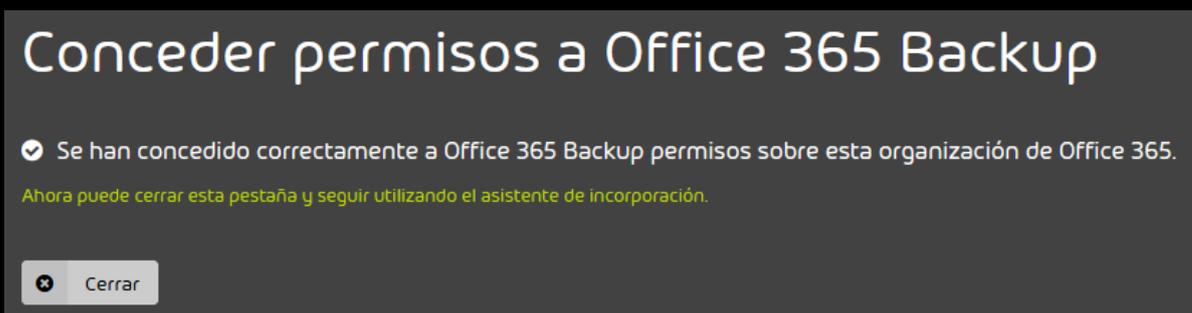


Figura 93: Ventana de confirmación



16. Haga clic en el paso 4.

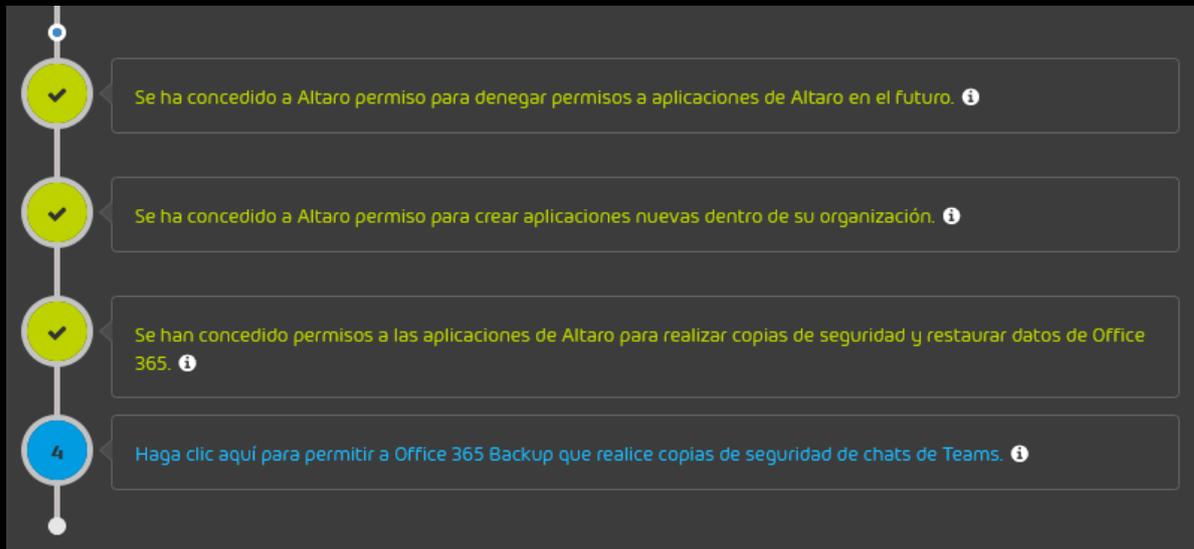


Figura 94: Realizar el paso 4



La página de inicio de sesión de Microsoft 365 se abre en una nueva pestaña.

17. Inicie sesión en Microsoft 365 con los datos de acceso de administrador del cliente.



Se muestra una página con los permisos solicitados.



18. Conceda los permisos solicitados.

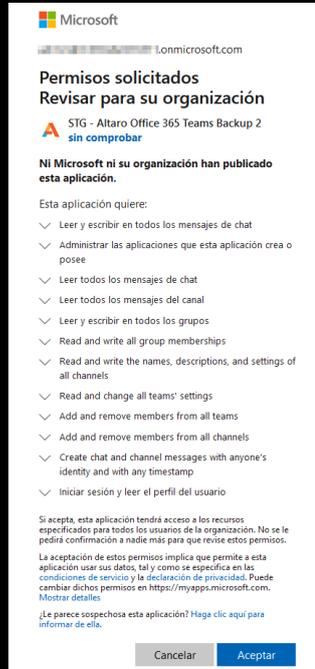


Figura 95: Conceder permisos



Se conceden los permisos. Se muestra un mensaje de confirmación.



Figura 96: Ventana de confirmación

19. Haga clic en **Cerrar**.



La pestaña se cierra. El resumen de los pasos de configuración se vuelve a mostrar.



20. Haga clic en **Finalizar**.

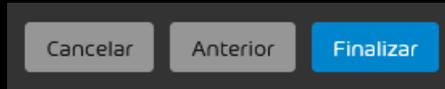


Figura 97: Finalizar la configuración



La pestaña se cierra. La configuración de 365 Total Backup se da por finalizada en el módulo **365 Total Protection > 365 Total Protection** de Control Panel.



Figura 98: Estado de la configuración de 365 Total Backup



365 Total Backup se ha configurado.



Configuración de los servicios de Microsoft

Tras la sincronización de los buzones de correo, es necesario configurar los servicios de Microsoft para todos los dominios creados para garantizar el correcto funcionamiento de 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6). Es posible realizar los siguientes ajustes:

- **Grundlegende Configuración** en la página 95: Estos ajustes son precisos para el correcto funcionamiento de 365 Total Protection.
- **Configuración avanzada** en la página 108: Estos ajustes solo son necesarios para servicios opcionales de 365 Total Protection.

Configuración básica

Grundlegende Configuración

365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) solo puede proteger sus buzones de correo dirigiendo a nuestros servidores todos los correos entrantes de remitentes externos a su organización, así como todos los correos salientes a destinatarios externos a su organización. Para ello deben cumplirse las siguientes condiciones:

- Los registros MX de las zonas de DNS de sus dominios apuntan a nuestros servidores (véase [Modificar los registros MX](#) en la página 96). Esto permite que los correos entrantes de sus dominios se dirijan primero a nuestros servidores. A continuación, nuestros servidores reenvían los correos entrantes a Microsoft 365.



Nota:

Nuestros servidores dirigen los correos entrantes a la dirección del servidor de destino de Microsoft 365 detectado automáticamente durante la sincronización inicial (véase [Instalar 365 Total Protection](#) en la página 10). Por tanto, no es necesario comunicarnos aparte esta dirección.

En cuanto se asigne un entorno primario o secundario a los buzones de correo, dejaremos de remitir los correos entrantes de dichos buzones de correo a la dirección detectada automáticamente y los enviaremos a las direcciones de los entornos asignados (véase [Configurar el entorno primario](#) y [Entornos secundarios](#)).

- Sus buzones de correo solo pueden recibir correos que hayan sido procesados por nuestros servicios. Para ello es preciso crear un conector para el tráfico de correo entrante en Microsoft



365 que solo admita correos de nuestros rangos de direcciones IP. Este conector puede crearse automáticamente (véase [Configurar automáticamente el tráfico de correo electrónico entrante y saliente](#) en la página 100).

- El filtro de spam de Microsoft 365 está desactivado para los rangos de direcciones IP de nuestros servidores (véase [Desactivar el filtro de spam de Microsoft 365 para el rango de direcciones IP de Hornetsecurity](#) en la página 102). De lo contrario, el filtro de spam de Microsoft 365 clasificaría como spam los correos procesados por nosotros.

**Importante:**

El filtro de spam de Microsoft 365 solo puede desactivarse para nuestro rango de direcciones IP después de que se haya habilitado la personalización de la organización Microsoft 365 en Exchange Online (véase [Habilitar la personalización de una organización](#) en la página 101).

- Se ha configurado un conector para el tráfico de correo saliente que reenvía los correos salientes de sus buzones de correo a nuestro smarthost. Solo así pueden nuestros servicios procesar todos los correos salientes dirigidos a buzones de correo externos a su organización. Tras el procesamiento, nuestro smarthost envía los correos salientes a sus remitentes. Este conector puede crearse automáticamente (véase [Configurar automáticamente el tráfico de correo electrónico entrante y saliente](#) en la página 100).
- Los registros SPF de sus dominios apuntan a nuestros registros SPF (véase [Modificar los registros SPF](#) en la página 107). Solo así pueden los correos enviados a través de nuestro smarthost ser declarados legítimos en comprobaciones SPF (véase [Comprobación SPF](#)) y aceptados por los servidores de recepción de correo de los destinatarios.

Modificar los registros MX



Ha configurado sus dominios.

**Nota:**

Si no está seguro de que haya finalizado la configuración de sus dominios, póngase en contacto con el soporte técnico.

Los registros MX apuntan a los servidores que reciben correos para los buzones de correo de un dominio. Puede indicar nuestros servidores en los registros MX de su dominio para que los correos entrantes de sus buzones de correos se envíen a nuestros servidores en primer lugar. Esto nos permite filtrar sus correos antes de reenviarlos a Microsoft 365.



1. Configure los registros MX en función de su región. Puede elegir entre las siguientes regiones:
 - Europa (véase [Registros MX para clientes de Europa](#) en la página 98)
 - EE.UU. (véase [Registros MX para clientes de EE.UU.](#) en la página 98)
 - Canadá (véase [Registros MX para clientes de Canadá](#) en la página 99)

**Nota:**

Los clientes cuya organización se encuentre fuera de las regiones indicadas pueden seleccionar una de ellas en función de criterios legales sobre protección de datos.

2. Para comprobar que los registros MX estén correctamente definidos, haga clic en **Mostrar configuración**.

**Figura 99: Mostrar configuración**

El informe de estado muestra que los registros MX se han modificado con éxito.

Informe de estado de MX:

Dominio	MX definidos
[Redacted]@[Redacted].com	✓

Figura 100: Informe de estado

Los registros MX se han modificado.

A continuación puede configurar automáticamente el tráfico de correo entrante y saliente (véase [Configurar automáticamente el tráfico de correo electrónico entrante y saliente](#) en la página 100).



Registros MX para clientes de Europa

Los clientes de Europa deben introducir determinados registros MX en la zona de DNS de sus dominios para que nuestros servicios puedan filtrar y procesar sus correos entrantes (véase [#unique_40](#)). El comodín **<dominio.tld>** debe reemplazarse por el dominio del cliente.

Tabla 1: Registros MX para clientes de Europa

Dominio	Clase	Tipo	Prioridad	Servidor de correo
<dominio.tld>	IN	MX	10	mx01.hornetsecurit
<dominio.tld>	IN	MX	20	mx02.hornetsecuril
<dominio.tld>	IN	MX	30	mx03.hornetsecuril
<dominio.tld>	IN	MX	40	mx04.hornetsecuril

Los clientes del proveedor de DNS 1&1 deben indicar en su lugar los siguientes registros MX:

Tabla 2: Registros MX para clientes del proveedor de DNS 1&1

Dominio	Clase	Tipo	Prioridad	Servidor de correo
<dominio.tld>	IN	MX	10	mx23a.antispameu
<dominio.tld>	IN	MX	20	mx23b.antispameu
<dominio.tld>	IN	MX	30	mx23c.antispameu
<dominio.tld>	IN	MX	40	mx23d.antispameu

Registros MX para clientes de EE.UU.

Los clientes de EE.UU. deben introducir determinados registros MX en la zona de DNS de sus dominios para que nuestros servicios puedan filtrar y procesar sus correos entrantes (véase [#unique_40](#)). El comodín **<dominio.tld>** debe reemplazarse por el dominio del cliente.



Tabla 3: Registros MX

Dominio	Clase	Tipo	Prioridad	Servidor de correo
<dominio.tld>	IN	MX	10	mx-cluster-usa01.hornetsecuri
<dominio.tld>	IN	MX	20	mx-cluster-usa02.hornetsecuri
<dominio.tld>	IN	MX	30	mx-cluster-usa03.hornetsecuri
<dominio.tld>	IN	MX	40	mx-cluster-usa04.hornetsecuri

Registros MX para clientes de Canadá

Los clientes de Canadá deben introducir determinados registros MX en la zona de DNS de sus dominios para que nuestros servicios puedan filtrar y procesar sus correos entrantes (véase [#unique_40](#)). El comodín **<dominio.tld>** debe reemplazarse por el dominio del cliente.

Tabla 4: Registros MX para clientes de Canadá

Dominio	Clase	Tipo	Prioridad	Servidor de correo
<dominio.tld>	IN	MX	10	mx-cluster-ca01.hornetsecuri
<dominio.tld>	IN	MX	20	mx-cluster-ca02.hornetsecuri
<dominio.tld>	IN	MX	30	mx-cluster-ca03.hornetsecuri
<dominio.tld>	IN	MX	40	mx-cluster-ca-fallback.hornetsecu



Configurar automáticamente el tráfico de correo electrónico entrante y saliente

Los conectores para el correo entrante y saliente garantizan que todos los correos de remitentes y a destinatarios externos a su organización se dirijan a nuestros servidores. Puede configurar estos conectores automáticamente desde la página de estado de **365 Total Protection** (véase [Acerca de 365 Total Protection](#) en la página 6).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **365 Total Protection > 365 Total Protection**.
4. Haga clic en **Configurar automáticamente**.

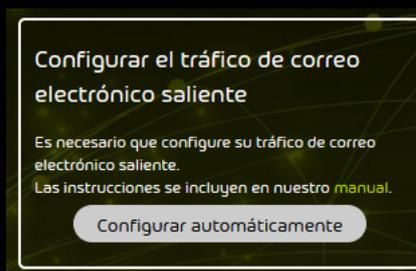


Figura 101: Configuración automática

Nota:

Al configurar automáticamente el tráfico de correo electrónico saliente se configura también automáticamente el tráfico de correo electrónico entrante.



Los tráficos de correo entrante y saliente se configuran.



Se han configurado conectores para el tráfico de correo entrante y saliente.



Figura 102: Configuración finalizada con éxito

**Importante:**

Conectores previamente instalados pueden provocar errores durante la configuración automática del tráfico de correo saliente.



Figura 103: Errores en la configuración

Solución de problemas

- Elimine los conectores que ya hubiera configurados y haga clic en **Configurar de nuevo** para reiniciar la configuración.
- Otra opción es hacer clic en **Soporte técnico** para ponerse en contacto con el soporte técnico.

A continuación puede desactivar el filtro de spam de Microsoft 365 para nuestro rango de direcciones IP (véase [Desactivar el filtro de spam de Microsoft 365 para el rango de direcciones IP de Hornetsecurity](#) en la página 102).

Habilitar la personalización de una organización

Las organizaciones Microsoft 365 están por defecto deshidratadas en Exchange Online. Esto significa que algunos objetos en los centros de datos de Microsoft están consolidados para reducir el espacio de almacenamiento. Por tal motivo, no es posible editar algunos objetos para organizaciones Microsoft 365 deshidratadas en Exchange Online. Antes de poder editar estos objetos, debe habilitar la personalización de su organización Microsoft 365 en Exchange Online



una vez ejecutando una orden. Por el mismo motivo, solo puede desactivar el filtro de spam de Microsoft 365 para nuestro rango de direcciones IP (véase [Desactivar el filtro de spam de Microsoft 365 para el rango de direcciones IP de Hornetsecurity](#) en la página 102) después de haber ejecutado la orden. La orden hidrata la organización.

**Importante:**

La orden solo puede ejecutarse una vez y no puede deshacerse.

1. Abra PowerShell de Exchange Online.
2. Opcional: Para comprobar si la personalización de su organización Microsoft 365 ya está habilitada, ejecute la siguiente orden: **Get-OrganizationConfig | fl IsDehydrated**.



Si la personalización ya está habilitada, se emite el valor **False**. Si la personalización aún no está habilitada, se emite el valor **True**.

3. Ejecute la siguiente orden: **Enable-OrganizationCustomization**.



La organización Microsoft 365 se hidrata en Exchange Online. Se habilita la personalización de su inquilino de Microsoft 365 en Exchange Online. Los cambios pueden tardar algún tiempo en hacerse efectivos.



Se ha habilitado la personalización de una organización Microsoft 365 en Exchange Online.

A continuación puede desactivar el filtro de spam de Microsoft 365 para nuestro rango de direcciones IP (véase [Desactivar el filtro de spam de Microsoft 365 para el rango de direcciones IP de Hornetsecurity](#) en la página 102).

Desactivar el filtro de spam de Microsoft 365 para el rango de direcciones IP de Hornetsecurity



Ha habilitado la personalización de su organización Microsoft 365 en Exchange Online (véase [Habilitar la personalización de una organización](#) en la página 101).

Si desea filtrar los correos entrantes mediante nuestros servicios deberá desactivar el filtro de spam de Microsoft 365. De lo contrario, el filtro de spam de Microsoft 365 clasificaría como spam los correos entrantes de sus dominios. Nuestros servicios filtran sus correos entrantes en busca de spam.



Nota:

La autenticación de correos mediante SPF no está activada por defecto. No es obligatorio activar la comprobación SPF, pero sí es recomendable. Para más información sobre la instalación, véase [Sobre Email Authentication](#).

1. Inicie sesión en admin.microsoft.com con sus datos de acceso de administrador.
2. Seleccione el punto **Seguridad** del menú **Centro de administración**.



Nota:

Si en su vista predeterminada no se le muestra el Centro de Administración, abra el menú con **Mostrar todos**.



Se abre la página de inicio de **Microsoft 365 Defender**.

3. Haga clic en el punto de menú **Reglas y directivas**, situado a la izquierda.

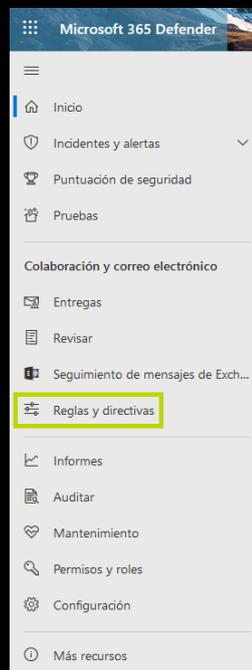


Figura 104: Seleccionar el punto de menú



- Haga clic en **Directivas de amenazas**.



Figura 105: Seleccionar Directivas de amenazas

- En **Directivas**, haga clic en **Contra spam**.

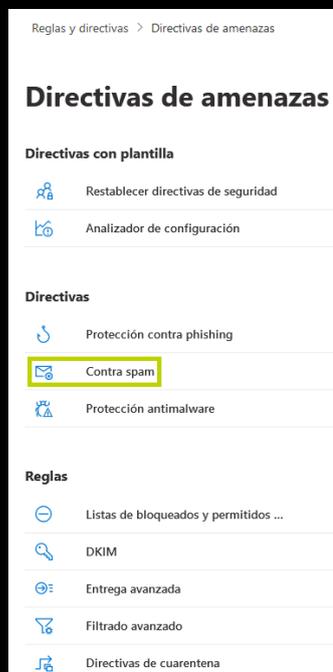


Figura 106: Seleccionar Contra spam



Se abre la página **Directivas de correo electrónico no deseado**.



6. Haga clic en **Directiva de filtro de conexión (predeterminado)**.

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

ⓘ Vaya a la página de la directiva de cuarentena para configurar la notificación de correo no deseado para el usuario final, pues la configuración de la directiva contra el correo no deseado se eliminará en diciembre de 2021. [Obtenga más información sobre la directiva de cuarentena](#)

Utilice esta página para configurar directivas que se incluyen en la protección contra correo no deseado. Estas directivas incluyen filtrado de conexión, filtrado de correo no deseado, filtrado de correo no deseado de salida e inteligencia de suplantación. [obtener más información](#)

+ Crear directiva ▾ Actualizar 1 de 3 seleccionados ≡ ▾

Nombre	Estado	Prioridad	Tipo
Directiva de entrada de correo no deseado (prede...	● Siempre activada	La más baja	
Directiva de filtro de conexión (predeterminado)	● Siempre activada	La más baja	
Directiva de salida de correo electrónico no desea...	● Siempre activada	La más baja	

Figura 107: Seleccionar Directiva de filtro de conexión (predeterminado)



Se abre la configuración de la directiva.



7. Haga clic en **Editar directiva de filtro de conexión**.

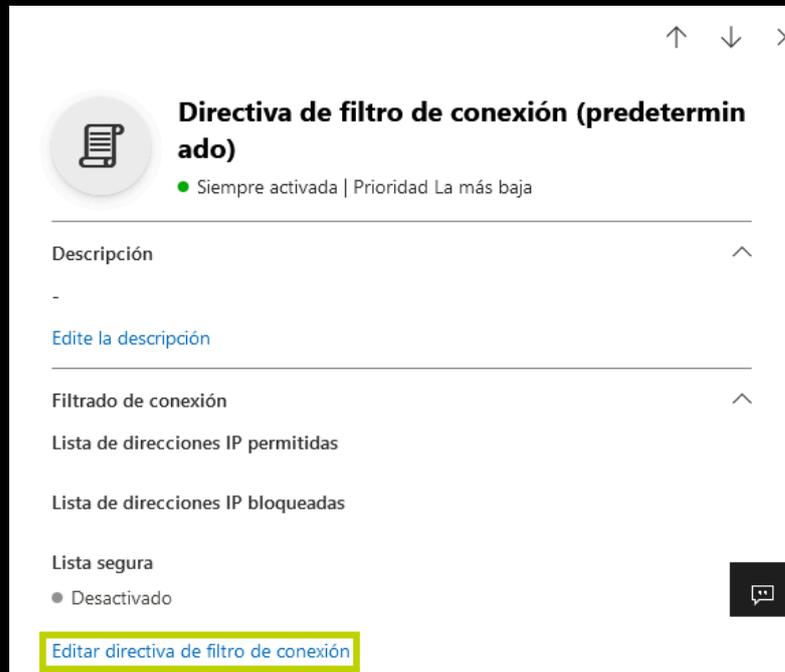


Figura 108: Editar directiva



Se muestran ajustes adicionales.

8. Introduzca las siguientes direcciones IP una tras otra en el campo **Always allow messages from the following IP addresses or address range**:

83.246.65.0/24	94.100.128.0/24	94.100.129.0/24
94.100.130.0/24	94.100.131.0/24	94.100.132.0/24
94.100.133.0/24	94.100.134.0/24	94.100.135.0/24
94.100.136.0/24	94.100.137.0/24	94.100.138.0/24
94.100.139.0/24	94.100.140.0/24	94.100.141.0/24
94.100.142.0/24	94.100.143.0/24	173.45.18.0/24
185.140.204.0/24	185.140.205.0/24	185.140.206.0/24



185.140.207.0/24



Nota:

Los clientes canadienses deben registrar adicionalmente los siguientes rangos IP:

108.163.133.224/27 199.27.221.64/27 209.172.38.64/27
216.46.2.48/29 216.46.11.224/27

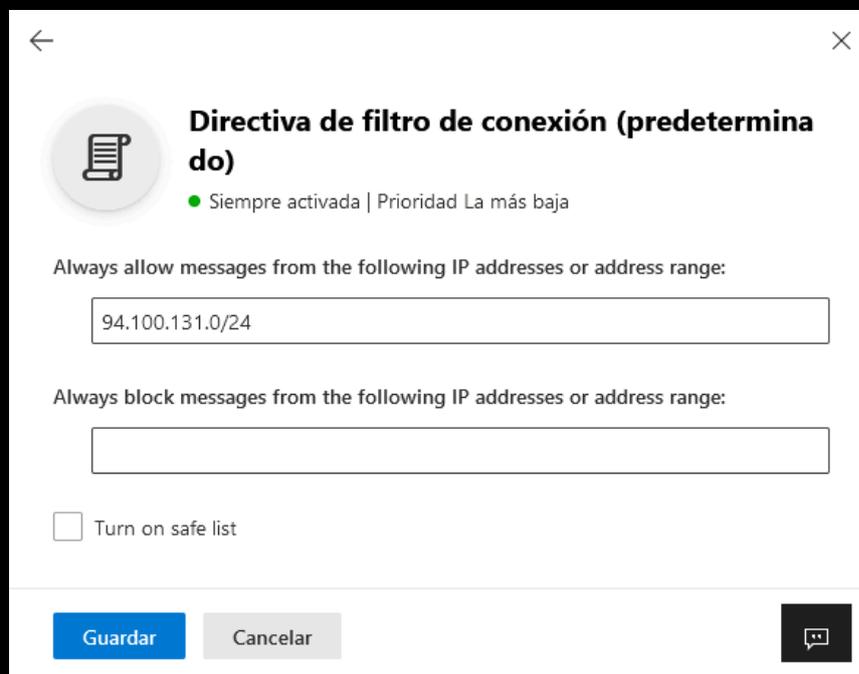


Figura 109: Introducir direcciones IP en la lista de direcciones IP permitidas

- Haga clic en **Guardar**.



Los ajustes se guardan.



El filtro de spam de Microsoft 365 se ha desactivado para correos de nuestro rango de direcciones IP.

Modificar los registros SPF

Los registros SPF de sus dominios deben hacer referencia a nuestros registros SPF. De este modo, los servidores de recepción de correo reconocerán a Hornetsecurity como remitente y los correos



enviados a través de nuestro smarthost no se clasificarán como spam durante la comprobación SPF (véase [Comprobación SPF](#)).

**Nota:**

Nuestro registro SPF no es necesario para clientes que hayan configurado su entorno primario con la opción **IP/Nombre de host** pero sin indicar direcciones de servidores de retransmisión para correos salientes. Para más información sobre cómo configurar el entorno primario, véase [Configuración del entorno primario](#).

1. Inicie sesión en el entorno de administración de Microsoft 365.
2. Vaya a **Configuración > Dominios**.
3. Seleccione el dominio que haya registrado en Hornetsecurity.
4. Añada el siguiente registro SPF: **TXT "v=spf1 include:spf.protection.outlook.com include:spf.hornetsecurity.com ~all"**

**Importante:**

Si dispone de sistemas adicionales que envíen correos salientes para este dominio, añádalos también al registro SPF.



Sus registros SPF se han modificado.

Configuración avanzada

Configuración avanzada

Para poder emplear funciones adicionales o evitar problemas ocurridos durante la configuración automática, además de la configuración básica (véase [Grundlegende Configuración](#) en la página 95), es posible realizar ajustes avanzados para 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6).

- Para facilitar el proceso de configuración de cuentas de usuario en programas de correo electrónico es posible activar el servicio de detección automática (véase [Activar la detección automática](#) en la página 109).
- Si fracasa la configuración automática de conectores para el tráfico de correo entrante y saliente (véase [Configurar automáticamente el tráfico de correo electrónico entrante y](#)



saliente en la página 100), existe la posibilidad de crear los conectores manualmente. En tal caso es preciso habilitar el archivo del tráfico de correo interno de su empresa creando una regla de diario. Encontrará más información al respecto en el manual **Configuración inicial manual de los servicios con Microsoft 365**

- Si desea administrar los buzones de correo de un dominio, en parte, mediante un entorno primario y, en parte, mediante otros entornos secundarios (véase **Entornos secundarios**), deberá establecer reenvíos a dichos entornos secundarios. De lo contrario, los correos dirigidos a los buzones de correo de los entornos secundarios se rechazarán. Para más información sobre la configuración, véase el manual **Reenvío de correos de Microsoft 365**
- La autenticación multifactor de cuentas de Microsoft 365 también se utiliza para iniciar sesión en Control Panel (véase **Autenticación multifactor** en la página 109),

Activar la detección automática

Configurando el servicio de detección automática se facilita el proceso de configuración de cuentas de usuarios en programas de correo electrónico. De este modo, los ya no necesitan indicar ningún nombre de servidor o número de puerto: el servicio de detección automática envía automáticamente dichos datos de correo electrónico.

Defina un registro CNAME para el servicio de detección automática:

Tabla 5: Añadir un registro MX

TIPO	PRIORIDAD	NOMBRE DE HOST	APUNTA A	TTL
CNAME		detección automática	autodiscover.hornetsecurity.com	1 hora



El servicio de detección automática se ha activado con éxito.

Autenticación multifactor

Todos los usuarios de un dominio protegido por 365 Total Protection inician sesión en Control Panel con sus datos de acceso de Microsoft 365. Si la autenticación multifactor está activada en Microsoft 365, también se utilizará en Control Panel.



Adquirir 365 Total Protection

Si desea continuar utilizando 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) tras el periodo de prueba de 14 días, puede adquirirlo directamente desde Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee adquirir 365 Total Protection.
3. Seleccione **365 Total Protection**.
4. Haga clic en **Adquirir ahora**.



Se muestra un resumen sobre su cantidad de buzones de correo y el precio.

◀ Comprar 365 Total Protection

Está a punto de adquirir una suscripción para 365 Total Protection Enterprise para 2 buzones de correo a un precio neto de 4,00€ por buzón. El importe total se calcula en base a la cantidad máxima de buzones de correo alcanzada durante el mes de facturación.

Aquí encontrará nuestras [condiciones generales de contratación](#) y la [descripción de servicio](#) de 365 Total Protection Enterprise.

Adquirir

5. Haga clic en **Adquirir** para adquirir 365 Total Protection.



Recibirá un correo de confirmación con un resumen sobre su producto.



Se ha adquirido 365 Total Protection.



Visualización de las cantidades de buzones de correo, licencias y dominios

Tras la incorporación, los clientes de 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) pueden ver la cantidad de buzones de correo, licencias y dominios en **365 Total Protection > 365 Total Protection**.



Figura 110: Cantidades de buzones de correo, licencias y dominios

En **Buzones** se muestra la cantidad de buzones de correo que se sincronizan con Microsoft 365. Esta cantidad contiene buzones de correo tanto de usuarios normales como de administradores.

En **licencias** se muestra la cantidad de licencias a facturar. La cantidad de licencias equivale a la cantidad de buzones de correo principales de los usuarios de 365 Total Protection sin contar los de los administradores. La cantidad mostrada se obtiene de distintos modos en función del estado de la licencia:

- Durante la fase de prueba de 365 Total Protection se muestra en cada momento la cantidad de buzones de correo principales determinada durante la sincronización más reciente con Microsoft 365.
- Durante el primer mes tras la finalización de la fase de prueba o la adquisición de la versión de pago de 365 Total Protection se muestra la cantidad de buzones de correo principales protegidos por 365 Total Protection en el momento en que finalizó la fase de prueba o se adquirió la versión de pago. Esta es la cantidad empleada para la facturación durante el primer mes.
- A partir del segundo mes tras la finalización de la fase de prueba o la adquisición de la versión de pago de 365 Total Protection se muestra el máximo de buzones de correo protegidos simultáneamente por 365 Total Protection durante el mes actual. Esta es la cantidad empleada para la facturación durante el mes en cuestión.

En **Dominios** se muestra la cantidad de dominios para los que está activado 365 Total Protection. Esta cantidad contiene tanto el dominio principal como también los dominios alias del cliente.



Administración de buzones de correo.

En el módulo **Configuración de cliente** > **Buzones** es posible administrar buzones de correo (véase "**Configuración de cliente**" en el manual de Control Panel). Además de buzones de Microsoft 365, los clientes de 365 Total Protection (véase **Acerca de 365 Total Protection** en la página 6) pueden administrar buzones de correo de otros proveedores creados manualmente (véase **Tipos de buzón de correo**). Los buzones de correo de Microsoft 365 y buzones de correo creados manualmente tienen conjuntos de funciones diferentes.

A diferencia de los buzones de Microsoft 365, los buzones de correo creados manualmente (véase "**Añadir un buzón de correo**" en el manual de Control Panel) no se sincronizan con Microsoft 365. A los buzones de correo creados manualmente se les pueden aplicar todas las funciones del módulo **Buzones**. A estos buzones de correo es preciso asignarles entornos secundarios (véase "**Entornos secundarios**" en el manual de Control Panel).

Las funciones del módulo **Buzones** disponibles para buzones de correo de Microsoft 365 son limitadas:

- Los buzones de correo de Microsoft 365 no pueden añadirse manualmente.
- Los buzones de correo de Microsoft 365 no pueden eliminarse manualmente.
- Los datos básicos de buzones de correo de Microsoft 365 no pueden editarse.
- Las contraseñas de buzones de correo de Microsoft 365 no pueden cambiarse.
- No es posible asignar direcciones alias a buzones de correo de Microsoft 365.

Para diferenciar entre buzones de correo de Microsoft 365 y buzones de correo creados manualmente, el módulo **Buzones** ofrece a los clientes de 365 Total Protection los siguientes tipos de buzón de correo adicionales:

- **Buzón de Microsoft 365**
- **Buzón funcional de Microsoft 365**
- **Buzón administrativo de Microsoft 365**



Administración de grupos en Control Panel

Control Panel permite realizar grupos de buzones de correo (véase "**Grupos**"). Si hay grupos disponibles, es posible realizar ajustes a nivel de grupo y no solo buzón a buzón. La pertenencia de buzones de correo de Microsoft 365 (véase **Tipos de buzón de correo**) a grupos se administra exclusivamente en Microsoft 365. Por tanto, los buzones de Microsoft 365 no pueden añadirse a grupos de Control Panel. Sin embargo, es posible visualizar grupos de Microsoft 365 en Control Panel creando en éste grupos con los mismos nombres (véase **Sincronizar grupos de Microsoft 365 en Control Panel** en la página 113). Pueden sincronizarse grupos de Microsoft 365, listas de correo, grupos de seguridad y grupos de seguridad habilitados para correo.

A excepción de algunas limitaciones descritas en el manual de Control Panel, los grupos sincronizados disponen de las mismas opciones que los grupos no sincronizados en Control Panel (véase "**Grupos**"). Además de buzones de Microsoft 365, es posible añadir buzones de entornos secundarios (véase "**Entornos secundarios**") a los grupos sincronizados. Estos buzones se ignoran durante la sincronización con Microsoft 365 y se mantienen en Control Panel.

Sincronizar grupos de Microsoft 365 en Control Panel

Puede sincronizar grupos de Microsoft 365 en Control Panel (véase **Administración de grupos en Control Panel** en la página 113). De este modo, Control Panel obtiene información sobre la composición de sus grupos de Microsoft 365 para que sea posible realizar ajustes específicos para dichos grupos.

**Nota:**

Pueden sincronizarse grupos de Microsoft 365, listas de correo, grupos de seguridad y grupos de seguridad habilitados para correo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente para el cual desee sincronizar un grupo con Microsoft 365.
3. Vaya a **Configuración de cliente > Grupos**.



- Haga clic en **Añadir**.



Se despliega un menú desplegable.

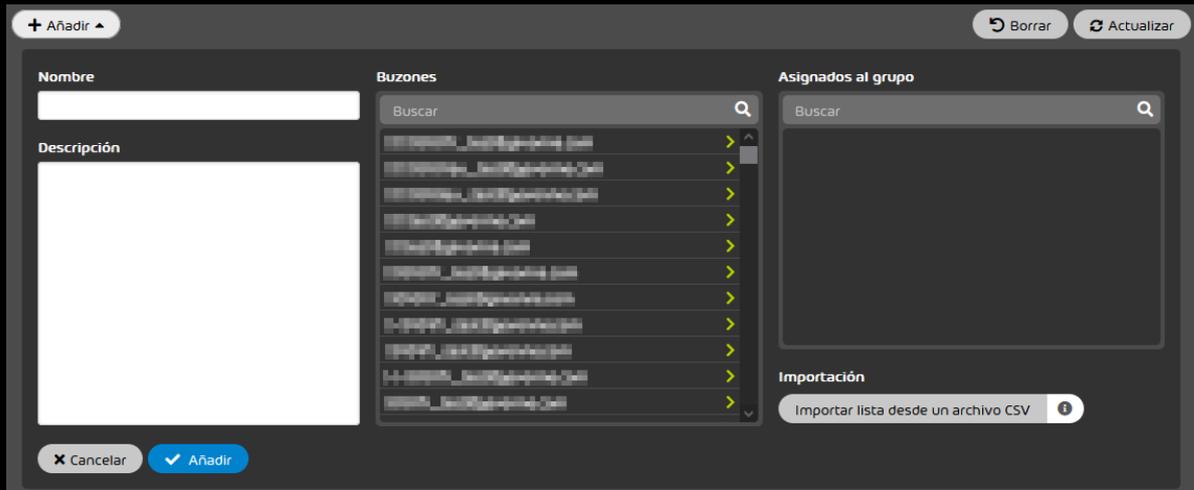


Figura 111: Añadir un nuevo grupo

-
-
-
-
-



Importante:

El nombre del grupo de Control Panel debe coincidir exactamente con el nombre del grupo de Microsoft 365 para que Control Panel pueda relacionarlos entre sí. De lo contrario, no es posible sincronizar el grupo.

En **Nombre**, introduzca el nombre del grupo de Microsoft 365 que desee sincronizar en Control Panel.

-
-
-
-
-
-



El grupo se añade a Control Panel. Durante la siguiente sincronización, los miembros del grupo de Microsoft 365 se añadirán al grupo.



Nota:

Control Panel sincroniza sus datos con Microsoft 365 varias veces por hora. Por tanto, los datos del grupo pueden tardar algunos minutos en estar disponibles en Control Panel.





Se ha transferido un grupo de Microsoft 365 a Control Panel y se ha sincronizado con Microsoft 365.



Interacción de 365 Total Protection con otros servicios

365 Total Protection incluye varios servicios (véase [Acerca de 365 Total Protection](#) en la página 6) que dependen de la configuración de 365 Total Protection. A continuación se describen algunos casos.



Nota:

En la página [365 Total Protection](#) del sitio web de Hornetsecurity se incluye una relación completa de las funciones de 365 Total Protection.

- Los administradores deben activar por separado el servicio Email Encryption (véase [Email Encryption](#) en la página 116).
- Los administrador deben activar por separado el servicio Continuity Service, disponible únicamente en 365 Total Protection Enterprise (véase [Activar Continuity Service \(solo para 365 Total Protection Enterprise\)](#) en la página 117).
- Para el servicio Signature and Disclaimer se sincronizan numerosos atributos de Azure Active Directory, el servicio de directorio de Microsoft 365 (véase [Atributos sincronizados desde Azure Active Directory](#) en la página 119).

Email Encryption

Email Encryption está incluido en los productos 365 Total Protection Business y Enterprise (véase [Acerca de 365 Total Protection](#) en la página 6). Email Encryption se activa manualmente, porque es necesario efectuar algunos ajustes. Para hacerlo, siga las instrucciones del capítulo "[Email Encryption](#)".



Importante:

En el módulo **Email Encryption**, los administradores a nivel de cliente pueden adquirir certificados S/MIME para usuarios. Un certificado S/MIME está vinculado a la dirección de correo principal de un usuario. Si la dirección de correo electrónico del usuario cambia, el certificado S/MIME ya no es válido para el usuario.

Si la dirección de correo electrónico de un usuario se renombra en Microsoft 365, también se renombrará en Control Panel durante la siguiente sincronización. Los administradores del cliente serán informados por correo electrónico sobre los cambios de nombre de los usuarios sincronizados que hasta ahora han tenido un certificado S/MIME válido. Para más información, véase [Añadir un usuario con S/MIME](#).



Activar Continuity Service (solo para 365 Total Protection Enterprise)

Si los servicios de Microsoft dejan de funcionar o no se encuentran disponibles temporalmente, el acceso a su buzón de correo también se ve afectado. En tal caso no es posible recibir ni enviar correos, lo cual puede afectar a todos sus procesos comerciales. Para estos casos está Continuity Service, un sistema de emergencia que se activa en pocos segundos y mantiene en movimiento su tráfico de correo electrónico. Para más información, véase [Sobre Continuity Service](#).

**Nota:**

Continuity Service solo está incluido en 365 Total Protection Enterprise, y es necesario activarlo manualmente y realizar algunos ajustes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a > .
4. Accione el interruptor .



Figura 112: Activar Continuity Service



Se muestra una ventana de confirmación.



5.

Atención:

Una vez activado Continuity Service, comenzará un periodo de prueba gratuito de 30 días. Al finalizar el periodo de prueba, el servicio se volverá de pago.

Continuity Service se factura por clientes y no por usuarios.

Importante:

Los administradores no pueden desactivar Continuity Service por sí mismos. Solo el soporte técnico puede desactivar Continuity Service para un dominio.

Haga clic en .

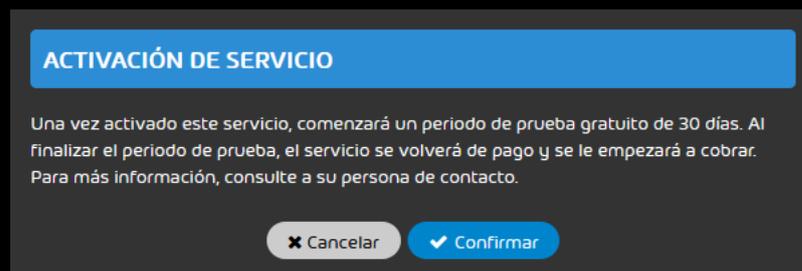


Figura 113: Confirmar



Continuity Service se activa.

6. Seleccione los usuarios para los cuales desee activar Continuity Service. Tiene dos opciones:

- **Todos los usuarios**: Todos los usuarios del dominio se añaden a Continuity Service. Para más pasos, véase [#unique_49](#).
- **Solo usuarios seleccionados**: Solo se añaden determinados usuarios del dominio a Continuity Service. Para más pasos, véase [#unique_50](#).

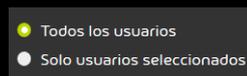


Figura 114: Seleccionar opción



Se ha activado Continuity Service.



Atributos sincronizados desde Azure Active Directory

Determinados atributos para Signature and Disclaimer (véase [#unique_51](#)) se sincronizan con Azure Active Directory de Microsoft.

! Importante:

No es posible sincronizar atributos desde Microsoft 365 y utilizar LDAP al mismo tiempo (véase ["Conexión mediante LDAP"](#)). Para los buzones de correo de Microsoft 365 (véase [Tipos de buzón de correo](#)) solo se sincronizan los atributos de la tabla de abajo. Para los buzones creados manualmente se emplean los datos básicos (véase [#unique_52](#)). Los atributos de LDAP no se sincronizan y no pueden emplearse.

Los siguientes atributos se sincronizan para buzones de correo de Microsoft 365 y pueden emplearse para crear firmas y notas legales:

Variable de AD	Significado
countryCode	País/región
department	Departamento
displayName	Nombre para mostrar – nombre completo
givenName	Nombre
info	Función/cargo
l (L minúscula)	Municipio
mail	Dirección de correo



Nota:

El campo "title" se emplea para otras muchas cosas. Por tanto, para el atributo de LDAP "title" (función/cargo) se emplea aquí la denominación "info".



Variable de AD	Significado
mobile	Número de teléfono móvil
postalCode	Código postal
sn	Apellido
st	Estado/cantón
streetAddress	Calle
telephoneNumber	Número de teléfono



Retirada tras el periodo de prueba o baja

Si un cliente ha terminado el periodo de prueba de 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) y no desea continuar utilizando el producto, o bien ha rescindido su contrato de 365 Total Protection, deberá revertir los ajustes realizados en su configuración de Microsoft 365 para poder seguir recibiendo sus correos.

1. El cliente deberá eliminar o desactivar el conector para el tráfico de correo entrante. (Configuración de cortafuegos)
2. Si el cliente ha modificado el tráfico de correo saliente, deberá también eliminar o desactivar el conector correspondiente. (Retransmisión)



Nota:

Para más información sobre cómo eliminar o desactivar conectores en el entorno de Microsoft 365, véase [Eliminar o desactivar el conector](#) en la página 121.

3. El cliente deberá eliminar los registros MX de la zona de DNS de su dominio.

En adelante, los correos del cliente dejarán de redirigirse a través de nuestros servicios.

Los administradores a nivel de partner pueden eliminar al cliente de Control Panel (véase [Eliminar clientes](#) en la página 122).

Eliminar o desactivar el conector

Si no desea seguir utilizando 365 Total Protection (véanse [Acerca de 365 Total Protection](#) en la página 6 y [Retirada tras el periodo de prueba o baja](#) en la página 121), deberá eliminar o desactivar los conectores para el tráfico de correo entrante y saliente en Microsoft 365.

1. Abra Office.com y acceda con sus datos de acceso de administrador.
2. Vaya a **Administrador > Centro de administración > Exchange**.
3. Seleccione **Flujo de correo** y, a continuación, la pestaña **Conectores**.
4. Seleccione el conector correspondiente.



5. Puede elegir entre eliminar o desactivar el conector:

- Para eliminar el conector, haga clic en **Eliminar**.
- Para desactivar el conector, haga clic en **Desactivar** en el resumen del conector.

Centro de administración de Exchange

panel reglas seguimiento de mensajes dominios aceptados dominios remotos **conectores**

destinatarios

permisos

administración de cumplimiento

organización

protección

flujo de correo

móvil

carpetas públicas

mensajería unificada

hibrido

Los conectores ayudan a controlar el flujo de los mensajes de correo electrónico desde y hacia su organización de Office 365. Sin embargo, muchas organizaciones no necesitan usar conectores, así que le recomendamos que primero [compruebe si debe crear uno](#).

¿Desea ayudarnos a mejorar los conectores? Simplemente [envíenos sus comentarios](#) y coméntenos qué le gustó, qué no y qué podemos hacer para mejorar su experiencia.

ESTADO	NOMBRE	DE	PARA
Activado	InboundConnector	Organización asociada	Office 365
Activado	OutboundConnector	Office 365	Organización asocia...

InboundConnector

Escenario de flujo de correo

De: Organización asociada

Para: Office 365

Descripción

Inbound Connector

Estado

Activado

Desactivarlo

Cómo identificar la organización de su asociado

Figura 115: Eliminar o desactivar el conector

6. Confirme el mensaje de advertencia con **Sí**.



Se ha eliminado o desactivado un conector.

Eliminar clientes

Como administrador a nivel de partner, puede eliminar clientes de 365 Total Protection (véase [Acerca de 365 Total Protection](#) en la página 6) durante o al final de la fase de prueba.



PRECAUCIÓN:

Una vez eliminado un cliente, todos los datos del mismo se eliminan de Control Panel. Los datos del cliente no pueden recuperarse. Asegúrese de que desee eliminar el cliente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.



2. En la selección de ámbitos, seleccione el partner cuyos clientes desee eliminar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Dashboard de servicios**.
5. Haga clic en la flecha de menú junto al cliente que desee eliminar.

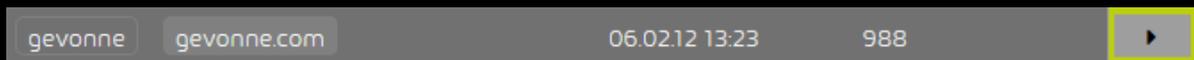


Figura 116: Abrir el menú



Se abre un menú.

6. Haga clic en **Eliminar el cliente seleccionado**.

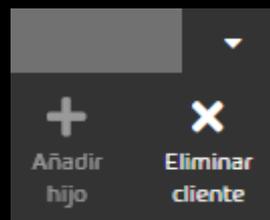


Figura 117: Eliminar cliente



Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.



Figura 118: Confirmar



El cliente se elimina.



HORNETSECURITY

Retirada tras el periodo de prueba o baja



Se ha eliminado el cliente de 365 Total Protection.

Números

- 365 Total Backup
 - configurar [14, 83](#)
- 365 Total Protection
 - actualización [25](#)
 - actualizar [25](#)
 - explicación [6](#)
 - migración de buzones, *Ver migración de buzones explicación*

A

- acceso
 - permitir ~ a servicios web de Exchange, *Ver servicios web de Exchange permitir el acceso*
- activar
 - Continuity Service [117](#)
- actualización
 - 365 Total Protection, *Ver 365 Total Protection actualización*
- actualizar
 - 365 Total Protection, *Ver 365 Total Protection actualizar*
- advertencias
 - explicación [4, 41](#)
- añadir
 - CNAME, registro [109](#)
- autenticación en dos fases, *Ver autenticación multifactor*
- autenticación multifactor [109](#)

B

- baja, *Ver retirada*
- borrar
 - conector [121](#)
- buzones de correo
 - migración [65](#)
 - migrar [73](#)
 - requisitos para la migración de buzones, *Ver migración de buzones requisitos para buzones*

C

- Canadá
 - Registros MX, *Ver Registros MX Canadá*
- cliente
 - crear [9](#)
 - eliminar [122](#)
 - incorporación, *Ver cliente crear*
- CNAME, registro
 - añadir, *Ver detección automática configurar*
- conceder
 - permisos de lectura y administración de buzones de correo en Microsoft 365, *Ver Microsoft 365 conceder permisos de lectura y administración de buzones de correo*
- conector
 - borrar [121](#)

- desactivar [121](#)
- configuración de DNS
 - configurar, *Ver registros MX* editar
- configurar
 - 365 Total Backup, *Ver 365 Total Backup* configurar
 - configuración de DNS [96](#)
 - detección automática [109](#)
- Continuity Service
 - activar [117](#)
- crear
 - cliente [9](#)
 - enlace de incorporación [8](#)
 - grupo de roles en Microsoft 365, *Ver Microsoft 365* crear grupo de roles
 - grupo de roles en servidor Exchange, *Ver migración de buzones* crear grupo de roles en servidor Exchange
- cumplimentar
 - formulario de incorporación [10](#)

D

- desactivar
 - conector [121](#)
 - filtro de spam de Microsoft 365, *Ver Microsoft 365* desactivar filtro de spam
 - limitación de servicios web de Exchange, *Ver servicios web de Exchange* desactivar limitación
- descartar
 - validación de un entorno, *Ver migración de buzones* descartar la validación de un entorno
- detección automática
 - configurar [109](#)
- documentación
 - indicaciones [4](#), [41](#)
 - símbolos [4](#), [41](#)

E

- editar
 - registros MX [96](#)
- EE.UU.
 - Registros MX, *Ver Registros MX* EE.UU.
- eliminar
 - cliente [122](#)
- enlace
 - crear, *Ver enlace de incorporación* crear
- enlace de incorporación
 - crear [8](#)
- entorno
 - validar, *Ver migración de buzones* validar entorno
- Europa
 - Registros MX, *Ver Registros MX* Europa
- Exchange Online
 - Habilitar la personalización de una organización [101](#)
- explicación
 - 365 Total Protection, *Ver 365 Total Protection* explicación
 - advertencias [4](#), [41](#)
 - indicaciones de seguridad [4](#), [41](#)
 - migración de buzones, *Ver migración de buzones* explicación

F

- filtro de spam
 - desactivar, *Ver* Microsoft 365 desactivar filtro de spam
- finalizar
 - migración de buzones, *Ver* migración de buzones finalizar
- formulario de incorporación
 - complimentar [10](#)

G

- grupo de roles
 - crear en Microsoft 365, *Ver* Microsoft 365 crear grupo de roles

H

- habilitar
 - personalización de una organización, *Ver* Exchange Online Habilitar la personalización de una organización

I

- identificación en dos fases, *Ver* autenticación multifactor
- incorporación
 - cliente, *Ver* crear cliente
- indicaciones
 - documentación [4](#), [41](#)
- indicaciones de seguridad
 - explicación [4](#), [41](#)

L

- limitaciones
 - migración de buzones, *Ver* migración de buzones limitaciones

M

- Microsoft 365
 - conceder permisos de lectura y administración de buzones de correo [57](#)
 - crear grupo de roles [53](#)
 - desactivar filtro de spam [102](#)
- migración
 - buzones de correo [65](#)
- migración de buzones
 - crear grupo de roles en servidor Exchange [48](#)
 - descartar la validación de un entorno [71](#)
 - ejecución, *Ver* buzones de correo migración
 - explicación [43](#)
 - finalizar [82](#)
 - limitaciones [45](#)
 - requisitos [46](#)
 - requisitos para buzones [47](#)
 - validar entorno [66](#)
- migrar
 - buzones de correo, *Ver* buzones de correo migrar

modificar
SPF, registro [107](#)

P

permisos
conceder ~ de lectura y administración de buzones de correo en Microsoft 365, *Ver* Microsoft 365 conceder permisos de lectura y administración de buzones de correo

permitir
acceso a servicios web de Exchange, *Ver* servicios web de Exchange permitir el acceso

personalización de una organización
habilitar, *Ver* Exchange Online Habilitar la personalización de una organización

R

registros MX
editar [96](#)

Registros MX
Canadá [99](#)
EE.UU. [98](#)
Europa [98](#)

requisitos
buzones para la migración de buzones, *Ver* migración de buzones requisitos para buzones
migración de buzones, *Ver* migración de buzones requisitos

retirada [121](#)

S

servicios web de Exchange
desactivar limitación [63](#)
permitir el acceso [60](#)

servidor Exchange
crear grupo de roles, *Ver* migración de buzones crear grupo de roles en servidor Exchange

símbolos
documentación [4](#), [41](#)

SPF, registro
modificar [107](#)

V

validar
descartar, *Ver* migración de buzones descartar la validación de un entorno
entorno, *Ver* migración de buzones validar entorno

verificación en dos pasos, *Ver* autenticación multifactor



HORNETSECURITY

Hornetsecurity GmbH
Am Listholze 78 | 30177 Hannover | Germany
Phone:+49 511 515 464-0 | info@hornetsecurity.com
www.hornetsecurity.com