

2025-07-21



HORNETSECURITY

SECURITY AWARENESS SERVICE

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Contents

Convenciones lingüísticas y símbolos en la documentación.....	5
Acerca de Security Awareness Service.....	7
Employee Security Index (ESI [®]).....	8
Preparativos para sistemas.....	9
Incorporación genérica.....	10
Añadir clientes de Microsoft 365 a Control Panel.....	11
Transmitir datos de un inquilino de Microsoft 365 a Control Panel.....	12
Crear un enlace para la incorporación genérica.....	15
Autorizaciones para el envío de correos de phishing simulados.....	17
Dominios de envío del simulacro de phishing.....	19
Configuración en Microsoft 365.....	27
Configurar automáticamente Microsoft 365.....	28
Configurar la entrega avanzada en Microsoft 365 Defender.....	31
Reglas de transporte para Security Awareness Service.....	34
Crear una directiva de vínculos seguros.....	64
Solución de problemas: Desactivar el botón de informe de Microsoft.....	71
Configuración de clientes.....	73
Crear excepciones para enlaces de phishing y páginas de aterrizaje para clientes en Microsoft Defender.....	73
Crear excepciones para enlaces de phishing y páginas de aterrizaje mediante la distribución de grupos.....	75
Activación de Security Awareness Service.....	77
Activar Security Awareness Service.....	77
Activar o desactivar el simulacro de phishing.....	79
Activar o desactivar los tutoriales.....	82
Anuncio interno de Security Awareness Service.....	85
Características de los correos de phishing simulado.....	88
Buscar correos de phishing simulado en Microsoft 365.....	89

Estadística.....	93
Filtro de grupos.....	95
Filtrar por grupos.....	95
Crear una configuración de filtro.....	97
Cargar una configuración de filtro.....	98
Eliminar una configuración de filtro.....	99
Seleccionar el periodo de visualización.....	100
Exportar estadísticas en formato CSV.....	102
Estadísticas del ESI [®]	104
Employee Security Index.....	104
Cronología del Employee Security Index.....	106
Estadísticas del simulacro de phishing.....	107
Ataques simulados.....	108
Correos de phishing con éxito.....	109
Niveles de usuarios.....	110
Niveles del simulacro de phishing.....	111
Correos marcados.....	113
Trucos psicológicos.....	113
Interacción con el Teachable Moment.....	115
Estadísticas de formación.....	116
Progreso de formación.....	116
Evolución de los usuarios en Single User Booster y Productivity Booster.....	117
Estado de formación de módulos y usuarios.....	118
Estadísticas de grupos.....	119
Programar informes mensuales automatizados.....	124
 Configuración.....	 127
Añadir grupos.....	127
Eliminar un grupo.....	130
Modificar prioridades de grupos.....	131
Añadir cargos.....	133
Sincronizar puestos e idiomas para Security Awareness Service.....	135
Códigos de idioma y puestos para la sincronización.....	137
Excluir un usuario.....	141
Filtrar usuarios excluidos.....	145
Eliminar usuarios de la lista de usuarios excluidos.....	146
Configurar el simulacro de phishing.....	148
Añadir información sobre su organización.....	155
Configurar el simulacro de suplantación de identidad.....	158

Modo de privacidad.....	160
Configuración de la infraestructura.....	160
Convenciones lingüísticas y símbolos en la documentación.....	173
Phishing Reporter.....	174
Marcado de correos sin complementos.....	197
Configurar los tutoriales.....	200
Awareness Engine.....	206
Programar tutoriales sin Awareness Engine.....	206
Supervisión.....	211
Usuarios excluidos automáticamente.....	211
Reincluir a un usuario.....	212
Reincluir a varios usuarios.....	213
Reincluir a todos los usuarios.....	216
Excluir a un usuario.....	217
Excluir a varios usuarios.....	219
Excluir a todos los usuarios.....	220
Mostrar el registro.....	222
Certificados.....	223
Certificado de cliente.....	223
Solicitar certificado de cliente.....	224
Certificado de usuario.....	224
Index.....	226



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	DESCRIPCIÓN	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	DESCRIPCIÓN	EXPLICACIÓN
	NOTA	Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores.
	CONSEJO	Indicación sobre opciones de configuración.



SÍMBOLO	DESCRIPCIÓN	EXPLICACIÓN
	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.
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.



Acerca de Security Awareness Service

El servicio Security Awareness Service permite formar a los usuarios de una organización en temas de seguridad informática mediante tutoriales y correos de phishing simulados sin que los administradores ni directores de seguridad de la información tengan que ser expertos en psicología y didáctica. El objetivo es que los usuarios detecten con precisión los ciberataques y puedan protegerse eficazmente contra ellos.

El servicio se basa en un procedimiento patentado de medición de la conducta de seguridad de todos los usuarios y grupos individuales. En base a las mediciones se calculan un índice científico denominado Employee Security Index (abreviado como ESI[®]) (véase [Employee Security Index \(ESI®\)](#) en la página 8) así como el KPI de formación (véase [Progreso de formación](#) en la página 116).

Los usuarios de la organización reciben tanta formación como sea preciso. La asignación de tutoriales y la simulación de ataques de phishing se automatizan mediante el Awareness Engine (véase [Awareness Engine](#) en la página 206) y el Spear Phishing Engine. El Awareness Engine es la piedra angular del servicio. Evalúa periódicamente la conducta de seguridad de los usuarios y, en base a esta evaluación, decide qué usuarios han de recibir tutoriales o correos de phishing simulados adicionales. Así, cada usuario obtiene tanta formación como sea necesaria para alcanzar un nivel de seguridad elevado. Este sistema permite también reducir la intensidad de la formación de usuarios que ya muestren una conducta de seguridad muy correcta. De este modo aumenta la productividad de estos usuarios, que ya no tienen que perder el tiempo con formación innecesaria. Sin embargo, los administradores también pueden administrar los tutoriales y asignarlos manualmente (véase [Programar tutoriales sin Awareness Engine](#) en la página 206). Para ello, los administradores deben desactivar antes el Awareness Engine (véase [Configurar los tutoriales](#) en la página 200).

Cada usuario obtiene acceso a su propio User Panel (véase [Acerca de User Panel](#)). Desde ahí, los usuarios pueden acceder a sus tutoriales (véase [#unique_8](#)). Los tutoriales pendientes se les recuerdan periódicamente a los usuarios por correo electrónico. Además, los usuarios pueden ver qué correos de phishing simulados han rechazado y cuáles les han hecho picar.



Employee Security Index (ESI®)

El Employee Security Index (ESI®) es un índice de concienciación de seguridad que permite medir lo concienciados que están los usuarios de un cliente respecto a la seguridad informática. El ESI® se determina durante la participación del cliente en Security Awareness Service.

El ESI® se basa en un marco estándar que tiene en cuenta diversos tipos de atacante simulando muchos ataques distintos con tiempos de preparación distintos.

Para poder evaluar la conducta de seguridad de los usuarios es preciso realizar una gran cantidad de simulacros de ataque distintos. Los resultados de estos ataques se resumen en el ESI®.



Nota:

Con el modo de privacidad activado (véase [Modo de privacidad](#) en la página 160), el ESI® solo puede determinarse para la organización completa o para grupos de al menos 10 usuarios.



Preparativos para sistemas

Para que un cliente pueda emplear Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) y sea posible enviar sin problemas correos de phishing simulados a los usuarios, es preciso realizar algunos preparativos.

Requisitos en Control Panel

En Control Panel deben cumplirse los siguientes requisitos:

- El cliente debe crearse en Control Panel (véase [Crear nuevos clientes o partners subordinados](#)). Como alternativa, los clientes con Microsoft 365 pueden sincronizar su inquilino de Microsoft 365 con Control Panel sin utilizar el servicio 365 Total Protection (véase [Incorporación genérica](#) en la página 10).
- Si los buzones de correo del cliente no se sincronizan con Microsoft 365 o un servicio de directorio mediante LDAP, los buzones de correo deben crearse manualmente en Control Panel o importarse desde un archivo CSV (véase [Buzones de correo](#)).

Requisitos para el envío de correos de phishing simulados

**Nota:**

Para poder utilizar todas las funciones de Security Awareness Service y Spear-Phishing-Engine, es necesario que al menos el 60 por ciento de los usuarios hayan introducido un nombre y un apellido en Control Panel (véase [Editar los datos básicos de un buzón de correo](#)). Sin esta información personalizada, no se pueden aplicar algunos escenarios de phishing, lo que reduce la eficiencia del servicio.

**Nota:**

Los ajustes necesarios para clientes con Microsoft 365 se describen en el capítulo [Configuración en Microsoft 365](#) en la página 27. Dichos clientes deben impedir que se les reescriban los enlaces contenidos en correos de phishing simulado, así como asegurarse de que dichos correos puedan entregarse a pesar de contener archivos adjuntos supuestamente peligrosos.

El simulacro de phishing de Security Awareness Service sirve para evaluar la conducta de seguridad de los usuarios. Por tanto, es importante que los correos de phishing simulados



puedan llegar a los buzones de correo de los usuarios sin ser interceptados por el servidor de correo electrónico o un proveedor de seguridad.

Para hacer posible la entrega de correos de phishing simulado, el cliente debe admitir determinadas direcciones IP y rangos IP, firmas DKIM o dominios en su entorno de correo electrónico (véase [Autorizaciones para el envío de correos de phishing simulados](#) en la página 17).

**Nota:**

El método de admisión que puede elegir un cliente depende de las opciones de configuración de su entorno de correo electrónico. Como solución de preferencia, los clientes deben admitir los correos en base a las direcciones IP del destinatario o a las firmas DKIM. Estos métodos son equivalentes. Si no es posible utilizar ninguno de estos métodos, el cliente puede admitir en su lugar una serie de dominios. Sin embargo, la admisión de dominios no es más que una solución de emergencia, ya que limita la funcionalidad del simulacro de phishing.

Incorporación genérica

Con la incorporación genérica, los administradores a nivel de partner pueden crear clientes de Microsoft 365 en Control Panel sin necesidad de adquirir 365 Total Protection (véase [Acerca de 365 Total Protection](#)). Esto es especialmente útil en caso de utilizar Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7), ya que permite transferir todos los datos relevantes del inquilino de Microsoft 365 a Control Panel.

**Nota:**

Para que el estado de formación y el resumen del simulacro de phishing de los usuarios en User Panel se transfieran durante una migración desde buzones de correo de tipo LDAP, buzones creados manualmente en Control Panel o buzones creados mediante la importación CSV a Microsoft 365, las direcciones de correo electrónico principales de los usuarios deben existir en Microsoft 365. Para ello, los usuarios deben migrar a Microsoft 365 con sus direcciones de correo electrónico principales (véase [Acerca de 365 Total Protection](#)).

**Nota:**

Con la incorporación genérica, los correos del cliente creado no están protegidos mediante 365 Total Protection. Por tanto, no se muestran correos en el módulo **Email Live Tracking**.

La incorporación genérica puede ser efectuada por un partner para su cliente (véase [Añadir clientes de Microsoft 365 a Control Panel](#) en la página 11) o por el propio cliente con un enlace de incorporación enviado por el partner (véase [Crear un enlace para la incorporación genérica](#) en la página 15).

A continuación, el partner o el cliente debe cumplimentar el formulario de incorporación y conceder en Microsoft los permisos necesarios para que los datos del inquilino de Microsoft 365 se puedan transferir automáticamente a Control Panel (véase [Transmitir datos de un inquilino de Microsoft 365 a Control Panel](#) en la página 12).

Añadir clientes de Microsoft 365 a Control Panel

Si dispone de datos de acceso de administrador a su inquilino de Microsoft 365, puede añadir un nuevo cliente con Microsoft 365 a 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 el nuevo cliente.



Figura 1: Seleccionar un partner en la selección de ámbitos

3. Vaya a **365 Total Protection > 365 Total Protection**.
4. Haga clic en el botón **Incorporar un cliente** de la opción **Incorporación genérica**.



Figura 2: Seleccionar versión

i Nota:

Dependiendo de la configuración del monitor, es posible que no se muestren al mismo tiempo todas las opciones del módulo **365 Total Protection**. En tal caso, los administradores pueden visualizar la opción haciendo clic en la flecha del lado izquierdo de la página.

➔ Se muestra el formulario de incorporación.

✓ Se ha iniciado la incorporación de un nuevo cliente de Microsoft 365.

A continuación debe usted cumplimentar el formulario de incorporación y conceder los permisos necesarios en Microsoft para que los datos del inquilino de Microsoft 365 puedan transferirse automáticamente a Control Panel (véase [Transmitir datos de un inquilino de Microsoft 365 a Control Panel](#) en la página 12).

Transmitir datos de un inquilino de Microsoft 365 a Control Panel

✓ Ha abierto el formulario de incorporación para clientes de Microsoft 365 (véase [Añadir clientes de Microsoft 365 a Control Panel](#) en la página 11).

**i Nota:**

Durante la sincronización se transmiten datos sobre dominios, buzones de correo y grupos (p. ej., listas de miembros de grupos o datos básicos de los buzones de correo) pero no contenidos (p. ej., textos de correos de buzones). Los buzones de reenvío que se crearon manualmente antes de configurar la sincronización con Microsoft 365 o LDAP no serán actualizados por la sincronización. Para hacerlo, los buzones de reenvío previos deben eliminarse y configurarse de nuevo (véase el [Añadir un buzón de reenvío](#)).

1. Introduzca sus datos de contacto en el formulario de incorporación.

i Nota:

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

Figura 3: Introducir datos de contacto

2. Marque la casilla bajo **Protección de datos**.
3. Haga clic en **Iniciar ahora** para iniciar el proceso de configuración.
- ➡ Se abre la página de inicio de sesión de Microsoft.
4. Inicie sesión en Microsoft 365 con sus datos de acceso de administrador.

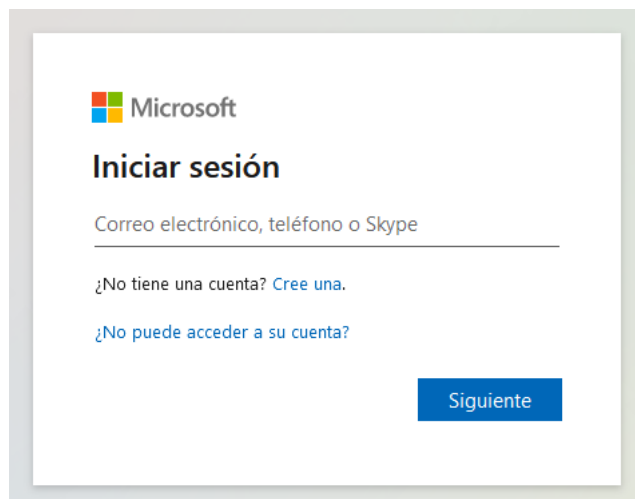


Figura 4: Introducir el nombre de usuario de Microsoft

i **Nota:**

Durante la posterior sincronización se transmiten únicamente datos sobre dominios y buzones de correo. Los contenidos (p. ej., correos de buzones de correo) no se transmiten. Tampoco se realizan cambios en la configuración de Microsoft. Los grupos de Microsoft 365 se sincronizan si un cliente ha creado manualmente grupos con los mismos nombres en Control Panel (véase [Administración de grupos en Control Panel](#)).

5. 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 del cliente se han representado 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.

Crear un enlace para la incorporación genérica

Puede crear un enlace de incorporación genérica para sus clientes de Microsoft 365. El enlace dirige a un formulario que sus clientes deben rellenar para iniciar la sincronización de buzones de correo, grupos y dominios. Puede compartir este enlace de incorporación con sus clientes para que éstos puedan efectuar por sí mismos la configuración de nuestros servicios (véase [Transmitir datos de un inquilino de Microsoft 365 a Control Panel](#) en la página 12). 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. Haga clic en el botón  de la opción .



Figura 6: Seleccionar versión

 Nota:

Dependiendo de la configuración del monitor, es posible que no se muestren al mismo tiempo todas las opciones del módulo **365 Total Protection**. En tal caso, los administradores pueden visualizar la opción haciendo clic en la flecha del lado izquierdo de la página.

 Se crea un enlace unívoco y se copia en el portapapeles.

 Se ha creado un enlace de incorporación genérica.



Autorizaciones para el envío de correos de phishing simulados

**Nota:**

Este capítulo está dirigido a clientes sin Microsoft 365 y contiene información sobre cómo admitir correos de phishing simulado independientemente del entorno de correo. Con esta información, los clientes pueden admitir correos de phishing simulado en sus entornos de correo. Los ajustes necesarios para clientes con Microsoft 365 se detallan en el capítulo [Configuración en Microsoft 365](#) en la página 27.

Para que el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) funcione correctamente, el cliente debe autorizar en su entorno de correo electrónico determinadas direcciones IP y rangos IP, firmas DKIM o dominios. De lo contrario, es posible que los sistemas de seguridad y los filtros del cliente intercepten o interactúen con los correos de phishing simulados (véase [Configuración de la infraestructura](#) en la página 160).

**Nota:**

El método de admisión que puede elegir un cliente depende de las opciones de configuración de su entorno de correo electrónico. Como solución de preferencia, los clientes deben admitir los correos en base a las direcciones IP del destinatario o a las firmas DKIM. Estos métodos son equivalentes. Si no es posible utilizar ninguno de estos métodos, el cliente puede admitir en su lugar una serie de dominios. Sin embargo, la admisión de dominios no es más que una solución de emergencia, ya que limita la funcionalidad del simulacro de phishing.

Direcciones IP y rangos IP

Los clientes deben permitir ciertas direcciones IP y ciertos rangos de direcciones IP en función de la región del cliente en su entorno de correo electrónico.

Para los clientes en Europa, se aplican las siguientes direcciones IP y rangos de direcciones IP. Las máscaras de red están indicadas entre paréntesis detrás:

- **83.246.65.0/24 (255.255.255.0)**
- **94.100.128.0/20 (255.255.240.0)**
- **185.140.204.0/22 (255.255.252.0)**



- **173.45.18.0/24 (255.255.255.0)**
- **173.124.136.160/27 (255.255.255.224)**

Para los clientes en los Estados Unidos, se aplican las siguientes direcciones IP y rangos de direcciones IP. Las máscaras de red están indicadas entre paréntesis detrás:

- **83.246.65.0/24 (255.255.255.0)**
- **94.100.128.0/20 (255.255.240.0)**
- **173.45.18.0/24 (255.255.255.0)**
- **185.140.204.0/22 (255.255.252.0)**

Para los clientes en Canadá, se aplican las siguientes direcciones IP y rangos de direcciones IP. Las máscaras de red están indicadas entre paréntesis detrás:

- **108.163.133.224 (255.255.255.224)**
- **199.27.221.64 (255.255.255.224)**
- **209.172.38.64 (255.255.255.224)**
- **216.46.2.48 (255.255.255.248)**
- **216.46.11.224 (255.255.255.224)**

**Nota:**

A los clientes que utilizan Security Awareness Service sin nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)) les bastan las direcciones IP **94.100.136.58 (255.255.255.255)** y **94.100.132.73 (255.255.255.255)**.

Admisión de firmas DKIM

Los clientes deben admitir correos con firmas DKIM de **sas.cloud-security.net** en su entorno de correo electrónico.

Autorización de dominios

Si el entorno de correo electrónico de un cliente no permite admitir determinadas direcciones IP o firmas DKIM, el cliente puede admitir dos grupos de dominios como solución de emergencia. Por una parte, el cliente puede admitir dominios desde los cuales se envían correos de phishing y, por otro, dominios a los que pertenecen enlaces incluidos en correos de phishing simulado. Dichos dominios dependen del sector de la organización del cliente.



Si un cliente necesita listas de dominios, puede generarlas en el módulo **Security Awareness Service** (véase [Generar listas de dominios permitidos](#) en la página 161). Las listas se generan individualmente para cada cliente. A continuación, las listas pueden descargarse desde el mismo módulo (véase [Descargar listas de dominios permitidos](#) en la página 166). Una vez generada una lista de dominios, en el simulacro de phishing del cliente solo se utilizan los dominios incluidos en la misma.

**IMPORTANTE:**

Dependiendo del entorno de correo electrónico del cliente, la configuración de las admisiones puede tardar algún tiempo. El cliente debe efectuar las autorizaciones antes de que empiece el simulacro de phishing, pues de lo contrario puede provocar problemas durante el simulacro de phishing. Los correos de phishing simulados comienzan a enviarse al cabo de siete días tras la activación de Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77). Si las autorizaciones no se pueden realizar hasta este momento, recomendamos que el cliente posponga la fecha de inicio del simulacro de phishing (véase [Configurar el simulacro de phishing](#) en la página 148).

**Nota:**

Los ajustes necesarios dependen del entorno de correo electrónico del cliente y, por tanto, son muy individuales. Para facilitar la configuración, proporcionamos instrucciones para filtros de correo de los proveedores de terceros más comunes (véase [Autorizaciones para Security Awareness Service en filtros de correo de terceros](#)).

Dominios de envío del simulacro de phishing

Tabla 1: Enviando dominios

Dominio de Nivel Superior (TLD)	Dominio
.at (Austria)	*.security-scanned.at/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.at (Austria)	security-scanned.at/*
.at (Austria)	*.vvien.at/*
.at (Austria)	vvien.at/*
.at (Austria)	*.download-sicherheit.at/*
.at (Austria)	download-sicherheit.at/*
.at (Austria)	*.365login.at/*
.at (Austria)	365login.at/*
.at (Austria)	*.meinesv.or.at/*
.at (Austria)	meinesv.or.at/*
.ch (Suiza)	*.ch-secure.com/*
.ch (Suiza)	ch-secure.com/*
.ch (Suiza)	*.ch-login.info/*
.ch (Suiza)	ch-login.info/*
.ch (Suiza)	*.ch-office365.cloud/*
.ch (Suiza)	ch-office365.cloud/*
.ch (Suiza)	*.ch-index.info/*
.ch (Suiza)	ch-index.info/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.ch (Suiza)	*.zuerick.ch/*
.ch (Suiza)	zuerick.ch/*
.ch (Suiza)	*.download-securise.ch/*
.ch (Suiza)	download-securise.ch/*
.ch (Suiza)	*.security-scanned.ch/*
.ch (Suiza)	security-scanned.ch/*
.ch (Suiza)	*.365login.ch/*
.ch (Suiza)	365login.ch/*
.ch (Suiza)	*.safe-browsing.ch/*
.ch (Suiza)	safe-browsing.ch/*
.cloud (General)	*.verification-portal.cloud/*
.cloud (General)	verification-portal.cloud/*
.cloud (General)	*.user-authentication.cloud/*
.cloud (General)	user-authentication.cloud/*
.cloud (General)	*.web-login.cloud/*
.cloud (General)	web-login.cloud/*
.cloud (General)	*.login-web.cloud/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.cloud (General)	login-web.cloud/*
.com (General)	*.com--login.info/*
.com (General)	com--login.info/*
.com (General)	*.corn-de.org/*
.com (General)	corn-de.org/*
.com (General)	*.com-office365.com/*
.com (General)	com-office365.com/*
.com (General)	*.com--login.com/*
.com (General)	com--login.com/*
.com (General)	*.security-scanned.com/*
.com (General)	security-scanned.com/*
.com (General)	*.com-index.cloud/*
.com (General)	com-index.cloud/*
.com (General)	*.mail-service-update.com/*
.com (General)	mail-service-update.com/*
.de (Alemania)	*.de-index.info/*
.de (Alemania)	de-index.info/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.de (Alemania)	*.safe-browsing.de/*
.de (Alemania)	safe-browsing.de/*
.de (Alemania)	*.de-files.de/*
.de (Alemania)	de-files.de/*
.de (Alemania)	*.download-sicherheit.de/*
.de (Alemania)	download-sicherheit.de/*
.de (Alemania)	*.access-365.de/*
.de (Alemania)	access-365.de/*
.de (Alemania)	*.secure-file.de/*
.de (Alemania)	secure-file.de/*
.de (Alemania)	*.info-login.de/*
.de (Alemania)	info-login.de/*
.de (Alemania)	*.secures-file.de/*
.de (Alemania)	secures-file.de/*
.de (Alemania)	*.365-access.de/*
.de (Alemania)	365-access.de/*
.eu (Europa)	*.it-index.eu/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.eu (Europa)	it-index.eu/*
.eu (Europa)	*.fr-services.eu/*
.eu (Europa)	fr-services.eu/*
.fr (Francia)	*.fr-secure.cloud/*
.fr (Francia)	fr-secure.cloud/*
.fr (Francia)	*.fr-index.info/*
.fr (Francia)	fr-index.info/*
.fr (Francia)	*.fr-services.eu/*
.fr (Francia)	fr-services.eu/*
.fr (Francia)	*.societes-anonymes.fr/*
.fr (Francia)	societes-anonymes.fr/*
.fr (Francia)	*.navigation-securisee.fr/*
.fr (Francia)	navigation-securisee.fr/*
.fr (Francia)	*.mega-telechargement.fr/*
.fr (Francia)	mega-telechargement.fr/*
.fr (Francia)	*.fr-fichiers.fr/*
.fr (Francia)	fr-fichiers.fr/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.fr (Francia)	*.securite-verifiee.fr/*
.fr (Francia)	securite-verifiee.fr/*
.fr (Francia)	*.securites-verifiee.fr/*
.fr (Francia)	securites-verifiee.fr/*
.info (General)	*.de-index.info/*
.info (General)	de-index.info/*
.info (General)	*.ch-index.info/*
.info (General)	ch-index.info/*
.info (General)	*.info-login.de/*
.info (General)	info-login.de/*
.info (General)	*.office365-login.info/*
.info (General)	office365-login.info/*
.info (General)	*.office356-login.info/*
.info (General)	office356-login.info/*
.it (Italia)	*.it-index.eu/*
.it (Italia)	it-index.eu/*
.it (Italia)	*.it-login.net/*



DOMINIO DE NIVEL SUPERIOR (TLD)	DOMINIO
.it (Italia)	it-login.net/*
.net (General)	*.it-files.net/*
.net (General)	it-files.net/*
.net (General)	*.it-login.net/*
.net (General)	it-login.net/*
.net (General)	*.it-file.net/*
.net (General)	it-file.net/*
.org (General)	*.corn-de.org/*
.org (General)	corn-de.org/*
.org (General)	*.tr-login.org/*
.org (General)	tr-login.org/*
.org (General)	*.account-access.org/*
.org (General)	account-access.org/*
.org (General)	*.service-access.org/*
.org (General)	service-access.org/*
.org (General)	*.portal-login.org/*
.org (General)	portal-login.org/*

**DOMINIO DE
NIVEL SUPERIOR
(TLD)****DOMINIO**

.org (General)	*.access-account365.org/*
.org (General)	access-account365.org/*
.tr (Turquía)	*.tr-index.com/*
.tr (Turquía)	tr-index.com/*
.tr (Turquía)	*.tr-login.org/*
.tr (Turquía)	tr-login.org/*
.com (General)	*.hornetsecurity.com/*
.com (General)	hornetsecurity.com/*

Configuración en Microsoft 365

Los clientes con Microsoft 365 deben realizar diversos ajustes en Microsoft 365 para que los usuarios puedan recibir los correos de phishing simulado de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) sin modificar.

Configuración automática

Los clientes pueden realizar automáticamente todos los ajustes necesarios mediante un interruptor de Control Panel (véase [Configurar automáticamente Microsoft 365](#) en la página 28). Durante el proceso se configura la entrega avanzada para Microsoft 365 Defender y se crean dos reglas de transporte. Estos ajustes se describen en mayor detalle en la siguiente sección.



Configuración manual

Si la configuración automática fallase, los clientes deberán realizar varios ajustes. Su objetivo es eludir diversos sistemas de seguridad de Microsoft 365 Defender.

En primer lugar, Microsoft 365 Defender emplea su mecanismo antiphishing para comprobar si los correos entrantes son correos de phishing y, en tal caso, ponerlos en cuarentena. Para impedir que los correos del simulacro de phishing se clasifiquen como auténticos correos de phishing, los clientes con Microsoft 365 Defender deben configurar la entrega avanzada (véase [Configurar la entrega avanzada en Microsoft 365 Defender](#) en la página 31).

A continuación, Microsoft 365 Defender utiliza el mecanismo "Vínculos seguros" para hacer clic en los enlaces contenidos en los correos, analizarlos y reescribirlos para prevenir ataques por esta vía. Finalmente, el mecanismo "Datos adjuntos seguros" comprueba los archivos adjuntos de los correos entrantes y pone en cuarentena aquéllos cuyos archivos adjuntos se consideren inseguros. Para evitar que los mecanismos "Vínculos seguros" y "Datos adjuntos seguros" intervengan en los correos del simulacro de phishing, los clientes deben crear dos reglas de transporte en Exchange Admin Center.

Aparte de estos dos mecanismos de seguridad, Microsoft 365 Defender Plan 2 ofrece la posibilidad de definir directivas propias para hacer frente a amenazas. Estas directivas se aplican antes del mecanismo "Vínculos seguros" y pueden contener ellas mismas reglas sobre el tratamiento de enlaces. Como no es posible eludir directivas personalizadas con las reglas de transporte ya descritas, los clientes deben crear una directiva adicional para vínculos seguros (véase [Crear una directiva de vínculos seguros](#) en la página 64) o modificar una directiva preexistente para que no se procesen los enlaces de correos del simulacro de phishing. Si un cliente tiene varias directivas para vínculos seguros, deberá ajustar la prioridad de la nueva directiva a 0 (véase [Prioridad de la directiva de vínculos seguros](#) en la página 69), para que se aplique antes que las demás.

Desactivar el botón de informe de Microsoft en Outlook

Para más detalles, véase [Solución de problemas: Desactivar el botón de informe de Microsoft](#) en la página 71.

Configurar automáticamente Microsoft 365



El cliente tiene un inquilino de Microsoft 365. Los buzones de correo del cliente se sincronizan en Control Panel con Microsoft 365 (véase [Incorporación genérica](#) en la página



10). Ha activado Security Awareness Service y el simulacro de phishing (véanse [Activar Security Awareness Service](#) en la página 77 y [Activar o desactivar el simulacro de phishing](#) en la página 79).

Para que los usuarios puedan recibir los correos de phishing simulado de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) sin modificaciones, debe usted realizar diversos ajustes en Microsoft 365. El objetivo es eludir diversos mecanismos de seguridad de Microsoft 365 para que los correos de phishing simulado no se clasifiquen como auténticos correos de phishing (véase [Configuración en Microsoft 365](#) en la página 27). Puede realizar dichos ajustes de modo automático.

**Nota:**

Como alternativa, también es posible realizar manualmente los ajustes en Microsoft 365 (véase [Configuración en Microsoft 365](#) en la página 27).

**IMPORTANTE:**

Si emplea sistemas de filtrado de correos adicionales, asegúrese de que no impidan la comprobación de la firma DKIM. Pueden comprobar si la firma DKIM es válida leyendo en el encabezado **Authentication-Results**. El encabezado debe contener el registro **dkim=pass**.

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 configurar automáticamente Microsoft 365.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. Accione el interruptor **Configuración de la infraestructura de Permitir la entrega de correos de phishing simulados en Microsoft 365**.

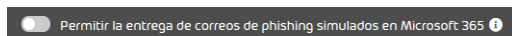


Figura 7: Configurar Microsoft 365 automáticamente

- ➔ Se muestra la página de inicio de sesión de Microsoft 365.
6. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
- ➔ Se muestra una ventana con los permisos necesarios.



7. Conceda los permisos solicitados.

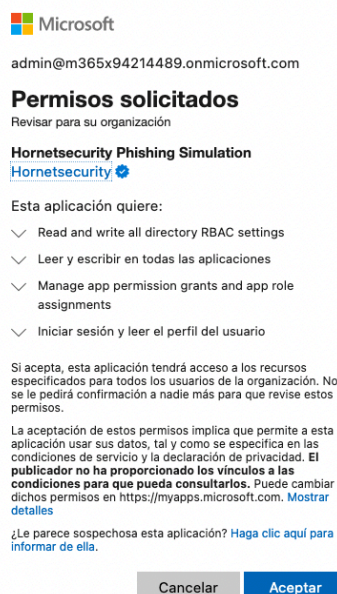


Figura 8: Conceder permisos

- ➔ Control Panel vuelve a mostrarse. Los ajustes se configuran automáticamente en Microsoft 365. En el proceso se configura la entrega avanzada de correos en Microsoft 365 Defender y se crean dos reglas de transporte que permiten eludir mecanismos de seguridad de Microsoft 365 Defender (véase [Configuración en Microsoft 365](#) en la página 27).



Nota:

La configuración de Microsoft 365 puede tardar un momento en hacerse efectiva.



Los ajustes de Microsoft 365 se han configurado automáticamente.

A continuación puede crear una directiva de vínculos seguros si emplea Microsoft 365 Defender Plan 2 y ha creado directivas para vínculos seguros (véase [Crear una directiva de vínculos seguros](#) en la página 64).



Configurar la entrega avanzada en Microsoft 365 Defender

Puede configurar la función **Entrega avanzada** en Microsoft 365 Defender para eludir su mecanismo antiphishing. De este modo impedirá que los correos de phishing simulado de Security Awareness Service se clasifiquen como auténticos correos de phishing y se pongan en cuarentena. Los siguientes ajustes permiten que la protección antiphishing de Microsoft 365 Defender admita los correos tanto en base a sus firmas DKIM como en base a las direcciones IP de sus remitentes.



IMPORTANTE:

Si emplea sistemas de filtrado de correos adicionales, asegúrese de que no impidan la comprobación de la firma DKIM. Pueden comprobar si la firma DKIM es válida leyendo en el encabezado **Authentication-Results**. El encabezado debe contener el registro **dkim=pass**.

1. Abra la página web <https://security.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
- ➔ Se abre Microsoft 365 Defender.
3. Vaya a **Reglas y directivas > Directivas de amenazas > Entrega avanzada**.
4. Seleccione la pestaña **Simulación de phishing**.
5. Haga clic en **Editar**.

Reglas y directivas > Directivas de amenazas > Entrega avanzada

Entrega avanzada

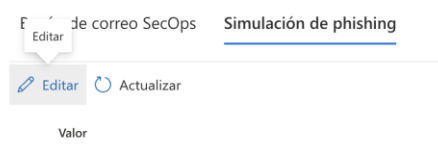


Figura 9: Editar la entrega avanzada

- ➔ Se muestra una ventana para introducir dominios de remitentes y direcciones IP.
6. Haga clic en **Dominio**.



- ➔ Se muestra un campo de introducción de datos.
7. Añada los dominios **sas.cloud-security.net** y **whitelisting.it-seal.de** uno tras otro introduciendo primero el dominio y luego haciendo clic en el dominio mostrado.

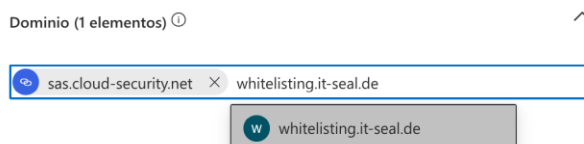


Figura 10: Añadir un dominio

- ➔ El dominio se añade como dominio de remitente.



Figura 11: Dominio añadido

8. Haga clic en **Enviando IP**.
- ➔ Se muestra un campo de introducción de datos.
9. Introduzca las siguientes direcciones IP una a una, haciendo clic en cada una de ellas después de introducirla.
- **83.246.65.0/24**
 - **94.100.128.0/20**
 - **185.140.204.0/22**
 - **173.45.18.0/24**
 - **173.124.136.160/27**

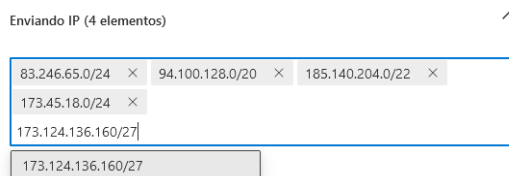


Figura 12: Añadir dirección IP

**Nota:**

A los clientes que utilizan Security Awareness Service sin nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)) les bastan las direcciones IP **94.100.136.58 (255.255.255.255)** y **94.100.132.73 (255.255.255.255)**.



Las direcciones IP se añaden como direcciones IP de remitentes.

Enviando IP (5 elementos)



83.246.65.0/24	×	94.100.128.0/20	×	185.140.204.0/22	×
173.45.18.0/24	×	173.124.136.160/27	×		

Figura 13: Dirección IP introducida

10. Haga clic en **Guardar**.



El dominio del remitente y las direcciones IP de remitentes. Se muestra una ventana con los cambios.

✓ Se han guardado los cambios en la invalidación de suplantación de identidad (phishing).

Dominio

Se agregó 1
sas.cloud-security.net

0 quitado

Enviando IP

Se agregó 5
83.246.65.0/24
94.100.128.0/20
185.140.204.0/22
173.45.18.0/24
173.124.136.160/27

0 quitado

Direcciones URL de simulación a permitir

Se agregó 0

0 quitado

Figura 14: Cambios



11. Haga clic en **Cerrar**.



Se ha configurado la entrega avanzada en Microsoft 365 Defender.

Reglas de transporte para Security Awareness Service

El servicio de seguridad Microsoft 365 Defender, que frecuentemente se encuentra integrado en Microsoft 365, utiliza diversos mecanismos de seguridad para asegurarse de que los enlaces y archivos adjuntos de los correos no provoquen riesgos. En primer lugar, el mecanismo "Vínculos seguros" hace clic en los enlaces contenidos en los correos, los analiza y los reescribe para prevenir ataques por esta vía. A continuación, el mecanismo "Datos adjunto seguros" comprueba los archivos adjuntos de los correos y pone en cuarentena aquéllos cuyos archivos adjuntos se consideren inseguros.

Para evitar que los mecanismos "Vínculos seguros" y "Datos adjuntos seguros" intervengan en los correos del simulacro de phishing, los clientes deben crear dos reglas de transporte en Exchange Admin Center.

Los clientes deben crear una regla de transporte para archivos adjuntos y una regla de transporte para enlaces. Las condiciones de las reglas de transporte varían en función de si el cliente dispone o no de Spam and Malware Protection (véase [Spam and Malware Protection](#)).

Los clientes con Spam and Malware Protection deben crear las siguientes reglas de transporte:

- Regla de transporte para archivos adjuntos (véase [Crear una regla de transporte para archivos adjuntos para clientes con Spam and Malware Protection](#) en la página 35)
- Regla de transporte para enlaces (véase [Crear una regla de transporte para enlaces para clientes con Spam and Malware Protection](#) en la página 43)

Los clientes sin Spam and Malware Protection deben crear las siguientes reglas de transporte:

- Regla de transporte para archivos adjuntos (véase [Crear una regla de transporte para archivos adjuntos para clientes sin Spam and Malware Protection](#) en la página 51)
- Regla de transporte para enlaces (véase [Crear una regla de transporte para enlaces para clientes sin Spam and Malware Protection](#) en la página 57)

Una vez creadas las reglas de transporte, los clientes deben activarlas (véase [Activar la regla de transporte](#) en la página 63) para que puedan aplicarse.



Crear una regla de transporte para archivos adjuntos para clientes con Spam and Malware Protection

Para que el mecanismo de seguridad "Datos adjuntos seguros" de Microsoft 365 Defender no abra y, posiblemente, bloquee los archivos adjuntos enviados en correos de phishing simulado de Security Awareness Service (véanse [Acerca de Security Awareness Service](#) en la página 7 y [Reglas de transporte para Security Awareness Service](#) en la página 34), sino que los trate como si fuesen seguros, debe crear una regla de transporte en Exchange Admin Center.

Nota:

Hay reglas de transporte diferentes dependiendo de si el cliente usa o no nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)). En este capítulo se describe la regla de transporte para clientes con Spam and Malware Protection. Para la regla de transporte para clientes sin Spam and Malware Protection, véase [Crear una regla de transporte para archivos adjuntos para clientes sin Spam and Malware Protection](#) en la página 51.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Flujo de correo > Reglas**.
4. Haga clic en **Agregar una regla**.

Reglas

Agregue, edite o realice otros cambios en las reglas de transporte. [Más información sobre las reglas de transporte](#)

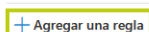
 + Agregar una regla  Editar  Duplicar  Actualizar  Subir  Bajar

Figura 15: Añadir una regla de transporte

-  Al lado derecho se muestra la página **Nueva regla de transporte**.
5. Introduzca un nombre para la regla de transporte en el campo **Nombre**.

Nota:

Recomendamos llamar a la regla de transporte **SAS SafeAttachments**.



Establecer las condiciones de la regla

Asigne un nombre y establezca las condiciones para la regla de transporte.

Nombre *

Figura 16: Introducir nombre

- En el menú desplegable **Aplique esta regla si**, seleccione la opción **El remitente**.

Aplique esta regla si *

El remitente ▼ Seleccionar uno ▼ +

Figura 17: Seleccionar un caso de uso

- El menú desplegable de la derecha se habilita.
- Seleccione la opción **tiene una dirección IP que está en uno de estos rangos o coincide exactamente con** en el menú desplegable de la derecha.

Seleccionar uno ▼ +

- es esta persona
- es externo o interno
- es miembro de este grupo
- tiene una dirección que incluye cualquiera de estas palabras
- tiene una dirección que coincide con alguno de estos patrones de texto
- está en una lista de supervisión de un destinatario
- tiene propiedades específicas que incluyen alguna de estas palabras
- tiene propiedades específicas que coinciden con estos patrones de texto
- ha reemplazado a la Sugerencia de directiva
- tiene una dirección IP que está en uno de estos rangos o coincide exactamente con**
- tiene un dominio que es

Figura 18: Seleccionar la condición para el remitente

- Se muestra la página **especificar los intervalos de direcciones IP**.
- Introduzca consecutivamente las siguientes direcciones IP en el campo de introducción de datos y haga clic en **Agregar**.
 - 83.246.65.0/24**
 - 94.100.128.0/20**
 - 185.140.204.0/22**
 - 173.45.18.0/24**



- 173.124.136.160/27

especificar los intervalos de direcciones IP

Ingresar una dirección IPv4 o IPv6 o un intervalo

Agregar

Editar Eliminar

0 elementos

Figura 19: Añadir dirección IP

- ➔ Las direcciones IP se añaden.

☐ 83.246.65.0/24

☐ 94.100.128.0/20

☐ 185.140.204.0/22

☐ 173.45.18.0/24

☐ 173.124.136.160/27

Figura 20: Direcciones IP añadidas

9. Haga clic en **Guardar**.

- ➔ La página **especificar los intervalos de direcciones IP** se cierra.

10. Haga clic en el símbolo de suma.

Aplique esta regla si *

El remitente

tiene una dirección IP que está en uno...

+

Figura 21: Añadir una condición adicional

- ➔ Se añade una condición adicional.

Y

Seleccionar uno

Seleccionar uno

🗑

Figura 22: Segunda condición

11. En el menú desplegable de Y, seleccione la opción **Los encabezados de mensaje....**



- ➔ El menú desplegable de la derecha se habilita.
- 12. Seleccione la opción **incluye cualquiera de estas palabras** en el menú desplegable de la derecha.
- 13. Haga clic en **Enter text**.

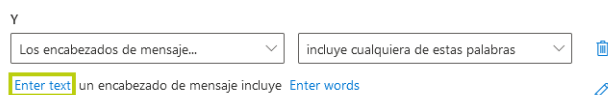


Figura 23: Determinar el nombre del encabezado

- ➔ Se abre la página **especificar nombre de encabezado**.
- 14. Introduzca **X-cloud-security-sas** en el campo de introducción de datos.

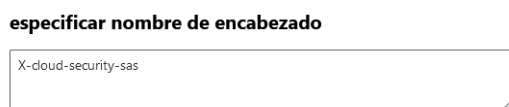


Figura 24: Introducir el nombre del encabezado

15. Haga clic en **Guardar**.
- ➔ La página **especificar nombre de encabezado** se cierra.
16. Haga clic en **Enter words**.

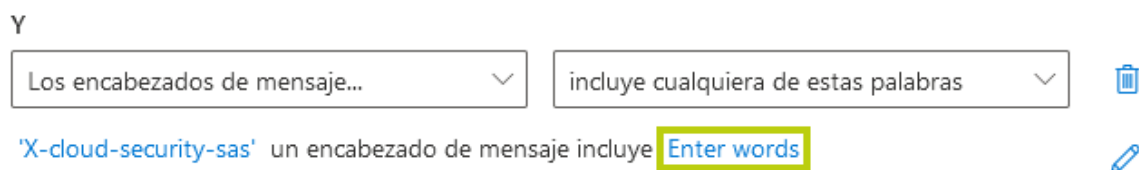


Figura 25: Determinar palabras del encabezado

- ➔ Se abre la página **especificar palabras o frases**.
- 17. Introduzca **true** en el campo de introducción de datos y haga clic en **Agregar**.



Figura 26: Introducir la expresión



- ➔ La expresión se añade.

☐ true

Figura 27: Expresión añadida

- Haga clic en **Guardar**.

- ➔ La página **especificar palabras o frases** se cierra.

- En el menú desplegable **Haga lo siguiente**, seleccione la opción **Modificar propiedades del mensaje**.

Haga lo siguiente *

Modificar propiedades del mensaje ▼	Seleccionar uno ▼	+
-------------------------------------	-------------------	---

Figura 28: Seleccionar la consecuencia

- ➔ El menú desplegable de la derecha se habilita.

- Seleccione la opción **establecer un encabezado de mensaje** en el menú desplegable de la derecha.

Haga lo siguiente *

Modificar propiedades del mensaje ▼	establecer un encabezado de mensaje ▼	+
-------------------------------------	---------------------------------------	---

Establezca el encabezado de mensaje [Enter text](#) en el valor [Enter text](#) 

Figura 29: Definir encabezado

- Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje ▼	establecer un encabezado de mensaje ▼	+
-------------------------------------	---------------------------------------	---

Establezca el encabezado de mensaje **Enter text** en el valor [Enter text](#) 

Figura 30: Introducir el nombre del nuevo encabezado



- ➔ Se abre la página **encabezado de mensaje**.
- 22. Introduzca **X-MS-Exchange-Organization-SkipSafeAttachmentProcessing** en el campo de introducción de datos.

encabezado de mensaje

X-MS-Exchange-Organization-SkipSafeAttachmentProcessing

Figura 31: Introducir el nombre del encabezado

23. Haga clic en **Guardar**.
- ➔ La página **encabezado de mensaje** se cierra.
24. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje

establecer un encabezado de mensaje

Establezca el encabezado de mensaje
'X-MS-Exchange-Organization-SkipSafeAttachmentProcessing' en el valor **Enter text**

Figura 32: Introducir el nuevo texto del encabezado

- ➔ Se abre la página **encabezado de mensaje**.
- 25. Introduzca **1** en el campo de introducción de datos.

encabezado de mensaje

1

Figura 33: Introducir el valor del encabezado

26. Haga clic en **Guardar**.
- ➔ La página **encabezado de mensaje** se cierra.
27. Haga clic en **Siguiente**.



- ➔ Se muestra la configuración de la regla.

Establecer la configuración de regla

Establecer la configuración de la regla de transporte

Modo de regla

- ☒ Exigir
- ☐ Probar con sugerencias de directivas
- ☐ Probar sin sugerencias de directivas

Gravedad *

Sin especificar

☐ Activar esta regla en

2/20/2023 - 1:00 PM

☐ Desactivar esta regla en

2/20/2023 - 1:00 PM

- ☐ Detener el procesamiento de más reglas
- ☐ Aplazar el mensaje si no se completa el procesamiento de la regla

La dirección del remitente debe coincidir en el mensaje. *

Encabezado

Figura 34: Configuración de la regla

28. No modifique la configuración de la regla.
29. Haga clic en **Siguiente**.

- ➔ Se muestra un resumen de la configuración de la regla de transporte.



Revisar y finalizar

Cuando termine de crear esta regla, se desactivará de forma predeterminada hasta que la active desde la página Reglas.

Nombre de la regla

SAS SafeAttachments

Comentarios de la regla

Condiciones de regla	Configuración de la regla
Aplique esta regla si Dirección IP del emisor en el rango '83.246.65.0/24' or '94.100.128.0/20' or '185.140.204.0/22' or '173.45.18.0/24' or '173.124.136.160/27' 'X-cloud-security-sas' un encabezado de mensaje incluye 'true'	Modo Enforce Definir intervalo de fechas No se ha establecido un intervalo de fechas específico Prioridad 0 Gravedad No especificado Para errores de procesamiento de reglas Ignore Detener el procesamiento de más reglas false
Haga lo siguiente Establezca el encabezado de mensaje 'X-MS-Exchange-Organization-SkipSafeAttachmentProcessing' en el valor '1' Excepto si Editar las condiciones de regla	Editar configuración de regla

Figura 35: Resumen de la configuración de la regla de transporte

30. Haga clic en **Finalizar**.

- ➔ La regla de transporte se crea. Este proceso puede tardar un momento. Una vez creada la regla de transporte, se muestra un mensaje de éxito.

✓ Regla de transporte creada correctamente

Figura 36: Mensaje de éxito

31. Haga clic en **Listo**.

- ➔ La página **Nueva regla de transporte** se cierra. La nueva regla de transporte se muestra en la lista de reglas de transporte de la página **Flujo de correo > Reglas** del Centro de Administración de Exchange.

- ✓ Se ha creado la regla de transporte para archivos adjuntos.



Nota:

Una vez activada la regla de transporte, los correos de phishing simulado de Security Awareness Service eludirán el mecanismo de seguridad "Datos adjuntos seguros" de Microsoft 365 Defender.



A continuación puede activar la regla de transporte (véase [Activar la regla de transporte](#) en la página 63).

Crear una regla de transporte para enlaces para clientes con Spam and Malware Protection

Para que los enlaces contenidos en correos de phishing simulados de Security Awareness Service se traten como enlaces seguros y el mecanismo de seguridad "Vínculos seguros" de Microsoft 365 no haga clic en ellos, los analice y los reescriba (véase [Acerca de Security Awareness Service](#) en la página 7), debe usted crear una regla de transporte en el Centro de Administración de Exchange.



Nota:

Hay reglas de transporte diferentes dependiendo de si el cliente usa o no nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)). En este capítulo se describe la regla de transporte para clientes con Spam and Malware Protection. Para la regla de transporte para clientes sin Spam and Malware Protection, véase [Crear una regla de transporte para enlaces para clientes sin Spam and Malware Protection](#) en la página 57.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Flujo de correo > Reglas**.
4. Haga clic en **Agregar una regla**.

Reglas

Agregue, edite o realice otros cambios en las reglas de transporte. [Más información sobre las reglas de transporte](#)

[+ Agregar una regla](#) Editar Duplicar Actualizar Subir Bajar

Figura 37: Añadir una regla de transporte



Al lado derecho se muestra la página **Nueva regla de transporte**.

5. Introduzca un nombre para la regla de transporte en el campo **Nombre**.

**Nota:**

Recomendamos llamar a la regla de transporte **SAS SafeLinks**.

Establecer las condiciones de la regla

Asigne un nombre y establezca las condiciones para la regla de transporte.

Nombre *

Figura 38: Introducir nombre

- En el menú desplegable **Aplique esta regla si**, seleccione la opción **El remitente**.

Aplique esta regla si *

El remitente

Seleccionar uno



Figura 39: Seleccionar un caso de uso

- El menú desplegable de la derecha se habilita.
- Seleccione la opción **tiene una dirección IP que está en uno de estos rangos o coincide exactamente con** en el menú desplegable de la derecha.

Seleccionar uno

- es esta persona
- es externo o interno
- es miembro de este grupo
- tiene una dirección que incluye cualquiera de estas palabras
- tiene una dirección que coincide con alguno de estos patrones de texto
- está en una lista de supervisión de un destinatario
- tiene propiedades específicas que incluyen alguna de estas palabras
- tiene propiedades específicas que coinciden con estos patrones de texto
- ha reemplazado a la Sugerencia de directiva
- tiene una dirección IP que está en uno de estos rangos o coincide exactamente con**
- tiene un dominio que es

Figura 40: Seleccionar la condición para el remitente

- Se muestra la página **especificar los intervalos de direcciones IP**.
- Introduzca consecutivamente las siguientes direcciones IP en el campo de introducción de datos y haga clic en **Agregar**.
 - 83.246.65.0/24**



- **94.100.128.0/20**
- **185.140.204.0/22**
- **173.45.18.0/24**
- **173.124.136.160/27**

especificar los intervalos de direcciones IP

Ingresar una dirección IPv4 o IPv6 o un intervalo

Agregar

Editar Eliminar

0 elementos

Figura 41: Añadir dirección IP

- ➔ Las direcciones IP se añaden.

☐	83.246.65.0/24
☐	94.100.128.0/20
☐	185.140.204.0/22
☐	173.45.18.0/24
☐	173.124.136.160/27

Figura 42: Direcciones IP añadidas

9. Haga clic en **Guardar**.
- ➔ La página **especificar los intervalos de direcciones IP** se cierra.
10. Haga clic en el símbolo de suma.

Aplique esta regla si *

El remitente

tiene una dirección IP que está en uno...

+

Figura 43: Añadir una condición adicional

- ➔ Se añade una condición adicional.



Figura 44: Segunda condición

11. En el menú desplegable de Y, seleccione la opción **Los encabezados de mensaje....**
- ➔ El menú desplegable de la derecha se habilita.
12. Seleccione la opción **incluye cualquiera de estas palabras** en el menú desplegable de la derecha.
13. Haga clic en **Enter text**.

Figura 45: Determinar el nombre del encabezado

- ➔ Se abre la página **especificar nombre de encabezado**.
14. Introduzca **X-cloud-security-sas** en el campo de introducción de datos.

Figura 46: Introducir el nombre del encabezado

15. Haga clic en **Guardar**.
- ➔ La página **especificar nombre de encabezado** se cierra.
16. Haga clic en **Enter words**.

Figura 47: Determinar palabras del encabezado

- ➔ Se abre la página **especificar palabras o frases**.
17. Introduzca **true** en el campo de introducción de datos y haga clic en **Agregar**.



especificar palabras o frases

Figura 48: Introducir la expresión

- ➔ La expresión se añade.

☐ true

Figura 49: Expresión añadida

18. Haga clic en **Guardar**.

- ➔ La página **especificar palabras o frases** se cierra.

19. En el menú desplegable **Haga lo siguiente**, seleccione la opción **Modificar propiedades del mensaje**.

Haga lo siguiente *

Modificar propiedades del mensaje

Seleccionar uno

+

Figura 50: Seleccionar la consecuencia

- ➔ El menú desplegable de la derecha se habilita.

20. Seleccione la opción **establecer un encabezado de mensaje** en el menú desplegable de la derecha.

Haga lo siguiente *

Modificar propiedades del mensaje

establecer un encabezado de mensaje

+

Establezca el encabezado de mensaje [Enter text](#) en el valor [Enter text](#)



Figura 51: Definir encabezado

21. Haga clic en **Enter text**.



Haga lo siguiente *

Modificar propiedades del mensaje

establecer un encabezado de mensaje



Establezca el encabezado de mensaje **Enter text** en el valor **Enter text**



Figura 52: Introducir el nombre del nuevo encabezado

- ➔ Se abre la página **encabezado de mensaje**.
- 22. Introduzca **X-MS-Exchange-Organization-SkipSafeLinksProcessing** en el campo de introducción de datos.

encabezado de mensaje

X-MS-Exchange-Organization-SkipSafeLinksProcessing

Figura 53: Introducir el nombre del encabezado

- 23. Haga clic en **Guardar**.
- ➔ La página **encabezado de mensaje** se cierra.
- 24. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje

establecer un encabezado de mensaje



Establezca el encabezado de mensaje **'X-MS-Exchange-Organization-SkipSafeLinksProcessing'** en el valor **Enter text**



Figura 54: Introducir el nuevo texto del encabezado

- ➔ Se abre la página **encabezado de mensaje**.
- 25. Introduzca **1** en el campo de introducción de datos.



encabezado de mensaje

Figura 55: Introducir el valor del encabezado

26. Haga clic en **Guardar**.

➔ La página **encabezado de mensaje** se cierra.

27. Haga clic en **Siguiente**.

➔ Se muestra la configuración de la regla.

Establecer la configuración de regla

Figura 56: Configuración de la regla

28. No modifique la configuración de la regla.

29. Haga clic en **Siguiente**.

➔ Se muestra un resumen de la configuración de la regla de transporte.



Revisar y finalizar

Cuando termine de crear esta regla, se desactivará de forma predeterminada hasta que la active desde la página Reglas.

Nombre de la regla

SAS SafeLinks

Comentarios de la regla

Condiciones de regla

Aplique esta regla si

Dirección IP del emisor en el rango '83.246.65.0/24' or '94.100.128.0/20' or '185.140.204.0/22' or '173.45.18.0/24' or '173.124.136.160/27' 'X-cloud-security-sas' un encabezado de mensaje incluye 'true'

Haga lo siguiente

Establezca el encabezado de mensaje 'X-MS-Exchange-Organization-SkipSafeLinksProcessing' en el valor '1'

Excepto si

[Editar las condiciones de regla](#)

Configuración de la regla

Modo

Enforce

Definir intervalo de fechas

No se ha establecido un intervalo de fechas específico

Prioridad

0

Gravedad

No especificado

Para errores de procesamiento de reglas

Ignore

Detener el procesamiento de más reglas

false

[Editar configuración de regla](#)

Figura 57: Resumen de la configuración de la regla de transporte

30. Haga clic en **Finalizar**.

- ➔ La regla de transporte se crea. Este proceso puede tardar un momento. Una vez creada la regla de transporte, se muestra un mensaje de éxito.

✓ Regla de transporte creada correctamente

Figura 58: Mensaje de éxito

31. Haga clic en **Listo**.

- ➔ La página **Nueva regla de transporte** se cierra. La nueva regla de transporte se muestra en la lista de reglas de transporte de la página **Flujo de correo > Reglas** del Centro de Administración de Exchange.

✓ Se ha creado la regla de transporte para enlaces.



Nota:

Una vez activada la regla de transporte, los correos de phishing simulado de Microsoft 365 Defender eludirán el mecanismo de seguridad "Vínculos seguros" de Security Awareness Service.



A continuación puede activar la regla de transporte (véase [Activar la regla de transporte](#) en la página 63).

Crear una regla de transporte para archivos adjuntos para clientes sin Spam and Malware Protection

Para que el mecanismo de seguridad "Datos adjuntos seguros" de Microsoft 365 Defender no abra y, posiblemente, bloquee los archivos adjuntos enviados en correos de phishing simulado de Security Awareness Service (véanse [Acerca de Security Awareness Service](#) en la página 7 y [Reglas de transporte para Security Awareness Service](#) en la página 34), sino que los trate como si fuesen seguros, debe crear una regla de transporte en Exchange Admin Center.



Nota:

Hay reglas de transporte diferentes dependiendo de si el cliente usa o no nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)). En este capítulo se describe la regla de transporte para clientes sin Spam and Malware Protection. Para la regla de transporte para clientes con Spam and Malware Protection, véase [Crear una regla de transporte para archivos adjuntos para clientes con Spam and Malware Protection](#) en la página 35.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Flujo de correo > Reglas**.
4. Haga clic en **Agregar una regla**.

Reglas

Agregue, edite o realice otros cambios en las reglas de transporte. [Más información sobre las reglas de transporte](#)

[+ Agregar una regla](#) [✎ Editar](#) [📄 Duplicar](#) [🔄 Actualizar](#) [^ Subir](#) [v Bajar](#)

Figura 59: Añadir una regla de transporte



Al lado derecho se muestra la página **Nueva regla de transporte**.

5. Introduzca un nombre para la regla de transporte en el campo **Nombre**.

**Nota:**

Recomendamos llamar a la regla de transporte **SAS SafeAttachments**.

Establecer las condiciones de la regla

Asigne un nombre y establezca las condiciones para la regla de transporte.

Nombre *

Figura 60: Introducir nombre

6. En el menú desplegable **Aplique esta regla si**, seleccione la opción **El remitente**.

Aplique esta regla si *

El remitente

Seleccionar uno

+

Figura 61: Seleccionar un caso de uso

- ➔ El menú desplegable de la derecha se habilita.
7. Seleccione la opción **tiene una dirección IP que está en uno de estos rangos o coincide exactamente con** en el menú desplegable de la derecha.

Seleccionar uno

+

es esta persona

es externo o interno

es miembro de este grupo

tiene una dirección que incluye cualquiera de estas palabras

tiene una dirección que coincide con alguno de estos patrones de texto

está en una lista de supervisión de un destinatario

tiene propiedades específicas que incluyen alguna de estas palabras

tiene propiedades específicas que coinciden con estos patrones de texto

ha reemplazado a la Sugerencia de directiva

tiene una dirección IP que está en uno de estos rangos o coincide exactamente con

tiene un dominio que es

Figura 62: Seleccionar la condición para el remitente

- ➔ Se muestra la página **especificar los intervalos de direcciones IP**.
8. Introduzca consecutivamente las siguientes direcciones IP en el campo de introducción de datos y haga clic en **Agregar**.
- **94.100.136.58**



- 94.100.132.73

especificar los intervalos de direcciones IP



Figura 63: Añadir dirección IP

- ➔ La dirección IP se añade.

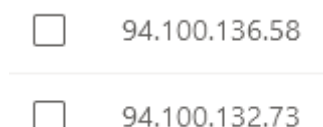


Figura 64: Direcciones IP añadidas

9. Haga clic en **Guardar**.

- ➔ La página **especificar los intervalos de direcciones IP** se cierra.

10. En el menú desplegable **Haga lo siguiente**, seleccione la opción **Modificar propiedades del mensaje**.



Figura 65: Seleccionar la consecuencia

- ➔ El menú desplegable de la derecha se habilita.

11. Seleccione la opción **establecer un encabezado de mensaje** en el menú desplegable de la derecha.

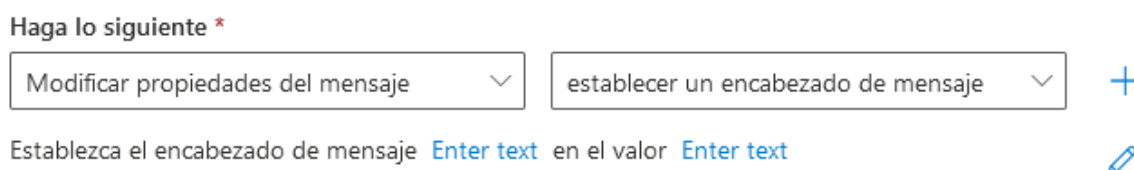


Figura 66: Definir encabezado



12. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje	establecer un encabezado de mensaje	+
-----------------------------------	-------------------------------------	---

Establezca el encabezado de mensaje **Enter text** en el valor **Enter text** 

Figura 67: Introducir el nombre del nuevo encabezado

- ➔ Se abre la página **encabezado de mensaje**.
13. Introduzca **X-MS-Exchange-Organization-SkipSafeAttachmentProcessing** en el campo de introducción de datos.

encabezado de mensaje

X-MS-Exchange-Organization-SkipSafeAttachmentProcessing

Figura 68: Introducir el nombre del encabezado

14. Haga clic en **Guardar**.
- ➔ La página **encabezado de mensaje** se cierra.
15. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje	establecer un encabezado de mensaje	+
-----------------------------------	-------------------------------------	---

Establezca el encabezado de mensaje **'X-MS-Exchange-Organization-SkipSafeAttachmentProcessing'** en el valor **Enter text** 

Figura 69: Introducir el nuevo texto del encabezado

- ➔ Se abre la página **encabezado de mensaje**.
16. Introduzca **1** en el campo de introducción de datos.



encabezado de mensaje

Figura 70: Introducir el valor del encabezado

17. Haga clic en **Guardar**.

➔ La página **encabezado de mensaje** se cierra.

18. Haga clic en **Siguiente**.

➔ Se muestra la configuración de la regla.

Establecer la configuración de regla

Figura 71: Configuración de la regla

19. No modifique la configuración de la regla.

20. Haga clic en **Siguiente**.

➔ Se muestra un resumen de la configuración de la regla de transporte.



Revisar y finalizar

Cuando termine de crear esta regla, se desactivará de forma predeterminada hasta que la active desde la página Reglas.

Nombre de la regla

SAS SafeAttachments

Comentarios de la regla

Condiciones de regla

Aplice esta regla si

Dirección IP del emisor en el rango '94.100.136.58' or '94.100.132.73'

Haga lo siguiente

Establezca el encabezado de mensaje 'X-MS-Exchange-Organization-SkipSafeAttachmentProcessing' en el valor '1'

Excepto si

[Editar las condiciones de regla](#)

Configuración de la regla

Modo

Enforce

Definir intervalo de fechas

No se ha establecido un intervalo de fechas específico

Prioridad

0

Gravedad

Sin especificar

Para errores de procesamiento de reglas

Ignore

Detener el procesamiento de más reglas

false

[Editar configuración de regla](#)

Figura 72: Resumen de la configuración de la regla de transporte

21. Haga clic en **Finalizar**.

- ➔ La regla de transporte se crea. Este proceso puede tardar un momento. Una vez creada la regla de transporte, se muestra un mensaje de éxito.

✓ Regla de transporte creada correctamente

Figura 73: Mensaje de éxito

22. Haga clic en **Listo**.

- ➔ La página **Nueva regla de transporte** se cierra. La nueva regla de transporte se muestra en la lista de reglas de transporte de la página **Flujo de correo > Reglas** del Centro de Administración de Exchange.

✓ Se ha creado la regla de transporte para archivos adjuntos.



Nota:

Una vez activada la regla de transporte, los correos de phishing simulado de Security Awareness Service eludirán el mecanismo de seguridad "Datos adjuntos seguros" de Microsoft 365 Defender.



A continuación puede activar la regla de transporte (véase [Activar la regla de transporte](#) en la página 63).

Crear una regla de transporte para enlaces para clientes sin Spam and Malware Protection

Para que los enlaces contenidos en correos de phishing simulados de Security Awareness Service se traten como enlaces seguros y el mecanismo de seguridad "Vínculos seguros" de Microsoft 365 no haga clic en ellos, los analice y los reescriba (véase [Acerca de Security Awareness Service](#) en la página 7), debe usted crear una regla de transporte en el Centro de Administración de Exchange.



Nota:

Hay reglas de transporte diferentes dependiendo de si el cliente usa o no nuestro servicio Spam and Malware Protection (véase [Spam and Malware Protection](#)). En este capítulo se describe la regla de transporte para clientes sin Spam and Malware Protection. Para la regla de transporte para clientes con Spam and Malware Protection, véase [Crear una regla de transporte para enlaces para clientes con Spam and Malware Protection](#) en la página 43.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Flujo de correo > Reglas**.
4. Haga clic en **Agregar una regla**.

Reglas

Agregue, edite o realice otros cambios en las reglas de transporte. [Más información sobre las reglas de transporte](#)

[+ Agregar una regla](#) [✎ Editar](#) [📄 Duplicar](#) [🔄 Actualizar](#) [^ Subir](#) [v Bajar](#)

Figura 74: Añadir una regla de transporte



Al lado derecho se muestra la página **Nueva regla de transporte**.

5. Introduzca un nombre para la regla de transporte en el campo **Nombre**.

**Nota:**

Recomendamos llamar a la regla de transporte **SAS SafeLinks**.

Establecer las condiciones de la regla

Asigne un nombre y establezca las condiciones para la regla de transporte.

Nombre *

Figura 75: Introducir nombre

6. En el menú desplegable **Aplique esta regla si**, seleccione la opción **El remitente**.

Aplique esta regla si *

El remitente

Seleccionar uno

+

Figura 76: Seleccionar un caso de uso

- ➔ El menú desplegable de la derecha se habilita.
7. Seleccione la opción **tiene una dirección IP que está en uno de estos rangos o coincide exactamente con** en el menú desplegable de la derecha.

Seleccionar uno

+

es esta persona

es externo o interno

es miembro de este grupo

tiene una dirección que incluye cualquiera de estas palabras

tiene una dirección que coincide con alguno de estos patrones de texto

está en una lista de supervisión de un destinatario

tiene propiedades específicas que incluyen alguna de estas palabras

tiene propiedades específicas que coinciden con estos patrones de texto

ha reemplazado a la Sugerencia de directiva

tiene una dirección IP que está en uno de estos rangos o coincide exactamente con

tiene un dominio que es

Figura 77: Seleccionar la condición para el remitente

- ➔ Se muestra la página **especificar los intervalos de direcciones IP**.
8. Introduzca consecutivamente las siguientes direcciones IP en el campo de introducción de datos y haga clic en **Agregar**.
- **94.100.136.58**



- 94.100.132.73

especificar los intervalos de direcciones IP



Figura 78: Añadir dirección IP

- ➔ La dirección IP se añade.

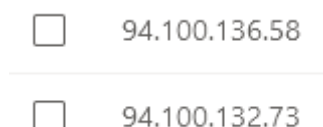


Figura 79: Direcciones IP añadidas

9. Haga clic en **Guardar**.

- ➔ La página **especificar los intervalos de direcciones IP** se cierra.

10. En el menú desplegable **Haga lo siguiente**, seleccione la opción **Modificar propiedades del mensaje**.



Figura 80: Seleccionar la consecuencia

- ➔ El menú desplegable de la derecha se habilita.

11. Seleccione la opción **establecer un encabezado de mensaje** en el menú desplegable de la derecha.

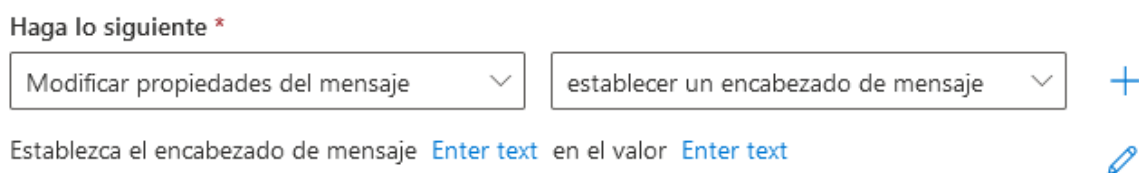


Figura 81: Definir encabezado



12. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje	establecer un encabezado de mensaje	+
-----------------------------------	-------------------------------------	---

Establezca el encabezado de mensaje **Enter text** en el valor **Enter text**

Figura 82: Introducir el nombre del nuevo encabezado

- ➔ Se abre la página **encabezado de mensaje**.
13. Introduzca **X-MS-Exchange-Organization-SkipSafeLinksProcessing** en el campo de introducción de datos.

encabezado de mensaje

X-MS-Exchange-Organization-SkipSafeLinksProcessing
--

Figura 83: Introducir el nombre del encabezado

14. Haga clic en **Guardar**.
- ➔ La página **encabezado de mensaje** se cierra.
15. Haga clic en **Enter text**.

Haga lo siguiente *

Modificar propiedades del mensaje	establecer un encabezado de mensaje	+
-----------------------------------	-------------------------------------	---

Establezca el encabezado de mensaje 'X-MS-Exchange-Organization-SkipSafeLinksProcessing' en el valor **Enter text**

Figura 84: Introducir el nuevo texto del encabezado

- ➔ Se abre la página **encabezado de mensaje**.
16. Introduzca **1** en el campo de introducción de datos.



encabezado de mensaje

Figura 85: Introducir el valor del encabezado

17. Haga clic en **Guardar**.

➔ La página **encabezado de mensaje** se cierra.

18. Haga clic en **Siguiente**.

➔ Se muestra la configuración de la regla.

Establecer la configuración de regla

Figura 86: Configuración de la regla

19. No modifique la configuración de la regla.

20. Haga clic en **Siguiente**.

➔ Se muestra un resumen de la configuración de la regla de transporte.



Revisar y finalizar

Cuando termine de crear esta regla, se desactivará de forma predeterminada hasta que la active desde la página Reglas.

Nombre de la regla

SAS SafeLinks

Comentarios de la regla

Condiciones de regla

Aplique esta regla si

Dirección IP del emisor en el rango '94.100.136.58' or '94.100.132.73'

Haga lo siguiente

Establezca el encabezado de mensaje 'X-MS-Exchange-Organization-SkipSafeLinksProcessing' en el valor '1'

Excepto si

[Editar las condiciones de regla](#)

Configuración de la regla

Modo

Enforce

Definir intervalo de fechas

No se ha establecido un intervalo de fechas específico

Prioridad

0

Gravedad

Sin especificar

Para errores de procesamiento de reglas

Ignore

Detener el procesamiento de más reglas

false

[Editar configuración de regla](#)

Figura 87: Resumen de la configuración de la regla de transporte

21. Haga clic en **Finalizar**.

- ➔ La regla de transporte se crea. Este proceso puede tardar un momento. Una vez creada la regla de transporte, se muestra un mensaje de éxito.

✓ Regla de transporte creada correctamente

Figura 88: Mensaje de éxito

- ✓ Se ha creado la regla de transporte para enlaces.



Nota:

Una vez activada la regla de transporte, los correos de phishing simulado de Microsoft 365 Defender eludirán el mecanismo de seguridad "Vínculos seguros" de Security Awareness Service.

A continuación puede activar la regla de transporte (véase [Activar la regla de transporte](#) en la página 63).



Activar la regla de transporte

✓ Ha creado reglas de transporte para Security Awareness Service (véanse [Crear una regla de transporte para archivos adjuntos para clientes con Spam and Malware Protection](#) en la página 35 y [Crear una regla de transporte para enlaces para clientes con Spam and Malware Protection](#) en la página 43 o [Crear una regla de transporte para archivos adjuntos para clientes sin Spam and Malware Protection](#) en la página 51 y [Crear una regla de transporte para enlaces para clientes sin Spam and Malware Protection](#) en la página 57).

Puede activar reglas de transporte para Security Awareness Service en el Centro de Administración de Exchange.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Flujo de correo > Reglas**.
4. Haga clic en el nombre de la regla de transporte que desee activar.



Figura 89: Añadir la regla de transporte

- ➔ La configuración de la regla de transporte se muestra a la derecha.
5. Accione el interruptor **Deshabilitado**.

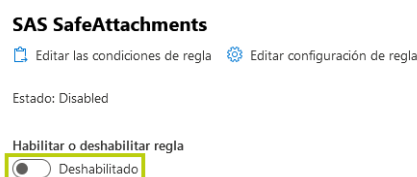


Figura 90: Activar la regla de transporte

- ➔ El interruptor se pone azul. La regla de transporte se activa. La activación puede tardar un momento. Una vez creada la regla de transporte, se muestra un mensaje de éxito.

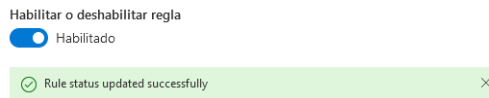


Figura 91: Regla de transporte activada

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

- ➔ La página de configuración de la regla de transporte se cierra. La regla de transporte está ahora en estado **Habilitado**.

✔ Se ha activado una regla de transporte.

Crear una directiva de vínculos seguros

✔ Su organización utiliza Microsoft 365 Defender Plan 2 y ha creado una directiva de vínculos seguros.

Para que las directivas de vínculos seguros no puedan reescribir enlaces incluidos en correos de phishing de Security Awareness Service (véanse [Acerca de Security Awareness Service](#) en la página 7 y [Configuración en Microsoft 365](#) en la página 27), puede usted crear una directiva de vínculos seguros. Con la nueva directiva puede usted excluir de la reescritura de URLs los dominios a los que pertenecen los enlaces utilizados en los correos de phishing simulado.



Nota:

En este capítulo se describe cómo crear una nueva directiva. Otra opción es incluir los dominios del paso 15 en la página 68 en una directiva previa.



IMPORTANTE:

La organización no debe tener activada ninguna directiva de seguridad predefinida de tipo **Protección estricta** en el apartado **Reglas y directivas** > > **Directivas de amenazas** > **Restablecer directivas de seguridad** de Microsoft 365 Defender, ya que una directiva de este tipo siempre tiene prioridad sobre las demás directivas sobre vínculos seguros.

1. Abra la página web <https://security.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Reglas y directivas**.

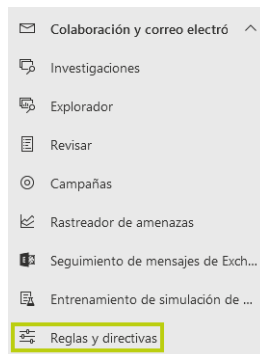


Figura 92: Abrir directivas y reglas

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

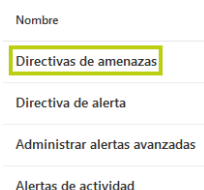


Figura 93: Abrir directivas sobre amenazas

5. En **Directivas**, haga clic en **Vínculos seguros**.

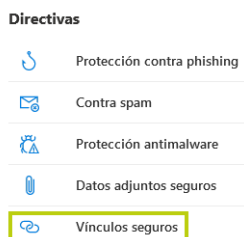


Figura 94: Abrir vínculos seguros

- ➔ Se muestra la página **Vínculos seguros**.

6. Haga clic en **Crear**.

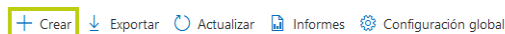


Figura 95: Crear una directiva

- ➔ Se muestra la página **Asigne un nombre a la directiva**.

7. Introduzca el nombre de la directiva en el campo de introducción de datos **Nombre**.

**Nota:**

Recomendamos llamar a la directiva **Bypass SafeLinks Rewriting**.

Asigne un nombre a la directiva

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

Nombre *

Bypass SafeLinks Rewriting

Descripción

Figura 96: Introducir el nombre de la directiva

8. Haga clic en **Siguiente**.



Se muestra la página **Usuarios y dominios**.

9. Introduzca el dominio al que pertenecen los usuarios de Security Awareness Service en el campo **Dominios** y haga clic en el dominio mostrado.

Dominios

n08n.onmicrosoft.com

Dominios sugeridos

n08n.onmicrosoft.com

Figura 97: Introducir el dominio



El dominio se añade.

Dominios

n08n.onmicrosoft.com X

Figura 98: Dominio añadido

10. Repita el paso 9 en la página 66 hasta que haya añadido todos los dominios.

11. Haga clic en **Siguiente**.



Se muestra la página **Configuración de protección de direcciones URL y clics**.

12. Realice los ajustes que desee.

**Nota:**

Los ajustes mostrados en la captura de pantalla son meros ejemplos. Los clientes pueden realizar otros ajustes si lo desean.

Correo electrónico

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

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

[Administrar 0 dirección URL](#)

Teams

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

Aplicaciones de Office 365

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

Configuración de protección de clics

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

Figura 99: Configurar la protección de direcciones URL y clics

13. Haga clic en **Administrar dirección URL**.

No vuelva a escribir las siguientes URL en el correo electrónico (0)
[Administrar 0 dirección URL](#)

Figura 100: Administrar URLs



Al lado derecho se muestra la página **Administrar las direcciones URL** que no se deben reescribir.

14. Haga clic en **Agregar direcciones URL**.



Figura 101: Añadir URLs



- ➔ Se muestra la página **Agregar direcciones URL**.

15. Introduzca todos los dominios del [Dominios de envío del simulacro de phishing](#) en la página 19 capítulo uno tras otro en el campo de entrada **URL** y haga clic en el dominio mostrado.

Figura 102: Introducir el dominio

- ➔ El dominio se añade.

Figura 103: Dominio añadido

16. Haga clic en **Guardar**.

- ➔ La página **Agregar direcciones URL** se cierra. Vuelve a mostrarse la página **Administrar las direcciones URL que no se deben reescribir**. En la página se muestran todos los dominios añadidos.

17. Haga clic en **Listo**.

- ➔ La página **Administrar las direcciones URL que no se deben reescribir** se cierra. Vuelve a mostrarse la página **Configuración de protección de direcciones URL y clics**.

18. Haga clic en **Siguiente**.

- ➔ Se muestra la página **Notificación**.

19. Realice los ajustes que desee.

Notificación

Figura 104: Configurar la notificación

20. Haga clic en **Siguiente**.

- ➔ Se muestra un resumen de la configuración de la directiva.

21. Haga clic en **Enviar**.



- ➔ Se muestra un mensaje de confirmación.

22. Haga clic en **Sí**.

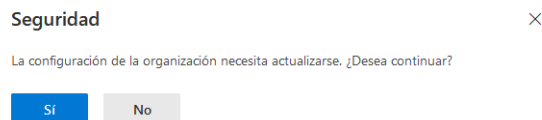


Figura 105: Confirmar la actualización de la configuración de la organización

- ➔ La directiva se crea. La creación de la directiva puede tardar un momento. Una vez creada la directiva se muestra un mensaje de éxito.



Figura 106: Mensaje de éxito

23. Haga clic en **Listo**.

- ➔ La página se cierra.

- ✓ Se ha creado una directiva de vínculos seguros.



IMPORTANTE:

Las directivas de vínculos seguros se procesan consecutivamente en función de su prioridad. Para que los enlaces incluidos en correos de phishing simulados nunca se reescriban, esta directiva tiene que tener la prioridad más alta. Si tiene otras directivas aparte de ésta y la directiva predefinida **Built-in protection (Microsoft)**, deberá cambiar la prioridad de esta directiva (véase [Prioridad de la directiva de vínculos seguros](#) en la página 69).

Prioridad de la directiva de vínculos seguros



- ✓ Su organización utiliza Microsoft 365 Defender Plan 2 y usted ha creado una directiva para vínculos seguros (véase [Crear una directiva de vínculos seguros](#) en la página 64).

Puede ajustar la prioridad de la directiva para enlaces seguros (véase [Crear una directiva de vínculos seguros](#) en la página 64) a 0 para que se procese antes que todas las demás directivas sobre enlaces seguros. De este modo, los enlaces contenidos en correos de phishing



simulados de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) no sean reescritos mediante otras directivas para vínculos seguros de Microsoft 365 Defender Plan 2.

1. Abra la página web <https://security.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador.
3. Vaya a **Reglas y directivas**.

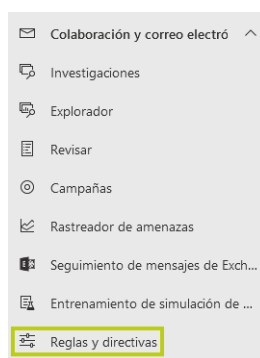


Figura 107: Abrir directivas y reglas

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

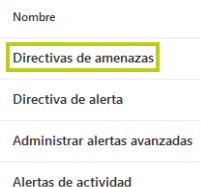


Figura 108: Abrir directivas sobre amenazas

5. En **Directivas**, haga clic en **Vínculos seguros**.

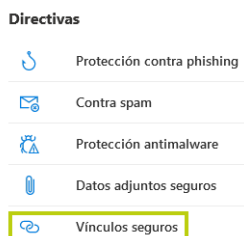


Figura 109: Abrir vínculos seguros



Se muestra la página **Vínculos seguros**.



- Haga clic en el nombre de la directiva que ha creado con anterioridad (véase [Crear una directiva de vínculos seguros](#) en la página 64).

☐ Bypass SafeLinks Rewriting

Figura 110: Seleccionar la directiva

- En el lado derecho se muestra la configuración de la directiva.
- Haga clic en **Aumentar prioridad**.



Figura 111: Aumentar la prioridad

- El número de la prioridad se reduce en 1. Esto incrementa la prioridad de la directiva.
 - Repita el paso 7 en la página 71 hasta que la directiva alcance la prioridad 0.
 - Haga clic en **Cerrar**.
 - La configuración de la directiva se cierra. La directiva se encuentra ahora en la posición más alta de la lista de directivas.
- ✓ La prioridad de la directiva de enlaces seguros se ha ajustado a 0.

Solución de problemas: Desactivar el botón de informe de Microsoft

Problema

Los usuarios desean informar sobre correos electrónicos de phishing simulados utilizando el Phishing Reporter o el Hornetsecurity Outlook Add-in, pero accidentalmente utilizan la función de informe integrada de Microsoft en su lugar.

Causa

De forma predeterminada, el botón de informe de Microsoft es visible en Outlook. Los usuarios a menudo encuentran difícil distinguir entre el Phishing Reporter, el Hornetsecurity Outlook Add-in y la función integrada de Microsoft.

Para evitar confusiones, los administradores de inquilinos pueden desactivar el botón de informe de Microsoft para que los usuarios solo tengan una opción para informar.



Solución

1. Abra el portal de Microsoft Defender utilizando el siguiente enlace: <https://security.microsoft.com/securitysettings/userSubmission>.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
- ➔ Se abre la página **Configuración notificada por el usuario** en la sección **Colaboración y correo electrónico**.
3. En la sección **Outlook**, desmarque la casilla **Supervisar mensajes notificados en Outlook**.
4. Establezca el interruptor debajo de la casilla en **Usar botón de un complemento que no es de Microsoft**.

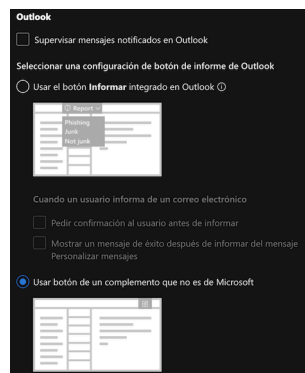


Figura 112: Desactivar el botón de informe integrado en Microsoft Outlook

5. En la sección **Microsoft Teams**, desmarque la casilla **Supervisar mensajes notificados en Microsoft Teams**.

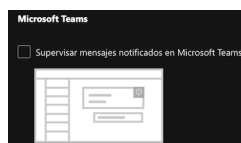


Figura 113: Desactivar la supervisión de los mensajes reportados en Microsoft Teams

6. En la parte inferior de la página, haga clic en **Guardar**.
- ➔ Los cambios se han guardado y la función de informe integrada de Microsoft ya no estará disponible en Outlook para sus usuarios.



Configuración de clientes

Crear excepciones para enlaces de phishing y páginas de aterrizaje para clientes en Microsoft Defender

-  Utiliza un ordenador con el sistema operativo Windows 10/11 y utiliza Internet Explorer o Microsoft Edge.

MS Defender SmartScreen es una función de Microsoft que está integrada en los sistemas operativos Windows 10 y 11. Está diseñada para advertir a los usuarios sobre phishing, sitios web maliciosos o la descarga de malware. A veces también ocurre que algunos sitios web se marcan como maliciosos y se bloquean aunque no lo son. La creación de una lista de excepciones resuelve este problema.

1. Pulse la tecla Windows.
-  Se abre el campo de búsqueda de Windows en la esquina inferior izquierda.
2. Introduzca **Panel de control** en el campo de búsqueda.
3. Haga clic en **Red e Internet**.
4. Haga clic en **Opciones de Internet**.
5. En la parte superior, haga clic en la pestaña **Seguridad**.

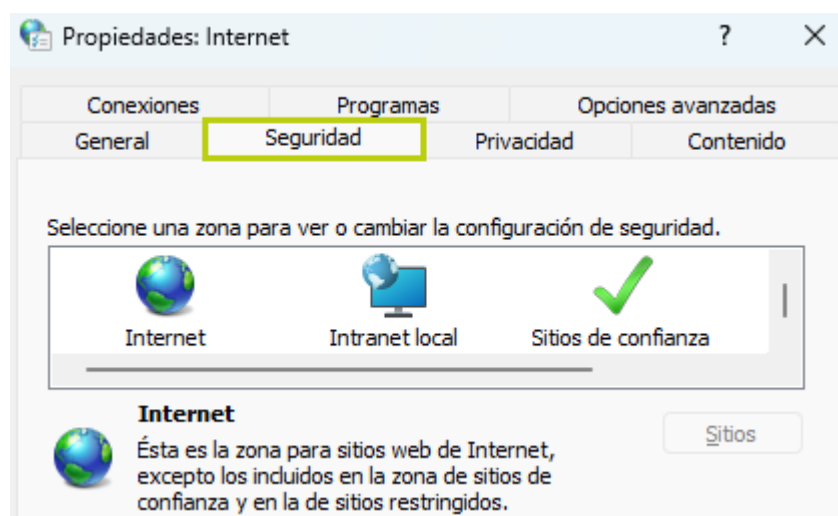


Figura 114: Ir a la pestaña Seguridad

6. Seleccione la zona **Sitios de confianza** y haga clic en **Sitios**.

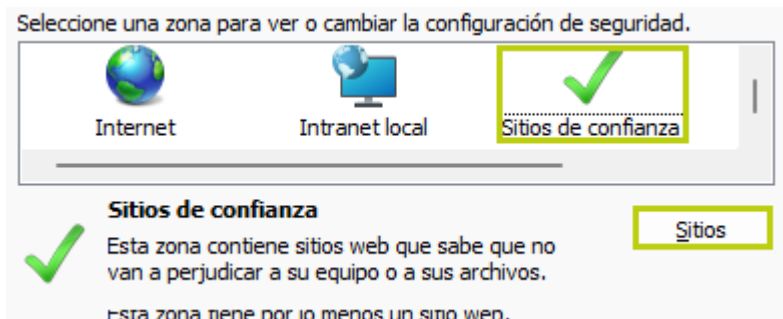


Figura 115: Seleccionar la zona correcta

7. Desmarque la casilla **Requerir comprobación del servidor (https:)** para todos los sitios de esta zona.
8. Añada la dirección del sitio web, el enlace de phishing o la página de aterrizaje a desbloquear y haga clic en **Agregar**.
9. Vuelva ahora a la zona **SitiOS de confianza**.
10. Haga clic en **Nivel personalizado**.

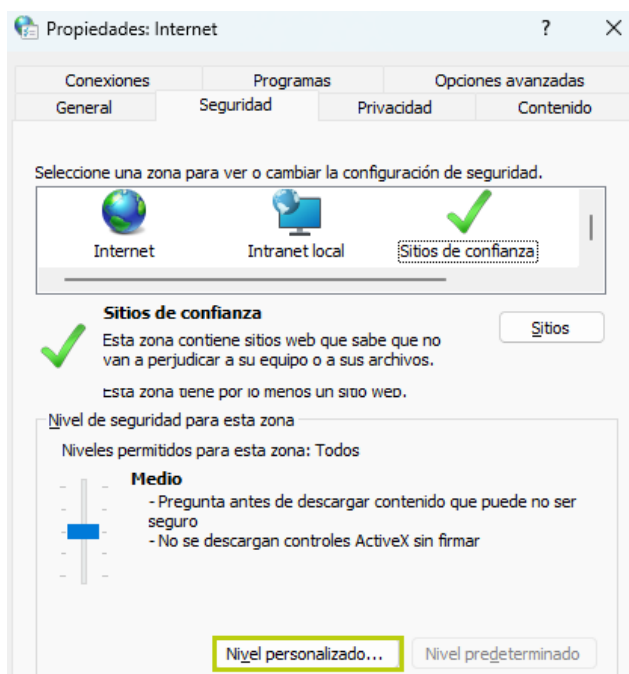


Figura 116: Seleccionar la personalización de nivel

11. Desplácese hasta **Usar SmartScreen de Windows Defender** y haga clic en **Deshabilitar**.

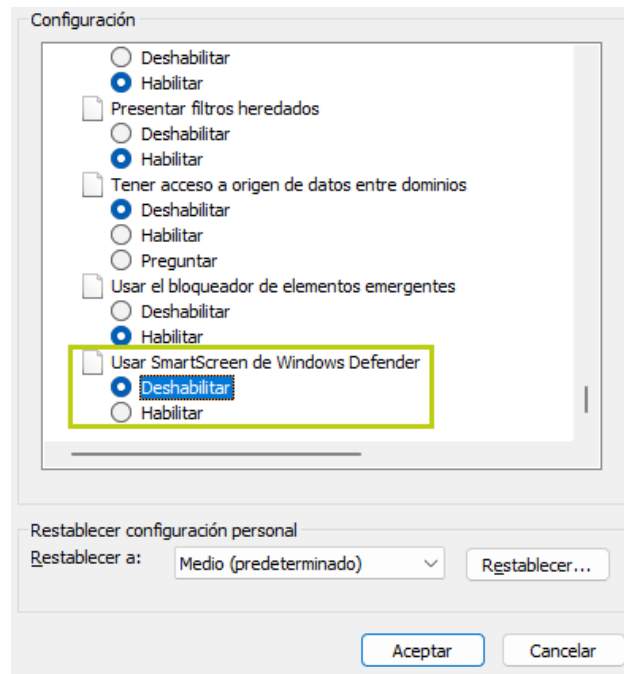


Figura 117: Desactivar MS Defender SmartScreen en la zona

- ✓ Los sitios web, los enlaces de phishing y las páginas de aterrizaje se han añadido correctamente a la lista de excepciones y MS Defender SmartScreen ya no los bloqueará.

Crear excepciones para enlaces de phishing y páginas de aterrizaje mediante la distribución de grupos

- ✓ Utiliza Microsoft 365 y tiene instalado Windows 10/11. Ya ha añadido las excepciones a la zona de sitios de confianza [Crear excepciones para enlaces de phishing y páginas de aterrizaje para clientes en Microsoft Defender](#) en la página 73.

Un administrador de red puede realizar ajustes para varios usuarios a la vez utilizando directivas de grupo. Un administrador puede definir los sitios web, los enlaces de phishing o los dominios de páginas de aterrizaje que MS Defender SmartScreen debe dejar de bloquear.

1. Pulse la tecla Windows.
- ➔ Se abre el campo de búsqueda de Windows en la esquina inferior izquierda.
2. Introduzca **Editar directiva de grupo** en el campo de búsqueda.
3. Haga clic en **Plantillas administrativas**.

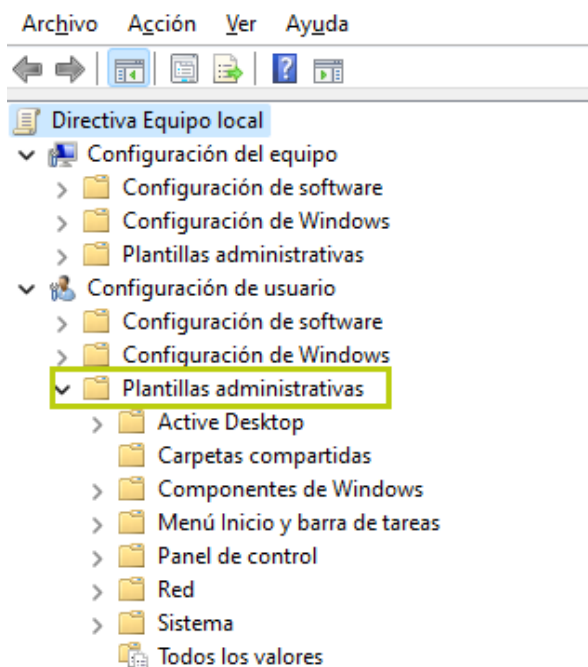


Figura 118: Ir a la carpeta Plantillas administrativas

4. Abra la subcarpeta **Componentes de Windows**.
5. Abra la subcarpeta **Internet Explorer**.
6. Abra la subcarpeta **Panel de control de Internet**.
7. Abra la subcarpeta **Página Seguridad**.
8. Abra la subcarpeta **Zona Sitios de confianza**.
9. Haga clic derecho en la fila **Activar detección de filtros SmartScreen**.

➔ Se muestra una nueva ventana con opciones adicionales.

10. Haga clic en **Editar**.

➔ En la esquina superior izquierda se muestra una nueva ventana con opciones de configuración adicionales.

11. En la esquina superior izquierda, seleccione la opción **Deshabilitada**.

✓ MS Defender SmartScreen se ha configurado para varios usuarios a la vez.



Activación de Security Awareness Service

Para poder utilizar Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7), los administradores deben activarlo en Control Panel (véase [Activar Security Awareness Service](#) en la página 77). De este modo se habilitan las opciones de configuración del servicio y el acceso a las estadísticas. También se activan el simulacro de phishing y los tutoriales con la configuración predeterminada.

Posteriormente es posible desactivar de nuevo el simulacro de phishing (véase [Activar o desactivar el simulacro de phishing](#) en la página 79) y los tutoriales (véase [Activar o desactivar los tutoriales](#) en la página 82).

**Nota:**

Tras al menos 12 meses de participación en Security Awareness Service, los clientes pueden solicitar un certificado (véase [Certificado de cliente](#) en la página 223).

Activar Security Awareness Service



Ha creado el cliente en Control Panel y ha añadido al menos un buzón de correo del cliente a Control Panel (véase [Preparativos para sistemas](#) en la página 9).

En el módulo **Security Awareness Service > Configuración** puede activar Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). De este modo se habilitan las opciones de configuración del servicio y el acceso a las estadísticas. También se activan el simulacro de phishing y los tutoriales con la configuración predeterminada.

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 activar Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Accione el interruptor .

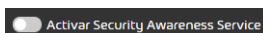


Figura 119: Activar Security Awareness Service



Se muestra una ventana de confirmación.



5.

**ATENCIÓN:**

La activación de Security Awareness Service conlleva costes adicionales conforme a la lista de precios. El servicio se factura en base a la cantidad de buzones de correo del cliente.

Haga clic en .

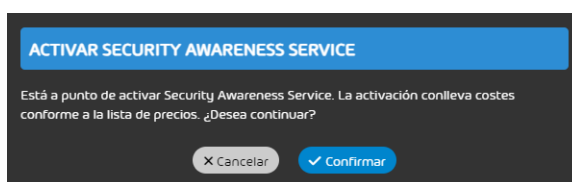


Figura 120: Confirmar la activación



El interruptor se pone verde. El servicio se activa con la configuración por defecto. Se abre una ventana con la configuración por defecto.

**Nota:**

Se activan el simulacro de phishing y los tutoriales. Los primeros tutoriales se asignan a los usuarios del cliente al día siguiente. Los correos de phishing simulados comienzan a enviarse a los usuarios del cliente al cabo de siete días tras la activación del servicio.

El modo de privacidad (véase [Modo de privacidad](#) en la página 160) está desactivado por defecto. De este modo, los administradores tienen acceso a los resultados individuales de sus usuarios.

Los administradores pueden modificar la configuración en el módulo **Security Awareness Service > Configuración**.

**Nota:**

Recomendamos informar a los usuarios sobre los tutoriales que se vayan a celebrar. Proporcionamos una plantilla para anunciarlos dentro de su organización. En la página con la configuración por defecto se incluye un enlace para descargarla.



Figura 121: Configuración por defecto

6. Marque las dos casillas.



El botón **Aceptar** se habilita.

7. Haga clic en **Aceptar**.



La ventana de la configuración por defecto se cierra.



Security Awareness Service se ha activado.

A continuación puede añadir grupos a Security Awareness Service (véase [Añadir grupos](#) en la página 127), asignar un cargo de su organización a los usuarios (véase [Añadir cargos](#) en la página 133) así como configurar el simulacro de phishing (véase [Configurar el simulacro de phishing](#) en la página 148) y los tutoriales (véase [Configurar los tutoriales](#) en la página 200). Si sus buzones de correo se sincronizan con Microsoft 365 o con un servicio de directorio mediante LDAP, puede introducir el puesto y el idioma de sus usuarios para correos de phishing simulado en su servicio de directorio y hacer que se sincronicen (véase [Sincronizar puestos e idiomas para Security Awareness Service](#) en la página 135). Si no desea utilizar el simulacro de phishing o los tutoriales, puede volver a desactivarlos (véanse [Activar o desactivar el simulacro de phishing](#) en la página 79 y [Activar o desactivar los tutoriales](#) en la página 82).

Activar o desactivar el simulacro de phishing



Ha activado Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77).

En el módulo **Security Awareness Service > Configuración** puede activar y desactivar el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness](#)



[Service](#) en la página 7). Si el simulacro de phishing se encuentra activado, los usuarios del cliente recibirán correos de phishing simulados.

**Nota:**

Por defecto, al activar Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77), el simulacro de phishing también se activa.

**Nota:**

En la simulación de phishing se emplea nuestro Spear Phishing Engine patentado. El Spear Phishing Engine elabora correos de phishing simulados de modo realista y a medida de cada usuario. Además, los ataques simulados se adaptan al nivel actual de los usuarios. Cuanto mejor se haya defendido un usuario de ataques simulados previos, más sofisticados serán los posteriores.

**Nota:**

Para poder utilizar todas las funciones de Security Awareness Service y Spear-Phishing-Engine, es necesario que al menos el 60 por ciento de los usuarios hayan introducido un nombre y un apellido en Control Panel (véase [Editar los datos básicos de un buzón de correo](#)). Sin esta información personalizada, no se pueden aplicar algunos escenarios de phishing, lo que reduce la eficiencia del servicio.

**Nota:**

Durante el simulacro de phishing, intentamos engañar a los usuarios con enlaces o direcciones de correo electrónico que pueden contener el nombre de la empresa del cliente o parecer proceder de una dirección de correo electrónico del administrador del cliente. A veces, accidentalmente coincidimos con una dirección de correo electrónico real del cliente. No se trata de una suplantación de dominio real. Los correos electrónicos de phishing simulados que utilizan este tipo de trampas sólo se utilizarán si la suplantación de dominio está activada en la configuración del Control Panel (véase la pestaña en **Security Awareness Service > Configuración** en el Control Panel).

Ejemplo 1: El correo electrónico contiene el enlace `http://intranet.company.com-office365/login.xyz`. En este caso, el dominio real es `com-office365.com` y el nombre de la empresa está en el subdominio.

Ejemplo 2: La vista previa de la dirección de correo electrónico en Outlook se parece a `admin@companyname.com`. Sin embargo, al comprobar los detalles, queda claro que el verdadero dominio remitente no es el de la empresa.

Evaluamos de cuáles de los ataques simulados ha sabido el usuario defenderse y con cuáles ha picado. En base a dicha información se elabora el Employee Security Index (véase [Employee Security Index \(ESI®\)](#) en la página 8), que mide la concienciación de seguridad dentro de la organización.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar o desactivar el simulacro de phishing.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. Accione el interruptor **Activar el simulacro de phishing (incluyendo nuestro Spear Phishing Engine patentado)**.

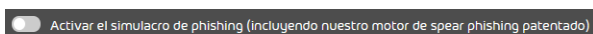


Figura 122: Activar el simulacro de phishing

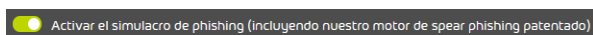


Figura 123: Desactivar el simulacro de phishing



- ➔ El simulacro de phishing se activa o desactiva.

Si el simulacro de phishing se ha activado, el interruptor se pondrá verde. Los ajustes de la pestaña se habilitan.

Si el simulacro de phishing se ha desactivado, el interruptor se pondrá gris. Los ajustes de la pestaña se bloquean.

- ✓ Se ha activado o desactivado el simulacro de phishing.

**Nota:**

Si el Awareness Engine está activado, el primer tutorial estará disponible para todos los usuarios desde el principio. Los demás tutoriales solo estarán disponibles después del inicio del simulacro de phishing. Es recomendable iniciar el simulacro de phishing dos semanas después del comienzo de la formación online.

Activar o desactivar los tutoriales



- ✓ Ha activado Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77).

En el módulo **Security Awareness Service > Configuración** puede activar y desactivar los tutoriales de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). Si los tutoriales están activados, se irán asignando paulatinamente tutoriales a los usuarios del cliente. Los tutoriales forman a los usuarios sobre temas de seguridad informática. Los tutoriales se proporcionan a cada usuario en su User Panel personal.

**Nota:**

Por defecto, al activar Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77), los tutoriales también se activan.

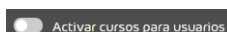
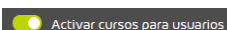
**Nota:**

Por defecto, los tutoriales son asignados automáticamente a los usuarios mediante nuestro Awareness Engine. Sin embargo, los administradores pueden desactivar el Awareness Engine y asignar los tutoriales manualmente a grupos de usuarios (véase [Configurar los tutoriales](#) en la página 200).

**Nota:**

En función del tiempo transcurrido tras el último tutorial de cada usuario, se calcula un KPI de formación (véase [Progreso de formación](#) en la página 116). El KPI de formación informa sobre el nivel de conocimientos de seguridad informática que tienen los usuarios de la organización.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar o desactivar los tutoriales.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. Accione el interruptor **Activar tutoriales para usuarios**.

**Figura 124: Activar tutoriales****Figura 125: Desactivar tutoriales**

Los tutoriales se activan o desactivan.

Si los tutoriales se han activado, el interruptor se pondrá verde. Los ajustes de la pestaña se habilitan.

Si los tutoriales se han desactivado, el interruptor se pondrá gris. Los ajustes de la pestaña se bloquean.



Se han activado o desactivado los tutoriales.



Nota:

Si el Awareness Engine está activado, el primer tutorial estará disponible para todos los usuarios desde el principio. Los demás tutoriales solo estarán disponibles después del inicio del simulacro de phishing. Es recomendable iniciar el simulacro de phishing dos semanas después del comienzo de la formación online.



Anuncio interno de Security Awareness Service

Recomendamos informar a los usuarios del cliente por adelantado acerca de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) por correo electrónico.

Fecha de último anuncio interno

El anuncio debería enviarse a los usuarios aproximadamente una semana antes del inicio del proyecto. De este modo, hay suficiente tiempo entre el anuncio y el envío de los primeros correos de phishing a los usuarios como para que éstos ya no estén pensando en el simulacro de phishing cada día. De este modo, es más fácil que los usuarios caigan en los ataques de phishing simulados.

¿Qué ocurre si no se realiza un anuncio interno?

Los usuarios no están informados acerca del proyecto, lo que puede provocarles descontento por sentirse engañados y controlados. Por otra parte, es posible que, por curiosidad, los usuarios empiecen a hacer clic en los enlaces de los correos a pesar de haberlos identificado como intentos de phishing, falseando así los resultados. Es posible que los empleados ignoren las invitaciones a los tutoriales si no se les ha informado previamente. La siguiente imagen es un ejemplo de una posible invitación a los tutoriales que pueden recibir los usuarios.

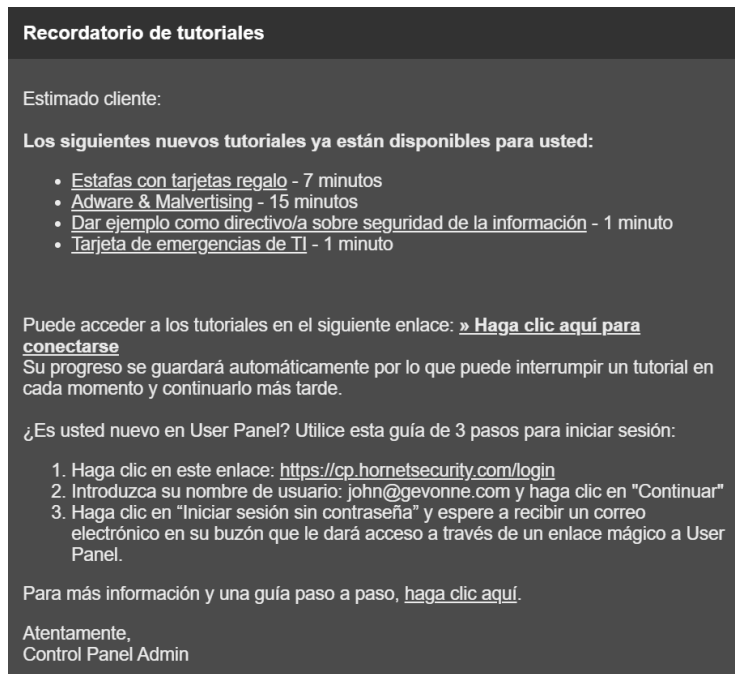


Figura 126: Ejemplo de un correo de recordatorio para los tutoriales

Plantilla para el anuncio interno

La plantilla de abajo puede emplearse para el anuncio interno. Por supuesto, el responsable del proyecto de la organización del cliente puede decidir libremente hasta qué punto modifica la plantilla.

Estimados compañeros:

Garantizar la seguridad informática es cada vez más complicado para las empresas. Mientras que los principales peligros para los usuarios privados derivan del uso de software obsoleto y del spam, las empresas tienen que lidiar a diario con la "negligencia digital" y las malas prácticas que ésta provoca.

Hemos decidido, en colaboración con Hornetsecurity GmbH, realizar un programa de concienciación en seguridad mediante Security Awareness Service, y para ello necesitamos su colaboración. En el contexto de un simulacro de phishing, se enviarán a los usuarios participantes correos que simularán ataques de phishing actuales y tendrán el objetivo de provocar actuaciones incorrectas como la apertura de enlaces o archivos adjuntos. La formación funciona del siguiente modo: si un usuario hace clic en un enlace potencialmente peligroso, lo dirigimos a una página interactiva con explicaciones. Allí se le muestra cómo habría podido detectar que se trataba de un correo falso.



En el contexto del simulacro también se envían correos en nombre de compañeros o compañeras de trabajo. Por tanto, es posible que usted también aparezca como remitente de un falso correo de phishing. Si lo desea, tiene la opción de impedirlo en el User Panel (<https://cp.hornetsecurity.com/usersettings/settings>).

Los datos obtenidos en el contexto de la formación se evalúan de modo anónimo y agrupado, de modo que no sea posible deducir nada sobre su comportamiento de clics individual. Una vez realizada la evaluación, se elimina toda referencia a los usuarios.

¡Muchas gracias por su colaboración!



Características de los correos de phishing simulado

Los correos de phishing simulado de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) poseen determinadas características que permiten a los clientes identificarlos.

Todos los correos de phishing simulado de Security Awareness Service tienen una firma DKIM. La firma DKIM contiene el dominio **sas.cloud-security.net**. Para comprobar si un correo forma parte del simulacro de phishing, los clientes pueden consultar el encabezado de un correo y comprobar si contiene una firma DKIM con dicho dominio.

Alternativamente, los clientes que no utilicen nuestro servicio Spam and Malware Protection pueden distinguir los correos de phishing simulado por las direcciones IP desde donde se envían. Los correos de phishing simulado se envían desde las direcciones IP **94.100.136.58** y **94.100.132.73**. Por tanto, los clientes que no utilicen nuestro servicio Spam and Malware Protection pueden buscar correos de phishing simulado en Microsoft 365 mediante el seguimiento de mensajes (véase [Buscar correos de phishing simulado en Microsoft 365](#) en la página 89).



IMPORTANTE:

Los clientes con Spam and Malware Protection no pueden distinguir los correos de phishing simulado por sus direcciones IP, pues todos sus correos entrantes (y no solo los correos de phishing simulado) se envían a través de nuestra infraestructura. Por tanto, todos los correos entrantes de estos clientes se envían desde las siguientes direcciones IP:

- **83.246.65.0/24**
- **94.100.128.0/20**
- **185.140.204.0/22**
- **173.45.18.0/24**
- **173.124.136.160/27**



Buscar correos de phishing simulado en Microsoft 365



✓ Su organización tiene un inquilino de Microsoft 365. Ha activado el simulacro de phishing de Security Awareness Service (véase [Activar o desactivar el simulacro de phishing](#) en la página 79). Su organización no utiliza nuestro servicio Spam and Malware Protection.

Con el seguimiento de mensajes de Microsoft 365 puede usted buscar correos de phishing simulado de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). El seguimiento de mensajes le permite descargar un informe en el que se indican los correos de phishing simulado.



Nota:

Este procedimiento solo es viable para clientes sin nuestro servicio Spam and Malware Protection, ya que la búsqueda se basa en las direcciones IP desde las cuales se envían los correos de phishing simulado.

Como todos los correos de los clientes Spam and Malware Protection se dirigen a través de nuestra infraestructura, todos sus correos entrantes (y no solo los correos de phishing simulado) se envían desde nuestras direcciones IP. Por tanto, en tal caso no es posible buscar correos de phishing simulado de modo individual con el seguimiento de mensajes.

1. Abra la página web <https://admin.exchange.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Flujo de correo > Seguimiento de mensajes**.

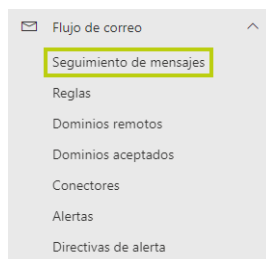


Figura 127: Abrir el seguimiento de mensajes

4. Haga clic en **Iniciar un seguimiento**.

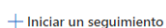


Figura 128: Iniciar el seguimiento de mensajes



- ➔ Se abre la pantalla **Nuevo seguimiento de mensajes**.
5. Introduzca el dominio del cliente según el patrón ***@dominiodecliente.tld** en el campo **Destinatarios** y haga clic en la recomendación mostrada.

Figura 129: Introducir destinatario

6. En **Intervalo de tiempo**, seleccione el periodo en el que desee buscar correos de phishing simulado.

i **Nota:**

Las direcciones IP desde las que se envían los correos se guardan durante 10 días. Por tanto, lo lógico es seleccionar como mucho un periodo de los últimos 10 días.

Figura 130: Seleccionar un periodo

7.

! **IMPORTANTE:**

Los correos de phishing simulado se envían desde las direcciones IP **94.100.136.58** y **94.100.132.73**. Sin embargo, no es posible definir un único seguimiento de mensajes que busque correos enviados desde las dos direcciones IP. Para buscar correos de phishing simulados enviados desde ambas direcciones IP, cree dos seguimientos de mensajes, uno para cada una de ellas.

Introduzca una de las siguientes direcciones en el campo **Dirección IP de cliente original**:

- **94.100.136.58**
- **94.100.132.73**

Figura 131: Introducir dirección IP



8. Seleccione la opción **Informe de resumen mejorado** en **Tipo de informe**.

**Nota:**

Este tipo de informe basta para obtener un listado de los correos de phishing simulado.

Tipo de informe

Todos los informes incluyen información esencial con la creación de informes más detallados en el informe mejorado y ampliado, que solo son descargables.

- ☐ Informe de resumen
Acceso en línea instantáneo ⓘ
- ☒ Informe de resumen mejorado
Solo archivo CSV descargable ⓘ
- ☐ Informe ampliado
Solo archivo CSV descargable ⓘ

Figura 132: Seleccionar el tipo de informe

9. Haga clic en **Siguiente**.



Se muestra la página **Preparar informe de seguimiento de mensajes**.

Preparar informe de seguimiento de mensajes

Prepararemos el informe y le avisaremos cuando esté listo.

Tipo de informe Informe de resumen mejorado	Intervalo de tiempo Los últimos 10 días
Remitentes Todo	Destinatarios *@gevonne.com
Estado de entrega Todas	Dirección Todas
Id. del mensaje Ninguno	Dirección IP de cliente original 94.100.136.58

Título del informe

Informe de seguimiento de mensajes (2023-05-04T07:45:12.504Z)

Quando el informe esté listo para descargarlo, se enviará una notificación al siguiente correo electrónico. *

admin@n08n.onmicrosoft.com

Figura 133: Preparación del informe

10. Opcional: Modifique el título del informe en el campo **Título del informe**.
11. Opcional: Si desea que se notifique a otro usuario del inquilino de Microsoft 365 en su lugar una vez el informe esté listo para descargar, introduzca la dirección de correo electrónico de dicho usuario en el campo **Quando el informe esté listo para descargarlo, se enviará una notificación al siguiente correo electrónico..**
12. Haga clic en **Preparar informe**.



- ➔ La orden de creación del informe se envía. El informe puede tardar algún tiempo en crearse. En cuanto el informe esté disponible, se enviará una notificación por correo electrónico. El informe puede descargarse en la pestaña **Informes descargables**.

Su solicitud se ha enviado

Puede comprobar el progreso en cualquier momento desde la sección "Informes descargables" desde la página principal de Seguimiento de mensajes.

Título del informe

Informe de seguimiento de mensajes (2023-05-04T07:45:12.504Z)

Tipo de informe

Informe de resumen mejorado

Cuando el informe esté listo para descargarlo, se enviará una notificación al siguiente correo electrónico.

admin@n08n.onmicrosoft.com

Figura 134: Orden de creación del informe

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

- ➔ La página se cierra.

14. Una vez el informe esté disponible, descárguelo desde la pestaña **Informes descargables**.

- ✔ Se ha creado un informe sobre correos de phishing simulado mediante el seguimiento de mensajes.



Estadística

El módulo **Security Awareness Service > Estadísticas** contiene estadísticas sobre Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) para un cliente. Hay estadísticas sobre los siguientes temas y cada uno tiene su propia pestaña:

- ESI[®] (véase [Estadísticas del ESI[®]](#) en la página 104)
- Simulacro de phishing (véase [Estadísticas del simulacro de phishing](#) en la página 107)
- Tutoriales (véase [Estadísticas de formación](#) en la página 116)
- Grupos (véase [Estadísticas de grupos](#) en la página 119)

Los administradores a nivel de cliente pueden filtrar los datos mostrados en el módulo **Estadísticas** por grupos específicos. En tal caso, el módulo **Estadísticas** solo muestra las estadísticas relacionadas con los grupos seleccionados (véase [Filtro de grupos](#) en la página 95).

Los administradores a nivel de cliente pueden seleccionar en cada pestaña un periodo de visualización para las estadísticas (véase [Seleccionar el periodo de visualización](#) en la página 100).

**Nota:**

Mientras Security Awareness Service aún esté sin activar, en el módulo **Estadísticas** se mostrarán datos de muestra para que los clientes puedan ver cómo se evalúan los datos. En la parte superior del módulo se incluirá una indicación sobre el uso de datos de muestra.



Figura 135: Información sobre los datos de muestra

**Nota:**

La estadística se actualiza cada 24 horas. Por tanto, los eventos de un día solo se tienen en cuenta en la estadística a partir del día siguiente.

Las estadísticas se calculan sobre la base de los usuarios incluidos actualmente en Security Awareness Service. Por tanto, las estadísticas se actualizarán cuando un usuario se excluya de Security Awareness Service o se elimine.



La cantidad de correos sospechosos marcados por los usuarios del cliente se muestra en la parte superior de todas las pestañas. Esta cantidad se refiere al periodo de visualización seleccionado. Este valor indica el grado de concienciación de seguridad en la organización del cliente.

Correos posiblemente peligrosos que los usuarios han marcado: 203

Figura 136: Cantidad de correos marcados

Los administradores a nivel de cliente pueden exportar los datos del módulo **Estadísticas** en formato CSV (véase [Exportar estadísticas en formato CSV](#) en la página 102). Es posible elegir una o varias de las siguientes opciones de exportación:

- **Resultados para toda la organización**
- **Resultados de grupos**
- **Resultados de usuarios**
- **Resultados de los temas de phishing**



Nota:

Si el modo de privacidad está activado (véase [Modo de privacidad](#) en la página 160), algunas opciones de exportación no están disponibles. Los siguientes ejemplos muestran cómo el modo de privacidad y los filtros de grupos afectan a las exportaciones:

Ejemplo 1: Si el modo de privacidad está activado y no se ha establecido ningún filtro de grupos, los resultados de los usuarios no se pueden exportar en formato CSV.

Ejemplo 2: Si el modo de privacidad está activado y no se ha establecido ningún filtro de grupos, los resultados de los grupos con menos de diez miembros no se pueden exportar en formato CSV.

Ejemplo 3: Si el modo de privacidad está desactivado y se ha establecido un filtro de grupos, los resultados de toda la organización no se pueden exportar en formato CSV.

Ejemplo 4: Si el modo de privacidad está activado y se ha establecido un filtro de grupos, solo se pueden exportar en formato CSV los resultados de los grupos con diez o más miembros.

Los administradores a nivel de cliente pueden programar informes mensuales automatizados (véase [Programar informes mensuales automatizados](#) en la página 124). Pueden configurar uno o más buzones de correo en Control Panel como destinatarios de los informes. También se pueden añadir buzones de correo externos como destinatarios. Los informes mensuales se envían el primer día de cada mes. Cada informe contiene los siguientes archivos:



- Un archivo ZIP con los resultados de toda la organización del mes anterior.
- Un archivo ZIP con los resultados de los grupos del mes anterior.
- Un archivo ZIP con los resultados de los usuarios del mes anterior.

Todos los informes incluyen un sello de tiempo.

**Nota:**

El informe mensual incluye un archivo ZIP con los resultados de los usuarios solo si el modo de privacidad está desactivado (véase [Modo de privacidad](#) en la página 160).

Filtro de grupos

En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93), los administradores pueden optar por mostrar las estadísticas de uno o varios grupos (véase [Filtrar por grupos](#) en la página 95).

Si los administradores seleccionan uno o varios grupos, las pestañas **ESI@**, **Phishing**, **Formación online** y **Grupos** solo muestran las estadísticas relacionadas con los grupos seleccionados.

Además, los administradores pueden crear configuraciones de filtro para guardar combinaciones específicas de grupos (véase [Crear una configuración de filtro](#) en la página 97). Después de crear una configuración de filtro, los administradores pueden aplicarla en cualquier momento (véase [Cargar una configuración de filtro](#) en la página 98).

Los administradores también pueden eliminar las configuraciones de filtro que ya no necesiten (véase [Eliminar una configuración de filtro](#) en la página 99).

Filtrar por grupos

En el módulo **Security Awareness Service > Estadísticas** puede filtrar las estadísticas por grupos específicos para mostrar solo los datos relacionados con los grupos seleccionados.

En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) puede filtrar las estadísticas por grupos específicos (véase [Filtro de grupos](#) en la página 95) para mostrar solo los datos relacionados con los grupos seleccionados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos datos desee ver.



3. Vaya a **Security Awareness Service > Estadísticas**.
4. Opcional: Para mostrar los datos de un rango de fechas específico, seleccione un periodo de visualización (véase [Seleccionar el periodo de visualización](#) en la página 100).
5. Haga clic en la barra de búsqueda en la parte superior de la página.

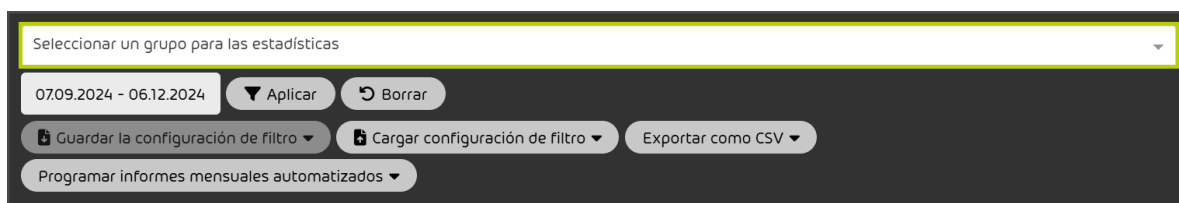


Figura 137: Hacer clic en la barra de búsqueda

- ➔ Se abre un menú desplegable con todos los grupos disponibles.

6. Seleccione uno o varios grupos haciendo clic en sus nombres.

i Nota:

Los grupos con menos de 10 miembros se muestran con el fondo rojo. Los datos de estos grupos se excluirán de las estadísticas si el modo de privacidad (véase [Modo de privacidad](#) en la página 160) está activado.

7. Opcional: Para quitar un grupo de la selección, haga clic en el icono x situado a la izquierda del nombre del grupo en la barra de búsqueda.

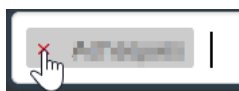


Figura 138: Quitar un grupo

8. Opcional: Para quitar todos los grupos seleccionados a la vez, haga clic en **Borrar**.
9. Haga clic en **Aplicar**.

- ➔ Las estadísticas se filtran en función de los grupos seleccionados.

- ✓ Las estadísticas se han filtrado por grupos específicos.

A continuación puede crear configuraciones de filtro (véase [Crear una configuración de filtro](#) en la página 97) o aplicar configuraciones de filtro existentes (véase [Cargar una configuración de filtro](#) en la página 98).



Crear una configuración de filtro

En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) puede crear una configuración de filtro (véase [Filtro de grupos](#) en la página 95) para facilitar la búsqueda de una combinación específica de grupos en el futuro.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos datos desee ver.
3. Vaya a **Security Awareness Service > Estadísticas**.
4. Haga clic en la barra de búsqueda en la parte superior de la página.

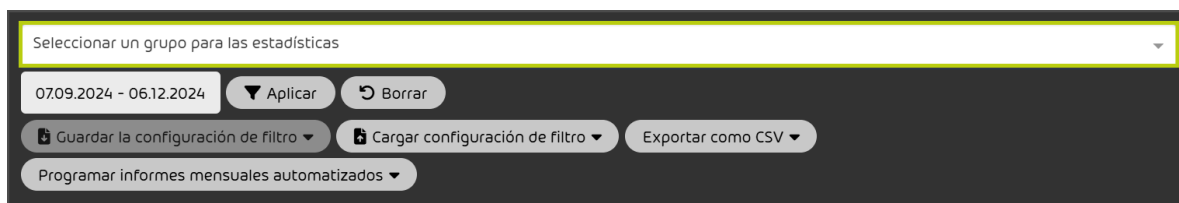


Figura 139: Hacer clic en la barra de búsqueda

- ➔ Se abre un menú desplegable con todos los grupos disponibles.
5. Seleccione uno o varios grupos haciendo clic en sus nombres.

Nota:

Los grupos con menos de 10 miembros se muestran con el fondo rojo. Los datos de estos grupos se excluirán de las estadísticas si el modo de privacidad (véase [Modo de privacidad](#) en la página 160) está activado.

6. Opcional: Para quitar un grupo de la selección, haga clic en el icono x situado a la izquierda del nombre del grupo en la barra de búsqueda.

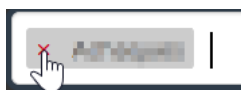


Figura 140: Quitar un grupo

7. Opcional: Para quitar todos los grupos seleccionados a la vez, haga clic en **Borrar**.
 8. Haga clic en **Aplicar**.
- ➔ Las estadísticas se filtran en función de los grupos seleccionados.



9. Haga clic en **Guardar la configuración de filtro**.

➔ Se abre una vista avanzada.

10. Introduzca un nombre para la configuración de filtro en el campo **Nombre de la configuración de filtro**.

**Nota:**

El nombre puede ser cualquier combinación de letras mayúsculas y minúsculas, números, espacios y caracteres especiales.

11. Haga clic en **Confirmar**.

**Nota:**

Si el nombre que ha introducido en el campo **Nombre de la configuración de filtro** ya es utilizado por un filtro existente, se muestra una ventana emergente preguntándole si desea actualizar el filtro existente con las nuevas opciones.

Si desea continuar con la actualización del filtro existente, haga clic en **Confirmar y sobrescribir**.

Si desea conservar el filtro existente y crear un nuevo filtro en su lugar, haga clic en **Cancelar y renombrar**, cambie el nombre del nuevo filtro y vuelva a hacer clic en **Confirmar**.

➔ La configuración de filtro se guarda.

✓ Se ha creado una configuración de filtro.

A continuación puede cargar una configuración de filtro creada (véase [Cargar una configuración de filtro](#) en la página 98).

Cargar una configuración de filtro

En el módulo **Security Awareness Service > Estadísticas** puede cargar una configuración de filtro creada previamente.



✓ Ha creado una configuración de filtro (véase [Crear una configuración de filtro](#) en la página 97).



En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) puede cargar una configuración de filtro creada previamente. Después de cargar una configuración de filtro, solo se muestran en las estadísticas los datos relacionados con dicha configuración de filtro.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
 2. En la selección de ámbitos, seleccione el dominio cuyos datos desee ver.
 3. Vaya a **Security Awareness Service > Estadísticas**.
 4. Haga clic en **Cargar configuración de filtro**.
 - ➔ Se abre una vista avanzada.
 5. Haga clic en el campo **Buscar configuración**.
 - ➔ Se abre un menú desplegable con todas las configuraciones de filtro existentes (véase [Crear una configuración de filtro](#) en la página 97).
 6. Seleccione una configuración de filtro en el menú desplegable.
 7. Haga clic en **Confirmar**.
 - ➔ Los grupos incluidos en la configuración de filtro se muestran en la barra de búsqueda en la parte superior de la página.
 8. Haga clic en **Aplicar**.
 - ➔ Las estadísticas se filtran en función de los grupos seleccionados.
- ✔ Se ha cargado y aplicado una configuración de filtro.

Eliminar una configuración de filtro

- ✔ Ha creado una configuración de filtro (véase [Crear una configuración de filtro](#) en la página 97).

En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) puede eliminar una configuración de filtro (véase [Crear una configuración de filtro](#) en la página 97) que ya no necesite.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuya configuración de filtro desee eliminar.
3. Vaya a **Security Awareness Service > Estadísticas**.



4. Haga clic en **Cargar configuración de filtro**.

➔ Se abre una vista avanzada.

5. Haga clic en el campo **Buscar configuración**.

➔ Se abre un menú desplegable con todas las configuraciones de filtro existentes (véase [Crear una configuración de filtro](#) en la página 97).

6. Haga clic en el icono x situado junto a la configuración de filtro que desee eliminar.



Figura 141: Eliminar una configuración de filtro

➔ Se muestra una ventana de confirmación.



Figura 142: Ventana de confirmación

7. Haga clic en **Confirmar**.

➔ La configuración de filtro se elimina.

✓ Se ha eliminado una configuración de filtro.

Seleccionar el periodo de visualización

✓ En el módulo **Security Awareness Service > Estadísticas** se muestran datos reales del cliente en lugar de datos de muestra.

En el módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) puede usted seleccionar el periodo de visualización de las estadísticas.

**Nota:**

Por defecto se muestran los datos de los últimos 12 meses.

**Nota:**

Solo es posible seleccionar un periodo de visualización si hay suficientes datos del cliente para que se muestren datos reales en lugar de datos de muestra en el módulo **Security Awareness Service > Estadísticas**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos datos desee ver.
3. Vaya a **Security Awareness Service > Estadísticas**.
4. Seleccione la pestaña cuyas estadísticas desee ver. Tiene las siguientes opciones:
 - ESI®
 - Phishing
 - Formación online
 - Grupos
5. Haga clic en el periodo de visualización en la esquina superior derecha de la página.

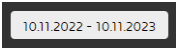


Figura 143: Hacer clic en el periodo de visualización



Se abre un calendario.

6. Seleccione un periodo de visualización del calendario haciendo clic en una fecha de inicio primero y en una fecha de finalización después.

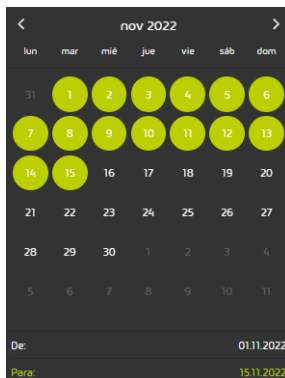


Figura 144: Seleccionar un periodo

- ➔ En la pestaña solo se seleccionan los datos del periodo de visualización seleccionado. A la izquierda del botón del periodo de visualización se muestra el botón adicional **Borrar**.



Nota:

Al hacer clic en el botón **Borrar**, el periodo de visualización seleccionado se restablece a los últimos 12 meses.

7. Haga clic fuera del calendario.



- El calendario se cierra.



- Se ha seleccionado el periodo de visualización de estadísticas.

Exportar estadísticas en formato CSV

En el módulo **Security Awareness Service > Estadísticas** puede exportar datos estadísticos en formato CSV.

**Nota:**

Si el modo de privacidad está activado (véase [Modo de privacidad](#) en la página 160), algunas opciones de exportación no están disponibles. Los siguientes ejemplos muestran cómo el modo de privacidad y los filtros de grupos afectan a las exportaciones:

Ejemplo 1: Si el modo de privacidad está activado y no se ha establecido ningún filtro de grupos, los resultados de los usuarios no se pueden exportar en formato CSV.

Ejemplo 2: Si el modo de privacidad está activado y no se ha establecido ningún filtro de grupos, los resultados de los grupos con menos de diez miembros no se pueden exportar en formato CSV.

Ejemplo 3: Si el modo de privacidad está desactivado y se ha establecido un filtro de grupos, los resultados de toda la organización no se pueden exportar en formato CSV.

Ejemplo 4: Si el modo de privacidad está activado y se ha establecido un filtro de grupos, solo se pueden exportar en formato CSV los resultados de los grupos con diez o más miembros.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos datos desee administrar.
3. Vaya a **Security Awareness Service > Estadísticas**.
4. Opcional: Para exportar los datos de un grupo específico, aplique filtros de grupos antes de continuar. Para más información, véase [Filtrar por grupos](#) en la página 95.
5. Haga clic en el botón **Exportar como CSV** en la parte superior de la página.

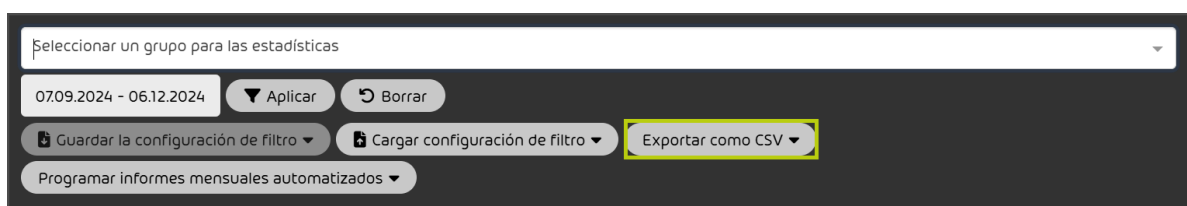


Figura 145: Botón Exportar como CSV



Se abre el menú **Exportación de datos**.

6. Seleccione los datos que desee exportar marcando las casillas correspondientes. Están disponibles las siguientes opciones:
 - **Resultados para toda la organización**



- Resultados de grupos
- Resultados de usuarios
- Resultados de los temas de phishing

**Nota:**

Puede seleccionar varias opciones a la vez.

7. Haga clic en **Confirmar** para generar el archivo CSV.



Los datos del módulo **Estadísticas** se han exportado en formato CSV.

Estadísticas del ESI®

La pestaña **ESI®** del módulo **Security Awareness Service > Estadísticas** (véase [Estadística](#) en la página 93) contiene estadísticas sobre el Employee Security Index (ESI®) (véase [Employee Security Index \(ESI®\)](#) en la página 8). Los datos de esta pestaña proporcionan información sobre la concienciación de seguridad de los usuarios de un cliente en materia de ataques de phishing.

La pestaña contiene las siguientes estadísticas:

- **Employee Security Index** (véase [Employee Security Index](#) en la página 104)
- **Cronología del Employee Security Index** (véase [Cronología del Employee Security Index](#) en la página 106)

Employee Security Index

En la estadística **Employee Security Index** de la pestaña **ESI®** (véase [Estadísticas del ESI®](#) en la página 104) del módulo **Security Awareness Service > Estadísticas** se muestra el ESI® medio actual, dividido en varios rangos dentro de un velocímetro. El ESI® (véase [Employee Security Index \(ESI®\)](#) en la página 8) se calcula tanto para la organización entera como los grupos de un cliente.

El ESI® se calcula sobre la base de los últimos 30 días. El ESI® se basa en la relación entre la cantidad de los correos del simulacro de phishing con éxito y la cantidad de todos los correos del simulacro de phishing enviados a los usuarios de la organización o del grupo. También se toma en cuenta el nivel de dificultad de los ataques de phishing simulados. De este modo, el ESI® disminuye más si los usuarios caen en ataques fácilmente identificables que si caen en ataques



más complejos. En cambio, los correos marcados del simulacro de phishing tienen una influencia positiva en el ESI[®]. Si los usuarios no interactúan con los correos electrónicos del simulacro de phishing, es decir, ni denuncian los correos ni abren un enlace o archivo adjunto, el ESI[®] también cambia de manera positiva. Sin embargo, el ESI[®] mejora aún más si los usuarios denuncian los correos del simulacro de phishing.

**Nota:**

Si se excluyen usuarios de Security Awareness Service, el ESI[®] del cliente se recalcula en función de los datos de los usuarios restantes. También se ajusta la evolución temporal del ESI[®].

**Nota:**

Es posible denunciar correos de phishing mediante el complemento Phishing Reporter (véase [Phishing Reporter](#) en la página 174) o mediante Hornetsecurity Outlook Add-in (véase [Sobre Hornetsecurity Outlook Add-in para clientes de 365 Total Protection](#)). Como alternativa, es posible marcar correos reenviándolos a una dirección de correo electrónico específica (véase [Marcado de correos sin complementos](#) en la página 197). Los clientes que no utilicen ninguno de estos métodos pueden alcanzar un valor de ESI[®] máximo de 90.

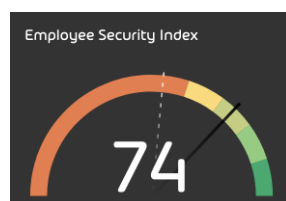


Figura 146: ESI[®] medio de la organización

El ESI[®] medio se divide en los siguientes rangos:

- ESI[®] 90 – 100 (verde): Muy buena media. Los usuarios casi nunca pican con correos de phishing.
- ESI[®] 80 – 90 (verde claro): Buena media. Los usuarios solo pican con correos de phishing muy sofisticados.
- ESI[®] 70 – 80 (verde lima): Media regular. Los usuarios pican con algunos correos de phishing.
- ESI[®] 60 – 70 (amarillo): Media insuficiente. Los usuarios pican con correos de phishing sencillos. Los usuarios deben ser formados para no suponer riesgo para la organización.



- ESI[®] inferior a 60 (naranja): Media mala. Los usuarios pican con correos de phishing muy sencillos. Es imprescindible formar a los usuarios para que no supongan riesgo para la organización.

**Nota:**

A continuación se indican las tasas de clics con las que un cliente de ejemplo alcanza diferentes valores de ESI[®]. El ejemplo se refiere a un cliente cuyos usuarios solo reciben correos de phishing simulados del nivel 1.

- Valor de ESI[®] ideal de 90: Este valor de ESI[®] se consigue hasta una tasa de clics de aproximadamente el 1 por ciento.
- Valor de ESI[®] de 50: Este valor de ESI[®] se consigue con una tasa de clics de aproximadamente el 5 hasta el 6 por ciento.
- Valor de ESI[®] más bajo de 0: Este valor de ESI[®] se consigue con una tasa de clics superior al 10 por ciento.

Bajo el velocímetro, el ESI[®] actual de la organización se compara con la media del sector indicado en **Security Awareness Service > Configuración** de la pestaña .



Figura 147: Información sobre el ESI[®]

Cronología del Employee Security Index

En la estadística **Cronología del Employee Security Index** de la pestaña ESI[®] (véase [Estadísticas del ESI[®]](#) en la página 104) del módulo **Security Awareness Service > Estadísticas** se muestra la evolución temporal del ESI[®]. La evolución se adapta al periodo de visualización seleccionado (véase [Seleccionar el periodo de visualización](#) en la página 100). El eje Y del sistema de coordenadas representa el ESI[®], y el eje X representa el tiempo. El diagrama muestra dos líneas. La línea superior muestra el ESI[®] medio de la organización mientras que la línea inferior muestra el ESI[®] del usuario más rezagado.

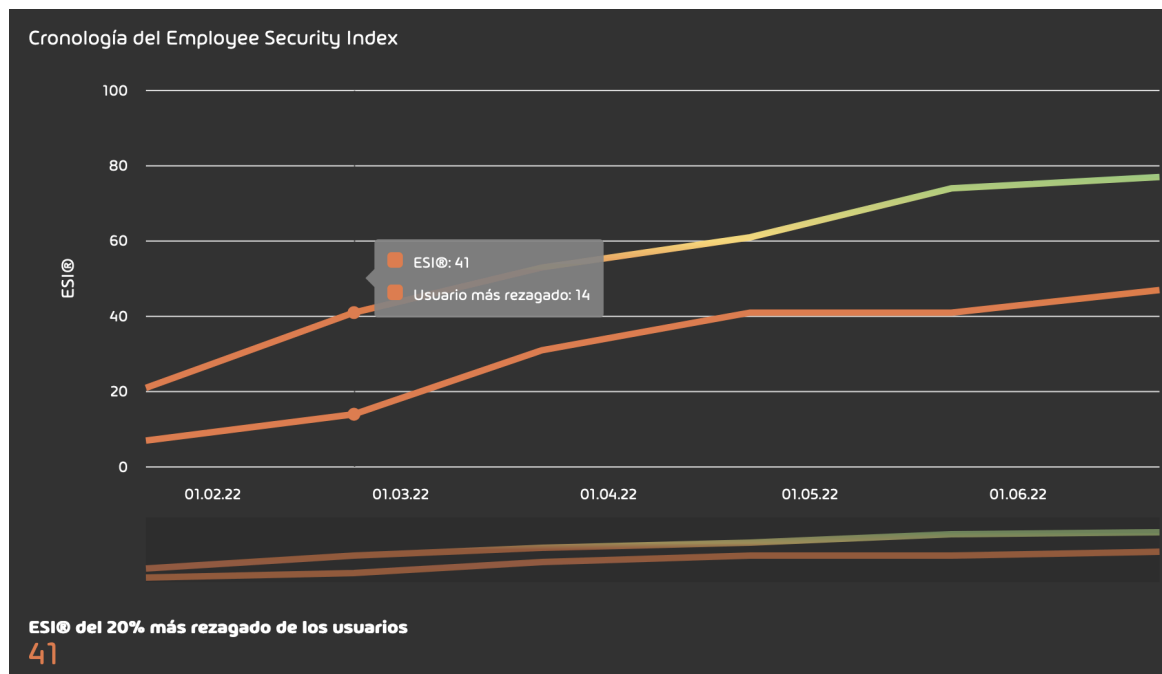


Figura 148: Evolución temporal del ESI® de la organización

Por debajo del sistema de coordenadas se muestran otra vez ambas líneas. Allí, los administradores pueden modificar el periodo de los datos mostrados dibujando un rectángulo con el puntero del ratón sobre las líneas.

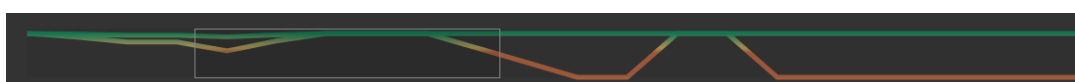


Figura 149: Selección del periodo de visualización en la gráfica inferior

Estadísticas del simulacro de phishing

La pestaña **Phishing** del módulo **Security Awareness Service** > **Estadísticas** (véase [Estadística](#) en la página 93) contiene estadísticas sobre el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). El número que aparece bajo **Correos posiblemente peligrosos que los usuarios han marcado**: en la parte superior de la página se refiere a todos los correos electrónicos marcados durante el periodo de tiempo seleccionado e incluye tanto correos electrónicos de phishing simulado como correos electrónicos regulares.

La pestaña contiene las siguientes estadísticas:



- **Simulacros de ataque** (véase [Ataques simulados](#) en la página 108)
- **Correos de phishing con éxito** (véase [Correos de phishing con éxito](#) en la página 109)
- **Niveles de usuarios** (véase [Niveles de usuarios](#) en la página 110)
- **Correos marcados** (véase [Correos marcados](#) en la página 113)
- **Trucos psicológicos** (véase [Trucos psicológicos](#) en la página 113)
- **Interacción de Teachable Moment** (véase [Interacción con el Teachable Moment](#) en la página 115)

Ataques simulados

El diagrama **Simulacros de ataque** de la pestaña **Phishing** (véase [Estadísticas del simulacro de phishing](#) en la página 107) del módulo **Security Awareness Service > Estadísticas** muestra la distribución de los correos del simulacro de phishing enviados en función de las acciones de los usuarios.

En el diagrama **Simulacros de ataque**, los correos de phishing enviados se dividen por las acciones con las que reaccionaron sus destinatarios. Los correos se dividen en las siguientes categorías:

- **Correos detectados:** Estos correos de phishing simulados fueron detectados como correos de phishing por los usuarios.
- **Clics en enlaces:** Estos correos de phishing simulados lograron que los usuarios hicieran clic en enlaces.
- **Datos de acceso introducidos:** Estos correos de phishing simulados lograron que los usuarios introdujeran datos de acceso en páginas web falsificadas.
- **Archivos abiertos:** Estos correos de phishing simulados lograron que los usuarios abrieran sus archivos adjuntos.
- **Macros ejecutadas:** Estos correos de phishing simulados lograron que los usuarios abrieran sus archivos adjuntos con macros.

El diagrama muestra el tiempo en el eje X y la cantidad de correos de phishing simulados enviados en el eje Y. Las acciones se muestran apiladas. Los correos se muestran en una tabla. Debajo del diagrama se muestra de nuevo la evolución de las líneas. Ahí es posible cambiar el periodo de los datos mostrados. Por debajo se muestran algunos datos del periodo de visualización seleccionado (véase [Seleccionar el periodo de visualización](#) en la página 100).

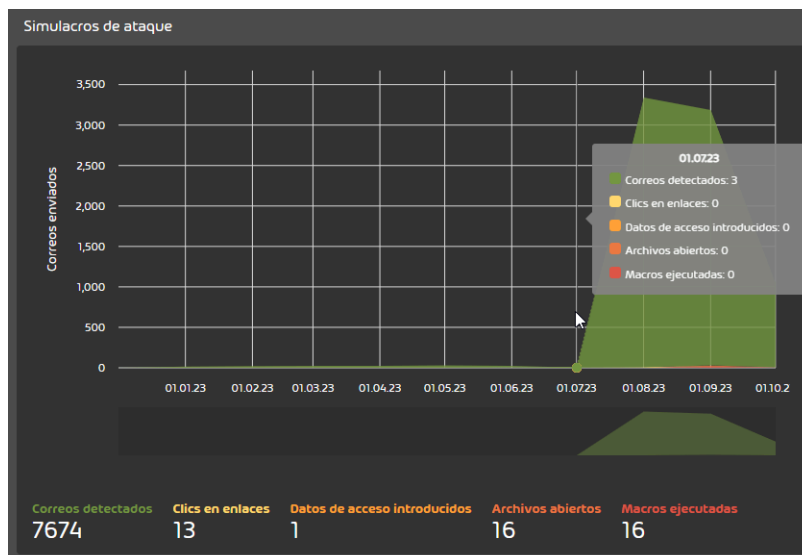


Figura 150: Simulacros de ataque

**Nota:**

Al colocar el puntero del ratón sobre un punto del diagrama, se muestran una fecha y las estadísticas correspondientes. En esta fecha se resumen todos los ataques simulados del mes anterior. Los datos del diagrama se refieren siempre a un mes entero y empiezan el día 1 del mes.

Ejemplo: En la figura anterior se muestra la fecha 1 de julio de 2023. Esto significa que se detectó un total de tres ataques simulados durante el periodo del 1 de junio hasta el 1 de julio de 2023.

Correos de phishing con éxito

La tabla **Correos de phishing con éxito** de la pestaña **Phishing** del módulo **Security Awareness Service > Estadísticas** muestra el éxito de determinados correos de phishing.



Correos de phishing con éxito

Asunto	Tasa de a...	Nivel	Cantidad	Enlaces	Datos de ...	Documen...	Macros
Korrektur der Steuerrückers...	20%	2	5	1	0	0	0
WeTransfer - shared files (n...	13%	2	8	1	0	0	0
Los datos en la papelera de...	13%	2	8	1	0	0	0
Encuesta online (nivel 2)	6%	2	16	1	0	0	0
Nueva declaración de prote...	4%	3	109	0	0	4	4
Migración a Outlook 2019 (...)	2%	1	116	2	1	0	0
Beschwerde eines erbosten...	1%	2	625	0	0	8	8
Nueva declaración de prote...	1%	3	86	0	0	1	1
Nueva declaración de prote...	1%	3	86	0	0	1	1
Genehmigung des Zugriffs ...	1%	1	115	1	0	0	0

1 / 10

¿Tiene una buena idea para un tema de phishing o ha recibido un correo de phishing bien hecho? Utilice este [formulario](#) para enviar ideas sobre temas de phishing realistas directamente al departamento de desarrollo de productos.

Figura 151: Correos de phishing con éxito

La tabla contiene las siguientes informaciones:

- **Asunto:** El asunto del correo de phishing enviado.
- **Tasa de aciertos:** Muestra en tanto por ciento lo exitoso que fue el correo de phishing.
- **Nivel:** Nivel que deben haber alcanzado los usuarios para recibir el correo de phishing.
- **Cantidad:** Indica cuántos correos de phishing se han enviado.
- **Enlaces:** Indica en cuántos enlaces han hecho clic los usuarios.
- **Datos de acceso:** Indica cuántas veces los usuarios han revelado sus datos de acceso debido al correo del simulacro de phishing.
- **Documentos:** Indica cuántas veces han abierto los usuarios documentos adjuntos del correo de phishing.
- **Macros:** Indica cuántas veces han ejecutado los usuarios macros en documentos adjuntos del correo de phishing.

Niveles de usuarios

El diagrama circular de la pestaña **Phishing** (véase [Estadísticas del simulacro de phishing](#) en la página 107) del módulo **Security Awareness Service > Estadísticas** muestra la distribución de los niveles de usuarios.



Los usuarios de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) se van dividiendo paulatinamente en 5 niveles según su rendimiento en el simulacro de phishing. Cuanto más alto sea el nivel de un usuario, más alto será el nivel de dificultad de los correos del simulacro de phishing que reciba (véase [Niveles del simulacro de phishing](#) en la página 111). En el diagrama circular, cada nivel tiene su propio color:

- Azul: Nivel 1
- Naranja: Nivel 2
- Rosa: Nivel 3
- Amarillo: Nivel 4
- Verde: Nivel 5

En el centro del diagrama circular se muestra el nivel medio de todos los usuarios del cliente. Bajo el diagrama circular se muestra la cantidad de los usuarios de cada nivel y el porcentaje de los usuarios de un nivel en relación con el total de los usuarios del cliente.

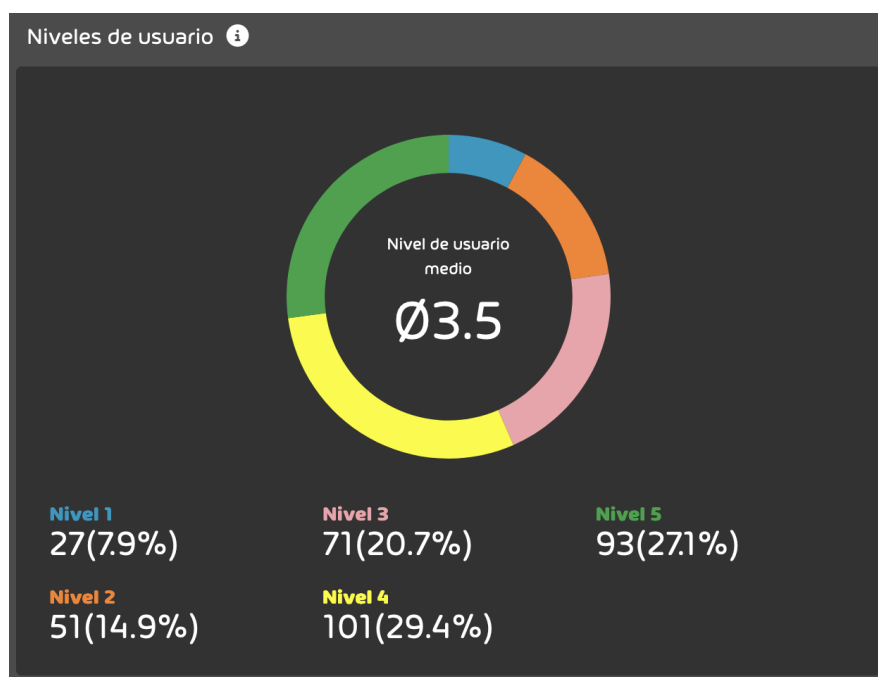


Figura 152: Niveles de usuarios

Niveles del simulacro de phishing

Los usuarios de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) se van dividiendo paulatinamente en 4 niveles según su rendimiento en el simulacro



de phishing. Cuanto más alto sea el nivel de un usuario, más alto será el nivel de dificultad de los correos del simulacro de phishing que reciba. A continuación se especifica cada nivel, empezando por el más fácil:

- Nivel 1:

Los correos electrónicos de phishing simulados de este nivel contienen phishing genérico y básico, como correos electrónicos de marcas conocidas. Estos correos electrónicos se envían a grandes grupos de usuarios para engañarlos y hacerles revelar información confidencial o sensible solicitándoles un inicio de sesión, el restablecimiento de la contraseña y mucho más. El dominio del remitente no es específico de la empresa ni del usuario.

- Nivel 2:

Los correos electrónicos de phishing simulado de este nivel contienen phishing dirigido, como los intentos de fraude al CEO. Estos correos electrónicos se hacen pasar por un usuario con un alto cargo o una autoridad dentro de la organización del usuario e instruyen a los empleados para que lleven a cabo actividades fraudulentas. A partir del nivel 2, los correos electrónicos de phishing simulado pueden incluir archivos adjuntos.

- Nivel 3:

Los correos electrónicos de phishing simulado de este nivel incluyen phishing dirigido con información pública de la empresa. Estos correos electrónicos van dirigidos a una persona o grupo específico. Los correos electrónicos de phishing simulado de nivel 3 contienen información que puede ser relevante para el usuario o la empresa. Los correos electrónicos de este nivel simulan proceder de un compañero directo y contienen información relacionada con el trabajo.

- Nivel 4:

Los correos electrónicos de phishing simulados de este nivel incluyen phishing específico de un departamento. Estos correos electrónicos se refieren directamente al puesto de trabajo individual del usuario y simulan proceder de compañeros o superiores directos.



Correos marcados



Nota:

El número que aparece bajo **Correos posiblemente peligrosos que los usuarios han marcado**: en la parte superior de la página se refiere a todos los correos electrónicos marcados durante el periodo de tiempo seleccionado e incluye tanto correos electrónicos de phishing simulado como correos electrónicos regulares.

En el diagrama circular **Correos marcados** de la pestaña **Phishing** (véase [Estadísticas del simulacro de phishing](#) en la página 107) del módulo **Security Awareness Service > Estadísticas** se muestra la relación entre los correos marcados y enviados.

El diagrama circular indica la cantidad de los correos del simulacro de phishing de Security Awareness Service que los usuarios han marcado y la cantidad de correos de phishing simulados que se han enviado a los usuarios.

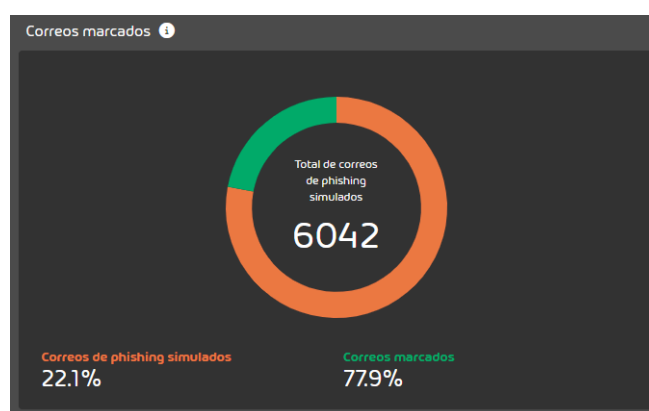


Figura 153: Correos marcados

Trucos psicológicos

En el diagrama **Trucos psicológicos** de la pestaña **Phishing** (véase [Estadísticas del simulacro de phishing](#) en la página 107) del módulo **Security Awareness Service > Estadísticas** se evalúa la conducta de los usuarios en respuesta a trucos psicológicos en los correos del simulacro de phishing.

Al colocar el puntero del ratón sobre un punto del diagrama, se indica en tanto por ciento cuántas veces los usuarios del cliente han caído en este truco.

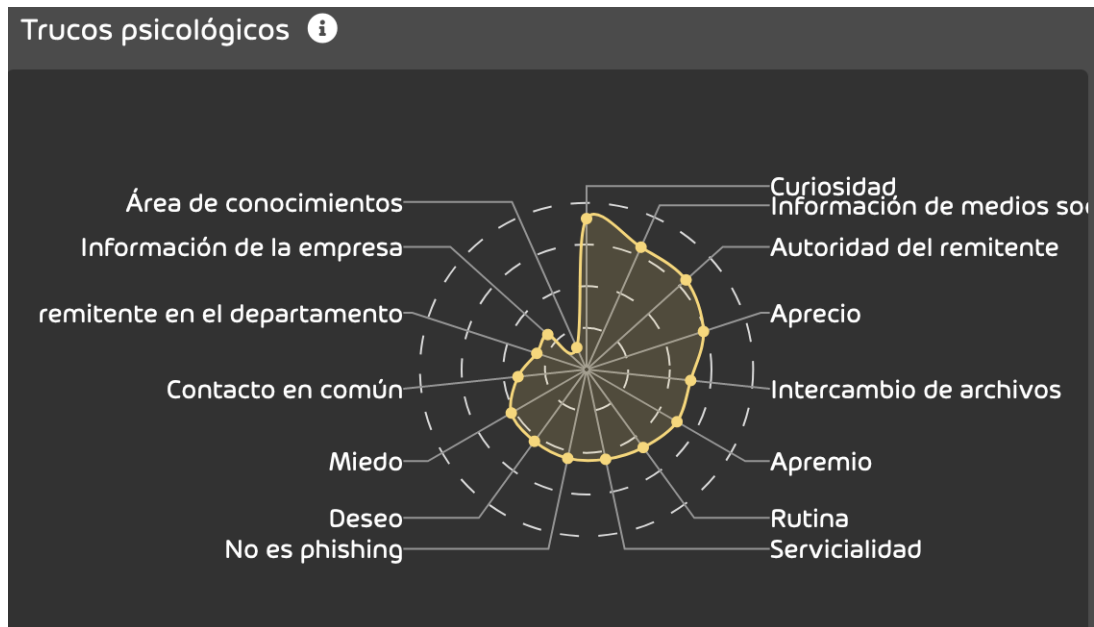


Figura 154: Trucos psicológicos

Clasificación de trucos psicológicos

Cuanto más elevados son los valores en la gráfica, más a menudo se logra hacer picar a los usuarios de la organización con estos trucos. A continuación se describen con más detalle los trucos empleados en los correos de phishing simulados.

- **Autoridad:** El correo de phishing simulado finge provenir de un organismo público.
- **Autoridad del remitente:** El correo de phishing simulado finge provenir de una persona que tiene autoridad sobre los usuarios.
- **Apremio:** El correo de phishing simulado provoca prisa en los usuarios.
- **Contacto en común:** El correo de phishing simulado finge provenir de un conocido.
- **Servicialidad:** El correo de phishing simulado pretende provocar compasión y apelar a la servicialidad de los usuarios.
- **Deseo:** El correo de phishing simulado provoca en los usuarios deseos por determinados objetos o por sentimientos como la aprobación.
- **Miedo:** El correo de phishing simulado provoca miedo en los usuarios.
- **Intercambio de archivos:** El correo de phishing simulado indica contener archivos que los usuarios quieren tener.



- **Área de competencias:** El correo de phishing simulado contiene información y consultas del área de especialización de los usuarios e intenta de este modo parecer legítimo y resultar creíble.
- **Rutina:** El correo de phishing simulado parece un mensaje estándar como aquéllos que suelen enviar determinados sistemas o servicios. Por tanto, los usuarios reaccionan a él de modo rutinario.
- **Aprecio:** El correo de phishing simulado intenta adular a los usuarios y provocar simpatía.
- **Autoridad del remitente en el departamento:** El correo de phishing simulado parece enviarse en nombre de la dirección del departamento. De este modo trata de llamar a la obediencia a los usuarios.
- **Información de medios sociales:** El correo de phishing simulado simula provenir de medios sociales y, de este modo, trata de obtener credibilidad.
- **No es phishing:** En el correo de phishing simulado está escrito que no es de spam o de phishing.
- **Información de la empresa:** El correo de phishing simulado contiene información interna sobre la organización (por ejemplo, respecto a ventajas para empleados o elementos de mobiliario).
- **Conocimiento sobre el sector:** El correo de phishing simulado contiene información específica de determinado sector y, de este modo, simula provenir de una fuente informada y legítima.

Interacción con el Teachable Moment

El diagrama circular **Interacción de Teachable Moment** en la pestaña **Phishing** (ver [Estadísticas del simulacro de phishing](#) en la página 107) del módulo **Security Awareness Service > Estadísticas** muestra cómo los usuarios han interactuado con el Teachable Moment.

La duración promedio de la interacción se muestra encima del diagrama circular **Interacción de Teachable Moment** y mide el tiempo promedio que tarda un usuario del grupo en interactuar con el Teachable Moment. El número total de Teachable Moments mostrados se muestra en el centro del diagrama circular **Interacción de Teachable Moment**.

El diagrama circular **Interacción de Teachable Moment** consta de tres colores. Cada color muestra el número absoluto de interacciones, así como el porcentaje correspondiente:

- **Sin interacción del usuario (Naranja):** Los usuarios no han interactuado con el Teachable Moment de ninguna manera.
 - **Interacción no completada (Azul):** Los usuarios han comenzado con el Teachable Moment, pero no lo han completado.
-



- **Amarillo: Interacción completada** (Amarillo): Los usuarios han completado el Teachable Moment.

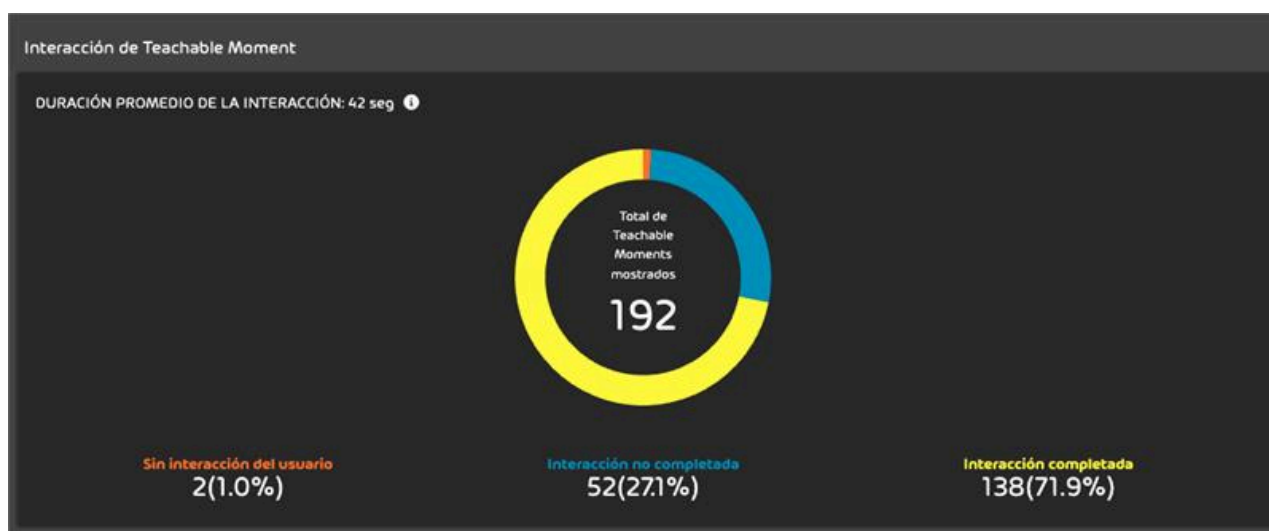


Figura 155: Interacción de Teachable Moment

Estadísticas de formación

Las estadísticas sobre los tutoriales se dividen en las siguientes secciones:

- **Progreso de formación** en la página 116: Este diagrama muestra cuántos tutoriales se han realizado y están en curso y cuántos aún no se han empezado.
- **Evolución de los usuarios en Single User Booster y Productivity Booster** en la página 117: Este diagrama muestra cuántos usuarios se encuentran en Booster Training y la evaluación temporal de los usuarios en formación de refuerzo.
- **Estado de formación de módulos y usuarios** en la página 118: Estas tablas muestran el progreso de la formación de grupos y usuarios individuales.

Progreso de formación

Progreso de la formación

En la esquina superior izquierda del módulo **Security Awareness Service > Estadísticas**, bajo la pestaña **Formación online**, se muestra un diagrama sobre el KPI de formación actual. El diagrama se divide en las tres áreas **Finalizado**, **Empezado** y **Sin empezar** cuyos porcentajes se indican



debajo del diagrama. Al colocar el ratón sobre el diagrama, se muestra la cantidad de los módulos de esta área.

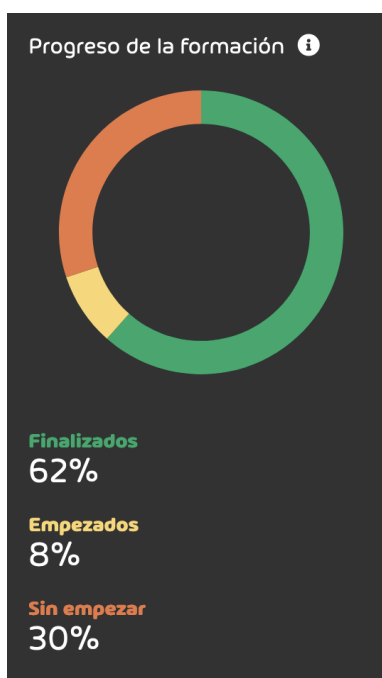


Figura 156: Diagrama del progreso de formación

Evolución de los usuarios en Single User Booster y Productivity Booster

En la pestaña **Formación online** del módulo **Security Awareness Service > Estadísticas** se muestra una estadística sobre la formación de refuerzo.

El diagrama muestra cuántos usuarios participan generalmente en la formación, cuántos usuarios participan en la formación de refuerzo y la evolución de los usuarios en formación de refuerzo a lo largo del tiempo.

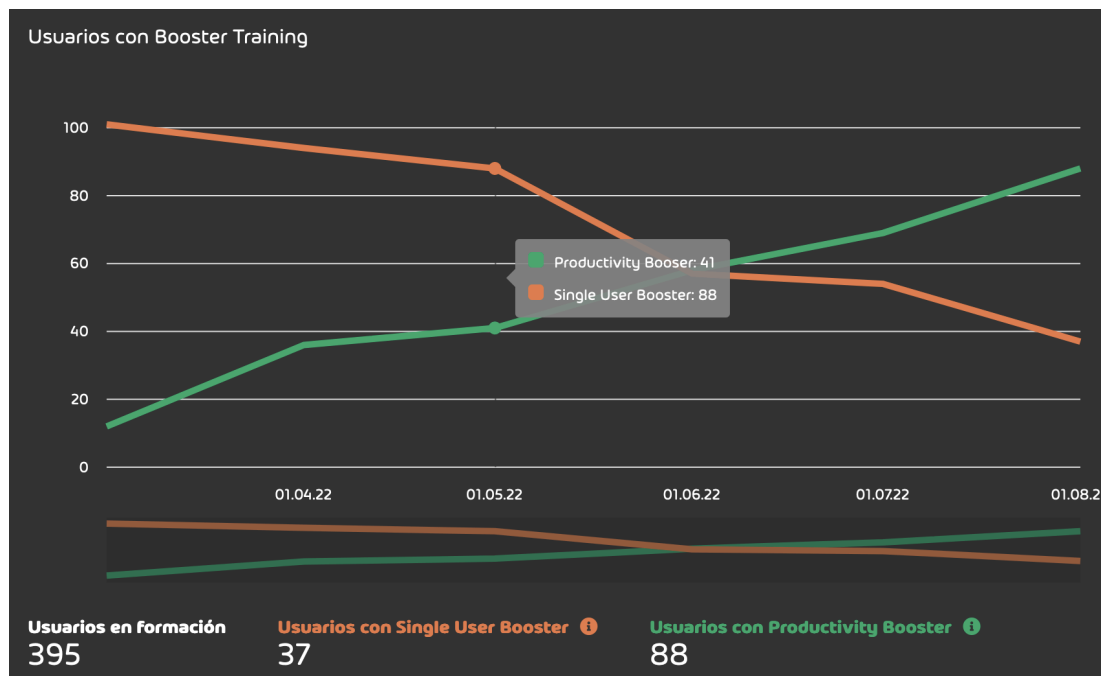


Figura 157: Usuarios en formación de refuerzo

Estado de formación de módulos y usuarios

Tabla sobre el estado de formación de los tutoriales

El estado de formación de todos los tutoriales disponibles se muestra en la pestaña **General** de la tabla sobre el estado de formación.

General		Usuarios
Módulo	Estado	
Estafas con tarjetas regalo		
Test rápido: Vishing		
Adware & Malvertising		
Test rápido: Informar de los incidentes de seguridad informática		

Figura 158: Tabla sobre el estado de formación de los tutoriales

Tabla sobre el estado de formación de los usuarios

En la pestaña **Usuarios** de la tabla sobre el estado de formación se muestran el progreso de usuarios individuales así como sus nombres, apellidos, direcciones de correo electrónico, tutoriales asignados y la fecha de la última asignación.



Nombre	Apellidos	Dirección de correo	Módulo	Fecha de última asign...
Thea	Tralisch	thea.tralisch@talitara.com		Sin asignar
Walter	Eiseit	walter.eiseit@talitara.com		Sin asignar

Figura 159: Tabla sobre el estado de formación de usuarios individuales

**NOTA:**

Al colocar el ratón sobre la barra de estado, se muestra la distribución exacta dentro de los tutoriales. La barra de estado se divide en las categorías **Finalizados**, **En curso**, **Sin empezar** y **Sin asignar**.

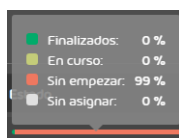


Figura 160: Vista detallada de la barra de estado

Estadísticas de grupos

ESI[®] medio de los grupos creados

En esta página se muestran datos y diagramas sobre el ESI[®] de los grupos creados.

Al lado izquierdo se muestra una selección de grupos con sus ESI[®] medios actuales. Los grupos aparecen ordenados por su ESI[®] medio de mayor a menor.

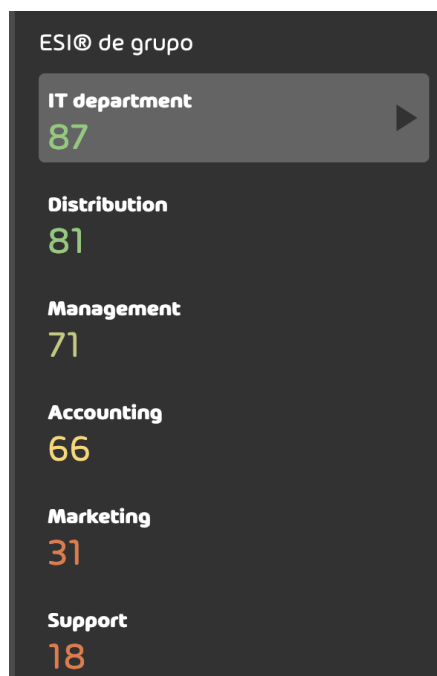


Figura 161: ESI® de grupos

Los grupos mostrados pueden seleccionarse con un clic. Al lado derecho se muestra la evolución temporal del ESI® del grupo seleccionado. Este diagrama es similar al diagrama sobre la evolución temporal del ESI® de la organización (véase [Employee Security Index](#) en la página 104), pero no incluye ninguna línea con los datos del usuario más rezagado.



Figura 162: Evolución temporal del ESI® del grupo seleccionado

Si el modo de privacidad se encuentra activado (véase [Modo de privacidad](#) en la página 160), el ESI® no se calcula ni se muestra para grupos con menos de 10 miembros. En lugar del ESI® medio actual a la izquierda y la evolución del ESI® a la derecha se muestra en ambos lados un aviso sobre el modo de privacidad.

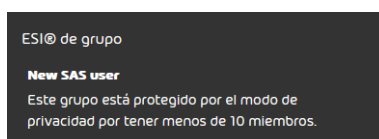


Figura 163: Grupos protegidos por el modo de privacidad

Distribución de niveles de grupos

Los diagramas y las tablas bajo **Distribución de niveles de grupos** en la pestaña **Grupos** del módulo **Security Awareness Service > Estadísticas** muestran la distribución de los niveles de usuarios en los grupos.

Los usuarios se van dividiendo paulatinamente en 5 niveles que permiten graduar la dificultad de los correos de phishing que se les envía. La distribución de los niveles de los usuarios se muestra con diferentes colores.



- Rojo: Nivel 1
- Naranja: Nivel 2
- Amarillo: Nivel 3
- Aceituna: Nivel 4
- Verde: Nivel 5

Bajo los diagramas circulares se indica el nombre del grupo correspondiente. Al colocar el ratón sobre el diagrama se muestra la cantidad de usuarios en el nivel seleccionado.

**Nota:**

Si el modo de privacidad se encuentra activado (véase [Modo de privacidad](#) en la página 160), la distribución de los niveles de usuarios no se muestra para grupos con menos de 10 miembros. En su lugar, el diagrama del grupo correspondiente muestra un mensaje acerca de que no hay datos suficientes.

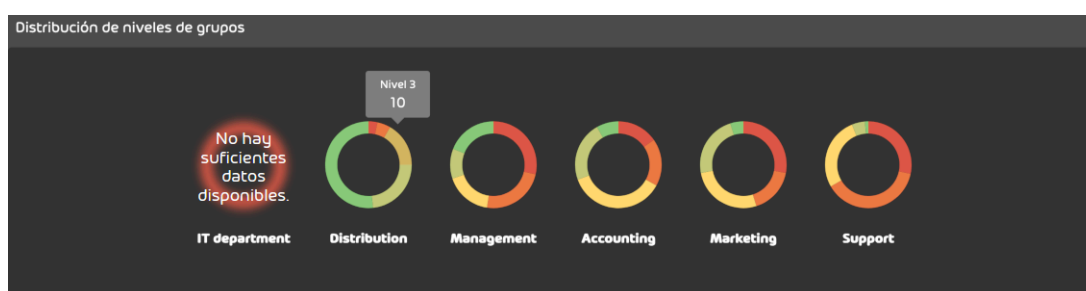


Figura 164: Distribución de niveles de grupos

Tabla de distribución de niveles en grupos

Por debajo de los diagramas de distribución de niveles de usuarios en los grupos se vuelve a mostrar la misma en una tabla.

**Nota:**

Si el modo de privacidad se encuentra activado (véase [Modo de privacidad](#) en la página 160), la tabla de distribución de niveles de usuarios en los grupos contiene el valor 0 en cada columna para grupos con menos de 10 miembros.



Grupo	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
IT department	0	0	0	0	0
Distribution	8	15	18	19	22
Management	18	15	11	7	12
Accounting	13	15	31	19	7
Marketing	23	14	22	19	4
Support	23	31	22	4	1

Figura 165: Tabla de distribución de niveles en grupos

Tabla de niveles de usuarios individuales

**Nota:**

Esta tabla no se muestra en modo de privacidad (véase [Modo de privacidad](#) en la página 160), pues pone datos en relación directa con usuarios de la organización.

En la pestaña **Usuarios** de la tabla de **Distribución de niveles de grupos** se muestran el nivel, el nombre, los apellidos, la dirección de correo electrónico y el grupo asignado a usuarios individuales de la organización.

Nombre	Apellidos	Dirección de correo	Grupo	Nivel
Eva	Davis	davis@gevonne.com	IT department	1
John	Smith	smith@gevonne.com	IT department	1
Alice	Miller	miller@gevonne.com	Management	1
Michael	Williams	williams@gevonne.com	Marketing	1

Figura 166: Tabla de niveles de usuarios individuales



Programar informes mensuales automatizados

En el módulo **Security Awareness Service > Estadísticas** puede programar informes mensuales automatizados para estadísticas. Los informes se envían el primer día de cada mes e incluyen tres archivos ZIP con los resultados de toda la organización, los resultados de los grupos y los resultados de los usuarios del mes anterior.

**Nota:**

Los resultados de los usuarios se incluyen solo si el modo de privacidad está desactivado (véase [Modo de privacidad](#) en la página 160).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos datos desee administrar.
3. Vaya a **Security Awareness Service > Estadísticas**.
4. Haga clic en **Programar informes mensuales automatizados**.

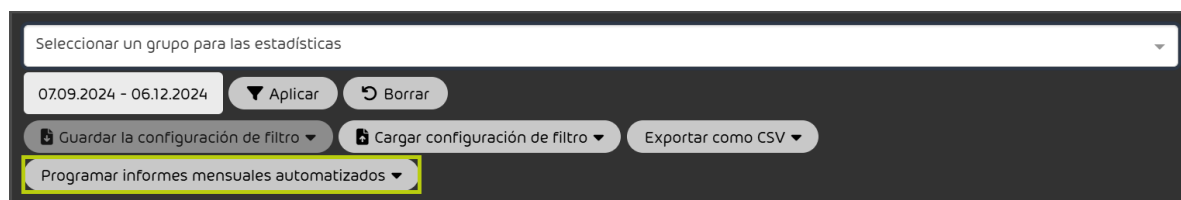


Figura 167: Programación de informes mensuales automatizados



Se abre el menú **Programar informes**.



Figura 168: Menú Programar informes

5. Seleccione un buzón de correo de la lista en **Buzones de correo en Control Panel**.
- ➔ El buzón seleccionado aparece en la lista **Destinatarios de los informes** a la derecha.
6. Opcional: Como alternativa, use la barra de búsqueda en la lista **Buzones de correo en Control Panel** para encontrar un buzón de correo.
7. Opcional: Para añadir buzones de correo externos, siga estos pasos:
 - a) Haga clic en la barra bajo **Buzón externo**.

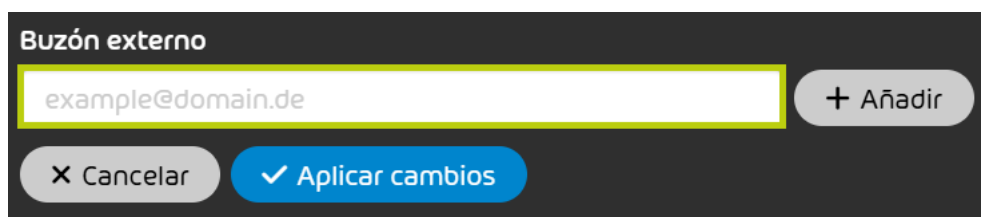


Figura 169: Barra de búsqueda para buzones de correo externos

- b) Introduzca la dirección del buzón de correo externo que debe recibir los informes mensuales.
 - c) Haga clic en **Añadir**.
- ➔ El buzón de correo externo se añade a la lista de destinatarios de los informes.
8. Opcional: Para quitar un buzón de correo de la lista **Destinatarios de los informes**, seleccione el buzón de correo o use la barra de búsqueda para localizarlo.



➔ El buzón de correo seleccionado se quita de la lista.

9. Opcional: Para descartar todos los cambios, haga clic en **Cancelar**.

10. Haga clic en **Aplicar cambios** para guardar la configuración.

✓ Los informes mensuales para las estadísticas de Security Awareness Service se han programado correctamente.



Configuración

En el módulo **Security Awareness Service > Configuración**, los administradores a nivel de cliente pueden realizar ajustes relativos al simulacro de phishing (véase [Configurar el simulacro de phishing](#) en la página 148) y a los tutoriales (véase [Configurar los tutoriales](#) en la página 200) de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). Además, los administradores pueden añadir grupos para la evaluación (véase [Añadir grupos](#) en la página 127). Los administradores pueden eliminar grupos añadidos previamente (véase [Eliminar un grupo](#) en la página 130) y modificar las prioridades de los grupos (véase [Modificar prioridades de grupos](#) en la página 131). Aparte de esto, los administradores pueden asignar a los usuarios su puesto dentro de la organización del cliente (véase [Añadir cargos](#) en la página 133) y un idioma para los correos del simulacro de phishing (véase [Editar los datos básicos de un buzón de correo](#)). Los clientes usuarios cuyos buzones de correo se sincronizan con Microsoft 365 o con un servicio de directorio mediante LDAP pueden administrar en su lugar los puestos e idiomas de sus usuarios en el servicio de directorio y sincronizarlos en Control Panel. También es posible excluir a usuarios concretos de Security Awareness Service (véase [Excluir un usuario](#) en la página 141).

**Nota:**

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)).

Añadir grupos



Ha creado grupos en Control Panel (véase [Crear un grupo](#)) y ha activado Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77).

La evaluación de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) funciona por grupos. Por eso puede añadir grupos de Control Panel al servicio en el módulo **Security Awareness Service > Configuración**. El grupo **Por defecto**, que contiene a todos los usuarios del dominio, está añadido por defecto y no se puede eliminar.

**Nota:**

Security Awareness Service se aplica a todos los usuarios del cliente. Tan solo los usuarios con buzones de correo desactivados en Control Panel (véase [Activar o desactivar un buzón de correo](#)) y los usuarios excluidos (véase [Excluir un usuario](#) en la página 141) están exentos de participar en el simulacro de phishing y de realizar tutoriales.

El grupo **Por defecto** está añadido por defecto a Security Awareness Service y no se puede eliminar. Este grupo contiene todos los usuarios del cliente que no se encuentren dentro de ningún otro grupo de Security Awareness Service.

**Nota:**

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)).

**Nota:**

Para que las evaluaciones sean significativas, recomendamos que cada grupo contenga 10 usuarios como mínimo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos grupos desee añadir a Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. Haga clic en **Añadir grupo**.

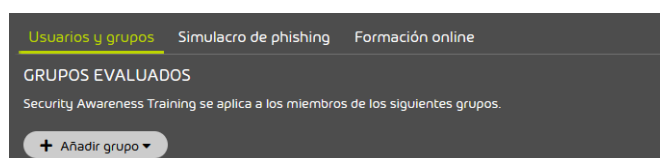


Figura 170: Añadir grupo



Se muestra un campo de búsqueda.

6. Haga clic en el campo de búsqueda.



- ➔ Se muestra una lista de grupos del cliente.

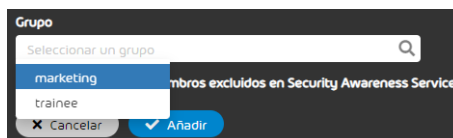


Figura 171: Lista de grupos

7. Para filtrar la lista, introduzca el nombre de un grupo en el campo de búsqueda.
 8. Haga clic en el grupo que desee añadir a Security Awareness Service.
- ➔ El grupo se selecciona. Se muestran el total de miembros del grupo, así como el número de miembros que se encuentran actualmente excluidos de Security Awareness Service (véase [Excluir un usuario](#) en la página 141).



Nota:

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Esto también afecta a los buzones de correo de reenvío incluidos en grupos añadidos.

Miembros en total: 3
Miembros excluidos de Security Awareness Service: 1

Figura 172: Cantidad de miembros del grupo

9. Opcional: Si desea que los miembros del grupo que se encuentran actualmente excluidos de Security Awareness Service continúen excluidos de dicho servicio, desmarque la casilla **Miembros excluidos de Security Awareness Service**.

☐ Incluir a todos los miembros excluidos en Security Awareness Service

Figura 173: Seguir excluyendo a los miembros excluidos



Nota:

Por defecto, al añadir un grupo se añaden a Security Awareness Service todos sus miembros que estuviesen excluidos del servicio hasta el momento.

10. Haga clic en **Añadir**.
- ➔ El grupo se añade a la lista de grupos en la pestaña **Usuarios y grupos**. El grupo se añade al final de la lista y recibe la prioridad más baja entre todos los grupos añadidos.



Grupo	
	Por defecto
1	marketing

Figura 174: Tabla de grupos

**Nota:**

Security Awareness Service considera a cada usuario dentro de un solo grupo. Si un usuario pertenece a varios grupos, se considerará dentro del grupo que tenga la mayor prioridad.



Se ha añadido un grupo a Security Awareness Service.

A continuación puede eliminar los grupos añadidos (véase [Eliminar un grupo](#) en la página 130) o cambiar la prioridad de los grupos (véase [Modificar prioridades de grupos](#) en la página 131).

Eliminar un grupo



Ha añadido grupos a Security Awareness Service (véase [Añadir grupos](#) en la página 127).

En el módulo **Security Awareness Service > Configuración** puede eliminar grupos de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7). Todos los usuarios que hayan sido miembros del grupo eliminado y no pertenezcan a ningún otro grupo de Security Awareness Service se volverán a asignar al grupo **Por defecto**.

**Nota:**

Security Awareness Service se aplica a todos los usuarios del cliente. Tan solo los usuarios con buzones de correo desactivados en Control Panel (véase [Activar o desactivar un buzón de correo](#)) y los usuarios excluidos (véase [Excluir un usuario](#) en la página 141) están exentos de participar en el simulacro de phishing y de realizar tutoriales.

El grupo **Por defecto** está añadido por defecto a Security Awareness Service y no se puede eliminar. Este grupo contiene todos los usuarios del cliente que no se encuentren dentro de ningún otro grupo de Security Awareness Service.

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 eliminar un grupo de Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. En la tabla de los grupos añadidos, haga clic en el aspa de la fila del grupo que desee eliminar.



Figura 175: Eliminar un grupo

- ➔ Se muestra una ventana de confirmación.
6. Haga clic en **Confirmar**.
- ➔ El grupo se elimina de la lista de grupos.

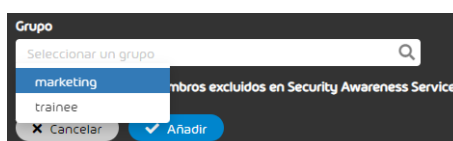


Figura 176: Lista de grupos

- ✓ Se ha eliminado un grupo de Security Awareness Service.

A continuación puede añadir grupos (véase [Añadir grupos](#) en la página 127) o modificar el orden de los grupos (véase [Modificar prioridades de grupos](#) en la página 131).

Modificar prioridades de grupos



- ✓ Ha añadido grupos a Security Awareness Service (véase [Añadir grupos](#) en la página 127).

En el módulo **Security Awareness Service > Configuración** puede modificar el orden y, de este modo, la prioridad de los grupos de Security Awareness Service. La prioridad determina a qué grupo se han de asignar usuarios que pertenezcan a varios grupos. Si un usuario pertenece a varios grupos, se considerará dentro del grupo que tenga la mayor prioridad.

**Nota:**

Cuanto mayor sea el número, menor será la prioridad de la regla. Así, el grupo con prioridad 1 tiene la prioridad más alta. El grupo **Por defecto** tiene la prioridad más baja, que no tiene número y no se puede modificar. Este grupo contiene todos los usuarios del cliente que no se encuentren dentro de ningún otro grupo de Security Awareness Service.

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 modificar el orden de los grupos de Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. Tiene dos opciones para modificar el orden de los grupos:
 - En la tabla de grupos, haga doble clic en el número de la primera columna de la fila del grupo cuya prioridad desee modificar e introduzca la prioridad deseada.

Grupo		Número de miembros	
	Por defecto	0	✕
1	marketing	9	✕
2	sales	6	✕

Figura 177: Indicar la prioridad

- En la tabla de grupos, haga clic en el icono de la primera columna de la fila del grupo cuya prioridad desee modificar, mantenga pulsado el botón del ratón y arrastre el grupo hasta la posición deseada.

Grupo		Número de miembros	
	Por defecto	0	✕
2	sales	6	✕
1	marketing	9	✕

Figura 178: Desplazar un grupo

El grupo se desplaza hasta la posición deseada.

Grupo		Número de miembros	
	Por defecto	0	✕
1	sales	6	✕
2	marketing	9	✕

Figura 179: Prioridad de los grupos



Se ha modificado la prioridad de un grupo en Security Awareness Service.

A continuación puede añadir más grupos (véase [Añadir grupos](#) en la página 127) o eliminar grupos (véase [Eliminar un grupo](#) en la página 130).

Añadir cargos



Ha activado Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77). Sus buzones de correo no se sincronizan con Microsoft 365 ni con un servicio de directorio mediante LDAP.

En la simulación de phishing de Security Awareness Service se emplean los nombres de usuarios reales de su organización para simular ataques de phishing realistas y selectivos. Para obtener resultados aún mejores, puede asignarles a los usuarios el cargo que tengan en su organización en el módulo **Security Awareness Service > Configuración**. En tal caso, los cargos se tendrán en cuenta en los correos de phishing simulados.



IMPORTANTE:

Como alternativa, los administradores pueden añadir el puesto de un usuario en los datos básicos de su buzón de correo (véase [#unique_76](#)). Los clientes usuarios cuyos buzones de correo se sincronizan con Microsoft 365 o con un servicio de directorio mediante LDAP pueden administrar en su lugar los puestos e idiomas de sus usuarios en el servicio de directorio y sincronizarlos en Control Panel (véase [Sincronizar puestos e idiomas para Security Awareness Service](#) en la página 135).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que quiera añadir cargos a Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. Haga clic en **Añadir registro**.



Se muestra un campo de introducción de datos.



Figura 180: Puesto

6. Introduzca la dirección de correo electrónico del usuario en el campo **Dirección de correo**.

Figura 181: Introducir Dirección de correo

7. En el menú desplegable de **Puesto**, seleccione el cargo que desee asignar al usuario.

Figura 182: Seleccionar Puesto

8. Haga clic en **Añadir**.

Figura 183: Puesto Añadir

- ➔ La dirección de correo electrónico y el cargo asignado se añaden a la tabla bajo **Puesto**.

Dirección de correo	Puesto	
klaus.trophobie@talltara.com	Director ejecutivo	x
thea.tralisch@talltara.com	Ventas	x
walter.eisheit@talltara.com	Ventas	x

Figura 184: Tabla de cargos



Se ha asignado un cargo de su organización a un usuario.



Sincronizar puestos e idiomas para Security Awareness Service

Puede sincronizar los puestos e idiomas de sus usuarios para correos de phishing simulado de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) con un servicio de directorio. Existen diferentes procedimientos dependiendo de si el cliente sincroniza sus buzones de correo con Microsoft 365 o con un servicio de directorio mediante LDAP.

Nota:

Si se realiza una actualización a 365 Total Protection, se sobrescribirán los cambios introducidos manualmente en los datos básicos, incluidos los atributos para puestos e idiomas. En tal caso, puede empezar con el paso 5 en la página 136 de estas instrucciones.

Si los puestos e idiomas de los usuarios de Security Awareness Service para los correos del simulacro de phishing se añadieron manualmente y ahora se realiza una sincronización mediante LDAP, también se sobrescribirán los cambios realizados previamente en los datos básicos. En tal caso, puede empezar con el paso 6 en la página 137 de estas instrucciones.

1. Elija el campo para atributos personalizados de su servicio de directorio en que desee almacenar el puesto y el idioma de sus usuarios.

Nota:

En caso de que se sincronicen datos de varios servicios de directorio mediante LDAP, en todos los directorios deberá emplearse el mismo campo para puestos e idiomas.

2. Introduzca el puesto y el idioma de cada usuario para Security Awareness Service en el campo seleccionado del servicio de directorio.

**Nota:**

El idioma y el puesto deben introducirse en el siguiente formato:

`sas_language={código de idioma};sas_position={puesto}`

En [Códigos de idioma y puestos para la sincronización](#) en la página 137 se incluye una lista de los valores admitidos en lugar de **`{código de idioma}`** y **`{puesto}`**.

Ejemplo de un usuario con idioma francés que trabaja en un departamento de desarrollo:

`sas_language=fr_FR;sas_position=Developer`

3. Inicie sesión en Control Panel con sus datos de acceso de administrador.
4. En la selección de ámbitos, seleccione el dominio para cuyos usuarios desee sincronizar el puesto y el idioma con el servicio de directorio.
5. Opcional: Si sus buzones de correo se sincronizan con Microsoft 365, proceda del siguiente modo:
 - a) Vaya a **Security Awareness Service > Configuración**.
 - b) Seleccione la pestaña **Usuarios y grupos**.
 - c) Seleccione el nombre del atributo de Active Directory para puestos e idiomas en el menú desplegable **Sincronización de puestos e idiomas**.

**Nota:**

La sección **Sincronización de puestos e idiomas** solo se muestra a clientes cuyos datos se sincronizan con Microsoft 365 en Control Panel.

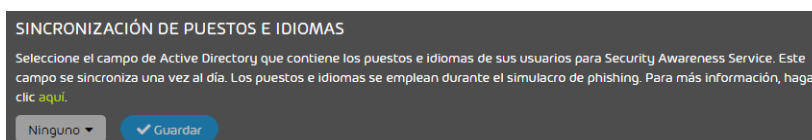


Figura 185: Seleccionar el atributo de Active Directory



El botón **Guardar** se habilita.



d) Haga clic en **Guardar**.

- ➔ Se guarda el nombre del atributo de Active Directory para puestos e idiomas de usuario para Security Awareness Service. Durante la próxima sincronización automática de los buzones de correo con Microsoft 365, este atributo también se leerá, y los valores de puesto e idioma se sincronizarán en Control Panel.

6. Opcional: Si sus buzones de correo se sincronizan con un servicio de directorio mediante LDAP, proceda del siguiente modo:

a) Vaya a **Dashboard de servicios**.

b) Seleccione la pestaña **Conexión LDAP**.

c) Seleccione el nombre del atributo de Active Directory para puestos e idiomas en el menú desplegable **Puestos e idiomas para Security Awareness Service** de **Atributos de LDAP**.

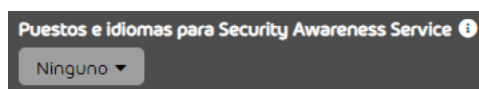


Figura 186: Seleccionar el atributo

d) Haga clic en **Aplicar cambios**.

- ➔ Se guarda el nombre del atributo para puestos e idiomas de usuario para Security Awareness Service. Durante la próxima sincronización automática de los buzones de correo con el servicio de directorio mediante LDAP, este atributo también se leerá, y los valores de puesto e idioma se sincronizarán en Control Panel.

- ✓ Se ha configurado la sincronización de puestos e idiomas de sus usuarios para correos de phishing simulado de Security Awareness Service.

Códigos de idioma y puestos para la sincronización

Para la sincronización de datos básicos de idiomas y puestos de usuario para Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) solo se admiten determinados códigos de idioma y denominaciones de puestos en el campo del atributo correspondiente del servicio de directorio (véase [Sincronizar puestos e idiomas para Security Awareness Service](#) en la página 135).



Para los idiomas de usuario de Security Awareness Service pueden emplearse los siguientes códigos:

Tabla 2: Códigos de idioma

CÓDIGO DE IDIOMA	IDIOMA
bg_BG	Búlgaro
bs_BA	Bosnio (Bosnia y Herzegovina)
cn_CH	Chino (RPC)
cnr_ME	Montenegrino
cs_CZ	Checo
de_AT	Alemán (Austria)
de_CH	Alemán (Suiza)
de_DE	Alemán
de_MIL	Alemán (Militar)
en_US	Inglés
ca_ES	Catalán
es_CL	Español (Chile)
es_CO	Español (Colombia)
es_ES	Español (España)
fr_FR	Francés
hr_HR	Croata



CÓDIGO DE IDIOMA	IDIOMA
hu_HU	Húngaro
it_IT	Italiano
ja_JP	Japonés
mk_MK	Macedonio
ms_MY	Malayo
nl_NL	Neerlandés
pl_PL	Polaco
pt_PT	Portugués
ro_RO	Rumano
sk_SK	Eslovaco
sl_SI	Esloveno
sq_AL	Albanés (Albania)
sq_XK	Albanés (Kosovo)
sr_RS	Serbio
sv_SE	Sueco
tr_TR	Turco
uk_UA	Ucraniano
zh_SG	Chino (Singapur)



Para los puestos de los usuarios de Security Awareness Service pueden indicarse los siguientes valores.

Tabla 3: Puestos

PUESTO	EXPLICACIÓN
CEO	Director ejecutivo
CFO	Director financiero
CIO	Director de sistemas de información
Consultant	Consultor
CTO	Director técnico
Customer Success	Empleado de un departamento de Customer Success Management
Developer	Empleado de un departamento de desarrollo
Doctor	Médico
DSB	Delegado de protección de datos
Engineer	Empleado de un departamento de ingeniería
External	Empleado externo
Finance	Empleado de un departamento de finanzas
Head of Department	Jefe de departamento
HR	Empleado de un departamento de Recursos humanos
Internship	Becario



PUESTO	EXPLICACIÓN
IT Admin	Administrador de sistemas
Legal	Empleado de un departamento jurídico
Manager	Empleado de un departamento de gestión
Marketing & Sales	Empleado de un departamento de ventas
Nurse	Enfermero
Operations	Operaciones
Other	Otros empleados
Politician	Político
PR	Empleado de un departamento de relaciones públicas y marketing
Purchasing	Empleado de un departamento de compras
Researcher	Empleado de un departamento de investigación
Secretary	Empleado de una secretaría

Excluir un usuario



Ha activado Security Awareness Service (véase [Activar Security Awareness Service](#) en la página 77).

En el módulo **Security Awareness Service > Configuración** puede excluir a usuarios de Security Awareness Service. Los usuarios excluidos no reciben correos de phishing simulados ni se les asignan tutoriales. Si los usuarios afectados habían hecho ajustes personales en User Panel, éstos se eliminan.

**Nota:**

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, tampoco es posible excluir los buzones de reenvío manualmente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyo usuario desee excluir de Security Awareness Service.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. Desplácese hasta la sección **Usuarios excluidos**.
- 6.

**Nota:**

Es posible excluir de Security Awareness Service por adelantado los usuarios que se añadan a Control Panel en el futuro mediante sincronización con Microsoft 365 o vía LDAP.

Opcional: Accione el interruptor **Excluir automáticamente de Security Awareness Service los usuarios que se sincronicen en el futuro**.

**Nota:**

Si se añaden usuarios a un grupo activo, participarán automáticamente en la formación en función de los ajustes realizados. Si el interruptor **Excluir automáticamente de Security Awareness Service los usuarios que se sincronicen en el futuro** no está activado, participarán automáticamente en la formación. Si antes no estaban asignados a ningún grupo, se añadirán automáticamente al grupo **Por defecto**.

Si el interruptor **Excluir automáticamente de Security Awareness Service los usuarios que se sincronicen en el futuro** está activado, los nuevos usuarios no participarán en la formación. Si se añaden posteriormente a un grupo, hay que quitarlos también de la lista de usuarios excluidos (véase [Eliminar usuarios de la lista de usuarios excluidos](#) en la página 146).

7. Puede excluir usuarios individuales mediante sus direcciones de correo electrónico.
 - a) En **Usuarios excluidos**, haga clic en **Excluir usuario**.

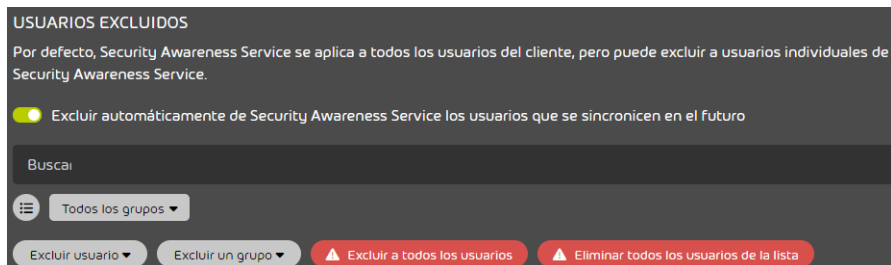


Figura 187: Excluir un usuario



Se abre una vista avanzada.

- b) Introduzca en el campo **Dirección de correo** la dirección de correo electrónico del usuario al que desee excluir de Security Awareness Service. Para activar la función de sugerencias automáticas, introduzca al menos tres caracteres seguidos.

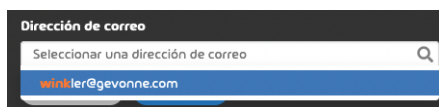


Figura 188: Introducir una dirección de correo electrónico

- c) Haga clic en **Añadir**.

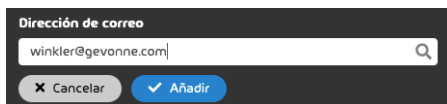


Figura 189: Añadir usuarios



El usuario se añade a la lista de usuarios excluidos en la pestaña **Usuarios y grupos**.

Dirección de correo	Grupo/s	
winkler@gevonne.com	Marketing	
winkski@gevonne.com	Marketing	

Figura 190: Tabla de usuarios excluidos

8. Puede excluir varios usuarios al mismo tiempo mediante su grupo:

- a) En **Usuarios excluidos**, haga clic en **Excluir un grupo**.

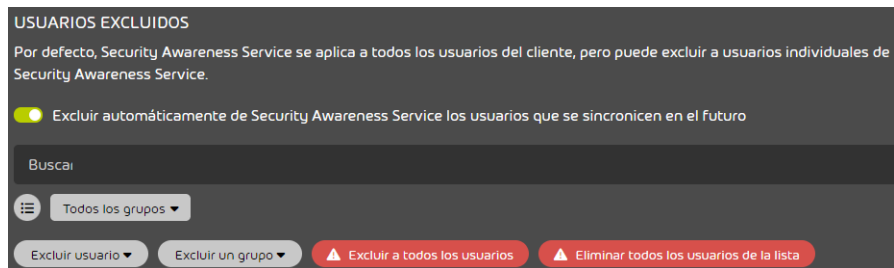


Figura 191: Excluir un grupo

➔ Se abre una vista avanzada.

- b) Haga clic en el campo **Seleccionar un grupo** y seleccione el grupo que desee excluir de Security Awareness Service. Para buscar grupos, introduzca caracteres en el campo de introducción de datos.



Figura 192: Excluir un grupo

- c) Haga clic en **Confirmar**.



Figura 193: Confirmar la exclusión del grupo

- ➔ Los usuarios del grupo se añaden a la lista de usuarios excluidos en la pestaña **Usuarios y grupos**. Los ajustes personales de los usuarios acerca de Security Awareness Service se eliminan.

Dirección de correo	Grupo/s	
winkler@gevonne.com	Marketing	
winkski@gevonne.com	Marketing	

Figura 194: Tabla de usuarios excluidos

- ✓ Se han excluido usuarios de Security Awareness Service. Los ajustes personales acerca de Security Awareness Service realizados por los usuarios excluidos se han eliminado.



Filtrar usuarios excluidos



Ha excluido usuarios de Security Awareness Service (véase [Excluir un usuario](#) en la página 141).

En el módulo **Security Awareness Service > Configuración** puede buscar usuarios excluidos de Security Awareness Service y filtrar usuarios excluidos por el grupo al que pertenezcan.

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 filtrar usuarios excluidos.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña **Usuarios y grupos**.
5. Desplácese hasta la sección **Usuarios excluidos**.
6. Haga clic en el campo **Buscar**.
7. Introduzca un término de búsqueda.

USUARIOS EXCLUIDOS

Por defecto, Security Awareness Service se aplica a todos los usuarios del cliente, pero puede excluir a usuarios individuales de Security Awareness Service.

☒ Excluir automáticamente de Security Awareness Service los usuarios que se sincronicen en el futuro

wink

Parámetro Dirección de correo Grupo

Figura 195: Búsqueda entre usuarios excluidos

8. Opcional: En **Parámetro**, seleccione el campo por el que desee buscar.
 - **Dirección de correo:** El término de búsqueda introducido solo se busca en el campo **Dirección de correo**.
 - **Grupo:** El término de búsqueda introducido solo se busca en el campo **Grupo**.

Dirección de correo: wink X Buscar

Parámetro Grupo

Figura 196: Limitar la búsqueda a determinados campos

9. Confirme la búsqueda con **Intro** o haciendo clic fuera del campo de introducción de datos.
10. En **Todos los grupos**, seleccione un grupo por el que desee filtrar.

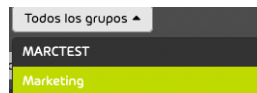


Figura 197: Seleccionar filtro de grupos

- ➔ La lista de usuarios excluidos muestra usuarios conforme a sus criterios de filtrado.

Dirección de correo	Grupo/s	
winkler@gevonne.com	Marketing	
winski@gevonne.com	Marketing	

Figura 198: Lista de usuarios excluidos con filtro

- ✓ Se ha aplicado un filtro a la lista de usuarios excluidos.

Eliminar usuarios de la lista de usuarios excluidos

- ✓ Ha excluido usuarios de Security Awareness Service (véase [Excluir un usuario](#) en la página 141) o se han excluido usuarios automáticamente del mismo.

En el módulo **Security Awareness Service > Configuración** puede eliminar usuarios de la lista de usuarios excluidos de Security Awareness Service.



PRECAUCIÓN:

Cuando un usuario es excluido automáticamente o manualmente de Security Awareness Service, los ajustes que éste haya hecho en su User Panel se eliminan (véase [Configuración de usuario](#)). Esto afecta también a ajustes relativos a la privacidad, como la prohibición de enviar correos de phishing simulado en nombre del usuario. Cuando un usuario se elimina de la lista de usuarios excluidos y, de este modo, vuelve a incluirse en Security Awareness Service, se le aplica la configuración por defecto. Por tanto, las prohibiciones que el usuario hubiese establecido en el pasado ya no están vigentes.

Informe al usuario acerca de su reinclusión en Security Awareness Service y pídale que vuelva a realizar sus ajustes de privacidad en User 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 eliminar usuarios de la lista de usuarios excluidos.
3. Vaya a **Security Awareness Service > Configuración**.



4. Seleccione la pestaña **Usuarios y grupos**.
5. Desplácese hasta la sección **Usuarios excluidos**.
6. Opcional: Para eliminar usuarios individuales de la lista de usuarios excluidos, haga clic en  al final de la fila con la dirección de correo electrónico del usuario correspondiente.

 Nota:

Puede filtrar la lista de usuarios excluidos para que muestre los usuarios que desee eliminar de la misma.

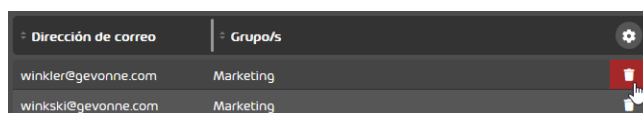


Figura 199: Eliminar usuarios individuales de la lista de usuarios excluidos

7. Opcional: Para eliminar varios usuarios de la lista de usuarios excluidos, proceda del siguiente modo:
 - a) Haga clic en .
 - b) Seleccione los usuarios de la lista de usuarios excluidos que desee eliminar.

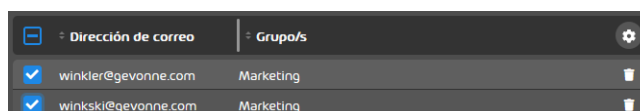


Figura 200: Seleccionar varios usuarios

- c) Haga clic en **Quitar de la lista**.

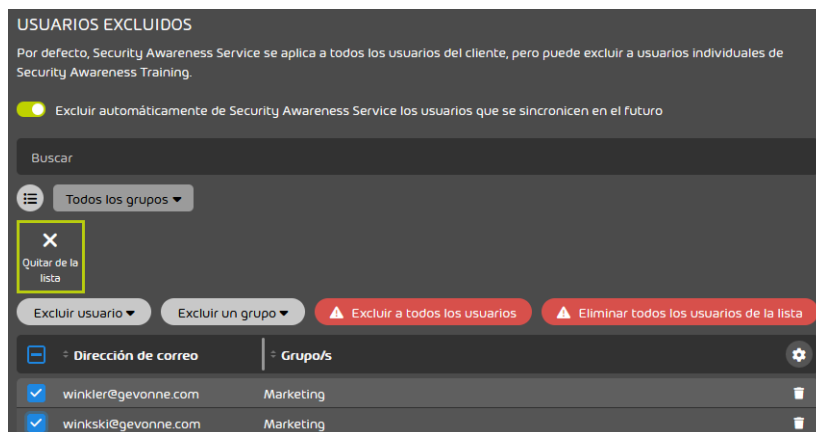


Figura 201: Eliminar varios usuarios de la lista de usuarios excluidos

8. Informe a todos los usuarios afectados acerca de su reinclusión en Security Awareness Service y pídeles que vuelvan a realizar sus ajustes de privacidad en User Panel.



Se han eliminado usuarios de la lista de usuarios excluidos.

Configurar el simulacro de phishing



Ha activado el simulacro de phishing (véase [Activar o desactivar el simulacro de phishing](#) en la página 79).

En el módulo **Security Awareness Service > Configuración** puede configurar el simulacro de phishing de Security Awareness Service e introducir información sobre su organización.

El Spear Phishing Engine envía correos de Spear Phishing realistas y personalizados con dificultad graduada.

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 configurar el simulacro de phishing.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. En **Inicio del simulacro de phishing**, seleccione la fecha en la que desee iniciar el simulacro de phishing.

**i Nota:**

En la fecha seleccionada se enviarán los primeros correos de phishing. La fecha seleccionada deberá ser al menos un día después de la actual. Una vez iniciado el simulacro de phishing no es posible cambiar la fecha.

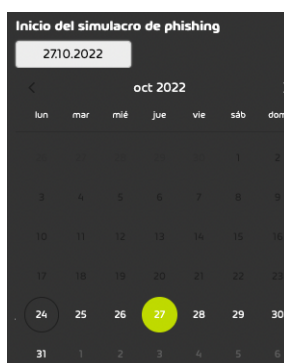


Figura 202: Definir Inicio del simulacro de phishing

6. En **Frecuencia de correos de phishing simulados**, seleccione si desea utilizar el Spear Phishing Engine para controlar la frecuencia de envío de los correos de phishing o si desea seleccionarla usted mismo.
 - **Automática:** El Spear Phishing Engine controla el número de correos de phishing que recibe al mes cada usuario en función de su nivel.
 - **Personalizada:** La frecuencia no se configura automáticamente. La frecuencia puede seleccionarse manualmente en un menú desplegable.

i Nota:

La opción **Automática** solo puede seleccionarse con el Awareness Engine activado (véase el paso 12 en la página 204 del capítulo Configurar los tutoriales).

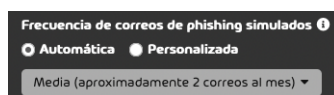


Figura 203: Configurar Frecuencia de correos de phishing simulados

7. Si ha seleccionado la opción **Personalizada**, seleccione la frecuencia en el menú desplegable. Tiene las siguientes opciones:
 - **Baja (aproximadamente 1 correo al mes)**



- Media (aproximadamente 2 correos al mes)
- Alta (aproximadamente 3 correos al mes)

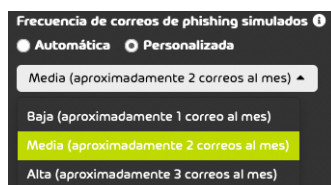


Figura 204: Seleccionar frecuencia personalizada

i Nota:

Estos valores son promedios determinados a lo largo de un periodo prolongado. Por ejemplo, si ha seleccionado la frecuencia **Media (aproximadamente 2 correos al mes)**, los usuarios no recibirán siempre exactamente dos correos del simulacro de phishing al mes. La cantidad exacta y el momento de envío de los correos del simulacro de phishing pueden variar. Estas irregularidades están destinadas a evitar que los usuarios se acostumbren a patrones específicos.

8. Opcional: Si no desea seguir recibiendo una evaluación personal del simulacro de phishing, active el modo de privacidad.

i Nota:

Esta opción está desactivada por defecto. Una vez activada esta opción, ya no podrá desactivarse. Para más información sobre el modo de privacidad, véase [Modo de privacidad](#) en la página 160.

- a) Accione el interruptor **Configuración general** de **Modo de privacidad**.

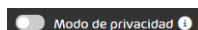


Figura 205: Activar el modo de protección de datos

- ➔ Se muestra una ventana de confirmación.



Figura 206: Ventana de confirmación

- a) Marque la casilla .
 - b) Haga clic en .
- ➔ La ventana de confirmación se cierra. El interruptor se pone verde.
9. Opcional: Si desea permitir a sus usuarios ver una evaluación personal del simulacro de phishing en su User Panel y tener acceso a certificados sobre los tutoriales completados, debe mostrar los módulos **Tutoriales** y **Simulacro de phishing** en User Panel (véase [Modificar los módulos mostrados en User Panel](#)).
 10. **! IMPORTANTE:**
Para poder utilizar Phishing Reporter, la infraestructura informática del cliente debe cumplir determinados requisitos técnicos (véase [Requisitos para el uso de Phishing Reporter](#) en la página 176).

Si desea añadir el complemento de Outlook "Phishing Reporter" a las aplicaciones de Outlook de sus usuarios, active la opción **Phishing Reporter** en **Configuración de Phishing Reporter**.

i Nota:

El complemento de Outlook "Phishing Reporter" permite a los usuarios del cliente marcar correos sospechosos en Outlook con un solo clic.

i Nota:

También es posible reportar correos sospechosos mediante el complemento de Outlook para clientes de 365 Total Protection. Por tanto, los clientes que ya utilicen dicho complemento no necesitarán Phishing Reporter.

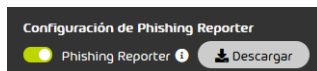


Figura 207: Activar Phishing Reporter

- ➔ El manifiesto para la instalación del complemento se habilita para su descarga.

**Nota:**

El manifiesto se necesita para instalar el complemento en las aplicaciones de Outlook de los usuarios (véanse [Instalar Phishing Reporter en Microsoft 365](#) en la página 182 y [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185).

Se muestra un campo de introducción de datos.

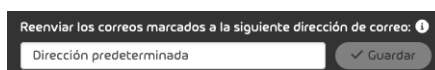


Figura 208: Campo para dirección para reenvíos

11.

**IMPORTANTE:**

El complemento Phishing Reporter solo comprueba si los correos reportados forman parte del simulacro de phishing y muestra un mensaje de éxito cuando un usuario identifica un mensaje de phishing simulado. Sin embargo, también es posible que los usuarios reporten correos sospechosos que no formen parte del simulacro de phishing y que posiblemente sean peligrosos. Estos correos se reenvían por defecto a un buzón de correo nuestro y no se procesan más. Es responsabilidad del cliente comprobar si dichos correos son peligrosos y, en tal caso, tomar medidas adicionales (p. ej., eliminar el correo del buzón del usuario).

Por eso es necesario definir una dirección para reenvíos. A dicha dirección de correo se enviarán automáticamente, para su comprobación, los correos que no formen parte del simulacro de phishing a modo de archivos adjuntos. Recomendamos utilizar una dirección de correo electrónico del soporte técnico informático del cliente.

Introduzca una dirección de correo electrónico en el campo de introducción de datos.

**i Nota:**

La dirección de correo electrónico debe pertenecer al dominio del cliente.

12. Opcional: Para desactivar la función de respuesta con un solo clic, accione el interruptor **Función de respuesta con un solo clic para los correos electrónicos marcados**.

i Nota:

Por defecto, los correos enviados a la dirección de reenvío (véase el paso 11 en la página 152) contienen un enlace a una página web. La página web contiene botones que permiten al soporte técnico informar al usuario acerca de si el correo resultó ser realmente peligroso tras comprobarlo. A continuación, se enviará un correo automático con la respuesta del soporte técnico a través de nuestra infraestructura al usuario que marcó el correo. Para que no se envíe una respuesta incorrecta antes de tiempo al usuario, los sistemas técnicos del cliente (p. ej., sistemas que hacen clic automáticamente en elementos de los correos) no deben interactuar con dichos correos.

Si la función de respuesta con un solo clic está desactivada, el soporte técnico no recibe ningún enlace a una página web, sino que debe ponerse en contacto con el usuario por sí mismo.

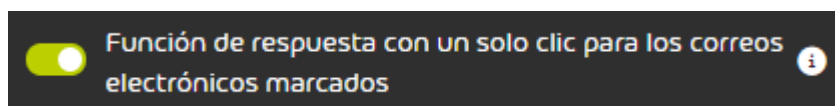


Figura 209: Desactivar la respuesta con un solo clic

13. Haga clic en **Guardar**.
- ➔ Se muestra una ventana de confirmación.
14. Haga clic en **Aceptar**.
- ➔ La ventana de confirmación se cierra.
15. Si desea que se envíen correos de phishing simulados con archivos adjuntos a sus clientes, active la opción **Archivos adjuntos** en **Tipos especiales de correos de phishing simulado**.

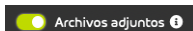


Figura 210: Activar los archivos adjuntos

16. Si desea que se envíen correos de phishing simulados con macros a sus clientes, active la opción **Macros** en **Tipos especiales de correos de phishing simulado**.



Figura 211: Activar las macros

17. Si desea que sus usuarios reciban correos de phishing simulados con enlaces a páginas de inicio de sesión falsas, active la opción **Phishing de datos de acceso** en **Tipos especiales de correos de phishing simulado**.

i Nota:

Las páginas de inicio de sesión falsas se basan en las de Microsoft, SAP, Netweaver y Dropbox.

i Nota:

Los datos de acceso que los usuarios introducen en las páginas de inicio de sesión falsificadas no se transmiten a nuestros servidores.



Figura 212: Activar phishing de datos de acceso

18. Si desea que los correos de phishing simulados utilicen las direcciones de correo de supuestos compañeros o conocidos, ocultando sus verdaderas direcciones de correo, active la opción **Suplantación de dominios** en **Tipos especiales de correos de phishing simulado**.



Figura 213: Activar la falsificación de dominios

19. Opcional: En **Temas de phishing desactivados**, seleccione los temas de phishing que no desee que se utilicen en los correos de phishing simulados de sus usuarios.

i Nota:

Es posible elegir varias opciones.

**Nota:**

En algunos casos, los títulos de los temas de phishing no se muestran en el idioma de Control Panel porque estos temas no están disponibles en el idioma de Control Panel.

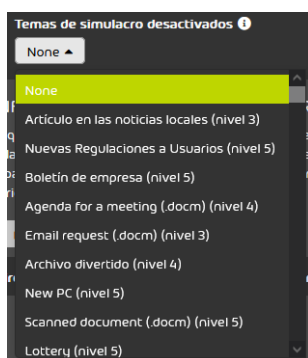


Figura 214: Temas de phishing desactivados



Se ha configurado el simulacro de phishing.

A continuación puede introducir información sobre su organización para que los correos de phishing simulados resulten más auténticos (véase [Añadir información sobre su organización](#) en la página 155). También puede configurar el simulacro de suplantación de identidad (véase [Configurar el simulacro de suplantación de identidad](#) en la página 158).

Añadir información sobre su organización



Ha configurado el simulacro de phishing (véase [Configurar el simulacro de phishing](#) en la página 148).

En el módulo **Security Awareness Service > Configuración** puede introducir información sobre su organización para que los correos de phishing simulados de Security Awareness Service resulten más auténticos.

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 añadir información sobre su organización.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .



- ➔ Al lado derecho de la página se encuentra la sección **Configuración de la organización**.

5. Introduzca el nombre de su organización en el campo **Nombre**.

Figura 215: Introducir el nombre de su organización

6. En **Tratamiento**, indique si sus usuarios se dirigen normalmente los unos a los otros por el nombre o por los apellidos.

i **NOTA:**

El tratamiento se emplea tanto en las notificaciones por correo electrónico de Security Awareness Service como en los correos de phishing.

Figura 216: Seleccionar el tratamiento

7. En **Idioma**, seleccione el idioma que más se utilice en su organización.

i **NOTA:**

Este idioma se emplea en las notificaciones por correo electrónico de Security Awareness Service. Si no se ha configurado ningún idioma a nivel del buzón de correo de un usuario concreto (véanse [Editar los datos básicos de un buzón de correo](#) y [Sincronizar puestos e idiomas para Security Awareness Service](#) en la página 135), este idioma también se empleará en los correos de phishing que se envíen a dicho usuario.

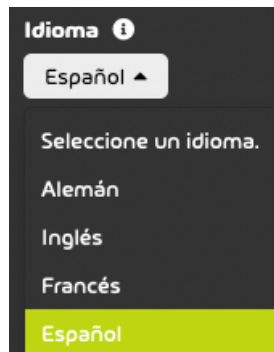


Figura 217: Seleccionar el idioma

8. Introduzca el URL de Kununu de su organización en el campo **Evaluación de los datos de la organización en Kununu** y haga clic en **Guardar**.

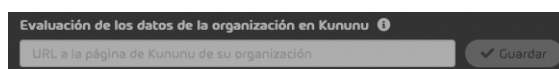


Figura 218: Introducir el URL de Kununu

- ➔ La página de la organización en Kununu se analiza para saber qué ventajas ofrece ésta a sus empleados. Si se encuentran ventajas para empleados, éstas se indicarán debajo del campo.

**Nota:**

Si al cabo de algunos minutos no se hubieran encontrado ventajas para empleados, recomendamos comprobar el URL y volver a confirmar.

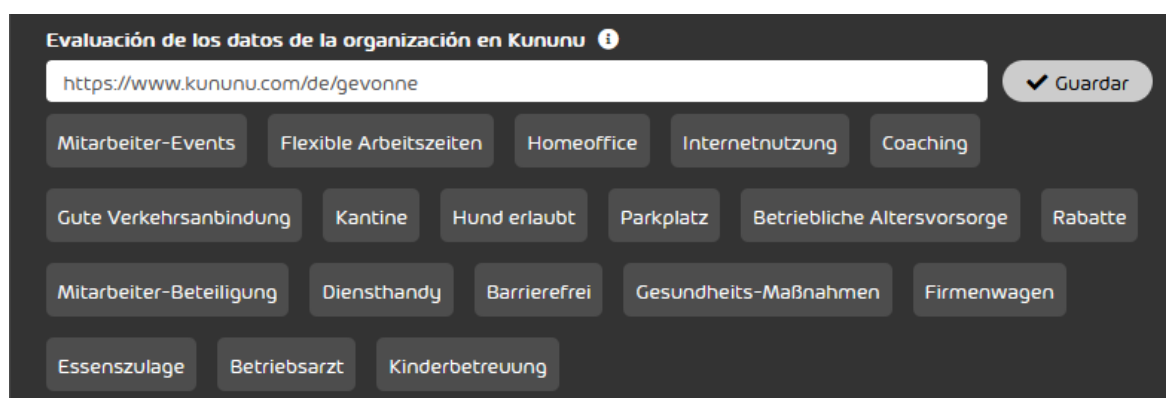


Figura 219: Ventajas para empleados de Kununu



9. En la sección **Tipo de organización**, marque la casilla correspondiente a su tipo de organización.

- Empresa
- Organismo público

Tipo de organización

☒ Empresa

☐ Organismo público

Figura 220: Seleccionar el tipo de organización.

10. Haga clic en **Guardar**.

Información acerca de su organización

Nombre
talitara.com

Tratamiento ⓘ
Apellidos ▾

Idioma ⓘ
Español ▾

Evaluación de los datos de la organización en Kununu ⓘ
[Vuelva a la página de Kununu de su organización](#)

Tipo de organización

☒ Empresa

☐ Organismo público

Figura 221: Guardar la información

➔ Se guarda la información de su organización.

✓ Se ha añadido información sobre su organización a Security Awareness Service.

Configurar el simulacro de suplantación de identidad

✓ Ha activado el simulacro de phishing (véase [Activar o desactivar el simulacro de phishing](#) en la página 79).

En el módulo **Security Awareness Service > Configuración** puede configurar el simulacro de suplantación de identidad durante el simulacro de phishing para tener mayor control sobre este ajuste.



Nota:

El simulacro de suplantación de identidad envía correos de phishing simulados en nombre de los usuarios de la organización.

**Nota:**

Independientemente de la configuración en el módulo **Security Awareness Service > Configuración**, cada usuario puede decidir por sí mismo si participa en el simulacro de suplantación de identidad y permite que se utilice su nombre en correos del simulacro de phishing de Security Awareness Service (véase [Activar o desactivar Simulacro de suplantación de identidad como usuario](#)).

Puede incluir automáticamente a todos los nuevos usuarios de Security Awareness Service en el simulacro de suplantación de identidad o desactivarlo para todos los usuarios existentes.

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 configurar el simulacro de suplantación de identidad.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. Opcional: Para incluir automáticamente a los nuevos usuarios en el simulacro de suplantación de identidad, accione el interruptor **Incluir a futuros usuarios en el simulacro de suplantación de identidad**.

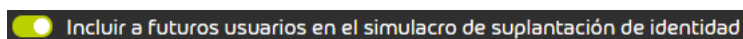


Figura 222: Incluir a usuarios futuros en el simulacro de suplantación de identidad



Todos los usuarios que se añaden a Security Awareness Service en el futuro, se incluirán automáticamente en el simulacro de suplantación de identidad.

**Nota:**

Los usuarios pueden en todo momento optar por excluirse del simulacro de suplantación de identidad en User Panel.

6. Opcional: Para desactivar el simulacro de suplantación de identidad para todos los usuarios existentes, haga clic en **Desactivar el simulacro de suplantación de identidad para todos los usuarios existentes**.

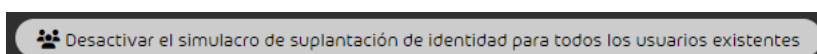


Figura 223: Desactivar el simulacro de suplantación de identidad para todos los usuarios existentes



- ➔ Todos los usuarios existentes de Security Awareness Service se excluyen del simulacro de suplantación de identidad.

**Nota:**

Los usuarios pueden en todo momento optar por incluirse en el simulacro de suplantación de identidad en User Panel.



El simulacro de suplantación de identidad se ha configurado.

Modo de privacidad

Los resultados individuales de los usuarios de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) son datos muy sensibles. Por tanto, los administradores tienen la opción de activar el modo de privacidad. En el modo de privacidad, los resultados individuales de Security Awareness Service se anonimizan.

Si el modo de privacidad se encuentra activado (véase [Configurar el simulacro de phishing](#) en la página 148), los administradores no pueden acceder a los niveles de usuarios individuales (véase [#unique_85](#)) en la pestaña **Phishing** del módulo **Security Awareness Service > Estadísticas**. Además, la estadísticas del ESI[®] (véase [Employee Security Index \(ESI®\)](#) en la página 8) y de distribución de niveles de usuarios en los grupos (véase [#unique_85](#)) se ocultan para grupos con menos de 10 miembros para que no sea posible averiguar nada acerca de los resultados de usuarios individuales. Además, con el modo de privacidad, los administradores no pueden acceder al User Panel personal de sus usuarios (véase [Iniciar sesión](#)). Además, los administradores no pueden acceder a las tasas de clics de sus usuarios. Los administradores solo pueden descargar las estadísticas, incluido el comportamiento de clics, si el modo de privacidad está desactivado.

Configuración de la infraestructura

Durante el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) se evalúa la conducta de seguridad de los usuarios. Por tanto, es preciso que los correos de phishing simulados se entreguen a los destinatarios. Para ello, el cliente debe asegurarse de que sus sistemas de seguridad y sus filtros no intercepten los correos de phishing simulados. Durante el simulacro de phishing, se evalúa si los usuarios han hecho clic en los enlaces de los correos del simulacro. Para no falsear los resultados, el cliente debe asegurarse de que sus sistemas de seguridad y sus filtros no interactúen con los correos de



phishing simulados. Para que el simulacro de phishing funcione bien, la infraestructura del cliente debe estar configurada correctamente (véase [Preparativos para sistemas](#) en la página 9). Los ajustes necesarios para clientes con Microsoft 365 se describen detalladamente a continuación.

En la sección **Configuración de la infraestructura** de la pestaña del módulo **Security Awareness Service > Configuración**, los administradores a nivel de cliente que utilizan Microsoft 365 Defender pueden realizar automáticamente todos los ajustes necesarios para autorizar la entrega de correos de phishing simulado en Microsoft 365 (véase [Configurar automáticamente Microsoft 365](#) en la página 28). Durante el proceso se configura la entrega avanzada para Microsoft 365 Defender y se crean dos reglas de transporte (véase [Configuración en Microsoft 365](#) en la página 27).

Los ajustes necesarios para clientes sin Microsoft 365 dependen del entorno de correo electrónico del cliente y no pueden describirse para cada caso. Recomendamos admitir los correos de phishing simulado en base a las direcciones IP o las firmas DKIM de los remitentes en el entorno de correo del cliente (véase [Autorizaciones para el envío de correos de phishing simulados](#) en la página 17). Solo si estos métodos no fuesen técnicamente practicables, el cliente deberá recurrir, como último recurso, a admitir los correos de phishing simulado en base a los dominios de sus remitentes y de los enlaces contenidos en los mismos. Para ello, los administradores pueden generar listas de dominios permitidos en la sección **Configuración de la infraestructura** de la pestaña del módulo **Security Awareness Service > Configuración** (véase [Generar listas de dominios permitidos](#) en la página 161) y descargarlas (véase [Descargar listas de dominios permitidos](#) en la página 166). Estas listas están adaptadas a la organización del cliente.

Los administradores también pueden comprobar mediante correos de prueba (véase [Enviar un correo de prueba](#) en la página 168) si la infraestructura del cliente está correctamente configurada. A continuación, los resultados de los correos de prueba enviados se muestran en una tabla (véase [Resultados de los correos de prueba](#) en la página 170).

Generar listas de dominios permitidos

Para que el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) funcione bien, es preciso que los correos de phishing simulado sean admitidos por su entorno de correo electrónico y se entreguen a sus destinatarios sin modificar. Los sistemas de seguridad o filtros de su organización no deben interceptar ni interactuar con los correos de phishing simulado (véase [Configuración de la infraestructura](#) en la página 160). Recomendamos admitir los correos de phishing simulado en el entorno de correo en base a las direcciones IP o las firmas DKIM de sus remitentes (véase [Autorizaciones](#)



para el envío de correos de phishing simulados en la página 17). Solo si estos métodos no fuesen técnicamente practicables, deberá recurrir, como último recurso, a admitir los correos de phishing simulado en su entorno de correo electrónico en base a dominios. En el módulo **Security Awareness Service > Configuración** puede generar una o dos listas de dominios permitidos. Las listas están adaptadas al sector de su organización. Una de las listas contiene los dominios de los remitentes de los correos de phishing simulado. La otra lista contiene los dominios de los enlaces que se incluyen en los correos de phishing simulado. A continuación, puede descargar estas listas y registrarlas en su entorno de correo electrónico.

**Nota:**

Una vez generada una nueva lista de dominios, en el simulacro de phishing del cliente solo se utilizan los dominios incluidos en la misma. Esto limita los temas de phishing que se pueden emplear para enviar correos a los usuarios del cliente. Esta limitación también afecta a los temas de phishing que se desarrollen en el futuro. Para que un cliente siempre disponga de los dominios utilizados en los temas de phishing actuales, recomendamos a los clientes que generen y descarguen listas de dominios y admitan los dominios en sus entornos de correo electrónico al menos una vez al año.

**Nota:**

Si ha utilizado listas de dominios anteriormente y ahora desea permitir los correos del simulacro de phishing basándose en las direcciones IP o firmas DKIM, no puede eliminar así sin más las listas de dominios que ha generado porque nosotros las hemos guardado también para reducir los temas de phishing. Solo si la lista de dominios se ha eliminado por ambas partes, los temas de phishing ya no están reducidos. En tal caso, debe ponerse en contacto con el soporte técnico.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee generar listas de dominios permitidos.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
- ➔ En la parte inferior de la página se encuentra la sección **Configuración de la infraestructura**.
5. En **Configuración de la infraestructura**, haga clic en **Generar lista(s) de dominios permitidos**.



Figura 224: Generar listas de dominios permitidos

i Nota:

Si ya se ha generado alguna lista de dominios permitidos para el cliente en el pasado, se mostrará en su lugar el texto **Generar nueva(s) lista(s) de dominios permitidos**.

➔ Se muestra una ventana de confirmación.

6. Haga clic en **Confirmar**.

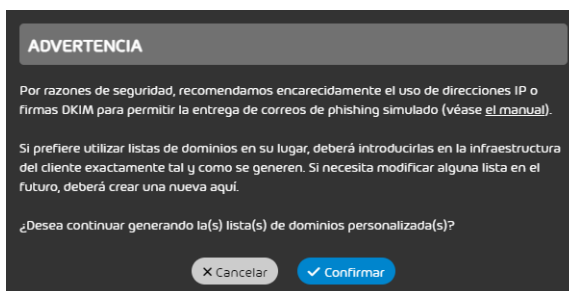


Figura 225: Confirmar

➔ Se abre una ventana para generar listas de dominios permitidos.

7. Opcional: Si desea generar una lista de dominios de remitentes, marque la casilla **Crear lista de dominios de remitentes** bajo **Lista de dominios de remitentes**.

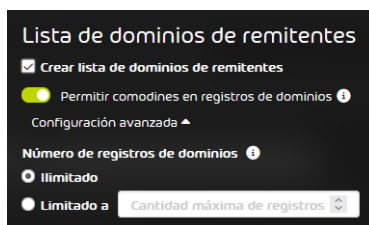


Figura 226: Lista de dominios de remitentes

➔ Los ajustes para listas de dominios de remitentes se habilitan.

8. Opcional: Si su entorno de correo electrónico no permite el uso de comodines en los registros de dominios, proceda del siguiente modo:



- a) Accione el interruptor **Permitir comodines en registros de dominios**.

**Nota:**

Los comodines están activados por defecto.

**Nota:**

Sin comodines, la lista de dominios contiene solo registros literales. Esto reduce la cantidad de subdominios que pueden emplearse en la simulación de phishing. Además, los usuarios no pueden recibir correos con temas de phishing basados en subdominios nuevos.



Aparece una ventana de confirmación.

- b) Haga clic en **Confirmar**.

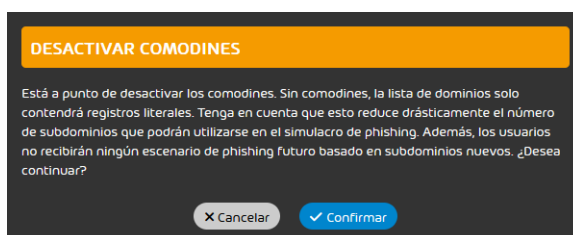


Figura 227: Confirmar la desactivación de los comodines.



El interruptor se pone gris. La configuración avanzada sobre comodines se bloquea.

9. Opcional: Si su entorno de correo electrónico permite el uso de comodines en los registros de dominios, proceda del siguiente modo:

- a) Haga clic en **Configuración avanzada** bajo el interruptor **Permitir comodines en registros de dominios**.



Se muestra la configuración avanzada sobre diversos tipos de comodines.

- b) Seleccione el valor del comodín en los registros de dominios.

**Nota:**

A modo de comodín, en las listas de dominios se emplea el asterisco *. Independientemente del tipo de comodines que permita el entorno de correo electrónico de un cliente, el cliente puede seleccionar el valor de dicho comodín.

- **Cualquier número de subdominios a la izquierda:** El asterisco equivale a un número ilimitado de subdominios a la izquierda. Por ejemplo, ***.dominioprincipal.com** es compatible con **subdominio1.dominioprincipal.com** y con **subdominio2.subdominio1.dominioprincipal.com**.
 - **Un solo subdominio en cualquier posición:** El asterisco equivale a un único subdominio en cualquier posición. Por ejemplo, **subdominio3*.dominioprincipal.com** es compatible con **subdominio3.subdominio1.dominioprincipal.com**, pero no con **subdominio3.subdominio2.subdominio1.dominioprincipal.com**.
 - **Un solo subdominio a la izquierda:** El asterisco equivale a un único subdominio a la izquierda. Por ejemplo, ***.dominioprincipal.com** es compatible con **subdominio1.dominioprincipal.com**, pero no con **subdominio2.subdominio1.dominioprincipal.com**.
10. Opcional: Si su entorno de correo electrónico limita el número de dominios que pueden admitirse, seleccione la opción **Limitado a** en **Número de registros de dominios** e indique el número máximo de registros de dominios en el campo de introducción de datos.

Figura 228: Introducir el número de registros de dominios

11. Opcional: Si desea generar una lista de dominios de enlaces, marque la casilla **Crear lista de dominios de enlaces** bajo **Lista de dominios de enlaces**.

Figura 229: Generar lista de dominios en enlaces



Los ajustes para listas de dominios de enlaces se habilitan.



12. Opcional: Repita los pasos [8](#) en la página 163 a [10](#) en la página 165 para configurar la lista de dominios en enlaces.
13. Haga clic en **Generar lista(s)**.
 - ➔ La ventana se cierra. La lista o listas se generan en segundo plano. El botón **Generar lista(s) de dominios permitidos** se bloquea durante el proceso. En cuanto terminan de generarse las listas, se muestra el nuevo botón **Descargar lista(s) de dominios permitidos**, siempre y cuando no estuviese ya visible por haberse generado listas previamente. Encima del botón se indican la fecha y la hora en que se generó la última lista.



Figura 230: Vista tras la generación de listas



Se han generado una o dos listas de dominios permitidos.

A continuación puede descargar la lista o listas generadas (véase [Descargar listas de dominios permitidos](#) en la página 166). Le recomendamos admitir los dominios en su entorno de correo electrónico a la mayor brevedad.

Descargar listas de dominios permitidos



Ha generado una o dos listas de dominios permitidos (véase [Generar listas de dominios permitidos](#) en la página 161).

En el módulo **Security Awareness Service > Configuración** puede descargar una o dos listas de dominios permitidos para el simulacro de phishing de Security Awareness Service. Puede utilizar los dominios de la lista como último recurso para admitir correos de phishing simulado en su entorno de correo electrónico (véase [Autorizaciones para el envío de correos de phishing simulados](#) en la página 17) siempre que no sea posible admitirlos en base a direcciones IP o firmas DKIM.

**i Nota:**

Una vez generada una nueva lista de dominios, en el simulacro de phishing del cliente solo se utilizan los dominios incluidos en la misma. Esto limita los temas de phishing que se pueden emplear para enviar correos a los usuarios del cliente. Esta limitación también afecta a los temas de phishing que se desarrollen en el futuro. Para que un cliente siempre disponga de los dominios utilizados en los temas de phishing actuales, recomendamos a los clientes que generen y descarguen listas de dominios y admitan los dominios en sus entornos de correo electrónico al menos una vez al año.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee descargar listas de dominios permitidos.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
- ➔ En la parte inferior de la página se encuentra la sección **Configuración de la infraestructura**.
5. En **Configuración de la infraestructura**, haga clic en **Descargar lista(s) de dominios permitidos**.
- ➔ Se abre una ventana de descarga de listas de dominios permitidos.

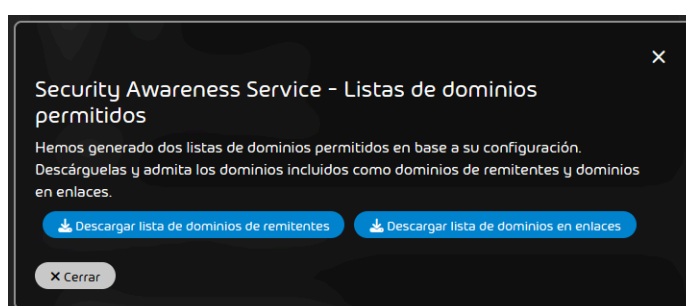


Figura 231: Listas de dominios permitidos

i Nota:

La imagen puede variar dependiendo de si se ha generado una o dos listas.

6. Si desea descargar la lista de dominios de remitentes, haga clic en **Descargar lista de dominios de remitentes**.



➔ La lista se descarga.

7. Si desea descargar la lista de dominios de enlaces, haga clic en **Descargar lista de dominios en enlaces**.

➔ La lista se descarga.

8. Haga clic en **Cerrar**.

➔ La ventana se cierra.

✓ Se han descargado una o dos listas de dominios permitidos.

A continuación puede admitir los dominios de las listas en su entorno de correo electrónico. Le recomendamos admitir los dominios a la mayor brevedad.

Enviar un correo de prueba

✓ Ha activado (véase [Activar o desactivar el simulacro de phishing](#) en la página 79) y configurado (véase [Configurar el simulacro de phishing](#) en la página 148) el simulacro de phishing.

En el módulo **Security Awareness Service > Configuración** puede enviar correos de prueba. Mediante los correos de prueba puede comprobar si la infraestructura del cliente está configurada correctamente (véase [Configuración de la infraestructura](#) en la página 160) para el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) y si los correos de phishing simulados se entregan a los destinatarios sin modificar.



Nota:

Los correos de prueba no se incluyen en la evaluación del simulacro de phishing.

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 enviar un correo de prueba.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. En la sección **Configuración de la infraestructura**, haga clic en **Enviar correo de prueba**.

➔ Se abre una vista avanzada.

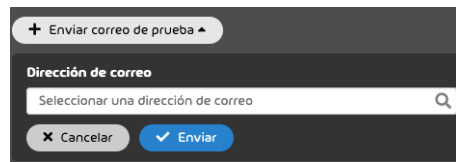


Figura 232: Correo de prueba

- Introduzca en el campo **Seleccionar una dirección de correo** la dirección de correo del usuario al cual desee enviar el correo de prueba. Para activar la función de sugerencias automáticas, introduzca al menos tres caracteres seguidos.

i Nota:

El correo de prueba solo se puede enviar a los usuarios del cliente incluidos en Security Awareness Service. Por tanto, no es posible enviar correos de prueba a usuarios que se hayan excluido manualmente (véase [Excluir un usuario](#) en la página 141) o automáticamente (véase [Usuarios excluidos automáticamente](#) en la página 211) del servicio.



Figura 233: Seleccionar una dirección de correo

- Haga clic en **Enviar**.



Figura 234: Enviar un correo de prueba

- ➔ El correo de prueba se envía a la dirección de correo indicada. A continuación, los resultados se muestran en la tabla de abajo (véase [Resultados de los correos de prueba](#) en la página 170).



Se ha enviado un correo de prueba a un usuario del cliente.



Resultados de los correos de prueba

En la pestaña del módulo **Security Awareness Service > Configuración** puede ver los resultados y los registros de envío de los correos de prueba enviados (véase [Enviar un correo de prueba](#) en la página 168).

Resultados de los envíos

Los resultados se muestran en una tabla. Cada fila es un correo de prueba enviado. La primera columna **Dirección de correo** contiene la dirección de correo electrónico a la cual se envió el correo de prueba. La segunda columna **Fecha y hora** contiene la fecha y la hora del envío del correo de prueba. Los datos de las demás columnas se explican en la siguiente tabla.

Tabla 4: Resultados de los correos de prueba

ACCIÓN	ESTADO
Enviado	 : El correo de prueba no se ha podido enviar.
	 : El correo de prueba todavía no se ha enviado. Está en cola.
	 : El correo de prueba se ha enviado. Al colocar el puntero del ratón sobre este icono se muestran la fecha y la hora del envío.



ACCIÓN

ESTADO

Recibido

! : El correo de prueba aún no se ha abierto. Security Awareness Service lo determina porque no se han descargado contenidos externos del correo. Este es el estado deseado después de enviar el correo de prueba e indica que ningún sistema del cliente lo ha abierto.

✓ : El correo de prueba se ha abierto. Security Awareness Service lo determina porque no se han descargado contenidos externos del correo. Al colocar el puntero del ratón sobre este icono se muestran la fecha y la hora en que se abrió el correo de prueba.

**IMPORTANTE:**

Si este estado se muestra directamente después del envío, es probable que un sistema del cliente haya abierto el correo. El cliente debe comprobar la configuración de su infraestructura y enviar otro correo de prueba a continuación.



ACCIÓN

ESTADO

Interactuado

! : No se ha hecho clic en el enlace del correo de prueba. Este es el estado deseado después de enviar el correo de prueba e indica que ningún sistema del cliente ha hecho clic en el enlace del correo de prueba.

✓ : Se ha hecho clic en el enlace del correo de prueba. Al colocar el puntero del ratón sobre este icono se muestran la fecha y la hora del clic.

**Nota:**

Los mecanismos de seguridad de correo electrónico son capaces de hacer clic en el enlace del correo de prueba sin descargar contenidos externos del mismo. Así puede darse el caso de que el correo de prueba esté sin abrir pero se haya hecho clic en su enlace. Este estado puede darse cuando los sistemas de seguridad del cliente realizan comprobaciones automáticas, y no es indicio de un fallo de detección por parte de Security Awareness Service.

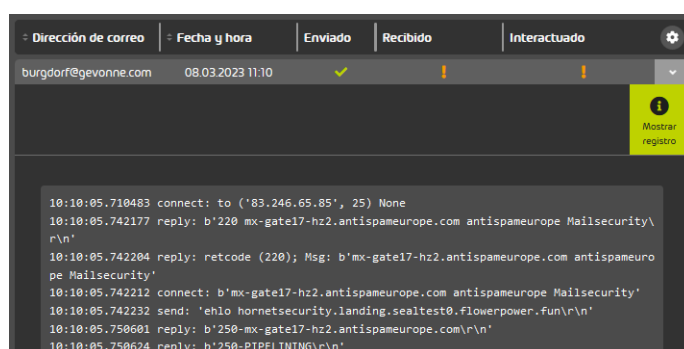
**IMPORTANTE:**

Si este estado se muestra directamente después del envío, es probable que un sistema del cliente haya hecho clic en el enlace del correo de prueba. El cliente debe comprobar la configuración de su infraestructura y enviar otro correo de prueba a continuación.



Registros de envío

Aparte de esto es posible visualizar registros acerca de la comunicación entre nuestro cliente de correo y el servidor de correo del cliente durante el envío de cada correo de prueba. Para ello es necesario hacer clic en el icono de flecha de la fila del correo de prueba deseado y, a continuación, hacer clic en **Mostrar registro**. El registro con el diálogo SMTP completo entre cliente y servidor se muestra debajo.



```
10:10:05.710483 connect: to ('83.246.65.85', 25) None
10:10:05.742177 reply: b'220 mx-gate17-hz2.antispameurope.com antispameurope Mailsecurity\r\n'
10:10:05.742204 reply: retcode (220); Msg: b'mx-gate17-hz2.antispameurope.com antispameurope Mailsecurity\r\n'
10:10:05.742212 connect: b'mx-gate17-hz2.antispameurope.com antispameurope Mailsecurity'
10:10:05.742232 send: 'ehlo hornetsecurity.landing.sealtest0.flowerpower.fun\r\n'
10:10:05.750601 reply: b'250-mx-gate17-hz2.antispameurope.com\r\n'
10:10:05.750624 reply: b'250-PIPELINING\r\n'
```

Figura 235: Ejemplo de registro

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	DESCRIPCIÓN	EXPLICACIÓN
	Requisito	Condición que debe cumplirse antes del siguiente paso.
	Resultado intermedio	Resultado alcanzado provisionalmente tras un paso concreto.



SÍMBOLO	DESCRIPCIÓN	EXPLICACIÓN
	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	DESCRIPCIÓN	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.
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.

Phishing Reporter

Los usuarios de Security Awareness Service (véase [Acerca de Security Awareness Service](#)) pueden denunciar correos sospechosos en Outlook mediante el complemento Phishing Reporter (véase [Utilizar Phishing Reporter en Outlook](#) en la página 194).

**Nota:**

Outlook ya dispone de una función nativa para marcar correos de phishing. Pero esta función no es la adecuada para marcar los correos del simulacro de phishing. Solo si los usuarios marcan los correos del simulacro de phishing mediante el complemento Phishing Reporter, podrán utilizar todas las funciones del simulacro de phishing.

**Nota:**

Los usuarios solo pueden marcar correos de un tamaño máximo de 39 MB.

**Nota:**

Los clientes que ya emplean el Hornetsecurity Outlook Add-in no necesitan el complemento Phishing Reporter.

Al marcar un correo, los usuarios pueden indicar la razón por la que les parece sospechoso. Si el correo marcado formaba parte del simulacro de phishing, se mostrará en Outlook un mensaje indicando que el usuario ha detectado correctamente el correo, y el correo detectado se computará en la evaluación del simulacro de phishing para el usuario. A continuación, el usuario puede eliminar el correo de su buzón de correo.

**Nota:**

Los usuarios también pueden marcar correos sin necesidad de complemento. Los usuarios pueden reenviar los correos sospechosos como archivos adjuntos a una dirección de correo electrónico determinada (véase [Marcado de correos sin complementos](#)). Esto permite incluir los correos de phishing simulado detectados correctamente en la evaluación del simulacro de phishing.

Para poder emplear el complemento Phishing Reporter deben cumplirse determinados requisitos (véase [Requisitos para el uso de Phishing Reporter](#) en la página 176).

Para que los usuarios de un cliente puedan utilizar el complemento Phishing Reporter, los administradores deben primero instalarlo para la organización del cliente. El complemento puede instalarse en un inquilino de Microsoft 365 o en un servidor Exchange local (véase [Instalar Phishing Reporter en Microsoft 365](#) en la página 182 o [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185). A continuación, los administradores deben proporcionar el complemento a los usuarios del servidor Exchange local (véase [Proporcionar](#)



[Phishing Reporter en un servidor Exchange local](#) en la página 187). Si los usuarios de un cliente no deben seguir utilizando Phishing Reporter, los administradores pueden desinstalar el complemento (véase [Desinstalar Phishing Reporter](#) en la página 188).

Requisitos para el uso de Phishing Reporter

Para poder utilizar el complemento Phishing Reporter (véase [Configurar el simulacro de phishing](#)), el cliente debe cumplir determinados requisitos técnicos.

Servidores de correo y servicios de correo electrónico en la nube

El funcionamiento del complemento Phishing Reporter está garantizado para clientes con un inquilino de Microsoft 365 y la versión más actual de Outlook.

Clientes de correo electrónico

El complemento Phishing Reporter es compatible con la versión más reciente de Outlook para Windows. También es compatible con los siguientes clientes de correo electrónico:

**Nota:**

Debido a las limitaciones técnicas de los servicios web de Exchange (EWS), el complemento Phishing Reporter está temporalmente disponible solo para dispositivos móviles cuando se utiliza Office 365 y la API de Graph.

- Outlook para Android
- Outlook para iOS
- Outlook para MacOS
- Outlook on the web

El complemento Phishing Reporter también puede emplearse con algunas versiones anteriores de Outlook para Windows, aunque puede haber ciertas limitaciones. Por motivos de seguridad, el complemento Phishing Reporter no es compatible con Internet Explorer, que ya no recibe actualizaciones. Sin embargo, algunas versiones de Outlook siguen empleando Internet Explorer para la ejecución de complementos. Por tanto, las versiones de Outlook incluidas en Office 2013 (independientemente del tipo de licencia) no son compatibles con el complemento Phishing Reporter:



Configuración de cortafuegos

El complemento Phishing Reporter debe tener acceso a determinadas direcciones a través del puerto 443. Por tanto, en el cortafuegos del cliente deben estar autorizadas las siguientes direcciones:

- **services.cp.hornetsecurity.com**
- **services.cp.cloud-security.net**
- **res.cdn.office.net**
- **outlook.office365.com**
- **appsforoffice.microsoft.com**
- **cdn.it-seal.de**
- **ajax.aspnetcdn.com**

Requisitos específicos para Outlook 2016 y Outlook 2019 que utilizan Trident.

Los clientes con Outlook 2016 (independientemente del tipo de licencia y utilizando Trident) o con Outlook 2016 y 2019 (licencias por volumen y utilizando Trident) también pueden usar el complemento Phishing Reporter si se cumplen los siguientes requisitos previos:

- Solo para Office 2016: El Service Pack requerido está instalado (véase <https://support.microsoft.com/en-us/topic/july-3-2018-update-for-office-2016-kb4022223-44a019be-e49a-25d2-a480-e1b1912551d0>)
- Para Outlook 2016 y 2019: Actualice la configuración de Opciones de Internet añadiendo las URL del siguiente procedimiento a las Zonas de confianza de Internet Explorer: [Preconfigurar una directiva de grupo para Outlook 2016 y 2019](#) en la página 177.

Cuando se cumplan estos requisitos previos, deberá realizar el procedimiento comenzando desde el paso 20: [Instalar Phishing Reporter en Microsoft 365](#) en la página 182.

Preconfigurar una directiva de grupo para Outlook 2016 y 2019

Para usar el Phishing Reporter complemento con Outlook 2016 (independientemente del tipo de licencia y usando Trident) o con Outlook 2016 y 2019 (versiones basadas en volumen y Trident), el cliente debe actualizar la configuración de Internet añadiendo las URL de este procedimiento a las zonas de confianza de Internet Explorer.

1. Inicie sesión en el servidor designado mediante Escritorio remoto (RDP) usando las credenciales de administrador ubicadas en la organización Vaultwarden Avengers.



2. Presione WIN+R para abrir la ventana **Ejecutar**, escriba **gpedit.msc** y haga clic en **OK**.

➔ Se abre la ventana del Editor de directivas de grupo local

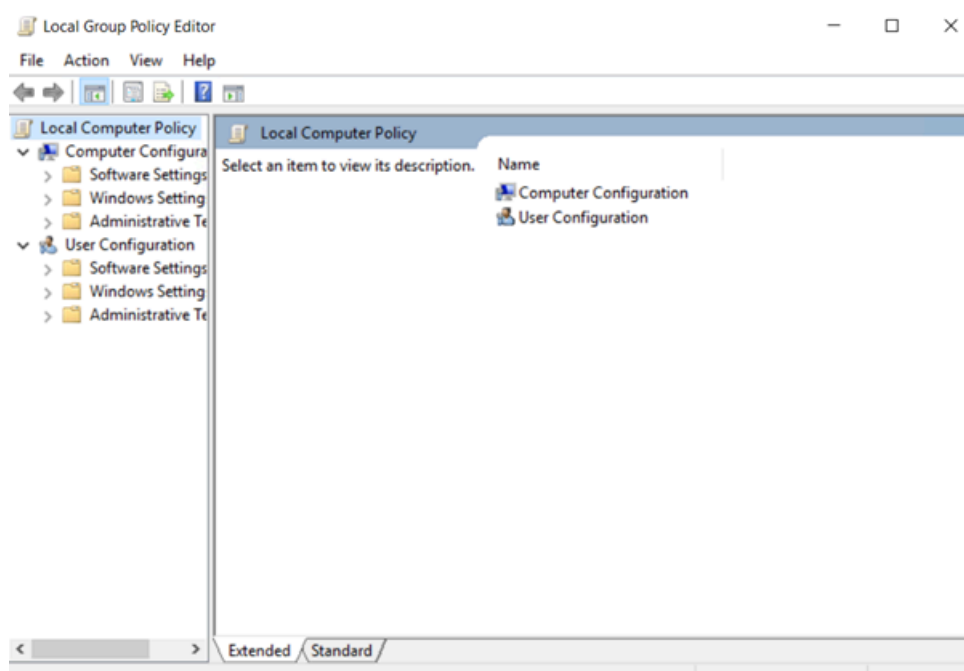


Figura 236: Ventana del Editor de directivas de grupo local

3. En el panel de navegación, vaya a **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Pestaña de seguridad** y localice **Lista de asignación de sitios a zonas**.

➔ Se muestra información sobre la lista de asignación de sitios a zonas.

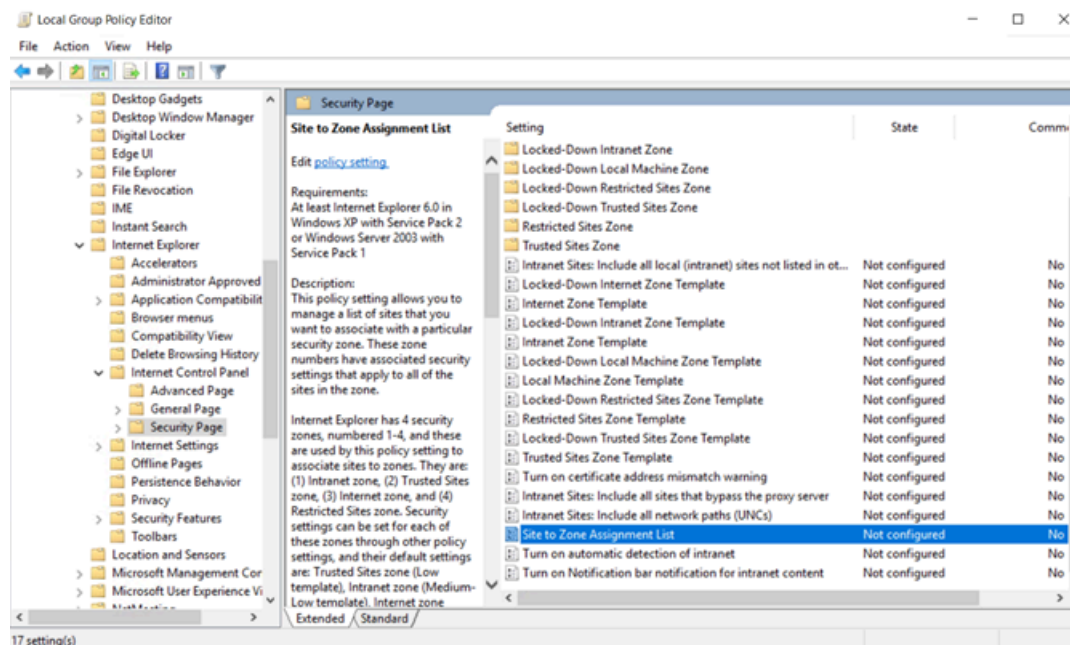


Figura 237: Ubicación de la lista de asignación de sitios a zonas

4. Haga doble clic en **Lista de asignación de sitios a zonas** para abrirla y active la opción **Habilitado**.

➔ La lista de asignación de sitios a zonas está habilitada.

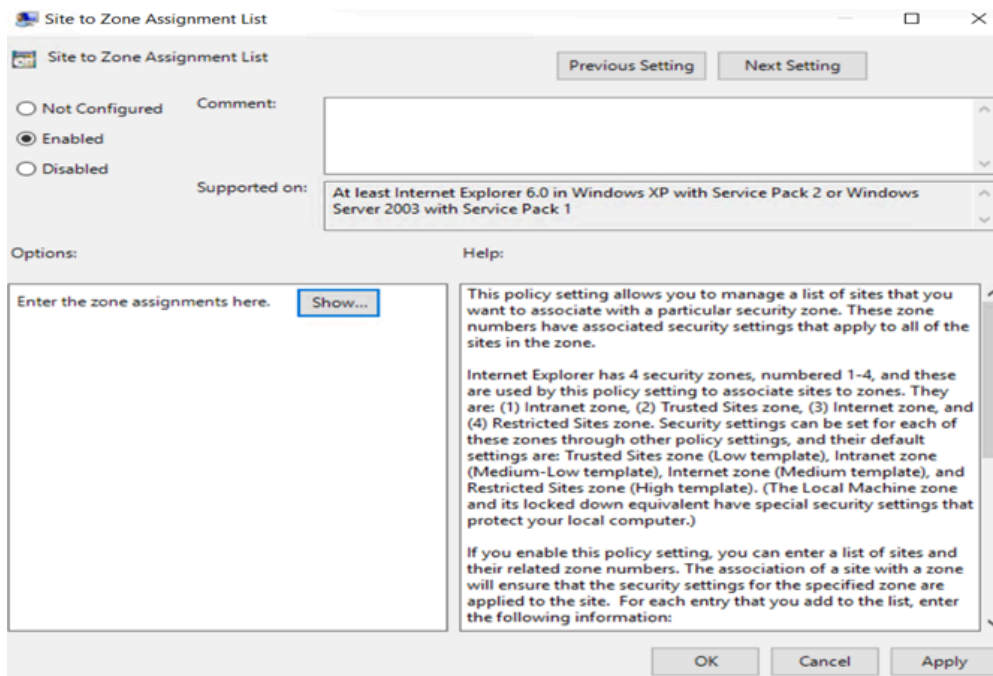


Figura 238: Lista de asignación de sitios a zonas habilitada

5. Haga clic en el botón **Mostrar...** e introduzca las siguientes URL con un valor de 2:

- https://*.msauth.net
- https://*.msftauth.net
- https://*.aspnetcdn.com
- https://*.microsoftonline.com
- https://*.cloud-security.net
- https://*.cp.cloud-security.net



Las URL requeridas se ingresan en la lista de asignación de sitios a zonas.

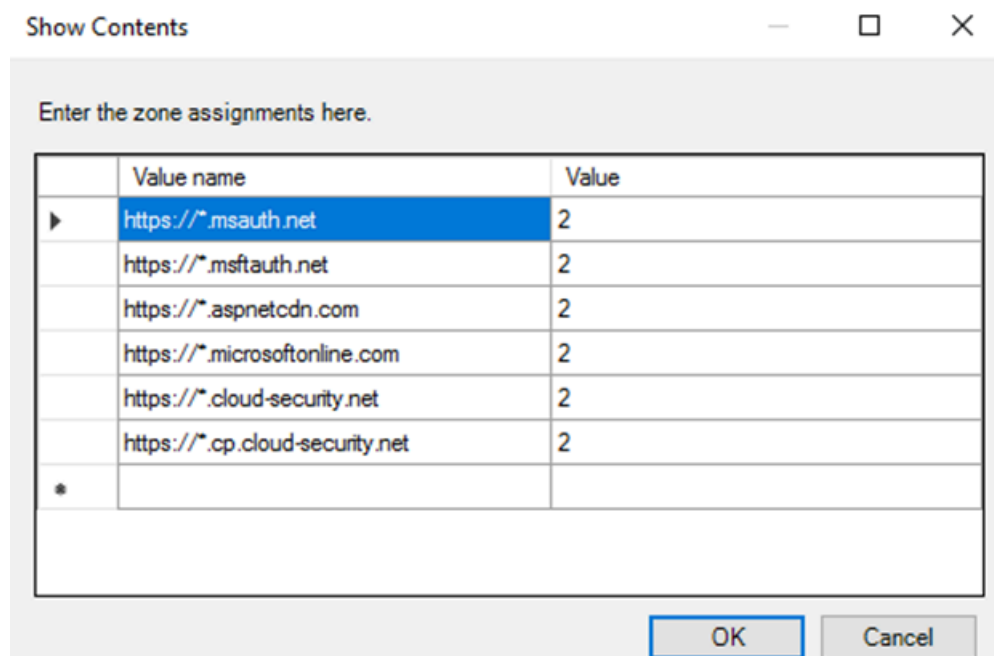


Figura 239: URL introducidas en la lista de asignación de sitios a zonas

6. Haga clic en OK, luego en **Aplicar**.

➔ Las URL se añaden a la lista de asignación de sitios a zonas.

7. Abra el símbolo del sistema (command prompt), escriba **gpupdate /force** y presione Enter.

➔ La directiva se ha actualizado.

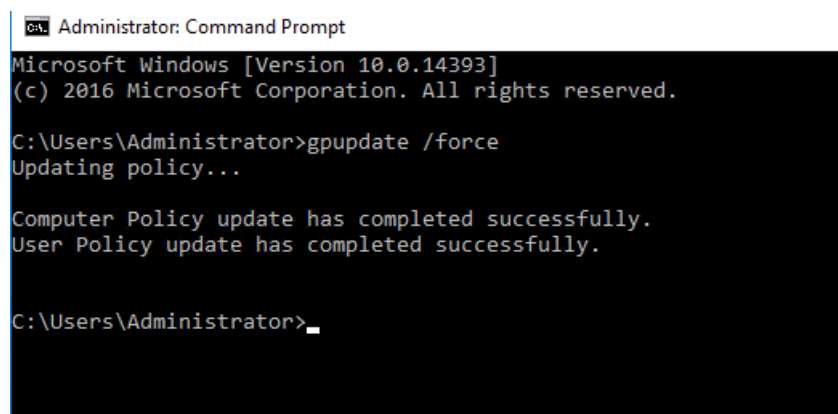


Figura 240: Directivas actualizadas en el símbolo del sistema de Windows

8. Verificar si la directiva de grupo se ha aplicado correctamente: Abra Internet Explorer, vaya a **Configuración > Opciones de Internet > Seguridad > Sitios de confianza > Sitios** y verifique si las URL añadidas están listadas.



- ➔ Puede ver que la directiva de grupo se actualizó correctamente.

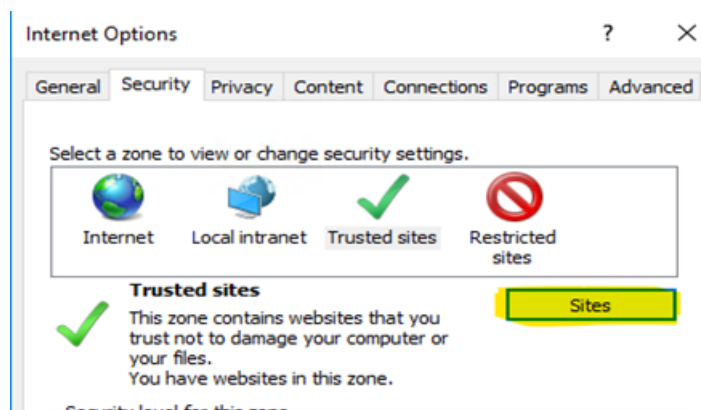


Figura 241: Acceder a sitios de confianza en Internet Explorer

- ✓ Ha preconfigurado una directiva de grupo para usar Phishing Reporter con Outlook 2016 y Outlook 2019.

Ahora puede realizar el siguiente procedimiento desde el paso 20 para comenzar la instalación del Phishing Reporter: [Instalar Phishing Reporter en Microsoft 365](#) en la página 182.

Instalar Phishing Reporter en Microsoft 365

- ✓ Ha descargado el manifiesto del complemento Phishing Reporter del módulo **Security Awareness Service > Configuración >** de Control Panel (véase [Configurar el simulacro de phishing](#)). Además, se cumplen los requisitos para que sus usuarios puedan emplear el complemento Phishing Reporter (véase [Requisitos para el uso de Phishing Reporter](#) en la página 176). Su organización utiliza Microsoft 365.

Para que sus usuarios puedan emplear el complemento Phishing Reporter (véase [Phishing Reporter](#) en la página 174), debe usted instalarlo en Outlook mediante un manifiesto y habilitar el complemento Phishing Reporter para que utilice la API de Microsoft Graph.



Nota:

Esta descripción se refiere a Microsoft 365. La instalación del complemento en un servidor Exchange local se describe en el capítulo [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185.

**Nota:**

Esta descripción se refiere al nuevo Centro de Administración de Exchange. Si emplea una versión antigua del Centro de Administración de Exchange, puede que la descripción no sea del todo precisa.

1. Abra la página web <https://admin.microsoft.com>.
2. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
3. Vaya a **Configuración > Aplicaciones integradas**.
4. Seleccione la pestaña **Aplicaciones implementadas**.
5. Haga clic en **Cargar aplicaciones personalizadas**.
- ➔ Se abre una ventana para implementar una nueva aplicación.
6. En, **Tipo de aplicación** seleccione **Complemento de Office**.
- ➔ Se muestran más opciones.
7. Seleccione **Cargar el archivo de manifiesto (.xml) desde el dispositivo**.
8. Haga clic en **Elegir archivo** y seleccione el manifiesto descargado.

Cargar las aplicaciones para implementar

Figura 242: Seleccionar el archivo

- ➔ Se comprueba el manifiesto.
9. Haga clic en **Siguiente**.
- ➔ Se muestra la página **Agregar usuarios** del asistente.
10. En **Asignar usuarios**, seleccione los usuarios para los que desee implementar el complemento. Tiene las siguientes opciones.
 - **Solo yo**: El complemento solo se implementará para el administrador seleccionado.
 - **Toda la organización**: El complemento se implementará para todos los usuarios de la organización.



- **Usuarios y grupos específicos:** El complemento se implementará para usuarios o grupos seleccionados.
11. Si ha seleccionado **Usuarios y grupos específicos**, seleccione los usuarios o grupos deseados mediante la búsqueda en el campo de introducción de datos **Buscar usuarios o grupos agregarlos**.

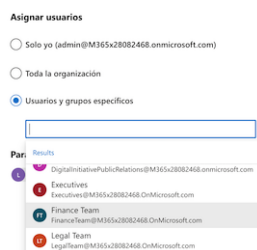


Figura 243: Añadir usuarios o grupos

- ➔ Los usuarios o grupos seleccionados se muestran debajo del campo de introducción de datos.
12. Haga clic en **Siguiente**.
 - ➔ Se muestra la página **Aceptar solicitudes de permisos** del asistente.
 13. Compruebe los permisos solicitados y haga clic en **Siguiente**.
 - ➔ Se muestra la página **Revisar y finalizar implementación** del asistente.
 14. Compruebe la configuración mostrada para la implementación del complemento.
 15. Haga clic en **Finalizar la implementación**.
 - ➔ Se inicia la implementación. Una vez finalizada la implementación, se muestra la página **Implementación completada**.
 16. Haga clic en **Done**.
 - ➔ El asistente para añadir una aplicación se cierra. El complemento Phishing Reporter se muestra en la lista de aplicaciones implementadas.

El complemento puede tardar hasta 6 horas en mostrarse en Outlook.

 17. Inicie sesión en Control Panel con sus datos de acceso de administrador.
 18. En la selección de ámbitos, seleccione el cliente para el que desee instalar el complemento Phishing Reporter.
 19. Vaya a **Security Awareness Service > Configuración > .**
 20. Haga clic en **Configuración de Phishing Reporter** en la sección **Conceder permisos**.

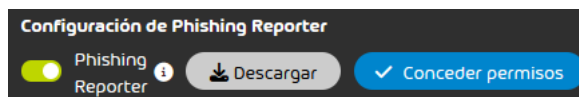


Figura 244: Conceder permisos

- ➔ Se abre la página de inicio de sesión de Microsoft 365.
- 21. Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
- ➔ Se muestra la página **Aceptar solicitudes de permisos** del asistente.
- 22. Compruebe los permisos solicitados y haga clic en **Aceptar**.
- ➔ La página **Aceptar solicitudes de permisos** se cierra. Se le redirige al Panel de control.
- ✓ El complemento Phishing Reporter se ha instalado y proporcionado a los usuarios de la organización, y se le han concedido los permisos requeridos.

Una vez proporcionado el complemento Phishing Reporter, los usuarios de la organización pueden utilizarlo para denunciar correos sospechosos desde Outlook (véase [Utilizar Phishing Reporter en Outlook](#) en la página 194).

Instalar Phishing Reporter en un servidor Exchange local

- ✓ Ha descargado el manifiesto del complemento Phishing Reporter del módulo **Security Awareness Service > Configuración >** de Control Panel (véase [Configurar el simulacro de phishing](#)). Además, se cumplen los requisitos para que sus usuarios puedan emplear el complemento Phishing Reporter (véase [Requisitos para el uso de Phishing Reporter](#) en la página 176). Su organización emplea un servidor Exchange local.

Para que sus usuarios puedan emplear el complemento Phishing Reporter (véase [Phishing Reporter](#) en la página 174), debe usted instalarlo en Outlook mediante un manifiesto.



Nota:

Esta descripción se basa en Microsoft Exchange Server 2016 y 2019.

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 con sus datos de acceso de administrador.
3. Vaya a **organización** en la parte superior izquierda.
4. Seleccione la pestaña **complementos**.
5. Haga clic en la parte superior izquierda de la página en el signo más.
- ➔ Se muestran las opciones para añadir un complemento.
6. Seleccione **Agregar desde archivo**.

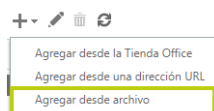


Figura 245: Añadir un complemento desde un archivo

- ➔ Se abre la pantalla **Agregar desde archivo**.
7. Haga clic en **Seleccionar archivo** y seleccione el manifiesto descargado.

agregar desde archivo

Elija la ubicación del archivo de manifiesto del complemento que desea instalar.

Ninguno archivo seleccionado

Figura 246: Seleccionar archivo

8. Haga clic en **Siguiente**.
- ➔ El asistente para añadir un complemento se cierra. El complemento Phishing Reporter se muestra en la lista de complementos.

**IMPORTANTE:**

La visualización del complemento en Outlook puede tardar varios días, dependiendo de las directivas internas de Microsoft y la configuración de caché del servidor.

9. Opcional: Si el complemento no aparece inmediatamente, puede ser útil recargar el sitio web de Outlook o la aplicación de Outlook.



El complemento Phishing Reporter se ha instalado.

A continuación puede proporcionar el complemento a los usuarios de su organización (véase [Proporcionar Phishing Reporter en un servidor Exchange local](#) en la página 187).

Proporcionar Phishing Reporter en un servidor Exchange local



Ha instalado el complemento Phishing Reporter en el servidor Exchange local de su organización (véase [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185).

Para que sus usuarios puedan denunciar correos sospechosos en Outlook con el complemento Phishing Reporter, debe usted proporcionárselo antes.

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 con sus datos de acceso de administrador.
3. Vaya a **organización** en la parte superior izquierda.
4. Seleccione la pestaña **complementos**.
5. En la lista de complementos, haga doble clic sobre el complemento Phishing Reporter.



Se abre una ventana con la configuración del complemento.



6. Marque la casilla **Hacer que este complemento esté disponible para los usuarios de su organización**.

☒ Hacer que este complemento esté disponible para los usuarios de su organización

Figura 247: Proporcionar el complemento

7. Seleccione los valores predeterminados de usuario para el complemento en **Especificar los valores predeterminados del usuario**:

 Nota:

Recomendamos seleccionar la opción **Opcional, habilitado de manera predeterminada**. Esta opción hace que el complemento se instale por defecto para todos los usuarios. Sin embargo, los usuarios pueden desactivar el complemento.

Especificar los valores predeterminados del usuario:

- ☒ Opcional, habilitado de manera predeterminada
☐ Opcional, deshabilitado de manera predeterminada
☐ Obligatorio, siempre habilitado. Los usuarios no pueden deshabilitar este complemento.

Figura 248: Seleccionar valores predeterminados de usuario

8. Haga clic en **Guardar**.



Los ajustes se guardan.



El complemento Phishing Reporter se ha proporcionado a los usuarios de la organización. Una vez proporcionado el complemento, los usuarios de la organización pueden utilizarlo para denunciar correos sospechosos desde Outlook (véase [Utilizar Phishing Reporter en Outlook](#) en la página 194).

Desinstalar Phishing Reporter



Ha activado Phishing Reporter (véase [Configurar el simulacro de phishing](#)) y lo ha instalado (véase [Instalar Phishing Reporter en Microsoft 365](#) en la página 182 o [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185).

Puede desactivar y desinstalar Phishing Reporter (véase [Phishing Reporter](#) en la página 174) si no desea seguir utilizando dicho complemento.

1. Opcional: Elimine Phishing Reporter de su inquilino de Microsoft 365. Proceda del siguiente modo:
 - a) Abra la página web <https://admin.microsoft.com>.



- b) Inicie sesión con sus datos de acceso de administrador del inquilino de Microsoft 365.
- c) Vaya a **Configuración > Aplicaciones integradas**.
- d) Seleccione la pestaña **Aplicaciones implementadas**.
- e) Haga clic en Phishing Reporter en la lista de aplicaciones.

➔ Se abre una ventana con la configuración del complemento Phishing Reporter.



Figura 249: Configuración del complemento Phishing Reporter

- f) Haga clic en **Quite la aplicación**.

➔ Se abre la pantalla **Quitar aplicaciones**.

- g) Marque la casilla **Sí, estoy seguro de que deseo quitar la aplicación y los datos asociados..**
- h) Haga clic en **Quitar**.

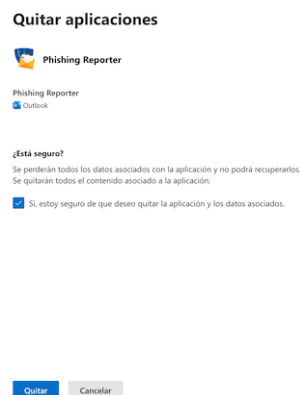


Figura 250: Eliminar Phishing Reporter



i) Haga clic en **Listo**.

➔ Phishing Reporter se elimina del inquilino de Microsoft 365 del cliente.

2. Opcional: Elimine Phishing Reporter de su servidor Exchange local. Proceda del siguiente modo:

a) 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.

b) Vaya a **organización**.

c) Seleccione la pestaña **complementos**.

d) Seleccione Phishing Reporter en la lista de complementos y haga clic en

➔ Se muestra una ventana de confirmación.

e) Haga clic en **Sí**.

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

4. En la selección de ámbitos, seleccione el dominio para el cual desee desactivar Phishing Reporter.

5. Vaya a **Security Awareness Service > Configuración**.

6. Seleccione la pestaña .

7. En **Configuración de Phishing Reporter**, desactive la opción **Phishing Reporter**.

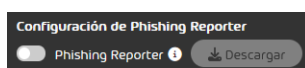


Figura 251: Desactivar Phishing Reporter

➔ Phishing Reporter se desactiva.



 Phishing Reporter se ha desactivado.

Solución de problemas: Phishing Reporter no funciona

Problema

Los usuarios no pueden utilizar el complemento Phishing Reporter a pesar de estar instalado. Cuando un usuario intenta utilizar el complemento se produce el error 403.

Causa

Tras la activación del complemento Phishing Reporter, un administrador ha vuelto a accionar el interruptor **Phishing Reporter** del módulo **Configuración de seguridad > Security Awareness Service**, desactivando de este modo el complemento (véase [Desinstalar Phishing Reporter](#) en la página 188, paso 7 en la página 190).

Solución

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 volver a activar Phishing Reporter.
3. Vaya a **Configuración de seguridad > Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. Active la opción **Phishing Reporter** de **Configuración de Phishing Reporter**.



Figura 252: Activar Phishing Reporter

-  El manifiesto para la instalación del complemento se habilita para su descarga.
6. Descargue el manifiesto y vuelva a instalar Phishing Reporter en su inquilino de Microsoft 365 o en su servidor Exchange local (véase [Instalar Phishing Reporter en Microsoft 365](#) en la página 182 o [Instalar Phishing Reporter en un servidor Exchange local](#) en la página 185).
-  La nueva instalación de Phishing Reporter sobrescribe la antigua.



7. Si ha instalado Phishing Reporter en un servidor Exchange local, proporcione el Phishing Reporter para los usuarios del servidor Exchange local (véase [Proporcionar Phishing Reporter en un servidor Exchange local](#) en la página 187).

Respuesta acerca de correos marcados

Los usuarios pueden marcar correos sospechosos mediante el complemento Phishing Reporter (véase [Phishing Reporter](#) en la página 174). Puede tratarse de correos del simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#)) o bien de correos que no forman parte del simulacro de phishing y que pueden ser peligrosos. Dependiendo del tipo de correo, el usuario recibe una respuesta de las siguientes maneras.

Correos del simulacro de phishing

Cuando un usuario marca un correo del simulacro de phishing de Security Awareness Service, se muestra directamente en Outlook un mensaje de éxito indicando que el usuario ha detectado correctamente el correo. El correo detectado se computará en la evaluación del simulacro de phishing del usuario.

Correos que no forman parte del simulacro de phishing

Si un usuario marca un correo que no forma parte del simulacro de phishing, el correo se reenvía al soporte técnico del cliente. El soporte técnico debe comprobar si el correo es peligroso y enviar una respuesta al usuario (véase [Responder acerca de un correo marcado](#) en la página 192). Por defecto, el soporte técnico puede responder a través de una página web. Entonces se enviará un correo automático con la respuesta al usuario.



IMPORTANTE:

Para que los correos marcados se puedan reenviar al soporte técnico del cliente, un administrador a nivel de cliente debe introducir la dirección de correo electrónico del soporte técnico en la pestaña del módulo **Security Awareness Service > Configuración** (véase [Configurar el simulacro de phishing](#)).

Responder acerca de un correo marcado



Se cumplen las siguientes condiciones:



- Un administrador a nivel de cliente ha introducido la dirección de correo electrónico del soporte técnico del cliente en el campo **Reenviar los correos marcados a la siguiente dirección de correo:** de la pestaña del módulo **Security Awareness Service > Configuración** (véase [Configurar el simulacro de phishing](#)).
- Un usuario ha marcado un correo que no forma parte del simulacro de phishing de Security Awareness Service mediante el complemento Phishing Reporter.

Como soporte técnico del cliente, puede responder a los usuarios que han marcado correos que no forman parte del simulacro de phishing mediante el complemento Phishing Reporter acerca de los correos marcados (véase [Respuesta acerca de correos marcados](#) en la página 192). Cuando un usuario marca un correo sospechoso, éste se envía por correo electrónico como archivo .eml adjunto al soporte técnico para su análisis. Después de analizar el correo marcado, puede enviar una respuesta al usuario.

**Nota:**

Por defecto, el soporte técnico puede dar su respuesta al usuario a través de una página web. Este proceso se describe a continuación. Sin embargo, si un administrador ha desactivado la función de respuesta con un solo clic (véase el paso 12 en la página 153 en el capítulo [Configurar el simulacro de phishing](#)), el soporte técnico no recibe ningún enlace a una página web, sino que debe ponerse en contacto con el usuario por sí mismo.

1. Abra el correo que se ha enviado a la dirección de correo electrónico indicada del soporte técnico.

2.

**PELIGRO:**

El correo marcado puede suponer un riesgo de seguridad. Por tanto, trate el correo con cuidado.

Compruebe si el correo marcado es peligroso.

3. Haga clic en el enlace de respuesta en el correo dirigido al soporte técnico.

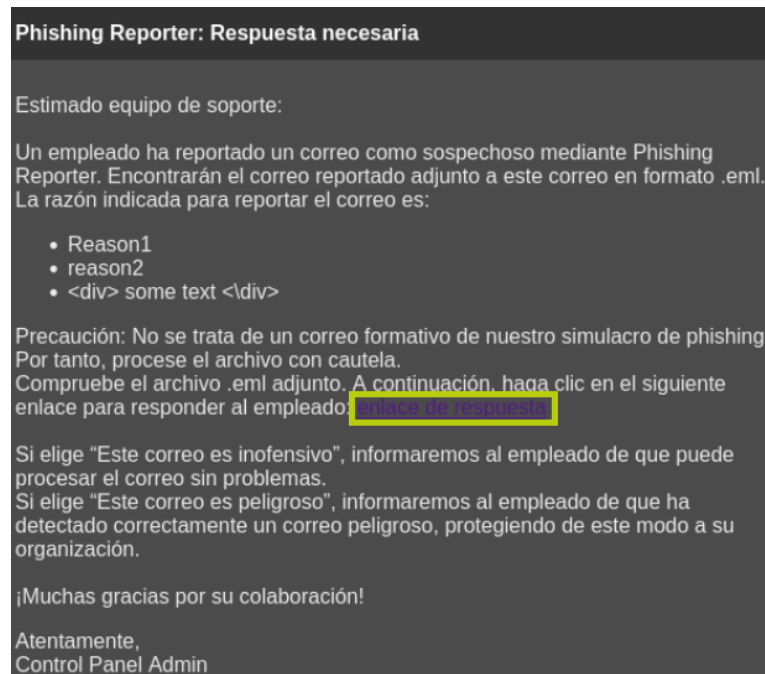


Figura 253: Abrir enlace

- ➔ Se abre una página web en el navegador. En esta página web puede dejar su respuesta acerca del correo marcado.

4. Deje su respuesta acerca del correo marcado. Tiene las siguientes opciones:

- **¡Este correo es peligroso!**
- **Este correo es seguro.**

- ➔ Un correo con su respuesta se envía al usuario que ha marcado el correo.

- ✓ Se ha enviado una respuesta acerca de un correo marcado que no forma parte del simulacro de phishing.

Si el correo marcado es peligroso, tome medidas adicionales (p. ej., eliminarlo del buzón de correo del usuario).

Utilizar Phishing Reporter en Outlook

Mediante el complemento Phishing Reporter, los usuarios pueden marcar correos en Outlook.

- ✓ Un administrador ha instalado el complemento Phishing Reporter y lo ha puesto a su disposición (véase [Instalar Phishing Reporter en Microsoft 365](#) en la página 182, [Instalar](#)



[Phishing Reporter en un servidor Exchange local](#) en la página 185 y [Proporcionar Phishing Reporter en un servidor Exchange local](#) en la página 187).

Mediante Phishing Reporter, puede marcar correos sospechosos en Outlook.

1. Abra Outlook.
2. En su bandeja de entrada, haga clic en el correo que desee marcar.

**PELIGRO:**

El correo puede contener contenido malicioso.

Los correos con contenido malicioso pueden causar daños en su ordenador, provocar pérdidas de datos irreversibles o dar lugar al robo de datos importantes.

No haga clic en ningún archivo adjunto o enlace del correo.

3. En la esquina superior izquierda, seleccione la pestaña **Inicio**.

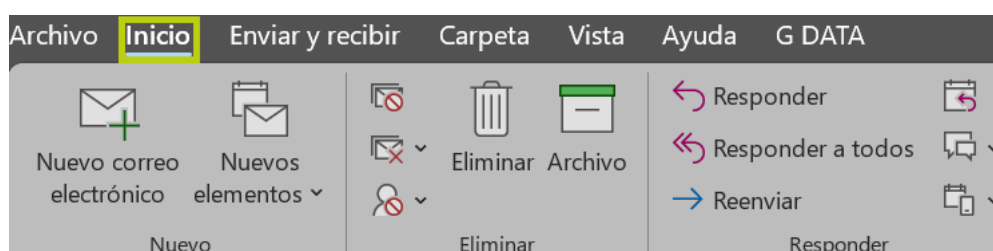


Figura 254: Seleccionar la pestaña Inicio

4. Busque el complemento Phishing Reporter en la barra de herramientas.

Si no se muestra el complemento Phishing Reporter, haga clic en la flecha a la derecha.

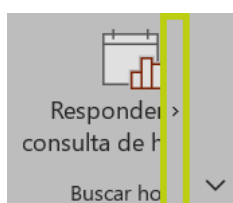


Figura 255: Flecha de la barra de herramientas

Si el complemento Phishing Reporter sigue sin mostrarse al llegar al final de la barra de herramientas, haga clic en **Todas las aplicaciones**.

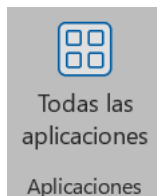


Figura 256: Todas las aplicaciones

Se abre una nueva ventana en la que se muestran todos los complementos.

5. Haga clic en **Marcar correo**.



Figura 257: Reportar correo

**Nota:**

Si ha marcado un correo del simulacro de phishing, recibe una respuesta inmediata.

Si el correo marcado no forma parte del simulacro de phishing, se reenviará a una dirección establecida por el administrador. Las personas responsables, p. ej., el soporte técnico, analizarán y comprobarán el correo. Por tanto, puede tardar un tiempo hasta que reciba una respuesta.

**PELIGRO:**

El correo marcado puede contener contenido malicioso.

Los correos con contenido malicioso pueden causar daños en su ordenador, provocar pérdidas de datos irreversibles o dar lugar al robo de datos.

Solo interactúe con el correo después de haber recibido información sobre el procedimiento a seguir.

6. Opcional: Puede indicar la razón por la que ha denunciado el correo. Haga clic en el campo de comentarios.



Un correo se ha marcado mediante el complemento Phishing Reporter en Outlook.

Solución de problemas: El Teachable Moment no se muestra

Problema

Después de que un usuario haya sido engañado por un correo del simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#)), la página explicativa sobre el ataque de phishing (el Teachable Moment) no se muestra en el navegador.

Causa

El cliente usa un proxy cuya lista blanca se basa en direcciones IP. La dirección IP del Teachable Moment no está autorizada en el proxy.

Solución

Añada la dirección IP 94.100.132.71 (Teachable Moment) a la lista blanca del proxy.



Teachable Moments se pueden mostrar en el navegador.

Marcado de correos sin complementos

Durante el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#)), los usuarios de clientes que emplean el complemento Phishing Reporter (véase [Phishing Reporter](#) en la página 174) o Hornetsecurity Outlook Add-in (véase el manual [Outlook Add-in para clientes de 365 Total Protection](#)) pueden denunciar correos sospechosos directamente en Outlook mediante el complemento correspondiente. Los correos de phishing simulado detectados correctamente se incluyen en la evaluación del simulacro de phishing del usuario.

Sin embargo, también es posible marcar correos sospechosos sin el complemento Phishing Reporter ni Hornetsecurity Outlook Add-in. Para hacerlo, los usuarios deben reenviar los correos sospechosos a la dirección **reportto@hornetsecurity.com** (véase [Marcar un correo sin complementos](#) en la página 198). Los correos enviados como archivo adjunto deben estar sin modificar. Todos los correos reenviados que formen parte del simulacro de phishing se añaden al cálculo del Employee Security Index (ESI[®], véase [Employee Security Index \(ESI[®]\)](#) en la página 8) en la evaluación del usuario.

**IMPORTANTE:**

Los correos que se marquen por reenvío a **reportto@hornetsecurity.com** (véase [Marcar un correo sin complementos](#) en la página 198) deben conservar su encabezado original. Si los correos se reenvían de entornos Exchange a entornos que no sean Exchange, el encabezado suele cambiar. Los correos reenviados cuyo encabezado haya cambiado no se añaden al cálculo del Employee Security Index (ESI[®], véase [Employee Security Index \(ESI®\)](#) en la página 8).

**Nota:**

Los usuarios de un cliente pueden utilizar el reenvío en paralelo con un complemento para marcar los correos electrónicos.

**Nota:**

También es posible que una persona distinta al destinatario original reenvíe el correo sospechoso. Por ejemplo, podría hacerlo el soporte técnico de la organización del cliente.

**IMPORTANTE:**

Los usuarios no reciben ninguna notificación acerca de si el correo reenviado realmente formaba parte del simulacro de phishing. Tampoco tomamos ninguna otra medida respecto a los correos marcados.

Los correos sospechosos pueden reenviarse en diversos clientes de correo electrónico. A modo de ejemplo se explica cómo reenviar un correo sospechoso en Outlook (véase [Marcar un correo sin complementos](#) en la página 198).

Marcar un correo sin complementos

Usted puede denunciar un correo sospechoso durante el simulacro de phishing de Security Awareness Service (véase [Acerca de Security Awareness Service](#)) sin utilizar ningún complemento (véase [Marcado de correos sin complementos](#) en la página 197) reenviando el correo en cuestión como archivo adjunto. El correo enviado como archivo adjunto debe estar sin modificar. Los correos sospechosos pueden reenviarse en diversos clientes de correo electrónico. A continuación se describe el procedimiento en Outlook a modo de ejemplo.

**Nota:**

Esta descripción se basa en Outlook para Microsoft 365 en su versión de 2023.

**Nota:**

También es posible que una persona distinta al destinatario original reenvíe el correo sospechoso. Por ejemplo, podría hacerlo el soporte técnico de la organización del cliente.

1.

**IMPORTANTE:**

Es preciso conservar el encabezado original del mensaje y abrir el correo tal y como lo recibió el destinatario original. Solo en ese caso puede identificarse como parte del simulacro de phishing. Sin embargo, no se identificará correctamente si se ha reenviado previamente en formato de texto y el destinatario del reenvío lo abre y, a continuación, lo reenvía en forma de archivo adjunto, pues los encabezados del correo habrán cambiado. Si los correos se reenvían de entornos Exchange a entornos que no sean Exchange, el encabezado suele cambiar. Los correos reenviados cuyo encabezado haya cambiado no se añaden al cálculo del Employee Security Index (ESI[®], véase [Employee Security Index \(ESI®\)](#) en la página 8).

Sin embargo, una persona a la que el destinatario original haya reenviado el correo en formato .eml podrá reportarlo reenviando el mismo archivo .eml. Como en este caso los encabezados del correo original no habrán cambiado, el correo se identificará correctamente como parte del simulacro de phishing.

Abra el correo sospechoso en Outlook.



El correo se muestra.

2. Haga clic en el icono de los tres puntos de la esquina superior derecha.

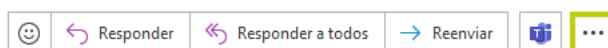


Figura 258: Abrir acciones avanzadas



Se muestran más opciones.

3. Haga clic en la acción **Reenviar como datos adjuntos**.

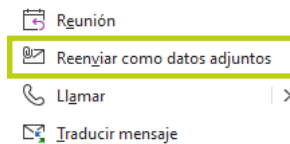


Figura 259: Seleccionar una acción

- ➔ Se abre una nueva ventana con un borrador de mensaje. El correo sospechoso está adjunto.
- 4. Introduzca la dirección de correo electrónico **reportto@hornetsecurity.com** en el campo **Para**.

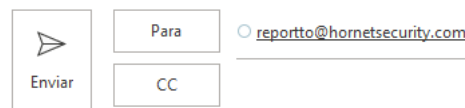


Figura 260: Introducir una dirección de correo electrónico

- 5. Haga clic en **Enviar**.
- ➔ El correo sospechoso se reenvía como archivo adjunto. Si el archivo reenviado forma parte del simulacro de phishing, el correo computa como correo identificado correctamente para el cálculo del ESI® (véase [Employee Security Index \(ESI®\)](#) en la página 8).

**IMPORTANTE:**

No se emite ninguna respuesta acerca de si el correo sospechoso realmente formaba parte del simulacro de phishing. Tampoco tomamos ninguna otra medida respecto al correo marcado.



Se ha marcado un correo sospechoso.

Configurar los tutoriales



Ha activado los tutoriales de Security Awareness Service (véase [Activar o desactivar los tutoriales](#) en la página 82).

En el módulo **Security Awareness Service > Configuración** puede usted configurar los tutoriales de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7), así



como activar y configurar el Awareness Engine. Los tutoriales forman a sus usuarios en temas de seguridad informática. Eso aumenta la seguridad dentro de su organización. Los tutoriales se proporcionan a cada usuario en su User Panel personal.

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 configurar los tutoriales.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .
5. En **Inicio del primer tutorial**, seleccione la fecha en la que desee que comiencen los primeros tutoriales.

i Nota:

A partir de esta fecha, los primeros tutoriales se les asignarán a los usuarios del cliente. Pero no todos los usuarios recibirán su primer tutorial en esta fecha. Los tutoriales se irán asignando a lo largo de los días siguientes. Solo es posible seleccionar días laborables, pues los tutoriales no pueden empezar el fin de semana.



Figura 261: Seleccionar una fecha

6. Opcional: Si desea que todos los tutoriales se proporcionen automáticamente a todos los usuarios, accione el interruptor **Poner todos los tutoriales a disposición de todos los usuarios**.

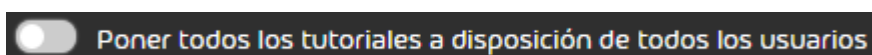


Figura 262: Activar la proporción automática de los tutoriales para todos los usuarios.

**i Nota:**

Por defecto, el interruptor está gris y los tutoriales se asignan o mediante Awareness Engine o mediante el calendario de tutoriales.

i Nota:

Si activa este interruptor, sus usuarios verán todos los tutoriales existentes en su User Panel. Cuando un usuario hace clic en un tutorial y lo inicia, el tutorial se le asignará a este usuario.

➔ El interruptor se pone verde.

7. Opcional: Si desea desactivar los correos de invitación para los tutoriales, desactive el interruptor **Enviar correos de invitación para los tutoriales**.



Figura 263: Desactivar los correos de invitación

8. Opcional: Si desea desactivar los correos de recordatorio para los tutoriales, desactive el interruptor **Enviar correos de recordatorio para los tutoriales no finalizados**.



Figura 264: Desactivar correos de recordatorio

i Nota:

Por defecto, el interruptor está verde y los usuarios reciben correos de recordatorio para los tutoriales. Los correos de recordatorio y las invitaciones a los tutoriales se enviarán a los usuarios en función de su zona horaria y dentro del horario laboral.

**Nota:**

Las invitaciones y los recordatorios de tutoriales se envían en uno de los cuatro idiomas de Control Panel (inglés, alemán, español, francés). Si un idioma para Security Awareness Service (véase [Sincronizar puestos e idiomas para Security Awareness Service](#) en la página 135) está configurado para un usuario y este idioma corresponde a uno de los idiomas de Control Panel, se utiliza este idioma. Sino, se utiliza el idioma seleccionado por el usuario en User Panel (véase ["Configuración de usuario"](#)). Si el usuario no ha configurado su idioma en User Panel, se utiliza en su lugar el idioma de Control Panel del cliente.

**Nota:**

Aunque haya desactivado el interruptor **Enviar correos de recordatorio para los tutoriales no finalizados**, se les seguirán asignando tutoriales a los usuarios.



El interruptor se pone gris.

9.

**IMPORTANTE:**

Solo puede establecer el intervalo de los correos de recordatorio si el interruptor **Enviar correos de recordatorio para los tutoriales no finalizados** está activado.

Opcional: Establezca el intervalo de los correos de recordatorio.

cada 30 días

Figura 265: Establecer el intervalo de los correos de recordatorio

10. En **Número máximo de meses sin tutoriales**, seleccione el número máximo de meses durante los cuales Awareness Engine no asignará nuevos tutoriales a los usuarios a menos que el usuario haya caído en correos del simulacro de phishing durante este tiempo.



Figura 266: Seleccionar periodo sin tutoriales

i Nota:

Durante los primeros 3 meses después de empezar los tutoriales, se les asignarán periódicamente nuevos tutoriales a los usuarios. Si un usuario no ha caído en los correos del simulacro de phishing hasta entonces, no recibirá más tutoriales durante el periodo seleccionado. Tomando el ejemplo de 2 meses, esto significa que solo se le asignará un nuevo tutorial a un usuario después de otros 2 meses (es decir, 5 meses después del inicio de los tutoriales).

Si el usuario cae en menos del 20 por ciento de los correos del simulacro de phishing, solo recibirá un nuevo tutorial después del periodo seleccionado, en este ejemplo, después de otros 2 meses. Pero si el usuario cae en al menos el 20 por ciento de los correos del simulacro de phishing durante este periodo, se le asignará inmediatamente un nuevo tutorial. El periodo seleccionado empieza de nuevo en la fecha en la que se asigna el tutorial.

11. Haga clic en **Aplicar cambios**.

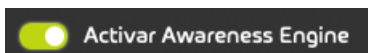


Los cambios se guardan.

12. Si desea activar el Awareness Engine, active la opción **Activar Awareness Engine** en **Awareness Engine**.

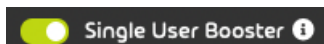
**Nota:**

El Awareness Engine automatiza procesos recurrentes como el envío de correos de phishing simulados y la asignación de tutoriales. Si no se desea que los tutoriales se asignen automáticamente a los usuarios, sino que sean en su lugar los administradores quienes los asignen, es preciso desactivar el Awareness Engine. En tal caso, los tutoriales pueden administrarse en el calendario de tutoriales (véase [Programar tutoriales sin Awareness Engine](#) en la página 206). De esta forma, un administrador también puede excluir tutoriales específicos al no establecer una fecha para uno o más tutoriales (véase los pasos 9 en la página 208 y 10 en la página 208 en el capítulo [Programar tutoriales sin Awareness Engine](#) en la página 206).

**Figura 267: Activar Awareness Engine**

Se habilitan ajustes adicionales en **Awareness Engine**.

13. Si desea que se forme selectivamente a los usuarios rezagados de grupos aventajados, active la opción **Single User Booster**.

**Figura 268: Activar Single User Booster**

14. Si desea que los usuarios más aventajados de grupos rezagados reciban menos tutoriales que el resto del grupo, active la opción **Productivity Booster**.
15. Si desea que los usuarios reciban únicamente los tutoriales que estén disponibles en el idioma del usuario o de la organización, desactive la opción **Enviar tutoriales independientemente del idioma del usuario**.

**Nota:**

Por defecto, esta opción está activada. En tal caso es posible que a los usuarios se les asignen tutoriales que no se encuentren ni en su idioma de usuario para Security Awareness Service (véase [Editar los datos básicos de un buzón de correo](#)) ni en el idioma de la organización (véase [Añadir información sobre su organización](#) en la página 155).



 Enviar tutoriales independientemente del idioma del usuario 

Figura 269: Tutoriales



Se han activado los tutoriales y el Awareness Engine.

Awareness Engine

El Awareness Engine de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) evalúa periódicamente la conducta de seguridad de los usuarios. Para ello, el Awareness Engine analiza cuándo el usuario hace clic en enlaces de correos de phishing simulados y cuándo los reporta. En base a esto, el Awareness Engine decide el modo en que deben seguir formándose los grupos de Security Awareness Service. Así, cada usuario obtiene tanta formación como sea necesaria, pero tan poca como sea posible. El Awareness Engine evalúa a los usuarios cada tres meses y planifica la formación para los siguientes tres meses.



Nota:

Las funciones automatizadas del Awareness Engine se pueden utilizar sin activar Single User Booster o Productivity Booster. Sin embargo, el Awareness Engine tiene en cuenta Single User Booster y Productivity Booster si éstos se encuentran activados.

Programar tutoriales sin Awareness Engine



Ha activado los tutoriales (véase [Activar o desactivar los tutoriales](#) en la página 82) y desactivado el Awareness Engine (véase el paso 12 en la página 204 del capítulo [Configurar los tutoriales](#) en la página 200).

En el módulo **Security Awareness Service > Configuración** puede programar los tutoriales de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) para sus usuarios con el calendario de tutoriales en lugar de usar el Awareness Engine (véase [Awareness Engine](#) en la página 206).

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 programar tutoriales por sí mismo.
3. Vaya a **Security Awareness Service > Configuración**.
4. Seleccione la pestaña .



5. Desplácese hasta la sección **Calendario de tutoriales**.

➔ Se muestra una tabla con los tutoriales disponibles.

CALENDARIO DE TUTORIALES

En la siguiente tabla puede asignar tutoriales manualmente. Sin embargo, le recomendamos emplear nuestro Awareness Engine en su lugar. Seleccione los tutoriales deseados e introduzca la fecha de asignación. En la fecha seleccionada, sus usuarios recibirán una invitación por correo electrónico para acceder a los nuevos contenidos. Es posible realizar cambios en todo momento antes de la fecha de asignación, pero no tras ella. Se enviarán recordatorios automáticos por correo electrónico a sus usuarios cuando tengan tutoriales pendientes.

+ Planificar asignación del tutorial

Título del tutorial	Asignado	Fecha de asignación
«Macros peligrosas: Emotet y la pandemia de virus de macro»	x	23-12-08
Estafas con tarjetas regalo	✓	23-12-07
Test rápido: Vishing	✓	23-12-08
Adware & Malvertising	✓	23-12-12
Tarjeta de emergencias de TI	✓	23-12-12

Figura 270: Calendario de tutoriales

6. Haga clic en **Planificar asignación del tutorial**.

CALENDARIO DE TUTORIALES

En la siguiente tabla puede asignar tutoriales manualmente. Sin embargo, le recomendamos emplear nuestro Awareness Engine en su lugar. Seleccione los tutoriales deseados e introduzca la fecha de asignación. En la fecha seleccionada, sus usuarios recibirán una invitación por correo electrónico para acceder a los nuevos contenidos. Es posible realizar cambios en todo momento antes de la fecha de asignación, pero no tras ella. Se enviarán recordatorios automáticos por correo electrónico a sus usuarios cuando tengan tutoriales pendientes.

+ Planificar asignación del tutorial

Título del tutorial	Asignado	Fecha de asignación
«Macros peligrosas: Emotet y la pandemia de virus de macro»	x	23-12-08
Estafas con tarjetas regalo	✓	23-12-07
Test rápido: Vishing	✓	23-12-08
Adware & Malvertising	✓	23-12-12
Tarjeta de emergencias de TI	✓	23-12-12

Figura 271: Vaya a Planificar asignación del tutorial.

➔ Se abre otro menú.

7. Haga clic en **Seleccionar un tutorial**.

+ Planificar asignación del tutorial

Título del tutorial

Seleccionar un tutorial

Fecha de asignación

2023-12-11

Añadir

Figura 272: Vaya a Seleccionar un tutorial.



- ➔ Se abre una lista con todos los tutoriales.
- 8. Desplácese hasta el tutorial que desee añadir y haga clic en el tutorial.

i Nota:

También puede buscar un tutorial específico introduciendo el título del tutorial en la barra de búsqueda.

- ➔ Se ha seleccionado un tutorial.
- 9. Haga clic en la fecha en **Fecha de asignación**.

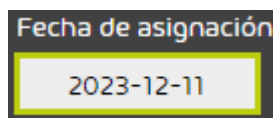


Figura 273: Vaya a Fecha de asignación.

- ➔ Se abre un calendario.
- 10. Seleccione la fecha deseada.
- 11. Haga clic en **Añadir**.
- 12. Opcional: Mientras que el tutorial no se haya asignado, todavía puede modificar la fecha de asignación.

i NOTA:

Una modificación posterior del tutorial solo es posible mientras que el tutorial no se haya asignado.

- a) Haga clic en la flecha de menú en la fila del tutorial cuya fecha de asignación desee modificar.



Figura 274: Ir a la flecha de menú

- ➔ Se abre otra barra de menú debajo del tutorial seleccionado.
- b) Haga clic en **Modificar fecha de asignación**.

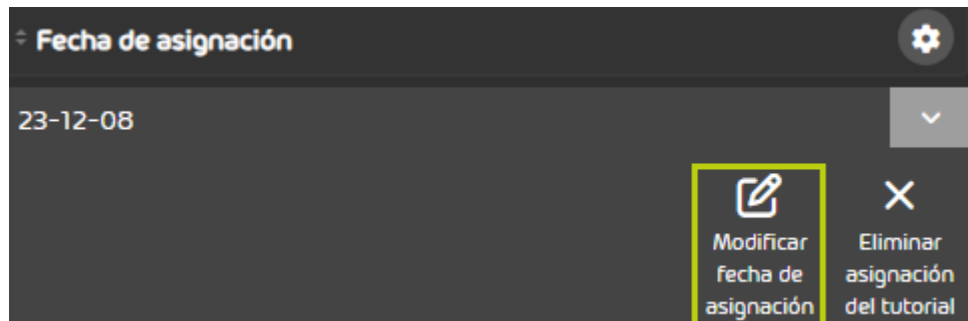


Figura 275: Vaya a Modificar fecha de asignación.

- ➔ En la esquina inferior izquierda se muestra la fila **Nueva fecha de asignación**.
 - c) Al lado izquierdo, haga clic en la fecha y seleccione una nueva fecha.
 - d) Haga clic en **Aplicar**.
 - ➔ Se ha modificado la fecha de asignación.
13. Opcional: Mientras que el tutorial no se haya asignado, todavía puede eliminar el tutorial.
- a) Haga clic en la flecha de menú en la fila del tutorial que desee eliminar.

Título del tutorial	Asignado	Fecha de asignación	
«Macros peligrosas: Emotet y la pandemia de virus de macros»	X	23-12-08	⌵

Figura 276: Ir a la flecha de menú

- ➔ Se abre otra barra de menú debajo del tutorial seleccionado.
 - b) Haga clic en **Eliminar asignación del tutorial**.



Figura 277: Vaya a Eliminar asignación del tutorial.



- ➔ Se muestra una nueva ventana.

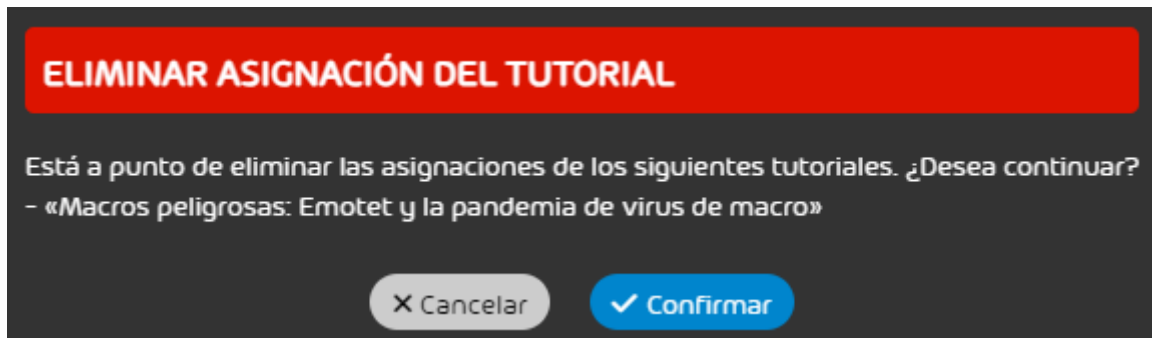


Figura 278: Muestra de la nueva ventana

- c) Haga clic en **Confirmar**.

- ➔ La asignación del tutorial seleccionado se ha eliminado.

- ✓ Se ha configurado la asignación manual de tutoriales mediante el calendario de tutoriales.



Supervisión

En el módulo **Security Awareness Service > Supervisión**, los administradores pueden ver qué usuarios se han excluido automáticamente (véase [Usuarios excluidos automáticamente](#) en la página 211) de Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) y, o bien excluirllos del mismo explícitamente o bien volver a incluirlos.

Usuarios excluidos automáticamente

Por defecto, Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) se aplica a todos los usuarios de un cliente. Sin embargo, también es posible excluir a usuarios del servicio. Por una parte, los administradores pueden excluirllos por sí mismos (véase [Excluir un usuario](#) en la página 141). Por otra parte, los usuarios a los que no se les haya podido entregar tres correos de phishing simulados seguidos se excluyen automáticamente del servicio.

Los usuarios excluidos automáticamente se enumeran en el módulo **Security Awareness Service > Supervisión** (véase [Supervisión](#) en la página 211). Allí, los administradores pueden volver a admitir a los usuarios en el servicio (véanse [Reincluir a un usuario](#) en la página 212, [Reincluir a varios usuarios](#) en la página 213 y [Reincluir a todos los usuarios](#) en la página 216). En tal caso, se volverá a intentar entregarles correos de phishing simulado. Sin embargo, en caso de otros tres intentos fallidos, los usuarios volverán a excluirse automáticamente.

Los administradores pueden excluir explícitamente de Security Awareness Service a usuarios excluidos automáticamente (véanse [Excluir a un usuario](#) en la página 217, [Excluir a varios usuarios](#) en la página 219 y [Excluir a todos los usuarios](#) en la página 220). En tal caso, los usuarios se añadirán a la lista de usuarios excluidos del módulo **Security Awareness Service > Configuración**.

Cuando un usuario es excluido automáticamente o manualmente de Security Awareness Service, los ajustes existentes del usuario acerca de Security Awareness Service se eliminan. Esto también afecta a ajustes relativos a la privacidad. Si el usuario vuelve a incluirse en Security Awareness Service más adelante, deberá volver a realizar dichos ajustes.

Además, los administradores pueden ver un registro para cada usuario excluido automáticamente en el que se incluye información sobre el último intento de entrega fallido de un correo de phishing simulado (véase [Mostrar el registro](#) en la página 222).



Reincluir a un usuario

Puede reincluir en Security Awareness Service a un usuario que haya sido excluido automáticamente del mismo (véase [Usuarios excluidos automáticamente](#) en la página 211).



PRECAUCIÓN:

Cuando un usuario es excluido automáticamente o manualmente de Security Awareness Service, los ajustes que éste haya hecho en su User Panel se eliminan (véase [Configuración de usuario](#)). Esto afecta también a ajustes relativos a la privacidad, como la prohibición de enviar correos de phishing simulado en nombre del usuario. Cuando un usuario vuelve a incluirse en Security Awareness Service, se le aplica la configuración por defecto. Por tanto, las prohibiciones que el usuario hubiese establecido en el pasado ya no están vigentes.

Informe al usuario acerca de su reinclusión en Security Awareness Service y pídale que vuelva a realizar sus ajustes de privacidad en User Panel.



Nota:

En lugar de reincluir a un solo usuario, los administradores pueden aplicar esta acción también a varios usuarios (véase [Reincluir a varios usuarios](#) en la página 213) o a todos los usuarios excluidos automáticamente (véase [Reincluir a todos los usuarios](#) en la página 216).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyo usuario excluido automáticamente de Security Awareness Service desee reincluir en el mismo.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en la flecha de menú junto al usuario que desee reincluir en Security Awareness Service.



Nota:

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, los buzones de reenvío no se muestran en la lista de usuarios excluidos automáticamente.



Figura 279: Abrir el menú

- ➔ Se abre un menú.



Figura 280: Menú

- Haga clic en **Reincluir**.

- ➔ Se muestra una ventana de confirmación.

- Haga clic en **Confirmar**.

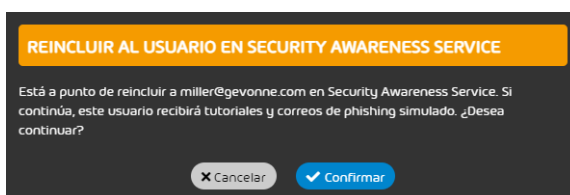


Figura 281: Confirmar

- ➔ El usuario se reincluye en Security Awareness Service y se elimina de la lista de usuarios excluidos automáticamente.

**Nota:**

Si la entrega de correos de phishing simulado al usuario falla tres veces consecutivas, éste volverá a excluirse automáticamente del servicio.

- Informe al usuario afectado acerca de su reinclusión en Security Awareness Service y pídale que vuelva a realizar sus ajustes de privacidad en User Panel.



- Un usuario excluido automáticamente de Security Awareness Service se ha reincluido en el mismo.

Reincluir a varios usuarios

Puede reincluir en Security Awareness Service a varios usuarios que hayan sido excluidos automáticamente del mismo (véase [Usuarios excluidos automáticamente](#) en la página 211).

**PRECAUCIÓN:**

Cuando un usuario es excluido automáticamente o manualmente de Security Awareness Service, los ajustes que éste haya hecho en su User Panel se eliminan (véase [Configuración de usuario](#)). Esto afecta también a ajustes relativos a la privacidad, como la prohibición de enviar correos de phishing simulado en nombre del usuario. Cuando un usuario vuelve a incluirse en Security Awareness Service, se le aplica la configuración por defecto. Por tanto, las prohibiciones que el usuario hubiese establecido en el pasado ya no están vigentes.

Informe al usuario acerca de su reinclusión en Security Awareness Service y pídale que vuelva a realizar sus ajustes de privacidad en User Panel.

**Nota:**

En lugar de reincluir a varios usuarios, los administradores pueden aplicar esta acción también a un solo usuario (véase [Reincluir a un usuario](#) en la página 212) o a todos los usuarios excluidos automáticamente (véase [Reincluir a todos los usuarios](#) en la página 216).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos usuarios excluidos automáticamente de Security Awareness Service desee reincluir en el mismo.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en
- ➔ En la lista de usuarios excluidos se muestra una columna con casillas. Por encima de la lista se muestran las acciones deshabilitadas **Reincluir** y **Excluir**.
5. Marque las casillas de los usuarios que desee reincluir en Security Awareness Service.

**Nota:**

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, los buzones de reenvío no se muestran en la lista de usuarios excluidos automáticamente.



Figura 282: Seleccionar usuarios

- ➔ Las acciones sobre la lista se habilitan.

6. Haga clic en **Reincluir**.

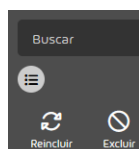


Figura 283: Reincluir usuarios seleccionados

- ➔ Se muestra una ventana de confirmación.

7. Haga clic en **Confirmar**.

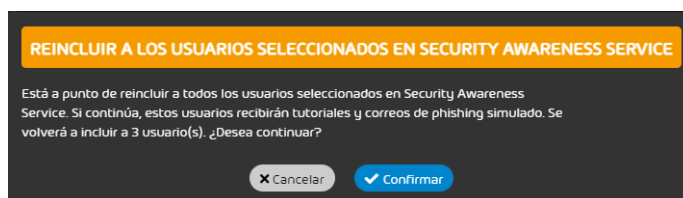


Figura 284: Confirmar

- ➔ Los usuarios seleccionados se reincluyen en Security Awareness Service y se eliminan de la lista de usuarios excluidos automáticamente.

**Nota:**

Si la entrega de correos de phishing simulado a un usuario falla tres veces consecutivas, éste volverá a excluirse automáticamente del servicio.

8. Informe a todos los usuarios afectados acerca de su reinclusión en Security Awareness Service y pídeles que vuelvan a realizar sus ajustes de privacidad en User Panel.



Varios usuarios excluidos automáticamente de Security Awareness Service se han reincluido en el mismo.



Reincluir a todos los usuarios

Puede reincluir en Security Awareness Service a todos los usuarios que hayan sido excluidos automáticamente del mismo (véase [Usuarios excluidos automáticamente](#) en la página 211).



PRECAUCIÓN:

Cuando un usuario es excluido automáticamente o manualmente de Security Awareness Service, los ajustes que éste haya hecho en su User Panel se eliminan (véase [Configuración de usuario](#)). Esto afecta también a ajustes relativos a la privacidad, como la prohibición de enviar correos de phishing simulado en nombre del usuario. Cuando un usuario vuelve a incluirse en Security Awareness Service, se le aplica la configuración por defecto. Por tanto, las prohibiciones que el usuario hubiese establecido en el pasado ya no están vigentes.

Informe al usuario acerca de su reinclusión en Security Awareness Service y pídale que vuelva a realizar sus ajustes de privacidad en User Panel.



Nota:

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, no es posible incluir buzones de reenvío en el servicio.



Nota:

En lugar de reincluir a todos los usuarios, los administradores pueden aplicar esta acción también a un solo usuario (véase [Reincluir a un usuario](#) en la página 212) o a varios usuarios excluidos automáticamente (véase [Reincluir a varios usuarios](#) en la página 213).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos usuarios excluidos automáticamente de Security Awareness Service desee reincluir en el mismo.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en **Reincluir a todos los usuarios**.

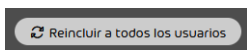


Figura 285: Reincluir todos los usuarios



➔ Se muestra una ventana de confirmación.

5. Haga clic en **Confirmar**.

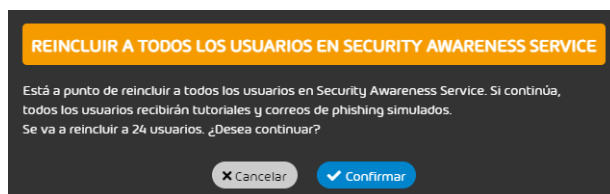


Figura 286: Confirmar

➔ Todos los usuarios se reincluyen en Security Awareness Service y se eliminan de la lista de usuarios excluidos automáticamente.



Nota:

Si la entrega de correos de phishing simulado a un usuario falla tres veces consecutivas, éste volverá a excluirse automáticamente del servicio.

6. Informe a todos los usuarios afectados acerca de su reinclusión en Security Awareness Service y pídeles que vuelvan a realizar sus ajustes de privacidad en User Panel.



Todos los usuarios excluidos automáticamente de Security Awareness Service se han reincluido en el mismo.

Excluir a un usuario

Puede excluir explícitamente de Security Awareness Service a un usuario que haya sido excluido automáticamente del mismo (véase [Usuarios excluidos automáticamente](#) en la página 211). Si el usuario afectado había hecho ajustes personales en User Panel, éstos se eliminan.



Nota:

En lugar de excluir a varios usuarios, puede aplicar esta acción también a varios usuarios (véase [Excluir a varios usuarios](#) en la página 219) o a todos los usuarios excluidos automáticamente (véase [Excluir a todos los usuarios](#) en la página 220).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyo usuario excluido automáticamente de Security Awareness Service desee excluir explícitamente del mismo.



3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en la flecha de menú junto al usuario que desee excluir de Security Awareness Service.

 Nota:

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, los buzones de reenvío no se muestran en la lista de usuarios excluidos automáticamente.



Figura 287: Abrir el menú

-  Se abre un menú.



Figura 288: Menú

5. Haga clic en **Excluir**.
-  Se muestra una ventana de confirmación.
6. Haga clic en **Confirmar**.

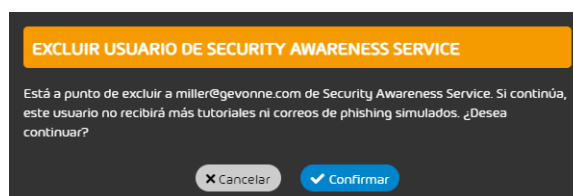


Figura 289: Confirmar

-  El usuario se excluye explícitamente de Security Awareness Service y se elimina de la lista de usuarios excluidos automáticamente. En su lugar, el usuario se añade a la lista de usuarios excluidos del módulo **Security Awareness Service > Configuración** (véase [Excluir un usuario](#) en la página 141). Los ajustes existentes del usuario acerca de Security Awareness Service se eliminan.

-  Se ha excluido explícitamente a un usuario de Security Awareness Service. Los ajustes personales del usuario excluido acerca de Security Awareness Service se han eliminado.



Excluir a varios usuarios

Puede excluir explícitamente de Security Awareness Service a varios usuarios que hayan sido excluidos automáticamente del mismo (véanse [Usuarios excluidos automáticamente](#) en la página 211 y Si los usuarios afectados habían hecho ajustes personales en User Panel, éstos se eliminan.).

**Nota:**

En lugar de excluir a varios usuarios, puede aplicar esta acción también a un solo usuario (véase [Excluir a un usuario](#) en la página 217) o a todos los usuarios excluidos automáticamente (véase [Excluir a todos los usuarios](#) en la página 220).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos usuarios excluidos automáticamente de Security Awareness Service desee excluir explícitamente del mismo.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en
- ➔ En la lista de usuarios excluidos se muestra una columna con casillas. Por encima de la lista se muestran las acciones deshabilitadas **Reincluir** y **Excluir**.
5. Marque las casillas de los usuarios que desee excluir explícitamente de Security Awareness Service.

**Nota:**

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, los buzones de reenvío no se muestran en la lista de usuarios excluidos automáticamente.



Figura 290: Seleccionar usuarios



Las acciones sobre la lista se habilitan.



- Haga clic en **Excluir**.

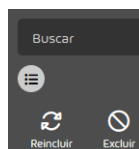


Figura 291: Excluir usuarios seleccionados

- Se muestra una ventana de confirmación.
- Haga clic en **Confirmar**.

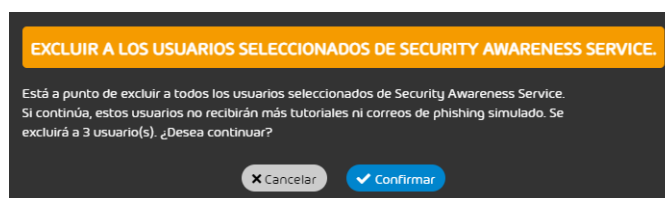


Figura 292: Confirmar

- Los usuarios seleccionados se excluyen explícitamente de Security Awareness Service y se eliminan de la lista de usuarios excluidos automáticamente. En su lugar, los usuarios se añaden a la lista de usuarios excluidos en el módulo **Security Awareness Service > Configuración** (véase [Excluir un usuario](#) en la página 141). Los ajustes existentes de los usuarios acerca de Security Awareness Service se eliminan.
- Varios usuarios excluidos automáticamente de Security Awareness Service se han excluido explícitamente. Los ajustes personales acerca de Security Awareness Service realizados por los usuarios excluidos se han eliminado.

Excluir a todos los usuarios

Puede excluir explícitamente de Security Awareness Service a todos los usuarios que hayan sido excluidos automáticamente del mismo (véanse [Usuarios excluidos automáticamente](#) en la página 211 y Si los usuarios afectados habían hecho ajustes personales en User Panel, éstos se eliminan.).



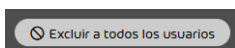
Nota:

Security Awareness Service no se aplica a buzones de correo de reenvío (véase [Tipos de buzón de correo](#)). Por tanto, tampoco es posible excluir buzones de reenvío del servicio.

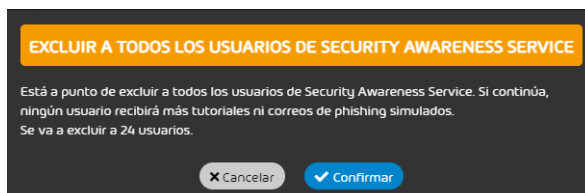
**Nota:**

En lugar de excluir a todos los usuarios, puede aplicar esta acción también a un solo usuario (véase [Excluir a un usuario](#) en la página 217) o a varios usuarios excluidos automáticamente (véase [Excluir a varios usuarios](#) en la página 219).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos usuarios excluidos automáticamente de Security Awareness Service desee excluir explícitamente del mismo.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en **Excluir a todos los usuarios**.

**Figura 293: Excluir a todos los usuarios**

- ➔ Se muestra una ventana de confirmación.
5. Haga clic en **Confirmar**.

**Figura 294: Confirmar**

- ➔ Todos los usuarios se excluyen explícitamente de Security Awareness Service y se eliminan de la lista de usuarios excluidos automáticamente. En su lugar, los usuarios se añaden a la lista de usuarios excluidos en el módulo **Security Awareness Service > Configuración** (véase [Excluir un usuario](#) en la página 141). Los ajustes existentes de los usuarios acerca de Security Awareness Service se eliminan.
- ✓ Todos los usuarios excluidos automáticamente de Security Awareness Service se han excluido explícitamente. Los ajustes personales acerca de Security Awareness Service realizados por los usuarios excluidos se han eliminado.



Mostrar el registro

Puede ver un registro del último intento de entrega fallido de un correo de phishing simulado a un usuario excluido automáticamente de Security Awareness Service (véase [Usuarios excluidos automáticamente](#) en la página 211). Dicho registro es realizado por nuestro servidor de correo electrónico que envió el correo de phishing simulado. El registro incluye datos acerca del envío del correo y puede ayudar a identificar la causa del fallo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el usuario cuyo registro desee ver.
3. Vaya a **Security Awareness Service > Supervisión**.
4. Haga clic en la flecha de menú junto al usuario cuyo registro desee ver.



Figura 295: Abrir el menú



Se abre un menú.



Figura 296: Menú

5. Haga clic en **Mostrar registro**.
- ➔ Se muestra un campo de texto con el registro.
6. Opcional: Si desea copiar el texto del registro, haga clic en  junto al campo de texto.
- ➔ El texto del registro se copia en el portapapeles.



El registro de un usuario excluido automáticamente de Security Awareness Service se ha visualizado.



Certificados

Los administradores a nivel de cliente pueden solicitar un certificado como parte del Security Awareness Service. Los usuarios pueden descargar sus logros de la formación online en forma de certificado.

Cuando un cliente haya participado con éxito en Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) durante al menos 12 meses, los administradores a nivel de cliente pueden solicitar un certificado (véase [Certificado de cliente](#) en la página 223 y [Solicitar certificado de cliente](#) en la página 224). Los usuarios también pueden descargar un certificado por sus tutoriales completados (véase [Tutoriales](#)) en el módulo **Logros** del User Panel (véase [Acerca de User Panel](#)) (véase [Descargar un certificado](#)).

Certificado de cliente

Cuando un cliente haya participado con éxito en Security Awareness Service (véase [Acerca de Security Awareness Service](#) en la página 7) durante al menos 12 meses, los administradores a nivel de cliente pueden solicitar un certificado (véase [Solicitar certificado de cliente](#) en la página 224). Este certificado de cliente sirve como prueba de la formación realizada y puede presentarse durante auditorías.

**Nota:**

Si el cliente ha pausado su participación en Security Awareness Service durante más de 3 meses, solo se tendrá en cuenta para el certificado el periodo transcurrido desde la reanudación.

Si, en el momento de solicitar el certificado, el período mínimo de participación de 12 meses se ha cumplido solo para el simulacro de phishing o solo para los tutoriales, el certificado solo se expedirá para esta parte de Security Awareness Service.

Solo se puede solicitar un certificado por año y cliente.

El certificado solo se expide a solicitud del cliente y es válido durante un año. La renovación del certificado puede solicitarse anualmente.



Solicitar certificado de cliente



El cliente participa en Security Awareness Service desde hace al menos 12 meses.

Cuando un cliente haya participado en Security Awareness Service durante al menos 12 meses, puede solicitar un certificado de cliente (véase [Certificado de cliente](#) en la página 223). Para solicitar un certificado de cliente, proceda del siguiente modo.

**Nota:**

Si el cliente ha pausado su participación en Security Awareness Service durante más de 3 meses, solo se tendrá en cuenta para el certificado el periodo transcurrido desde la reanudación.

Si, en el momento de solicitar el certificado, el período mínimo de participación de 12 meses se ha cumplido solo para el simulacro de phishing o solo para los tutoriales, el certificado solo se expedirá para esta parte de Security Awareness Service.

Solo se puede solicitar un certificado por año y cliente.

**Nota:**

Solo los administradores del cliente están autorizados a solicitar un certificado de cliente.

1. Prepare un correo electrónico con la solicitud.
2. Incluya la siguiente información en el correo:
 - Dominio para el que se solicita el certificado
 - Nombre oficial del cliente, tal como debe figurar en el certificado
3. Envíe el correo a certificate@cloud-security.net.



El soporte técnico tramita la solicitud y le envía el certificado por correo electrónico.



Se ha solicitado un certificado de cliente.

Certificado de usuario

En el módulo **Logros** de User Panel, los usuarios pueden descargar un certificado sobre los tutoriales que han completado.



Los usuarios pueden descargar un certificado por los tutoriales completados (véase [Tutoriales](#)) en el módulo **Logros** del User Panel (véase [Acerca de User Panel](#)) (véase [Descargar un certificado](#)).



Nota:

Si los certificados de usuario se descargan a través del módulo **Logros**, el logotipo de Hornetsecurity se incluye en el certificado. El idioma del certificado es personalizable.

Index

A

activación

Security Awareness Service, *See* Security Awareness Service activación

activar

regla de transporte, *See* regla de transporte activar

Security Awareness Service, *See* Security Awareness Service activar

simulacro de phishing, *See* Security Awareness Service activar el simulacro de phishing

tutoriales, *See* Security Awareness Service activar tutoriales

advertencias

explicación [5](#), [173](#)

ajustar

entrega avanzada en Microsoft 365 Defender, *See* Microsoft 365 configurar automáticamenteSecurity Awareness Service

Microsoft 365 automáticamenteSecurity Awareness Service, *See* Microsoft 365 configurar automáticamenteSecurity Awareness Service

simulacro de phishing, *See* Security Awareness Service configurar el simulacro de phishing

tutoriales, *See* Security Awareness Service configurar los tutoriales

anuncio

Security Awareness Service, *See* Security Awareness Service anuncio

añadir

cargo a Security Awareness Service, *See* Security Awareness Service añadir cargo

grupo a Security Awareness Service, *See* Security Awareness Service añadir un grupo

archivos adjuntos

crear regla de transporte, *See* Security Awareness Service crear regla de transporte para archivos adjuntos

asignar

cargo de su organización, *See* usuario asignar cargo de su organización

ataques simulados

estadísticaSecurity Awareness Service [108](#)

aumentar

prioridad de la directiva de enlaces seguros, *See* enlaces seguros aumentar la prioridad de la directiva

Awareness Engine

explicación, *See* Security Awareness Service Awareness Engine

B

botón de informe de Microsoft

desactivar, *See* desactivar botón de informe de Microsoft para usuarios en Outlook

Botón de informe de Microsoft para usuarios en Outlook

desactivar, *See* desactivar botón de informe de Microsoft para usuarios en Outlook

buscar

correos de phishing simulado en Microsoft 365Security Awareness Service, *See* simulacro de phishing buscar

correos en Microsoft 365Security Awareness Service

C

cambiar

orden de grupos en Security Awareness Service, *See* Security Awareness Service modificar orden de grupos

características

correos de phishing simuladoSecurity Awareness Service, *See* simulacro de phishing características de correos de phishing simuladoSecurity Awareness Service

- cargar
 - configuración de filtroSecurity Awareness Service, *See* configuración de filtro cargarSecurity Awareness Service
- cargo
 - añadir a Security Awareness Service, *See* Security Awareness Service añadir cargo
- certificado de cliente
 - Security Awareness Service, *See* Security Awareness Service certificado de cliente
 - solicitarSecurity Awareness Service [224](#)
- certificado de usuario
 - Security Awareness Service, *See* Security Awareness Service certificado de usuario
- cliente
 - incorporación genérica, *See* cliente con Microsoft 365 crear
- cliente con Microsoft 365
 - crear [11](#)
- clientes de Microsoft 365
 - sincronizar automáticamente en Control Panel [12](#)
- códigos de idioma
 - sincronizaciónSecurity Awareness Service [137](#)
- complemento
 - Phishing ReporterSecurity Awareness Service [174](#)
- comprobar
 - correo marcado mediante el complemento Phishing ReporterSecurity Awareness Service, *See* Phishing Reporter
 - enviar respuesta acerca de un correo marcadoSecurity Awareness Service
- configuración
 - Security Awareness Service, *See* Security Awareness Service configuración
- configuración con Microsoft 365, *See* incorporación genérica
- configuración de filtro
 - cargarSecurity Awareness Service [98](#)
 - crearSecurity Awareness Service [97](#)
 - eliminarSecurity Awareness Service [99](#)
- correo de prueba
 - enviar para el simulacro de phishing, *See* simulacro de phishing enviar correo de prueba
 - registro de envío, *See* registro envío de correos de prueba
 - resultados, *See* simulacro de phishing resultados de los correos de prueba
- correo electrónico
 - marcar correo mediante el complemento Phishing ReporterSecurity Awareness Service, *See* Phishing Reporter
 - respuesta acerca de correos marcadosSecurity Awareness Service
 - marcar sin complementoSecurity Awareness Service, *See* simulacro de phishing marcar correos sospechosos sin complementoSecurity Awareness Service
- correos de phishing con éxito
 - estadísticaSecurity Awareness Service [109](#)
- correos marcados
 - estadísticaSecurity Awareness Service [113](#)
- crear
 - cliente con Microsoft 365 [11](#)
 - configuración de filtroSecurity Awareness Service, *See* configuración de filtro crearSecurity Awareness Service
 - enlace para la incorporación genérica [15](#)

D

- desactivar
 - botón de informe de Microsoft para usuarios en Outlook [71](#)
 - simulacro de phishing, *See* Security Awareness Service desactivar el simulacro de phishing
 - simulacro de suplantación de identidad para todos los usuarios, *See* simulacro de suplantación de identidad
 - configurar
 - tutoriales, *See* Security Awareness Service desactivar tutoriales

descargar

- lista de dominios de remitentes permitidos, *See simulacro de phishing* descargar listas de dominios permitidos
- lista de dominios para enlaces en correos de phishing, *See simulacro de phishing* descargar listas de dominios permitidos
- listas de dominios permitidos, *See simulacro de phishing* descargar listas de dominios permitidos

description

- niveles de phishingSecurity Awareness Service, *See niveles simulacro de phishing*Security Awareness Service

desinstalar

- Phishing ReporterSecurity Awareness Service, *See Security Awareness Service* desinstalar complemento Phishing Reporter

direcciones IP

- correos de phishing simuladoSecurity Awareness Service, *See simulacro de phishing* características de correos de phishing simuladoSecurity Awareness Service

DKIM, firma

- correos de phishing simuladoSecurity Awareness Service, *See simulacro de phishing* características de correos de phishing simuladoSecurity Awareness Service

documentación

- indicaciones [5, 173](#)
- símbolos [5, 173](#)

dominios

- simulacro de phishing, *See Security Awareness Service* dominios de envío para simulacro de phishing

dominios de remitentes para correos de phishing

- descargar lista, *See simulacro de phishing* descargar listas de dominios permitidos
- generar lista, *See simulacro de phishing* generar listas de dominios permitidos

dominios para enlaces en correos de phishing

- descargar lista, *See simulacro de phishing* descargar listas de dominios permitidos
- generar lista, *See simulacro de phishing* generar listas de dominios permitidos

E

eliminar

- configuración de filtroSecurity Awareness Service, *See configuración de filtro* eliminarSecurity Awareness Service
- grupo de Security Awareness Service, *See Security Awareness Service* eliminar un grupo
- usuarios de la lista de usuarios excluidos, *See Security Awareness Service* eliminar usuarios de la lista de usuarios excluidos

emplear

- Phishing ReporterSecurity Awareness Service, *See Security Awareness Service* utilizar el complemento Phishing Reporter

Employee Security Index [8](#)

- estadísticaSecurity Awareness Service, *See ESI[®]* estadísticaSecurity Awareness Service
- estadísticasSecurity Awareness Service, *See ESI[®]* estadísticasSecurity Awareness Service
- evolución temporalSecurity Awareness Service, *See ESI[®]* evolución temporalSecurity Awareness Service

enlace

- crear regla de transporte, *See Security Awareness Service* crear regla de transporte para enlaces

enlace para la incorporación genérica

- crear [15](#)

enlaces seguros

- aumentar la prioridad de la directiva [69](#)

entrega avanzada

- configurar automáticamente en Microsoft 365 Defender, *See Microsoft 365* configurar automáticamenteSecurity Awareness Service

ESI[®]

- estadísticaSecurity Awareness Service [104](#)
- estadísticasSecurity Awareness Service [104](#)
- evolución temporalSecurity Awareness Service [106](#)
- See also* Employee Security Index

estadística

ataques simuladosSecurity Awareness Service, *See* ataques simulados estadísticaSecurity Awareness Service
correos de phishing con éxito, *See* correos de phishing con éxito estadísticaSecurity Awareness Service
correos marcadosSecurity Awareness Service, *See* correos marcados estadísticaSecurity Awareness Service
ESI[®] Security Awareness Service, *See* ESI[®] estadísticasSecurity Awareness Service
evolución temporal del ESI[®] Security Awareness Service, *See* ESI[®] evolución temporalSecurity Awareness Service
grupos, *See* estadísticas de grupos Security Awareness Service
niveles de usuariosSecurity Awareness Service, *See* niveles de usuarios estadísticaSecurity Awareness Service
progreso de formación, *See* progreso de formación Security Awareness Service
Security Awareness Service, *See* Security Awareness Service estadística
simulacro de phishingSecurity Awareness Service, *See* simulacro de phishing estadísticasSecurity Awareness Service
trucos psicológicos, *See* trucos psicológicos Security Awareness Service
tutorial, *See* tutorial estadística
usuarios en formación de refuerzo, *See* formación de refuerzo Security Awareness Service

estadísticas

cargar una configuración de filtroSecurity Awareness Service, *See* configuración de filtro cargarSecurity Awareness Service
crear una configuración de filtroSecurity Awareness Service, *See* configuración de filtro crearSecurity Awareness Service
eliminar una configuración de filtroSecurity Awareness Service, *See* configuración de filtro eliminarSecurity Awareness Service
estado de formación, *See* estado de formación Security Awareness Service
exportar en formato CSVSecurity Awareness Service [102](#)
filtrar por gruposSecurity Awareness Service [95](#)
filtro de gruposSecurity Awareness Service [95](#)
interacción con el Teachable MomentSecurity Awareness Service, *See* interacción con el Teachable Moment estadísticasSecurity Awareness Service
niveles de phishingSecurity Awareness Service, *See* niveles simulacro de phishingSecurity Awareness Service
seleccionar el periodo de visualizaciónSecurity Awareness Service, *See* periodo de visualización
seleccionarSecurity Awareness Service

estadísticas de grupos

Security Awareness Service [119](#)

estadísticas de Security Awareness Service

programar informes mensualesSecurity Awareness Service, *See* Security Awareness Service programar informes mensualesSecurity Awareness Service

estado de formación

Security Awareness Service [118](#)

Exchange

configuración para Security Awareness Service, *See* Security Awareness Service autorizaciones para el simulacro de phishing

excluir

usuario de Security Awareness Service, *See* Security Awareness Service excluir un usuario

explicación

advertencias [5](#), [173](#)

indicaciones de seguridad [5](#), [173](#)

Security Awareness Service, *See* Security Awareness Service explicación

exportar en formato CSV

estadísticas, *See* estadísticas exportar en formato CSVSecurity Awareness Service

F

Filtrar

estadísticas por gruposSecurity Awareness Service, *See* estadísticas filtrar por gruposSecurity Awareness Service
usuarios excluidos, *See* Security Awareness Service filtrar usuarios excluidos

filtro de grupos

estadísticasSecurity Awareness Service, *See* estadísticas filtro de gruposSecurity Awareness Service

filtros

estadísticas, *See* estadísticas filtro de gruposSecurity Awareness Service

formación de refuerzo

Security Awareness Service [117](#)

G

generar

lista de dominios de remitentes permitidos, *See* simulacro de phishing generar listas de dominios permitidos

lista de dominios para enlaces en correos de phishing, *See* simulacro de phishing generar listas de dominios permitidos

listas de dominios permitidos, *See* simulacro de phishing generar listas de dominios permitidos

grupo

añadir a Security Awareness Service, *See* Security Awareness Service añadir un grupo

eliminar de Security Awareness Service, *See* Security Awareness Service eliminar un grupo

grupos

filtrar estadísticasSecurity Awareness Service, *See* estadísticas filtrar por gruposSecurity Awareness Service

I

identificar

correos de phishing simuladoSecurity Awareness Service, *See* simulacro de phishing características de correos de phishing simuladoSecurity Awareness Service

idioma

sincronizarSecurity Awareness Service, *See* sincronizar puesto e idiomaSecurity Awareness Service

incluir automáticamente a nuevos usuarios

simulacro de suplantación de identidad, *See* simulacro de suplantación de identidad configurar

incorporación genérica [10](#)

cliente con Microsoft 365, *See* crear cliente con Microsoft 365

indicaciones

documentación [5](#), [173](#)

indicaciones de seguridad

explicación [5](#), [173](#)

infraestructura

configuración para el simulacro de phishing [160](#)

instalar

Phishing Reporter en Microsoft 365Security Awareness Service, *See* Security Awareness Service instalar el complemento Phishing Reporter en Microsoft 365

Phishing Reporter en un servidor Exchange localSecurity Awareness Service, *See* Security Awareness Service

instalar el complemento Phishing Reporter en un servidor Exchange local

interacción con el Teachable Moment

estadísticasSecurity Awareness Service [115](#)

L

lista blanca

Security Awareness Service, *See* Security Awareness Service autorizaciones para el simulacro de phishing simulacro de phishing, *See* Security Awareness Service autorizaciones para el simulacro de phishing

listas de dominios permitidos

descargar, *See* simulacro de phishing descargar listas de dominios permitidos

generar, *See* simulacro de phishing generar listas de dominios permitidos

M

marcar

correos sin complementoSecurity Awareness Service, *See* simulacro de phishing marcar correos sospechosos sin complementoSecurity Awareness Service

Microsoft 365

aumentar la prioridad de la directiva de enlaces seguros, *See* enlaces seguros aumentar la prioridad de la directiva configuración para el simulacro de phishing, *See* Security Awareness Service configuración en Microsoft 365

configurar automáticamenteSecurity Awareness Service [28](#)

crear directiva de vínculos seguros, *See* Security Awareness Service crear directiva de vínculos seguros

habilitar entrega de correos de phishing simulados, *See* Security Awareness Service configurar la entrega avanzada en Microsoft 365 Defender

Microsoft 365 Defender

configurar la entrega avanzada automáticamente, *See* Microsoft 365 configurar automáticamenteSecurity Awareness Service

modo de privacidad

Security Awareness Service, *See* Security Awareness Service modo de privacidad

mostrar

registro de un usuario excluido automáticamenteSecurity Awareness Service, *See* Security Awareness Service

mostrar registro de un usuario excluido automáticamente

N

niveles

simulacro de phishingSecurity Awareness Service [111](#)

niveles de phishing

descriptionSecurity Awareness Service, *See* niveles simulacro de phishingSecurity Awareness Service

niveles de usuarios

estadísticaSecurity Awareness Service [110](#)

O

onprem

configuración para Security Awareness Service, *See* Security Awareness Service autorizaciones para el simulacro de phishing

orden de grupos

modificar en Security Awareness Service, *See* Security Awareness Service modificar orden de grupos

organización

añadir información para Security Awareness Service, *See* Security Awareness Service añadir información sobre su organización

Outlook

reenviar correos sospechososSecurity Awareness Service, *See* simulacro de phishing marcar correos sospechosos sin complementoSecurity Awareness Service

P

periodo de visualización

seleccionarSecurity Awareness Service [100](#)

Phishing Reporter

desinstalarSecurity Awareness Service, *See* Security Awareness Service desinstalar complemento Phishing Reporter

emplearSecurity Awareness Service, *See* Security Awareness Service utilizar el complemento Phishing Reporter

enviar respuesta acerca de un correo marcadoSecurity Awareness Service [192](#)

explicación [174](#)

instalar en Microsoft 365Security Awareness Service, *See* Security Awareness Service instalar el complemento Phishing Reporter en Microsoft 365

- instalar en un servidor Exchange localSecurity Awareness Service, *See* Security Awareness Service instalar el complemento Phishing Reporter en un servidor Exchange local
- proporcionar en un servidor Exchange localSecurity Awareness Service [187](#)
- requisitos técnicos [176](#)
- respuesta acerca de correos marcadosSecurity Awareness Service [192](#)
- solución de problemas, *See* solución de problemas Phishing Reporter
- plantilla
 - anuncio de Security Awareness Service, *See* Security Awareness Service anuncio
- preparativos
 - Security Awareness Service, *See* Security Awareness Service preparación de los sistemas
- prioridad de los grupos
 - modificar en Security Awareness Service, *See* Security Awareness Service modificar orden de grupos
- programar
 - Security Awareness Service, *See* Security Awareness Service programar informes mensualesSecurity Awareness Service
 - tutoriales sin Awareness Engine, *See* Security Awareness Service programar tutoriales sin Awareness Engine
- programar informes mensuales
 - estadísticas de Security Awareness ServiceSecurity Awareness Service, *See* Security Awareness Service programar informes mensualesSecurity Awareness Service
- progreso de formación
 - Security Awareness Service [116](#)
- proporcionar
 - Phishing Reporter en un servidor Exchange localSecurity Awareness Service, *See* Phishing Reporter proporcionar en un servidor Exchange localSecurity Awareness Service
- puesto
 - sincronizaciónSecurity Awareness Service [137](#)
 - sincronizarSecurity Awareness Service, *See* sincronizar puesto e idiomaSecurity Awareness Service

R

- reenviar
 - correos sospechososSecurity Awareness Service, *See* simulacro de phishing marcar correos sospechosos sin complementoSecurity Awareness Service
- reenvío
 - correo sospechosoSecurity Awareness Service, *See* simulacro de phishing marcar correos sospechosos sin complementoSecurity Awareness Service
- registro
 - envío de correos de prueba [170](#)
 - mostrar para un usuario excluido automáticamenteSecurity Awareness Service, *See* Security Awareness Service mostrar registro de un usuario excluido automáticamente
- regla de transporte
 - activar [63](#)
 - crear para archivos adjuntos, *See* Security Awareness Service crear regla de transporte para archivos adjuntos
 - crear para enlaces, *See* Security Awareness Service crear regla de transporte para enlaces
- reglas de transporte
 - Security Awareness Service, *See* Security Awareness Service reglas de transporte
- requisitos
 - Phishing Reporter, *See* Phishing Reporter requisitos técnicos
- respuesta
 - correo marcado mediante el complemento Phishing ReporterSecurity Awareness Service, *See* Phishing Reporter enviar respuesta acerca de un correo marcadoSecurity Awareness Service

S

- Security Awareness Service
 - activación [77](#)

- activar [77](#)
- activar el simulacro de phishing [79](#)
- activar tutoriales [82](#)
- anuncio [85](#)
- añadir cargo [133](#)
- añadir información sobre su organización [155](#)
- añadir un grupo [127](#)
- autorizaciones para el simulacro de phishing [17](#)
- Awareness Engine [206](#)
- certificado de cliente [223](#), [223](#)
- certificado de usuario [223](#), [224](#)
- configuración [127](#)
- configuración del servidor Exchange local, *See* Security Awareness Service autorizaciones para el simulacro de phishing
- configuración en Microsoft 365 [27](#)
- configurar el simulacro de phishing [148](#)
- configurar la entrega avanzada en Microsoft 365 Defender [31](#)
- configurar los tutoriales [200](#)
- crear directiva de vínculos seguros [64](#)
- crear regla de transporte para archivos adjuntos [35](#), [51](#)
- crear regla de transporte para enlaces [43](#), [57](#)
- desactivar el simulacro de phishing [73](#), [75](#), [79](#)
- desactivar tutoriales [82](#)
- desinstalar complemento Phishing Reporter [188](#)
- dominios de envío para simulacro de phishing [19](#)
- eliminar un grupo [130](#)
- eliminar usuarios de la lista de usuarios excluidos [146](#)
- enviando dominios, *See* Security Awareness Service dominios de envío para simulacro de phishing
- estadística [93](#)
- excluir explícitamente a todos los usuarios excluidos automáticamente [220](#)
- excluir explícitamente a un usuario excluido automáticamente [217](#)
- excluir explícitamente a varios usuarios excluidos automáticamente [219](#)
- excluir un usuario [141](#)
- explicación [7](#)
- filtrar usuarios excluidos [145](#)
- instalar el complemento Phishing Reporter en Microsoft 365 [182](#)
- instalar el complemento Phishing Reporter en un servidor Exchange local [185](#)
- lista blanca, *See* Security Awareness Service autorizaciones para el simulacro de phishing
- modificar orden de grupos [131](#)
- modo de privacidad [160](#)
- mostrar registro de un usuario excluido automáticamente [222](#)
- preparación de los sistemas [9](#)
- programar informes mensualesSecurity Awareness Service [124](#)
- programar tutoriales sin Awareness Engine [206](#)
- reglas de transporte [34](#)
- reincluir a todos los usuarios excluidos automáticamente [216](#)
- reincluir a un usuario individual [212](#)
- reincluir a varios usuarios [213](#)
- supervisión [211](#)
- usuarios excluidos automáticamente [211](#)
- utilizar el complemento Phishing Reporter [194](#)
- seguimiento de mensajes
 - buscar correos de phishing simuladoSecurity Awareness Service, *See* simulacro de phishing buscar correos en Microsoft 365Security Awareness Service
- seleccionar
 - período de visualización, *See* periodo de visualización seleccionarSecurity Awareness Service

servidor Exchange local

- configuración para Security Awareness Service, *See* Security Awareness Service autorizaciones para el simulacro de phishing
- proporcionar Phishing ReporterSecurity Awareness Service, *See* Phishing Reporter proporcionar en un servidor Exchange localSecurity Awareness Service

símbolos

- documentación [5](#), [173](#)

simulacro de phishing

- activar, *See* Security Awareness Service activar el simulacro de phishing
- ajustar, *See* Security Awareness Service configurar el simulacro de phishing
- buscar correos en Microsoft 365Security Awareness Service [89](#)
- características de correos de phishing simuladoSecurity Awareness Service [88](#)
- configuración de la infraestructura [160](#)
- configuración en Microsoft 365, *See* Security Awareness Service configuración en Microsoft 365
- configurar la entrega de correos en Microsoft 365, *See* Security Awareness Service configurar la entrega avanzada en Microsoft 365 Defender
- desactivar, *See* Security Awareness Service desactivar el simulacro de phishing
- descargar listas de dominios permitidos [166](#)
- direcciones IP, *See* Security Awareness Service autorizaciones para el simulacro de phishing
- enviando dominios, *See* Security Awareness Service dominios de envío para simulacro de phishing
- enviar correo de prueba [168](#)
- estadísticasSecurity Awareness Service [107](#)
- generar listas de dominios permitidos [161](#)
- marcar correos sospechosos sin complementoSecurity Awareness Service [197](#), [198](#)
- preparativos, *See* Security Awareness Service preparación de los sistemas
- reglas de transporte, *See* Security Awareness Service reglas de transporte
- resultados de los correos de prueba [170](#)

simulacro de suplantación de identidad

- configurar [158](#)
- incluir automáticamente a nuevos usuarios, *See* simulacro de suplantación de identidad configurar

simulacro de suplantación de identidad para todos los usuarios

- desactivar, *See* simulacro de suplantación de identidad configurar

sincronización

- idioma y puestoSecurity Awareness Service [137](#)

sincronizar

- buzones de Microsoft 365, *See* clientes de Microsoft 365 sincronizar automáticamente en Control Panel
- dominios de Microsoft 365, *See* clientes de Microsoft 365 sincronizar automáticamente en Control Panel
- grupos de Microsoft 365, *See* clientes de Microsoft 365 sincronizar automáticamente en Control Panel
- puesto e idiomaSecurity Awareness Service [135](#)

solicitar

- certificado de clienteSecurity Awareness Service, *See* certificado de cliente solicitarSecurity Awareness Service

solución de problemas

- Phishing Reporter [191](#), [197](#)

soporte técnico

- correos marcados mediante el complemento Phishing ReporterSecurity Awareness Service, *See* Phishing Reporter
- respuesta acerca de correos marcadosSecurity Awareness Service
- respuesta acerca de un correo marcadoSecurity Awareness Service, *See* Phishing Reporter enviar respuesta acerca de un correo marcadoSecurity Awareness Service

supervisión

- Security Awareness Service, *See* Security Awareness Service supervisión
- usuarios excluidos automáticamente, *See* Security Awareness Service usuarios excluidos automáticamente

T

Teachable Moment

- solución de problemas, *See* solución de problemas Phishing Reporter

trucos psicológicos

Security Awareness Service [113](#)

tutorial

estadística [116](#)

tutoriales

activar, *See* Security Awareness Service activar tutoriales

ajustar, *See* Security Awareness Service configurar los tutoriales

desactivar, *See* Security Awareness Service desactivar tutoriales

programar sin Awareness Engine, *See* Security Awareness Service programar tutoriales sin Awareness Engine

U

usuario

asignar cargo de su organización [133](#)

excluir de Security Awareness Service, *See* Security Awareness Service excluir un usuario

excluir explícitamente de Security Awareness Service (individual) [217](#)

excluir explícitamente de Security Awareness Service (todos) [220](#)

excluir explícitamente de Security Awareness Service (varios) [219](#)

reincluir en Security Awareness Service (individual) [212](#)

reincluir en Security Awareness Service (todos) [216](#)

reincluir en Security Awareness Service (varios) [213](#)

usuarios excluidos

eliminar, *See* Security Awareness Service eliminar usuarios de la lista de usuarios excluidos

filtrar, *See* Security Awareness Service filtrar usuarios excluidos

V

vínculos seguros

crear directiva

Microsoft 365

Crear una directiva de vínculos seguros, *See* Security Awareness Service crear directiva de vínculos seguros



HORNETSECURITY

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