Manual de configuración segura

Outlook empresarial

Desde el **Centro de Protección Digital SURA** queremos acompañarte para que tu experiencia en el entorno digital sea confiable y tranquila. Para ello es necesario que con cada paso que des, tu información se encuentre siempre protegida. Por eso, te invitamos a leer y poner en práctica las siguientes recomendaciones para la configuración segura de tus cuentas de correo en Outlook.

Nota: *las instrucciones que encontrarás a continuación están diseñadas para realizarlas en los sitios web de las aplicaciones, es decir, desde un computador. Esto se debe a que la configuración de seguridad de las aplicaciones desde la versión móvil varía según el tipo de celular. Al realizar la configuración desde la web, esta quedará aplicada en tu cuenta para tus dispositivos personales.*

Contenido

Riesgos asociados a la falta de configuración de seguridad

La importancia de configurar de forma segura tu cuenta de Outlook radica en que puedas estar más protegido frente a los siguientes riesgos:

- Suplantación de identidad en correos electrónicos que tenga un impacto en la reputación de la empresa o dé pie al robo de posibles negocios.
- Robo de información asociada a tus clientes, que se encuentren en correos o en tus sistemas de gestión de clientes asociados con Outlook empresarial.
- Robo de información de tus empleados con cuentas en Outlook.

Configuración de seguridad

A la hora de poner a punto una plataforma de correo empresarial como la de Outlook, enmarcado en Office 365, debes tener en cuenta la seguridad como punto de partida, pues es uno de los frentes más utilizados por los cibercriminales a la hora de intentar entrar a una organización.

Por eso te presentamos una lista de 10 recomendaciones a la hora de configurar de forma segura tu plataforma.

1 Configurar autenticación multifactor

Usar autenticación multifactor es una de las maneras más fáciles y efectivas de incrementar la seguridad de tu organización. La autenticación multifactor hace que, por medio de un código desde tu teléfono o simplemente haciendo clic en un botón de autorización en el mismo, se dé acceso a la plataforma de correo Outlook/Office 365. Esto puede prevenir el acceso de ciberdelincuentes a las cuentas, incluso si estos conocen las contraseñas. El multifactor también es llamado verificación de 2 pasos.

En la configuración de la plataforma de tu organización agrega una opción en la que se requiera que los usuarios inicien sesión usando la autenticación multifactor. Cuando realices este cambio, la plataforma le pedirá a los usuarios que configuren su teléfono para la autenticación de dos factores la próxima vez que inicien sesión.

Para activar la autenticación multifactor, se debe activar los valores predeterminados de seguridad:

- Inicie sesión en el **Centro de administración de Microsoft 365** con credenciales de administrador global.
- En la barra de navegación izquierda, elija **Mostrar todo** y, en **Centros de administración** , elija **Azure Active Directory**.
- En el **centro de administración de Azure Active Directory**, elija **Azure Active Directory** > **Propiedades**.
- En la parte inferior de la página, elija **Administrar valores predeterminados de seguridad.**
- Elija **Sí** para habilitar los valores predeterminados de seguridad o **No** para deshabilitarlos y luego elija **Guardar**

Conoce más sobre la configuración de doble factor: **Clic aquí**

2 Entrenamiento a usuarios

Además de los controles anteriormente mencionados, es esencial fomentar una cultura de ciberseguridad en los usuarios, para evitar ataques y otros riesgos asociados. Por eso, te recomendamos llevar a cabo una iniciativa de sensibilización y cultura en ciberseguridad enfocada en:

- Contraseñas seguras y protección de las mismas
- Protección de dispositivos
- Precauciones con información confidencial
- Protección frente a estafas por correo

Ten en cuenta las siguientes recomendaciones: **Clic aquí**

3 Cuentas administrativas dedicadas exclusivamente a la administración

Al momento de realizar las configuraciones de seguridad para tu organización, es indispensable el uso de una cuenta administradora. Es aconsejable utilizarla única y exclusivamente para dichas tareas y por ningún motivo debería, por ejemplo, recibir correos de clientes o manejar operaciones diferentes a la de administración del Outlook.

Ten en cuenta que los ciberdelincuentes buscarán la forma de entrar a tu organización y si logran tener acceso a la cuenta administradora, estarás en mayor riesgo. En ese orden de ideas, debes proteger dicha cuenta especialmente. Para lograrlo, asegúrate de que:

- La cuenta administradora cuente con múltiple factor de autenticación.
- Antes de utilizar cuentas administradoras, hayas cerrado la sesión de los sitios en tu navegador que no estén relacionados con dicha gestión, por ejemplo: Whatsapp, Facebook, entre otros.
- Haber cerrado bien la sesión de administrador luego de terminar las tareas administrativas y antes de navegar hacia sitios diferentes a la administración.

4 Elevar el nivel de protección contra malware

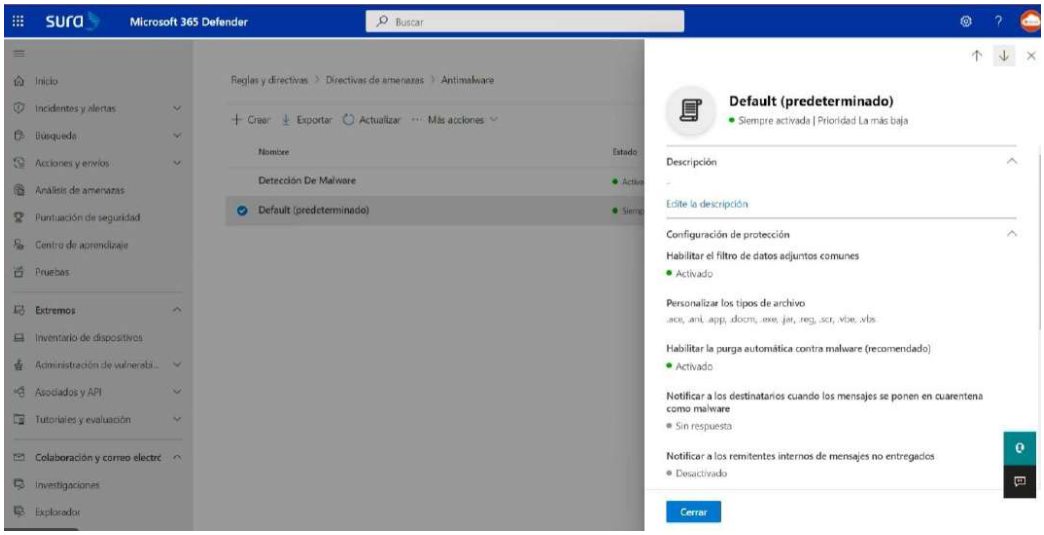
Como medida preventiva, Outlook viene configurado para protegerte contra algunos tipos de malware. Sin embargo, también es posible elevar este nivel de protección al bloquear los archivos adjuntos que te envíen con aquellas extensiones que son utilizadas frecuentemente para infectar los equipos de tu compañía (.exe, .ps1, .bat, entre otros).

Para habilitar dicha protección, completa los siguientes pasos:

- En el centro de administración de Microsoft 365 ingresar a la opción del panel izquierdo en el menú de centros de administración en la opción de **seguridad** al portal de **Microsoft 365 Defender** , vaya a **Colaboración y correo electrónico** > **Reglas y directivas** >**Directivas de amenazas**> **Protección Antimalware**.

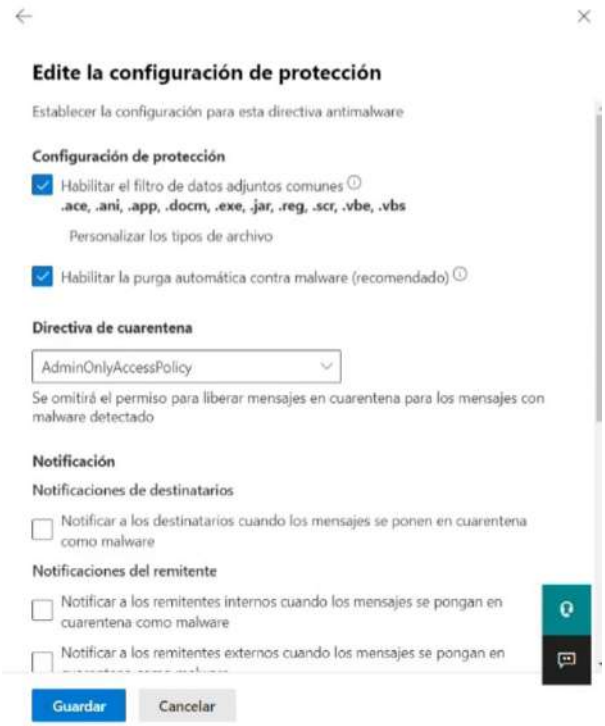
- En la página **Antimalware**, haga doble clic en **Predeterminado o Default**.

- Luego de esto, selecciona **Editar configuración de protección** en la parte inferior del menú.



- En la página siguiente, en **Configuración de protección**, selecciona la casilla de verificación junto a **Habilitar el filtro de archivos adjuntos comunes**. Los tipos de archivos que están bloqueados se enumeran directamente debajo de esta opción. Para agregar o eliminar tipos de archivos, selecciona **Personalizar tipos de archivos** al final de la lista.

- Guarda la configuración.



5 Protégete del secuestro de información o *ransomware*

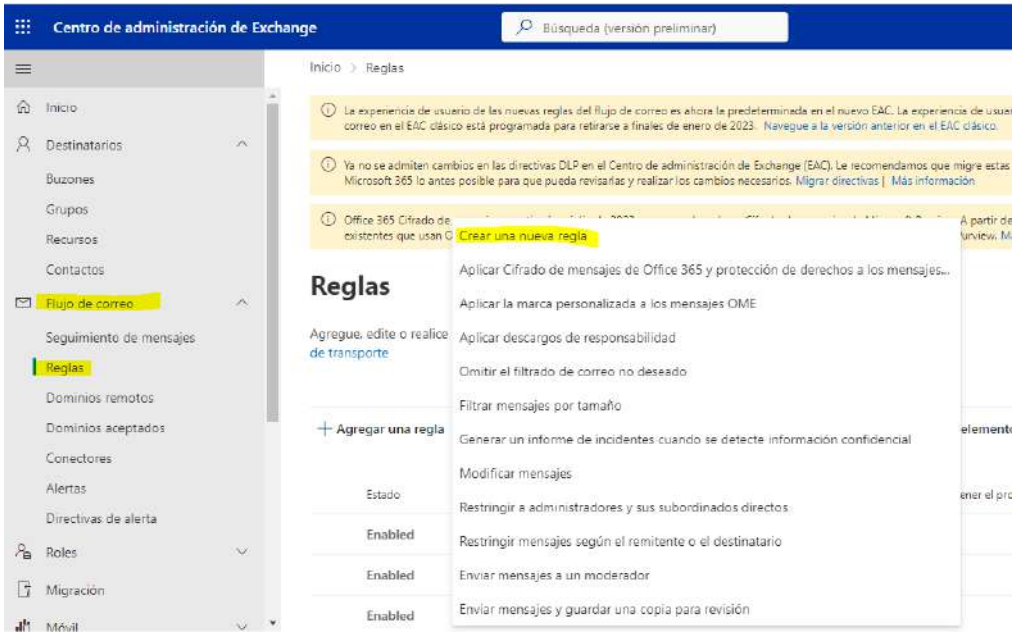
Outlook te permite protegerte frente al secuestro de información por medio de bloqueo de adjuntos. De igual forma, avisa a tus empleados sobre la amenaza en caso de que reciban el correo. Te recomendamos dos opciones como punto de partida:

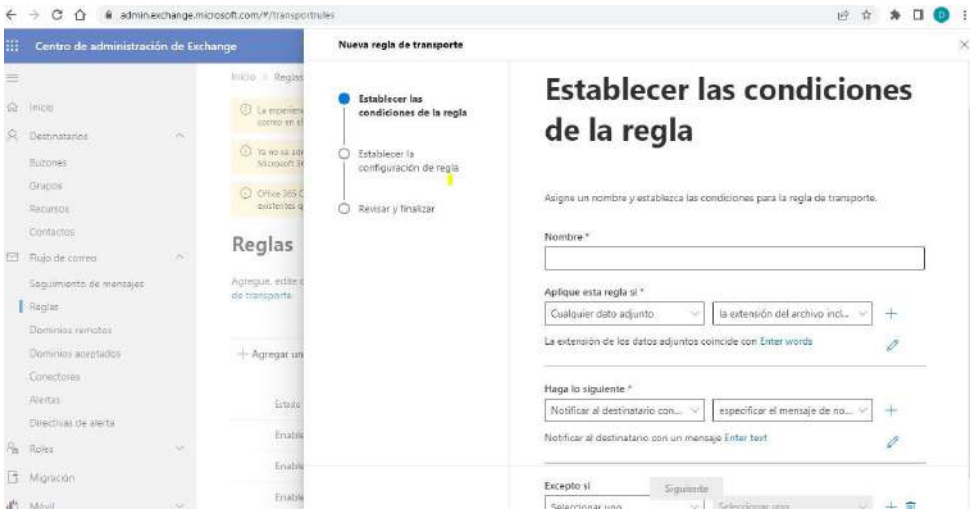
a. Alerta automáticamente a tus empleados cuando reciban un archivo Office sobre los riesgos que pueden tener, de manera que no vayan a abrir archivos enviados por personas desconocidas.

b. Bloquea extensiones comunes utilizadas por programas de secuestro de información Para hacerlo adecuadamente, sigue estas recomendaciones:

- Ve a **Exchange Admin Center(Centro de administración de Exchange)**

- En la categoría **Flujo de correo**, selecciona **Reglas,** luego **+** y **Crear nueva regla.**





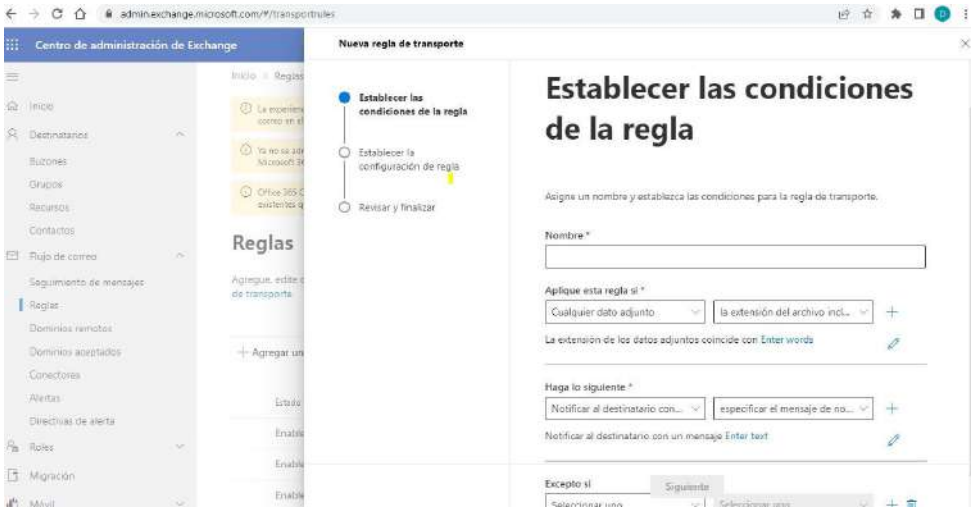
Configuración	Alerta a usuarios sobre los riesgos de abrir archivos de baja confianza	Bloquea extensiones más comunes para ransomware
Nombre	Regla anti-ransomware: Alertar usuarios	Anti-ransomware rule: bloquear extensiones
Aplicar esta regla si	Cualquier archivo. Archivos que marquen la extensión.	Cualquier archivo. Archivos que marquen la extensión.
Especificar palabras o frases	Aplicar a las siguientes extensiones: dotm, docm, xlsm, sltm, xla, xlam, xll, pptm, potm, ppam, ppsm, sldm	Aplicar a las siguientes extensiones: ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif
Hacer lo siguiente	Notificar al destinatario con un mensaje	Bloquea el correo. Rechaza el correo y añade una explicación.
Mensaje al destinatario	No abras este tipo de archivos, a menos de que los estés esperando. Pueden traer contenido malicioso y robar tu información	

6 Evitar el reenvío automático de correo

Es común que una cuenta que haya sido intervenida por un atacante posea redirección de correo a la cuenta del ciberdelincuente. Desde Outlook te puedes proteger frente a este hecho, evitando que se reenvíe automáticamente correo a cuentas fuera de tu organización.

Para hacerlo, completa los siguientes pasos:

a. Ve a **Exchange admin center(Centro de administración de Exchange)**
b. En la categoría **Flujo de correo**, selecciona **Reglas**, luego **+** y Crear nueva regla.
c. Selecciona **Más opciones** en la parte inferior del cuadro de diálogo para ver el conjunto completo de opciones.
d. Aplica las configuraciones presentes en la tabla a continuación y guarda los cambios.



Configuración	Prevenir reenvíos de correo
Nombre	Impedir el reenvío de correo a cuentas por fuera de tu dominio
Aplicar esta regla sí	El remitente . . . es externo/interno . . . Al interior de la organización
Adicionar mensaje	El reenvío de correos al exterior de la organización está prohibido por razones de seguridad.

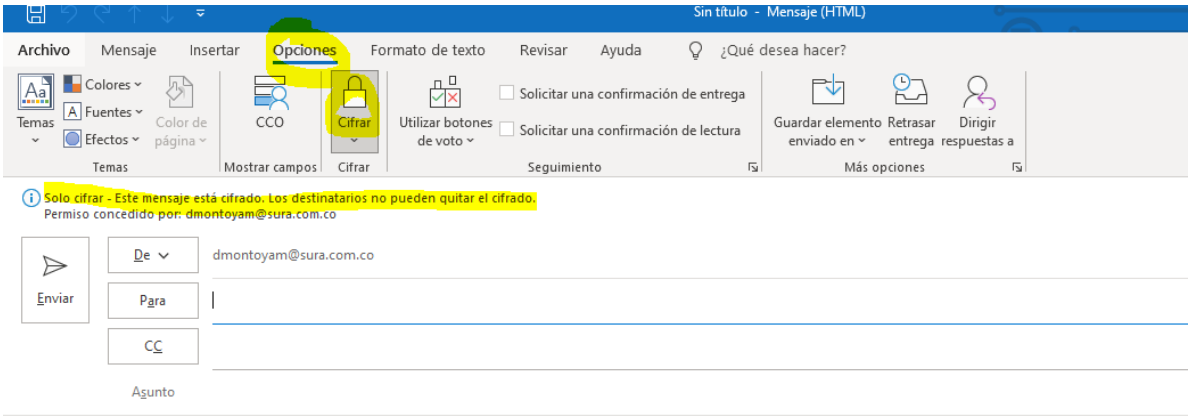
7 Utilizar el cifrado de mensajes de Outlook

El cifrado de mensajes de correo te permitirá garantizar que solo los destinatarios especificados podrán visualizar tus mensajes, lo que garantiza la confidencialidad de los mismos, evitando que terceros puedan visualizar la información que no va dirigida a ellos.

Para enviar un correo protegido por cifrado:

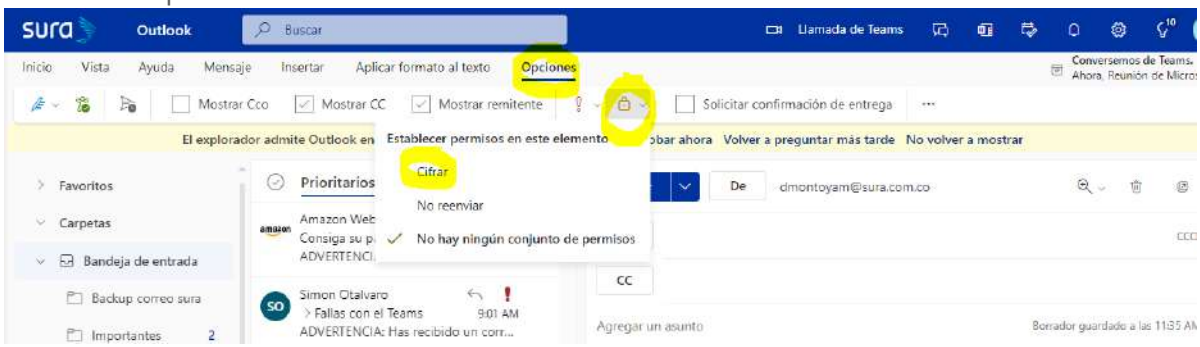
a. En Outlook para PC:

- Selecciona la opción de **Nuevo Correo Electrónico**
- Selecciona **Opciones**
- Habilita la opción de **Cifrar**



b. En Outlook web:

- Selecciona la opción de Nuevo Correo Electrónico
- Habilita la opción de **Cifrar**



8 Protege tu correo frente a ataques de *phishing*

Para protegerte frente a amenazas persistentes que tengan como foco a tu organización, lleva a cabo los siguientes pasos.

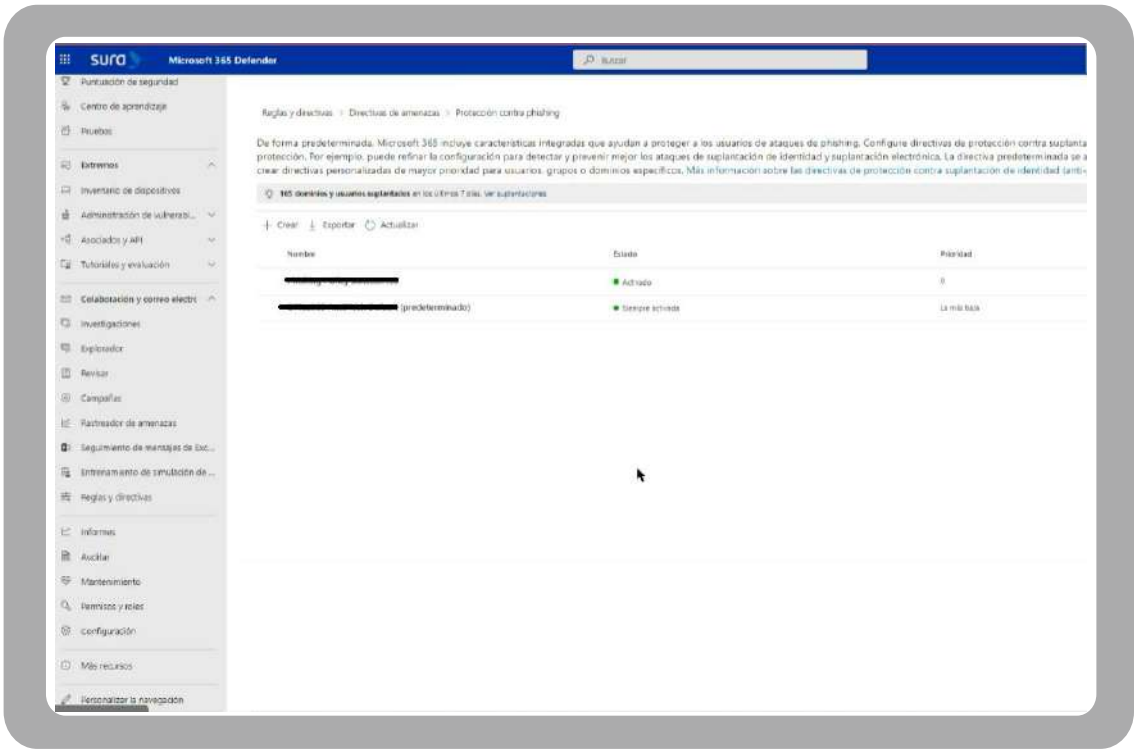
a. Ingresa con tu cuenta administradora al centro de administración de Microsoft 365 ingresar a la opción del panel izquierdo en el menú de centros de administración en la opción de **seguridad** al portal de **Microsoft 365 Defender**

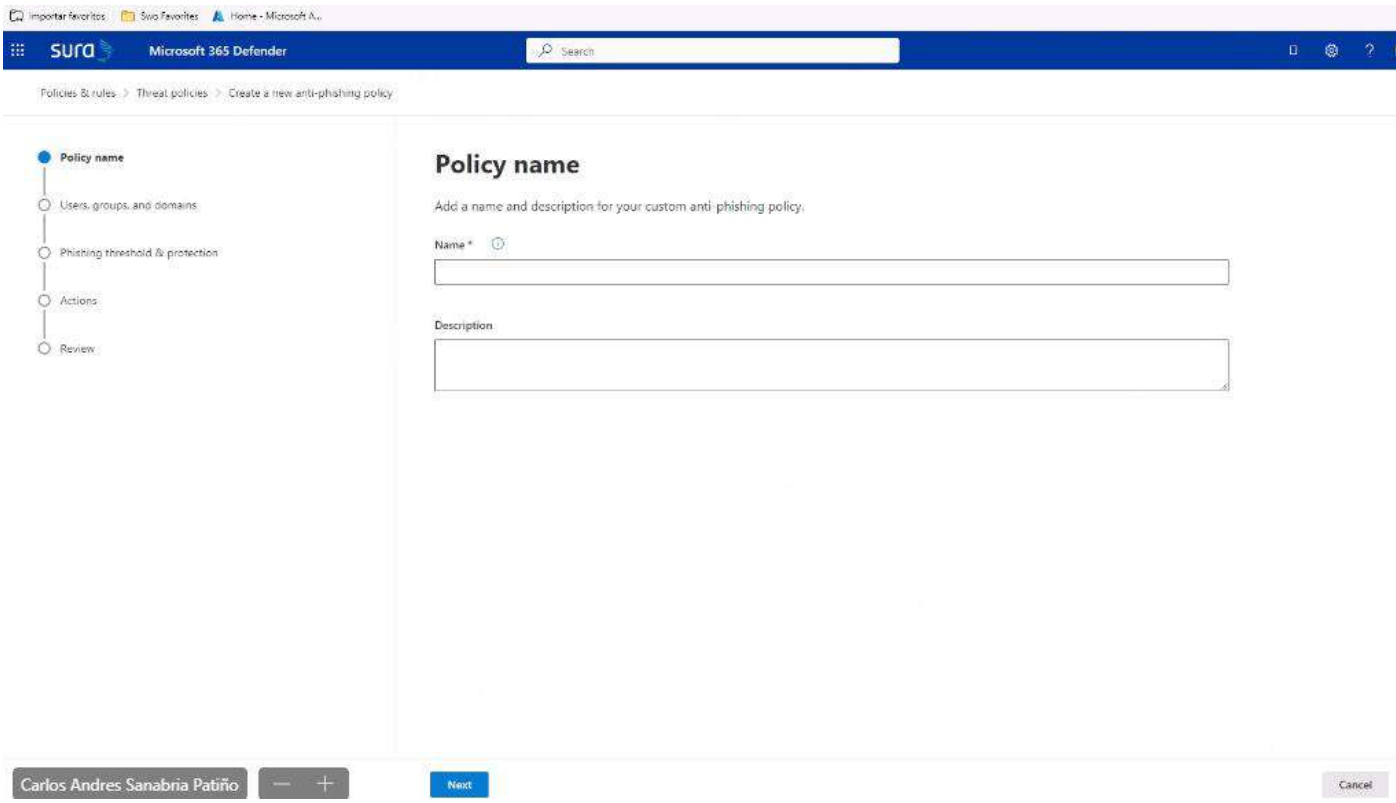
b. Dirigite a **Colaboración y correo electrónico** > **Reglas y directivas** > **Directivas de Amenazas** > **Protección contra Phishing.**

c. En el menú de **Protección contra Phishing**, selecciona **+** y **Crear.**

d. Especifica el nombre, la descripción y las configuraciones para tus políticas, de acuerdo con lo recomendado en la tabla que te presentamos a continuación.

e. Guarda los cambios.





Opciones	Configuraciones recomendadas
Nombre	Dominios y empleados de alto perfil.
Descripción	Asegura a empleados de alto perfil y a tus dominios de no ser suplantados.
Adiciona usuarios a proteger	Indica el nombre de usuario o los correos de los empleados a proteger de suplantación. Puedes adicionar hasta 20 direcciones de correo internas y externas.
Adiciona dominios a proteger	Ingresa el dominio asociado a tu suscripción de Outlook. Puedes adicionar más de un dominio.

Selecciona acciones	Si el correo es enviado por un suplantador: puedes redireccionar dicho correo a la cuenta de correo del administrador de seguridad. Si el correo es enviado desde un dominio de suplantación: puedes poner en cuarentena el mensaje.
Inteligencia	Al comenzar esta nueva política antiphishing se habilita el módulo de inteligencia de correo. Deja esta casilla activada para mejores resultados.

9 Protégete frente a adjuntos maliciosos

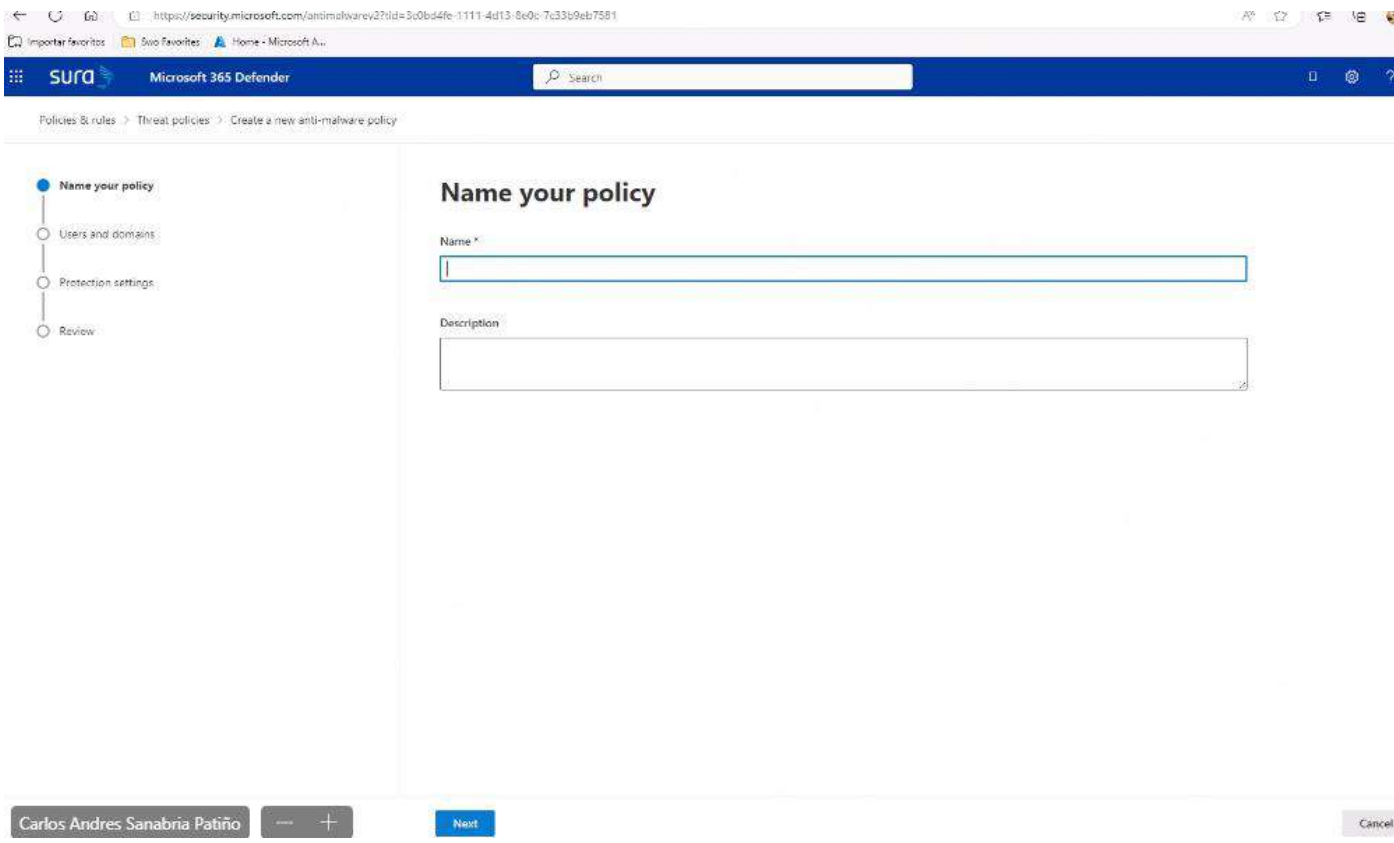
Te permitirá protegerte de archivos maliciosos que envíen a tu correo. Esto gracias a que, si activas esta funcionalidad, Outlook analizará los adjuntos en busca de virus y bloqueará aquellos que encuentre como maliciosos. Para activarla, completa estos pasos:

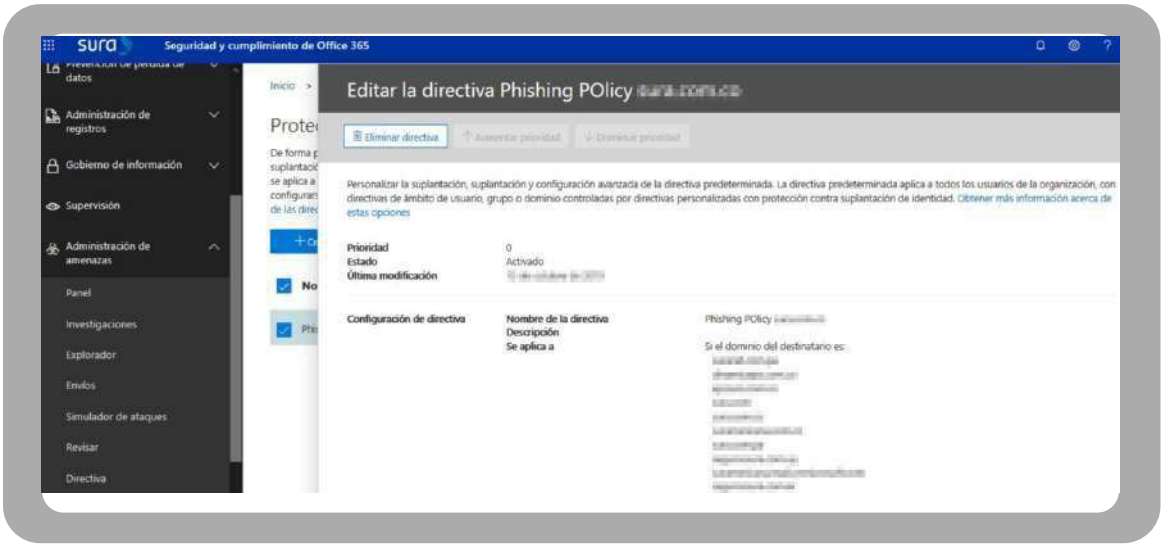
a. Ingresa con tu cuenta administradora al centro de administración de Microsoft 365 ingresar a la opción del panel izquierdo en el menú de centros de administración en la opción de **seguridad** al portal de **Microsoft 365 Defender.**

b. Una vez en el Centro de seguridad y dirígete **Colaboración y correo electrónico** > **Reglas y directivas** > **Directivas de amenazas** > **Protección Antimalware.**

c. Selecciona **+** para **crear** una nueva política y aplica las configuraciones descritas en la siguiente tabla.

d. Guarda la configuración.





Opciones	Configuraciones recomendadas
Nombre	Bloquear los correos actuales y futuros con adjuntos con malware detectado
Descripción	Bloquear los correos actuales y futuros con adjuntos con malware detectado

Guardar adjuntos con respuesta a malware desconocida	Seleccionar bloqueo – Bloquear los correos actuales y futuros con adjuntos con malware detectado.
Redirigir adjunto al momento de la detección	Habilitar esta opción si el escaneo de malware para archivos en está presentando problemas e indica el correo del administrador para la redirección de los correos maliciosos.
Aplicar a	El dominio del destinatario es ... Selecciona tu dominio

10 Protégete frente a ataques de phishing con enlaces seguros

Es probable que a tu empresa lleguen correos maliciosos con presentación de entidades financieras o instituciones importantes. Por eso es importante que no solo te protejas de las suplantaciones que puedan hacer a tus dominios, sino también de los otros mencionados.

Para crear una nueva directiva:

a. Ingresa con tu cuenta administradora al centro de administración de Microsoft 365 ingresar a la opción del panel izquierdo en el menú de centros de administración en la opción de **seguridad** al portal de **Microsoft 365 Defender**

b. Una vez en el Centro de seguridad y dirígete **Colaboración y correo electrónico** > **Reglas y directivas** > **Directivas de amenazas** > **Protección Antimalware**

c. Selecciona **+** para **crear** una nueva política y aplica las configuraciones descritas en la siguiente tabla.

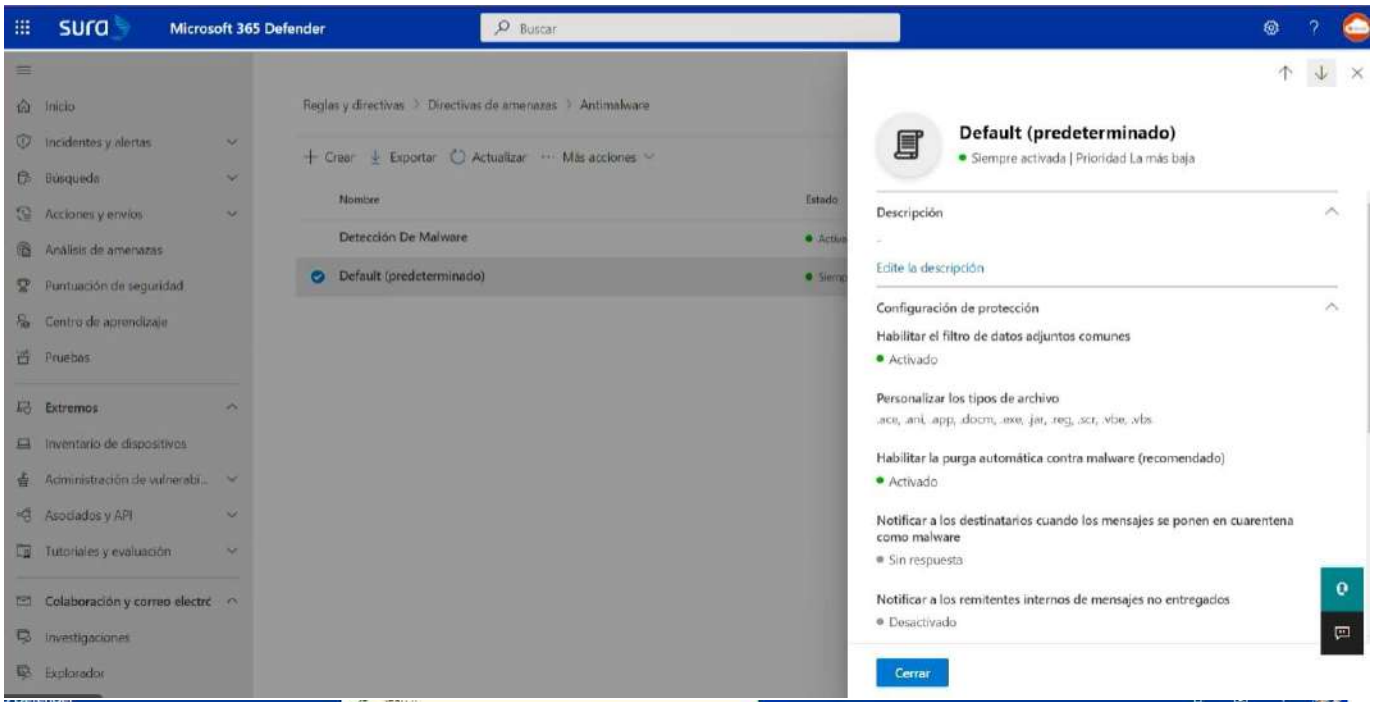
d. Guarda la configuración.

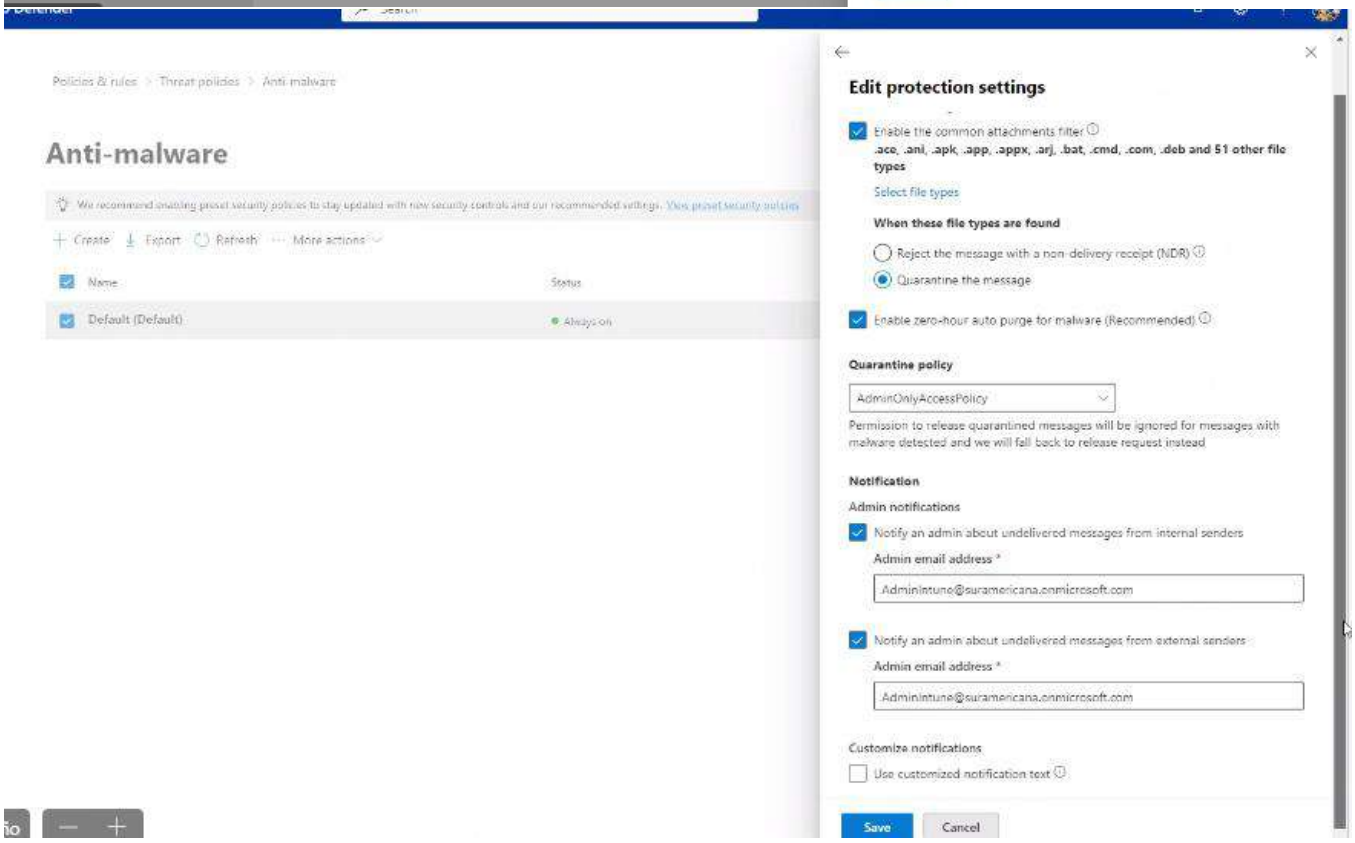
Para modificar la directiva predeterminada

a. Haz doble clic en la directiva **predeterminada**. Aparece un control flotante.

b. Selecciona **Editar configuración de protección** en la parte inferior del menú flotante.

c. Después de modificar la política predeterminada, selecciona **Guardar**.





Para esto completa los siguientes pasos:	
Opciones	**Configuraciones recomendadas**
Nombre	Links seguros para todos los destinatarios en el dominios
Seleccionar la acción para los vínculos potencialmente maliciosos en los mensajes	Selecciona este ítem. Las URLs serán reescritas y validadas frente a una lista de links maliciosos cuando el usuario da click en el link
Utilizar la funcionalidad Adjuntos Seguros para escanear el contenido descargable	Seleccionar este item
Aplicar a	El dominio del destinatario es . . . Selecciona tu dominio

Nota: Basado en el artículo Las 10 mejores formas de proteger los planes de Office 365 y Microsoft 365 Business [1]

Al momento de gestionar Outlook empresarial con tu celular, puedes hacerlo desde las apps que Outlook ha destinado para ello, las cuales son -de forma más representativa- Microsoft 365 Admin y Microsoft Outlook. Al momento de descargarlas en el móvil, hazlo desde tiendas oficiales como App Store, Google Play o Galaxy Store. Esto es de gran importancia para que evites descargar softwares maliciosos que desde otras tiendas pudieran agregarse a estas apps.

Algunas recomendaciones generales:

- Procura mantener tus credenciales sin compartir con algún empleado u otra persona.
- Cuando accedas a la gestión de tu Outlook empresarial, hazlo desde redes de confianza como la de tu casa o la de tu celular. Evita el uso de redes públicas de centros comerciales o parques. •

Mantén actualizada la aplicación de Outlook, de manera que personas malintencionadas no puedan aprovecharse de las brechas de seguridad en versiones desactualizadas.

Bibliografía

[1] © Microsoft 2022, «Top 10 ways to secure Office 365 and Microsoft 365 Business plans,» 03 01 2022. [En línea]. Available: https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/secure-your-business-data?view=o365worldwide#encryption. [Último acceso: 01/03/2022].

Centro de Protección Digital SURA

SURA, conectado con tu seguridad para que no te desconectes.

Conoce más aquí