ESET Cloud Office Security

Manual de usuario

Haga clic aquí para ver la versión de la Ayuda de este documento

Digital Security
Progress. Protected.

Copyright ©2023 de ESET, spol. s r.o.

ESET Cloud Office Security está desarrollado por ESET, spol. s r.o.

Para obtener más información, visite https://www.eset.com.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación ni transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de aplicación descrito sin previo aviso.

Soporte técnico: https://support.eset.com

REV. 20/12/2023

1 Visión general ... 1
1.1 Características principales ... 2
1.2 Novedades ... 5
1.3 Integración ... 6
2 Especificaciones ... 6
2.1 Requisitos ... 7
2.2 Planes de Microsoft 365 compatibles ... 7
2.3 Planes de Google Workspace compatibles ... 8
2.4 Navegadores de Internet compatibles ... 8
2.5 Limitaciones y política de retención de datos ... 9
3 Licencias de ESET Cloud Office Security ... 10
3.1 ESET Business Account ... 11
3.1 Crear una nueva cuenta de ESET Business Account ... 11
3.1 Agregar licencia de ESET Cloud Office Security en ESET Business Account ... 11
3.1 Administrar ESET Business Account ... 12
3.2 ESET MSP Administrator ... 13
4 Activación de ESET Cloud Office Security ... 14
4.1 Desactivar ESET Cloud Office Security ... 16
5 Administrar los inquilinos en Configuración ... 17
5.1 Agregue su primer inquilino ... 19
5.2 Inquilino de Microsoft 365 ... 21
5.3 Inquilino de Google Workspace ... 24
5.4 Eliminar inquilino de ESET Cloud Office Security ... 30
5.5 Quitar ESET Cloud Office Security del portal de Azure ... 31
6 Navegar por ESET Cloud Office Security ... 31
7 ESET LiveGuard Advanced ... 33
8 Panel ... 33
9 Usuarios ... 36
10 Equipos y sitios ... 37
11 Detecciones ... 38
12 Informes ... 39
13 Cuarentena ... 42
14 Registros del análisis ... 43
15 Políticas ... 44
15.1 Configuración de la protección de Exchange Online ... 47
15.2 Ajustes de protección de Gmail ... 50
15.3 Configuración de la protección de OneDrive ... 53
15.4 Configuración de la protección de Google Drive ... 54
15.5 Configuración de la protección de Grupos del equipo ... 55
15.6 Configuración de la protección de sitios de SharePoint ... 56
15.7 Ajustes de protección de ESET LiveGuard Advanced ... 57
15.8 Protección de informes y aprendizaje automático ... 58
16 Administración de licencias ... 60
16.1 Acceso de usuario de ESET Cloud Office Security a una empresa concreta ... 62
17 Registro de auditoría ... 63
18 Enviar opinión ... 64
19 Soporte técnico ... 64
20 Disponibilidad de los servicios ... 65

20.1 Seguridad para ESET Cloud Office Security 65
20.2 Términos de uso 69
20.2 Acuerdo de licencia para el usuario final 74
20.2 Acuerdo de procesamiento de datos 80
20.2 Cláusulas contractuales tipo 82
20.3 Política de privacidad 108

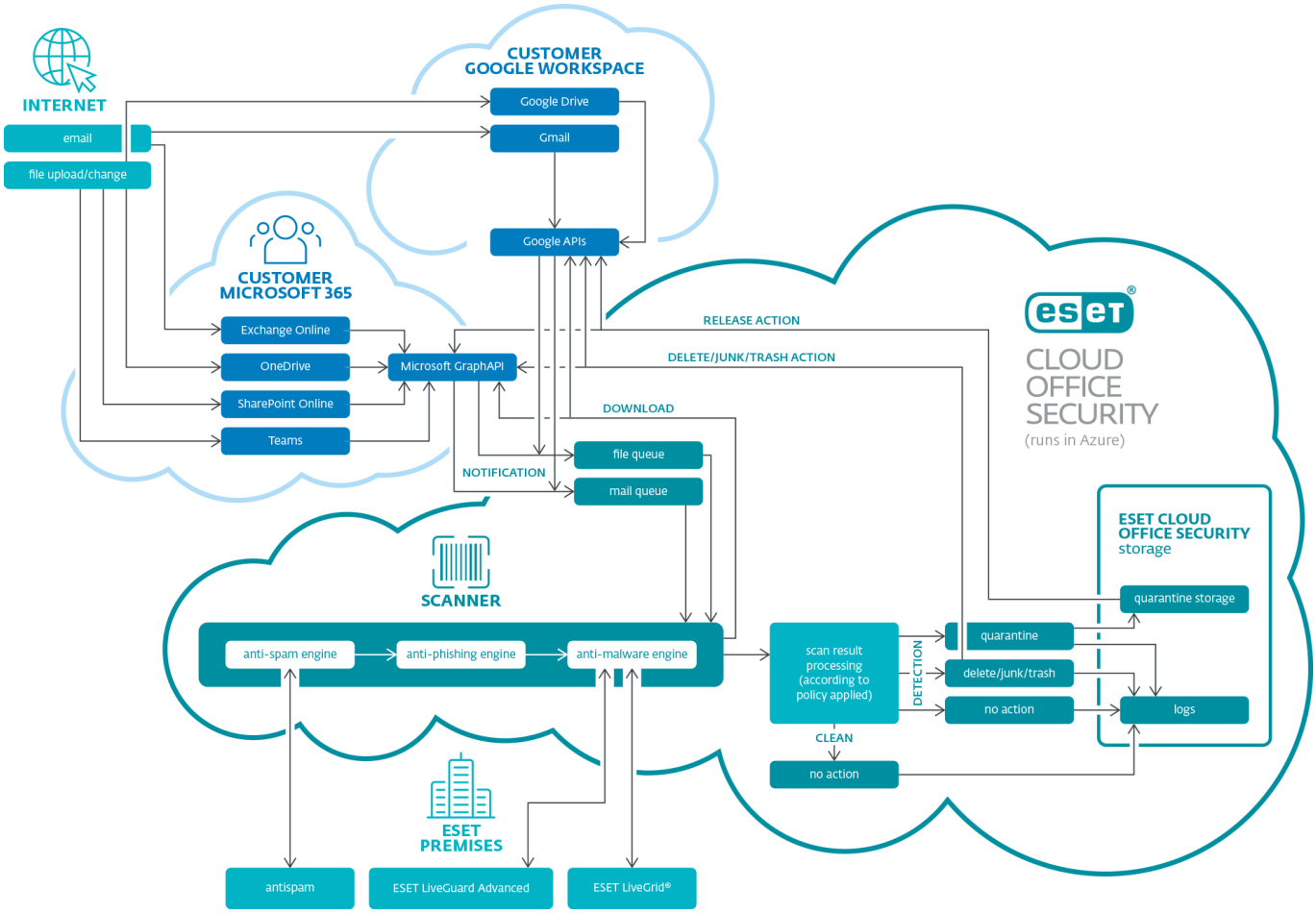
Visión general

ESET Cloud Office Security es un servicio en la nube multiinquilino y escalable en Microsoft Azure. ESET Cloud Office Security se ofrece como un Software-as-a-Service (SaaS) que funciona totalmente en la nube sin necesidad de hardware. Supone la combinación perfecta de filtrado de correo no deseado, análisis antimalware y protección antiphishing que ayuda a proteger las comunicaciones de su empresa frente al malware, minimiza los efectos negativos de los mensajes no solicitados en la productividad diaria, y evita que los correos electrónicos externos entrantes se utilicen como canal para ataques dirigidos.

Los servicios de seguridad de ESET Cloud Office Security cubren a los principales proveedores de plataformas en la nube y ofrecen una protección integral del correo electrónico con motores antimalware de última generación y ESET LiveGuard Advanced. Esta solución ofrece una defensa avanzada contra amenazas mediante entornos de prueba basados en la nube y análisis de muestras sospechosas en un entorno aislado.

La arquitectura de ESET Cloud Office Security le permite iniciar la protección rápidamente tras conectarse a una plataforma en la nube (Microsoft 365 y Google Workspace). Podrá administrar la protección en una consola basada en la web accesible desde cualquier lugar.

ESET Cloud Office Security proporciona protección preventiva avanzada para proteger las aplicaciones de Microsoft 365 de su empresa (Exchange Online, OneDrive, SharePoint Online y Teams). Se ofrece la misma protección en las aplicaciones de Google Workspace (Gmail y Google Drive).



ESET Cloud Office Security protege OneDrive y el buzón de correo de los usuarios con licencia, así como los grupos del equipo y los sitios de SharePoint. Cada almacén de estas aplicaciones de Microsoft 365 está protegido, independientemente del usuario que cargó el archivo o quién envía el mensaje de correo electrónico. El contenido en sí está protegido, sea cual sea el autor. El autor también puede ser un usuario invitado para garantizar la mejor protección posible.

Características principales

En la siguiente tabla se incluye una lista de funciones disponibles en ESET Cloud Office Security.

Varios inquilinos	Puede proteger y administrar varios inquilinos de Microsoft 365 y Google Workspace desde una consola ESET Cloud Office Security. Azure Active Directory (Azure AD) organiza objetos como usuarios y aplicaciones en grupos denominados inquilinos. Los inquilinos le permiten establecer políticas sobre los usuarios y las aplicaciones de su organización para cumplir las políticas de seguridad y operativas.

Antispam	Antispam es un componente básico para cualquier servidor de correo. ESET Cloud Office Security emplea un moderno motor antispam que protege de intentos de spam y de phishing con unas tasas de captura muy altas. ESET Cloud Office Security ha ganado de forma consecutiva las pruebas de filtrado de spam de Virus Bulletin, una empresa de pruebas de seguridad líder, y ha recibido la certificación VBSpam+ durante varios años. El motor de Antispam ha logrado una tasa de captura de spam del 99,99 % con cero falsos positivos, lo que lo convierte en la tecnología de protección contra el spam líder del sector. ESET Cloud Office Security Antispam está en la nube, y la mayoría de las bases de datos de la nube están en centros de datos de ESET. Los servicios en la nube Antispam permiten actualizar los datos rápidamente, lo que significa una reacción más rápida en caso de nuevo spam.
Protección Anti-Phishing	Esta función impide a los usuarios acceder a páginas web conocidas por sus actividades de phishing. Los mensajes de correo electrónico pueden contener vínculos que dirijan a páginas web de phishing, ESET Cloud Office Security utiliza un analizador sofisticado que busca en el cuerpo y asunto de los mensajes de correo electrónico entrantes para identificar dichos vínculos (URL). Los vínculos se comparan con una base de datos de phishing que se actualiza continuamente.
Protección antimalware	Una defensa galardonada e innovadora contra el malware; una tecnología de vanguardia que impide ataques. Elimina todo tipo de amenazas, incluidos virus, ransomware, rootkits, gusanos y spyware con análisis en la nube para conseguir tasas de detección todavía mejores. Ocupa poco espacio y no requiere demasiados recursos del sistema, por lo que no reduce su rendimiento. La detección contra malware utiliza un modelo de seguridad por capas. Cada capa, o fase, presenta un número de tecnologías centrales. La fase de ejecución previa incluye las siguientes tecnologías: Análisis UEFI (Unified Extensible Firmware Interface), Protección contra los ataques de red, Reputación y caché, Sandbox en el producto, Detecciones de ADN. Las tecnologías de la fase de Ejecución son Bloqueador de exploits, Protección contra ransomware, Análisis avanzado de memoria y Análisis de scripts (AMSI). En la fase Posterior a la ejecución se utilizan Protección contra botnets, Sistema de protección de malware en la nube y Entorno de pruebas. Este rico conjunto de funciones con tecnologías básicas proporciona un nivel de protección sin rival.
Políticas	Las organizaciones de mayor tamaño suelen tener varios departamentos y desean configurar diferentes ajustes de protección para cada unidad organizativa. ESET Cloud Office Security ofrece ajustes de protección basados en políticas que se pueden asignar a los inquilinos, usuarios, grupos del equipo o sitios de SharePoint seleccionados. Puede personalizar cada política de acuerdo con sus necesidades.
Administrador de la cuarentena	Inspeccione los objetos en cuarentena y realice una acción adecuada (descargar, eliminar o liberar). Esta función ofrece una administración sencilla de los mensajes de correo electrónico, los archivos adjuntos y los archivos de Exchange Online/OneDrive/Grupos del equipo/Sitios de SharePoint que ha puesto en cuarentena ESET Cloud Office Security. La descarga le ofrece la opción de analizar los objetos en cuarentena con herramientas de terceros, si es necesario, lo que puede resultar útil a la hora de decidir qué acción realizar.
Panel con estadísticas de detección	Consiga rápidamente información general sobre las actividades de seguridad de Microsoft 365. El panel contiene información esencial en cada una de sus pestañas de información general (Exchange Online/OneDrive/Grupos del equipo/Sitios de SharePoint). La información general de Usuario muestra el número de inquilinos y el uso de licencias, así como estadísticas de cada inquilino: número de usuarios, principales destinatarios de spam/phishing/malware y principales cuentas de OneDrive, grupos del equipo y sitios de SharePoint sospechosos. Puede elegir un periodo de tiempo y un inquilino para los que mostrar las estadísticas. En las pestañas de información general Exchange Online, OneDrive, Grupos del equipo y Sitios de SharePoint se pueden ver estadísticas y gráficos de detección adicionales. Se trata de estadísticas como el número de correos electrónicos y archivos analizados y el número de spam/phishing/malware detectado. Los gráficos muestran el tráfico de cada tipo de detección: spam, malware y phishing.

Detecciones con opciones de filtrado	Esta función contiene todos los registros sobre detecciones. Incluye registros de todas las detecciones realizadas por el análisis del correo electrónico en la pestaña Exchange Online, así como las realizadas por el análisis de archivos en la pestaña OneDrive/Grupos del equipo y Sitios de SharePoint. Esto permite filtrar y buscar de forma eficaz mediante información adicional sobre la detección específica (por ejemplo, el nombre de la amenaza, el hash del archivo, etc.).
Usuarios	La entidad central que protege ESET Cloud Office Security es la cuenta de usuario. Para obtener información útil, abra los detalles de un usuario, como la información general, la configuración definida por políticas, la lista de políticas asignadas al usuario y las detecciones de Exchange Online y OneDrive. Esta función ayuda cuando es necesario investigar las detecciones relacionadas con un usuario específico. También puede elegir qué usuarios desea proteger. Los usuarios se clasifican en grupos. Cada grupo es un inquilino de Microsoft 365 que contiene sus usuarios. Utilice múltiples criterios de filtrado para facilitar la búsqueda de un usuario específico dentro de un grupo.
Protección de informes y aprendizaje automático	El aprendizaje automático avanzado forma parte del motor de detección como capa de protección avanzada, que mejora la detección gracias al aprendizaje automático. Puede obtener más información sobre este tipo de protección en el glosario. Puede configurar niveles de información para las siguientes categorías: Malware, Aplicaciones potencialmente indeseables (PUA), Aplicaciones potencialmente sospechosas y Aplicaciones potencialmente peligrosas.
Informes (estadísticos y de cuarentena de correo electrónico)	Reciba datos estadísticos de Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint por correo electrónico, o genere y descargue un informe único para un período elegido. Puede programar informes para que se generen y distribuyan periódicamente a los destinatarios de correo electrónico especificados. Elija PDF o CSV como formato de salida. Los informes contienen datos, como un número de correos electrónicos analizados y malware, phishing y spam detectados. El formato PDF incluye gráficos con datos. Hay un gráfico para cada tipo de datos: correos electrónicos analizados, tráfico de malware, tráfico de phishing y tráfico de spam. También contienen estadísticas independientes de los destinatarios más destacados de cada categoría: malware, phishing y spam. Hay varias opciones disponibles para generar informes. Además, puede enviar a los destinatarios seleccionados un informe de Cuarentena de correo electrónico, que es una lista de los mensajes de correo electrónico puestos en cuarentena. El informe de Cuarentena de correo electrónico se envía en la fecha y a la hora especificadas, pero solo si hay elementos nuevos que notificar.
Equipos y sitios	ESET Cloud Office Security ofrece protección para grupos del equipo o sitios de SharePoint. De esta forma, se amplía la protección de las soluciones de colaboración de Microsoft 365 con la protección de SharePoint y grupo del equipo mediante el uso compartido seguro de archivos. Si ha estado utilizando ESET Cloud Office Security, es posible que se le pida que actualice el consentimiento antes de usar Equipos y sitios.
ESET LiveGuard Advanced	Una capa de protección adicional contra amenazas avanzadas de día cero. ESET LiveGuard Advanced es una solución de entorno de pruebas basada en la nube que analiza los archivos enviados ejecutando el código sospechoso en un entorno aislado para evaluar su comportamiento. ESET Cloud Office Security envía a analizar los archivos adjuntos de correo electrónico y los archivos de Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint que son sospechosos a ESET LiveGuard Advanced. Active y configure la característica ESET LiveGuard Advanced mediante las políticas. Los resultados del análisis se muestran en los Registros del análisis.
Registro de auditoría	El registro de auditoría permite al Administrador comprobar las actividades realizadas en ESET Cloud Office Security. Esta función puede resultar útil, especialmente cuando hay varios usuarios de la consola de ESET Cloud Office Security. Las entradas del registro de auditoría muestran las actividades y la secuencia en la que se realizaron. Los registros de auditoría almacenan información sobre la operación o el evento específicos. Los registros de auditoría se generan siempre que se crea o modifica un objeto ESET Cloud Office Security (grupo de licencias, usuario, política, informe o elemento de cuarentena como datos adjuntos).

Google Workspace (protección de Gmail y Google Drive)	ESET Cloud Office Security amplía la cobertura de servicios de seguridad a otro proveedor líder de correo electrónico en la nube, Google Workspace. ESET Cloud Office Security ofrece protección integral a los usuarios de Gmail y Google Drive mediante el uso de todas sus funciones. Mantiene a los usuarios de Google Workspace a salvo del malware, el phishing y el spam.

Novedades

Información sobre nuevas funciones y mejoras implementadas en cada versión de ESET Cloud Office Security:

^ Versión del portal 353 publicada el 23 de noviembre de 2023

- Integración con Google Workspace
- Navegador de productos para acceder rápidamente a ESET Business Account (más consolas disponibles en los próximos meses).
- *Otras correcciones de errores y mejoras administrativas.*

^ Versión del portal 342.3 publicada el 24 de octubre de 2023

- Se ha añadido la integración con Google Workspace (función de vista previa).
- Se ha añadido una columna de tipo Usuario.
- *Otras correcciones de errores y mejoras administrativas.*

^ Versión del portal 311.2 publicado el 31 de julio de 2023

- Se agregó Google Workspace (protección de Gmail y Google Drive): acceda a las funciones de vista previa desde los enlaces rápidos.
- Se agregó el tema Modo oscuro.
- Se agregó el Navegador de productos para los usuarios de acceso anticipado de ESET HUB.
- *Otras correcciones de errores y mejoras administrativas.*

^ Versión del portal 293.7 publicado el 13 de julio de 2023

- Se agregó la asociación de inquilinos a los sitios de ESET Business Account (EBA). Este cambio garantiza la compatibilidad con el futuro portal de clientes ESET PROTECT HUB, que sustituirá ESET MSP Administrator (EMA) y ESET Business Account (EBA). Afecta solo a unos cuantos clientes que usan licencias de varios sitios para proteger a un solo inquilino. Si este es su caso, se le pedirá que asocie a sus inquilinos con sitios EBA.
- Otras mejoras menores y correcciones de errores.

^ Versión del portal 251.1 Publicada el 21 de marzo de 2023

- Mejoras en la carga lenta de pantallas para apoyar mejor a los inquilinos con decenas de miles de usuarios.
- Cambios en el asistente para agregar inquilinos.
- Actualizaciones en la página Acerca de.
- Actualizaciones de los Términos de uso y la Política de privacidad (Política de retención de datos y limitaciones).

^ Versión del portal 205 publicada el 9 de noviembre de 2022

- Se ha agregado la ventana Novedades, que aparecerá la primera vez que inicie sesión en la consola ESET Cloud Office Security y describirá las funciones recién agregadas.
- Opción para exportar los Registros del análisis y el Registro de auditoría a un archivo CSV.
- Se ha agregado un nuevo ajuste para Fusionar políticas con listas y correos electrónicos de notificación.

^ Versión del portal 180.2 publicado el 27 de julio de 2022

- La nueva función de registro de auditoría.
- Cambie la sección Registros a Registros del análisis.

^ Versión del portal 156.2 publicado el 26 de abril de 2022

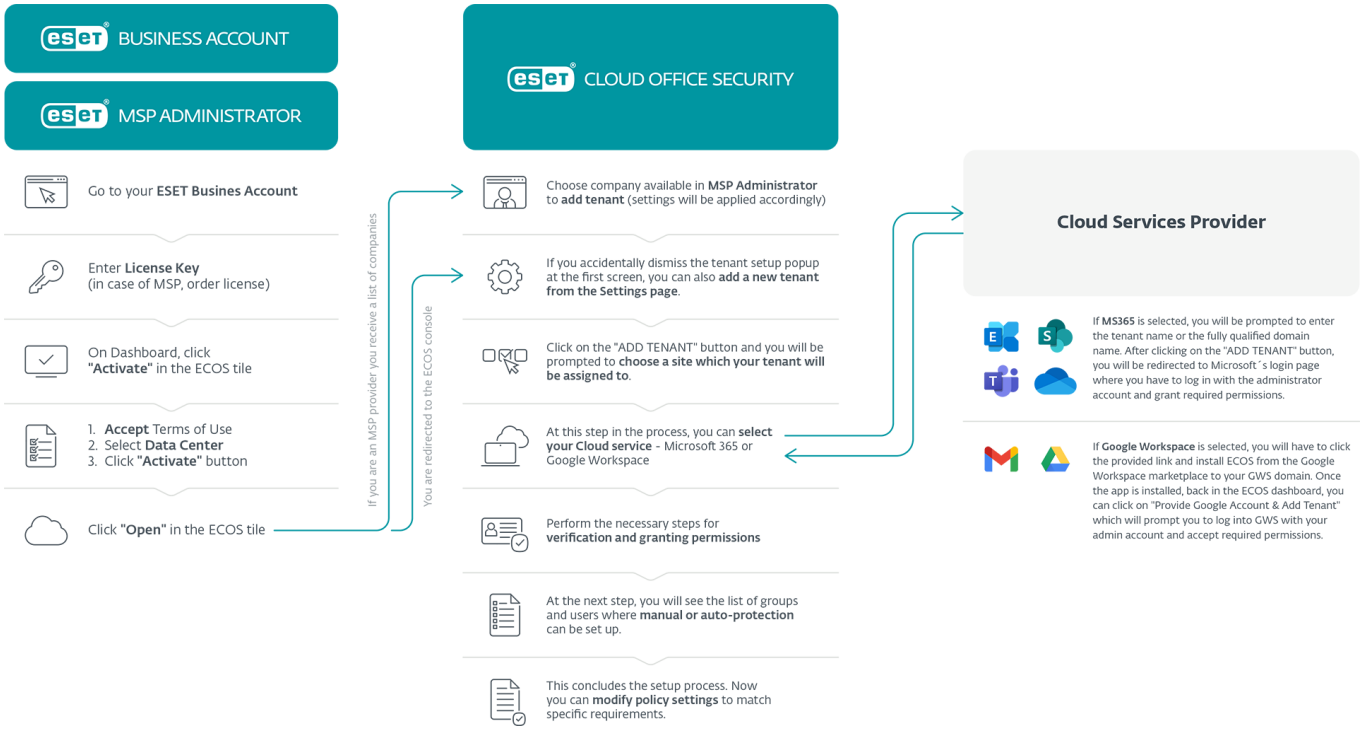
- Se ha cambiado el nombre de Dynamic Threat Defense a ESET LiveGuard Advanced.
- Envío de muestras de falso positivo/falso negativo para el análisis.
- Listas de importación/exportación aprobadas, bloqueadas e ignoradas en Políticas.
- En el Panel se muestra el número de usuarios no protegidos en la ficha Información general.
- Se ha corregido un error que colocaba los correos electrónicos de notificación en la cuarentena.

Versión del portal 140.6 Publicada el 9 de febrero de 2022

- Capacidad para crear informes de marca blanca (imagen de marca conjunta o solo logotipo personalizado).
- Opción para definir el idioma preferido para los correos electrónicos de notificaciones (notificaciones del propietario del buzón de correo).
- Opción para definir el idioma preferido para las notificaciones por correo electrónico de los miembros del inquilino.
- Filtrar correos electrónicos por ID del mensaje.

Integración

El flujo de integración de ESET Cloud Office Security con su proveedor de servicios en la nube:



Especificaciones

Especificaciones técnicas de referencia para ESET Cloud Office Security:

- Requisitos
- Planes de Microsoft 365 compatibles
- Planes de Google Workspace compatibles
- Navegadores de Internet compatibles
- Limitaciones y política de retención de datos

Requisitos

Para aprovechar la protección del servicio ESET Cloud Office Security para su Microsoft 365, se requiere lo siguiente:

- Plan de suscripción compatible de Microsoft 365
- Acceso de administrador a Azure Active Directory (Azure AD)
- Azure Cloud Services: Exchange | OneDrive
- Una cuenta en el portal de ESET Business Account o ESET MSP Administrator

Planes de Microsoft 365 compatibles

ESET Cloud Office Security es compatible con los siguientes planes de Microsoft 365, Exchange Online y OneDrive.

Planes de Microsoft 365 para grandes empresas:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Planes de Microsoft 365 para empresas:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Planes de Microsoft 365 para el sector educativo:

- Microsoft 365 A3
- Microsoft 365 A5

Planes de Exchange Online:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

Planes de OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Planes de Google Workspace compatibles

ESET Cloud Office Security es compatible con los siguientes planes de Google Workspace.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Navegadores de Internet compatibles

Para disfrutar de la mejor experiencia con la Consola web de ESET Cloud Office Security, le recomendamos que mantenga actualizados los navegadores web.

Puede utilizar la consola de ESET Cloud Office Security con los siguientes navegadores web:

- Mozilla Firefox 69 y versiones más recientes
- Microsoft Edge 44 y versiones más recientes
- Google Chrome 77 y versiones más recientes
- Opera 63 y versiones más recientes
- Safari 13.x y versiones más recientes

No se admite Microsoft Internet Explorer.

Limitaciones y política de retención de datos

En determinadas circunstancias, existen limitaciones de análisis en ESET Cloud Office Security. Un archivo no se analiza y aparecerá en los Registros del análisis como **No escaneado** si ocurre lo siguiente:

- El archivo tiene más de 200 MB
- El análisis tarda más de 2 minutos y se agota el tiempo de espera
- El archivo de almacenamiento tiene un nivel de anidamiento de 10 o más (suele ser un archivo que se conoce como bomba de archivo o bomba zip)
- El archivo comprimido está protegido con contraseña
- El archivo está dañado

Límites de cuarentena (cuando se libera de la cuarentena):

- 15 MB para un archivo adjunto de correo electrónico
- 150 MB para todo el mensaje de correo electrónico, incluidos los archivos adjuntos

Política de retención de datos:

Entidad	Periodo de retención	Comentario
Objetos en cuarentena	30 días	Los objetos con una antigüedad superior a los 30 días se eliminarán de forma permanente.
Detecciones	90 días	Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente.
Registros del análisis	90 días	Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente.
Registros del análisis con resultado Limpio	3 días	Si tiene una política que utiliza Registrar todos los objetos, los análisis con resultado Limpio realizados hace más de 3 días se eliminarán de forma permanente.
Copia de seguridad de base de datos de ESET Cloud Office Security	90 días	Las copias de seguridad de más de 90 días se eliminarán de forma permanente.
Registros de auditoría	90 días	Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente.
Registros de Application Insights	90 días	Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente.

Inquilino eliminado de la consola ESET Cloud Office Security

Cuando elimina un inquilino de la consola ESET Cloud Office Security, el periodo de retención de los datos del inquilino es 30 días (la cuarentena, los registros del análisis y las estadísticas se eliminan a los 30 días). Si agrega el inquilino de nuevo en un plazo de 30 días, se restaurarán todos los datos. Los demás objetos (inquilinos, usuarios, grupos, sitios, informes y políticas) se eliminan de forma permanente a los 90 días.

ESET Cloud Office Security desactivado en ESET Business Account o ESET MSP Administrator

Si desactiva ESET Cloud Office Security en ESET Business Account o ESET MSP Administrator, este proceso también quitará los inquilinos de ESET Cloud Office Security. La acción de quitar ESET Cloud Office Security es permanente, y los datos eliminados no se pueden restaurar.

Análisis antispam:

ESET Cloud Office Security analiza los mensajes de correo electrónico almacenados en buzones de correo en busca de spam. Por este motivo, ESET Cloud Office Security no puede impedir que un usuario envíe un mensaje de spam a una dirección de correo electrónico externa. En raras ocasiones, si se roban las credenciales de usuario de Office 365, un remitente de correo no deseado puede utilizarlas para enviar mensajes de correo no deseado en bloque (tráfico de correo electrónico saliente).

Licencias de ESET Cloud Office Security

Administre las licencias de ESET Cloud Office Security desde ESET Business Account o ESET MSP Administrator. Pruebe ESET Cloud Office Security con una licencia de prueba de 30 días.

- Consulte ESET Business Account para crear una cuenta y agregar o administrar una licencia.
- Consulte ESET MSP Administrator si es MSP.

ESET Business Account y ESET MSP Administrator (cuenta de licencias híbridas)

Si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede cambiar entre la vista de ESET Business Account y ESET MSP Administrator. Proteger a los usuarios o empresas que utilizan la Administración de licencias de ESET Cloud Office Security.

Periodo de gracia para licencias próximas a caducar en ESET Business Account

Cuando su licencia esté a punto de caducar, verá una alerta en la interfaz de ESET Business Account. Si pasa la fecha de caducidad y no ha renovado su licencia ni ha activado una nueva licencia, verá una alerta de licencia caducada en ESET Business Account. Si no hay ninguna licencia válida, se mostrará en ESET Business Account una notificación de que su licencia se suspenderá dentro de catorce días y recibirá un mensaje de correo electrónico en la dirección especificada en su cuenta de administrador.

Contará con un periodo de gracia de catorce días para renovar la licencia después de que esta haya caducado. Recibirá una notificación en ESET Business Account y por correo electrónico cuando haya transcurrido la mitad del periodo de gracia. Después de catorce días, se suspenderá su uso de ESET Cloud Office Security. La cuenta dejará de ser accesible y no estará operativa. La cuenta de ESET Cloud Office Security suspendida se almacenará, y podrá acceder a ella de nuevo si agrega una nueva licencia de ESET Cloud Office Security a ESET Business Account. Su cuenta de ESET Cloud Office Security puede permanecer suspendida hasta 30 días. Después de este periodo, se eliminará de forma permanente.

Si su cuenta se suspende, recibirá una notificación en ESET Business Account y por correo electrónico cuando queden 14 días para que se elimine dicha cuenta. Debe activar una nueva licencia de ESET Cloud Office Security para restaurar el acceso a su cuenta de ESET Cloud Office Security.

> Los usuarios siguen estando totalmente protegidos durante el periodo de gracia. Cuando termina el periodo de gracia, los usuarios pierden la protección.

Licencia suspendida

Si no hay ninguna licencia de ESET Cloud Office Security válida presente en ESET Business Account, se suspenderá su instancia de ESET Cloud Office Security. No podrá acceder a la instancia, que tampoco funcionará. Su instancia de ESET Cloud Office Security puede permanecer suspendida hasta 30 días. Después de este periodo, se eliminará de forma permanente. Debe activar una nueva licencia válida de ESET Cloud Office Security para restaurar el acceso a su instancia de ESET Cloud Office Security.

ESET Business Account

ESET Business Account funciona como un punto de acceso unificado para ESET Business Account y ESET Cloud Office Security. Utilice la página de inicio de sesión de ESET Cloud Office Security o ESET Business Account para acceder a ESET Cloud Office Security. Ambas páginas le redirigen a la autenticación de ESET Business Account para verificar su inicio de sesión.

- Cree una nueva cuenta si no tiene una cuenta registrada en ESET Business Account.
- Si tiene una cuenta de ESET Business Account, agregue su licencia de ESET Cloud Office Security.
- Administrar ESET Business Account.

Crear una nueva cuenta de ESET Business Account

1. Abra la página de inicio de sesión de ESET Business Account y haga clic en **Regístrese de forma gratuita**. Rellene el formulario con detenimiento para su registro. La dirección de correo electrónico introducida se utilizará como nombre de inicio de sesión.

2. La contraseña debe tener al menos 10 caracteres. Escriba su **Nombre** y su **Información de empresa** y haga clic en **Continuar**. Lea y confirme que acepta los **Términos de uso de ESET**. Complete el formulario de reCAPTCHA y haga clic en **Registrar**.

3. Recibirá un mensaje de correo electrónico de confirmación tras registrarse correctamente (puede tardar hasta quince minutos). Haga clic en el vínculo del mensaje de correo electrónico de confirmación para abrir una nueva ventana de **Activar cuenta**.

4. Escriba su contraseña y haga clic en **Activar** para activar su ESET Business Account. Recibirá otro mensaje de correo electrónico en el que se verificará que su cuenta de ESET Business Account se ha creado correctamente. Ya puede iniciar sesión en ESET Business Account.

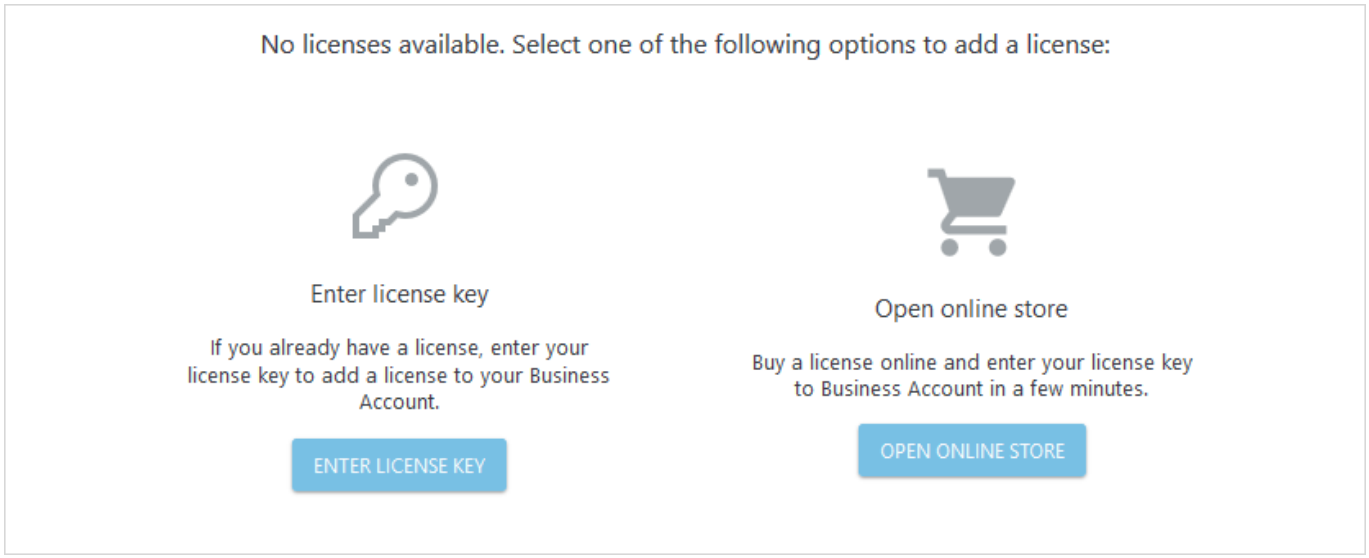
Tras activar ESET Business Account, agregue la licencia de ESET Cloud Office Security.

Agregar licencia de ESET Cloud Office Security en ESET Business Account

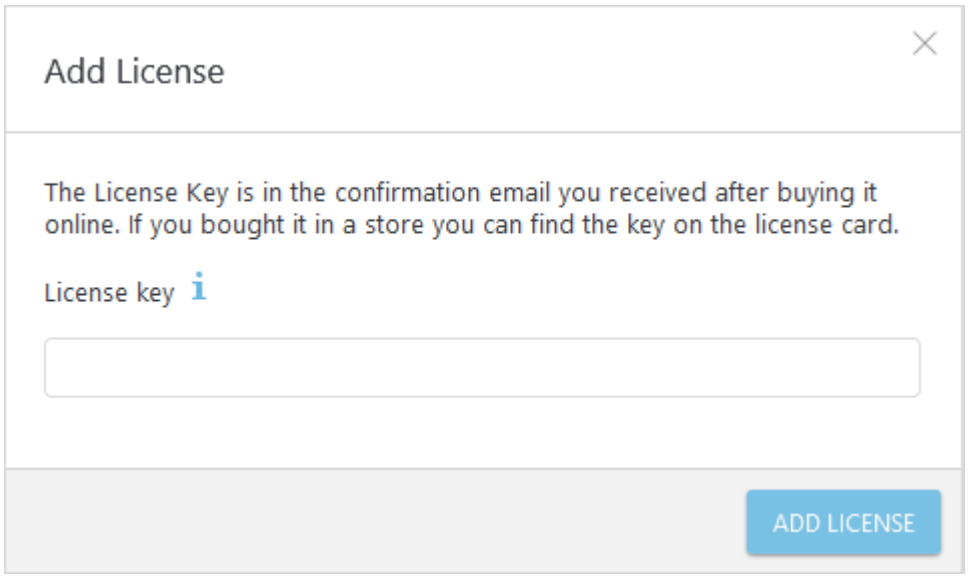
Tras un inicio de sesión correcto en ESET Business Account, verá una pantalla de bienvenida de ESET Business Account si es la primera vez que entra.

1. Haga clic en **Agregar licencia** para abrir la ventana de licencia. Si es un usuario habitual de ESET Business

Account, diríjase a la pestaña **Licencia** y haga clic en **Agregar licencia**.



2. Introduzca su **Clave de licencia** y haga clic en **Agregar licencia**.



3. Recibirá un mensaje de correo electrónico con un vínculo de verificación. Haga clic en el vínculo e introduzca sus credenciales de inicio de sesión en el portal de ESET Business Account cuando se le solicite. Si desea obtener más información sobre la administración de licencias, los usuarios y los sitios, consulte la guía de ESET Business Account .

Administrar ESET Business Account

Actividades habituales relacionadas con las licencias:

Sitios y grupo de licencias

Las licencias y los grupos de licencias se cargan desde ESET Business Account. Los grupos de licencias solo están disponibles si tiene sitios en ESET Business Account.

Crear un nuevo usuario en ESET Business Account

Puede crear un usuario que le ayude a administrar el uso compartido de sus licencias.

1. Abra ESET Business Account e inicie sesión.

2. Seleccione **Administración de usuarios**, haga clic en **Nuevo usuario** y escriba la información necesaria.

3. Seleccione los **derechos de acceso** de ESET Cloud Office Security para un usuario:

   • **Lectura**: el usuario tiene acceso a ESET Cloud Office Security y ve usuarios, registros y detecciones, pero no puede administrar políticas, proteger a los usuarios ni liberar elementos de la cuarentena.

   • **Escritura**: el usuario tiene acceso total a ESET Cloud Office Security, ve y administra usuarios, pone elementos en cuarentena o crea políticas.

   • **Sin acceso**: el usuario no puede acceder a ESET Cloud Office Security.

4. Establezca un idioma en las **preferencias** del usuario para la consola ESET Cloud Office Security.

5. Haga clic en **Crear**: se creará el usuario.

Crear un nuevo sitio en ESET Business Account

Los sitios le permiten dividir o fusionar sus licencias en grupos de licencias. Los sitios son grupos individuales que pueden tener sus propios administradores y ubicaciones.

1. Abra ESET Business Account e inicie sesión.

2. Seleccione **Detalles**, haga clic en **Crear sitio** y escriba la información personal necesaria.

3. Haga clic en **Agregar usuario**, seleccione el usuario y haga clic en **Confirmar**.

4. En el grupo de licencias, haga clic en **Agregar unidades** y seleccione una licencia de ESET Cloud Office Security. Puede cambiar **Unidades secundarias** y hacer clic en **Confirmar**.

5. Haga clic en **Crear**: se creará el sitio.

ESET MSP Administrator

ESET MSP Administrator es un sistema de administración de licencias que permite a los usuarios de MSP crear varios clientes de MSP y generar licencias específicas con un recuento de puestos. El portal de licencias de ESET MSP Administrator es compatible con precios por volumen y facturación en función del número exacto de puestos y días que se hayan adquirido.

ESET Cloud Office Security está disponible para todos los MSP Managers, MSPs y managed MSPs. El usuario de ESET MSP Administrator con acceso de escritura puede activar ESET Cloud Office Security. Los usuarios pueden acceder a ESET Cloud Office Security con derechos de acceso de escritura, lectura o personalizados.

• Crear un nuevo cliente de MSP (la dirección de correo electrónico del cliente es necesaria para la activación de la consola de ESET Cloud Office Security).

- Activar ESET Cloud Office Security desde ESET MSP Administrator.

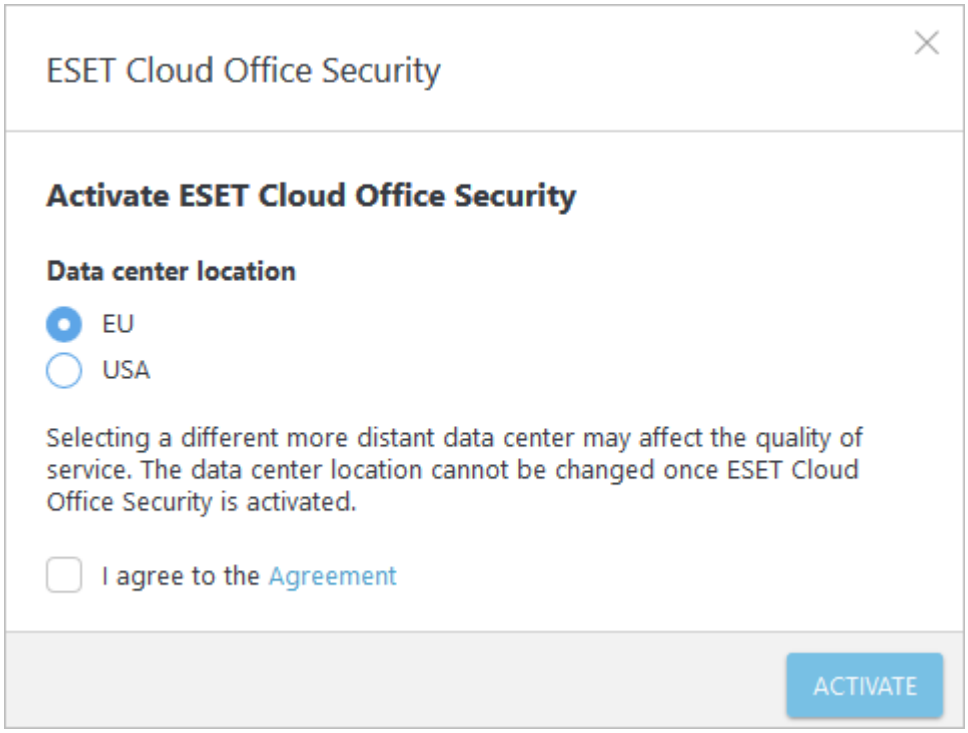
Activación de ESET Cloud Office Security

1. Inicie sesión en ESET Business Account o ESET MSP Administrator y localice la ventana ESET Cloud Office Security ventana en el **Panel**.

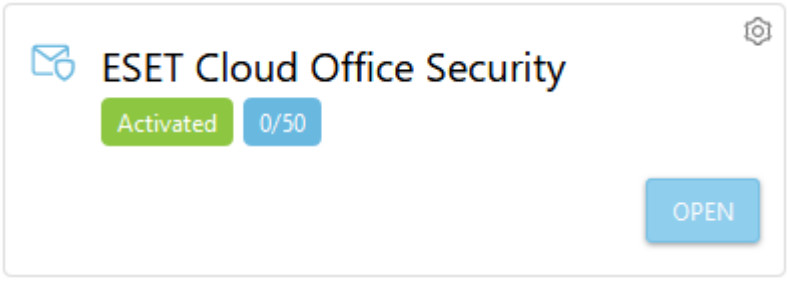
2. Haga clic en **Activar** en la esquina inferior derecha de la ventana de ESET Cloud Office Security.

3. El asistente de activación consultará los Términos de uso de ESET Cloud Office Security y mostrará la ubicación del centro de datos óptimo en función de su ubicación actual. Seleccione **Acepto los términos de uso** y haga clic en **Activar**. No se recomienda cambiar la ubicación del centro de datos; sin embargo, puede realizar una elección distinta si necesita utilizar otra ubicación.

Los centros de datos son totalmente independientes. Una vez que seleccione la ubicación del centro de datos, no se podrá cambiar y no podrá migrar a otra ubicación. Para cambiar el centro de datos, inicie el proceso de activación desde el principio.

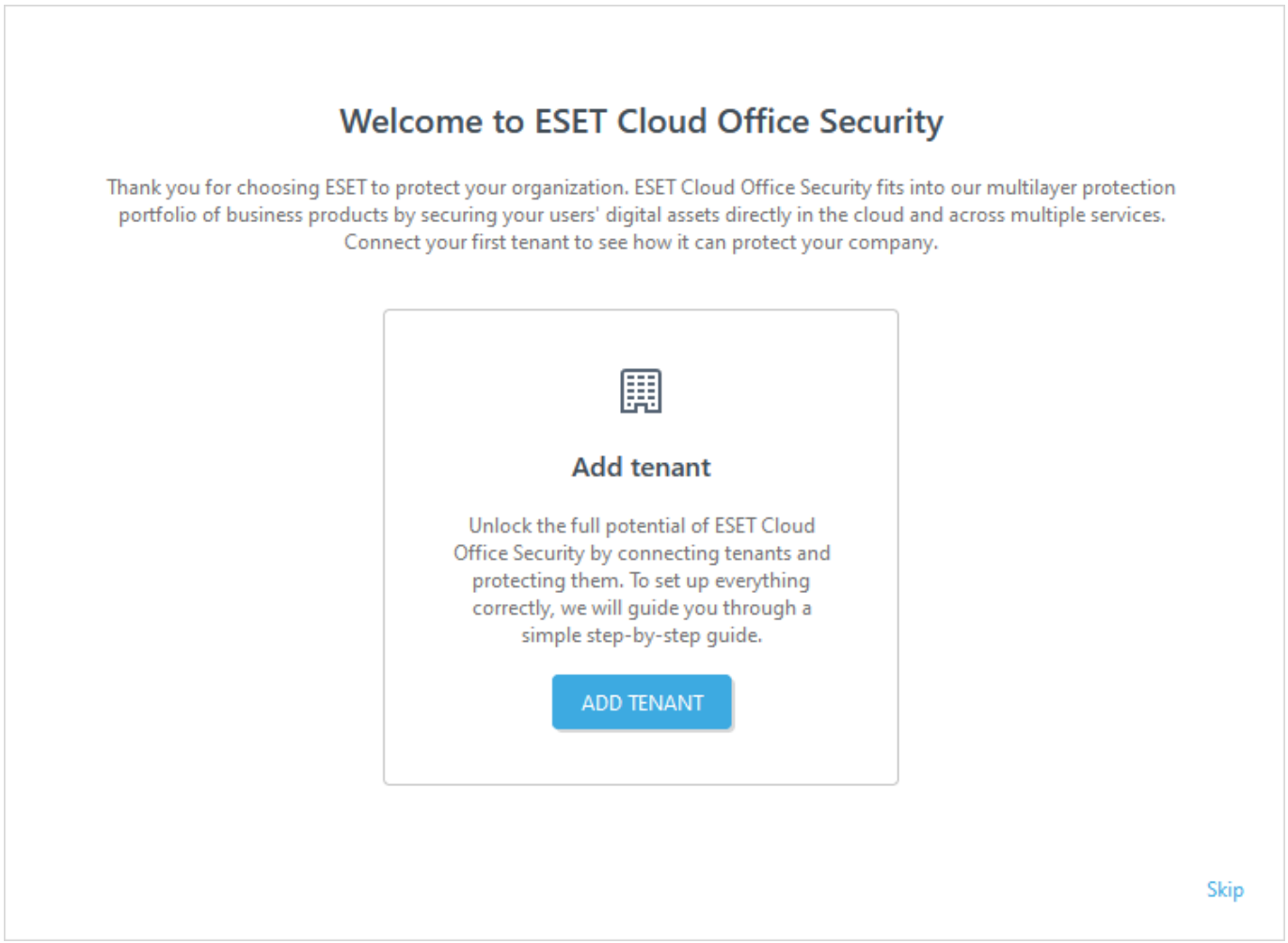


4. Haga clic en **Abrir** en la ventana de ESET Cloud Office Security. El Panel de ESET Cloud Office Security se abre en una nueva pestaña del navegador.

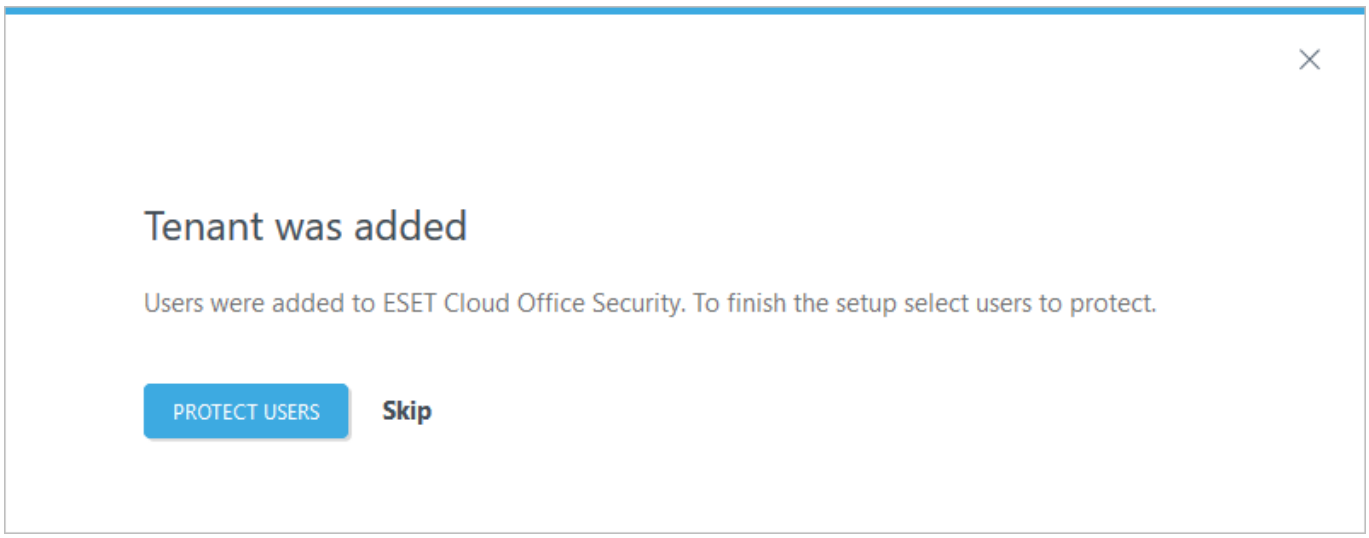


Cuando inicie sesión en ESET Cloud Office Security por primera vez, aparecerá un **asistente de inicio**. Este asistente le guía por el proceso de implementación inicial.

1. Agregue el inquilino (Microsoft 365 o Google Workspace).



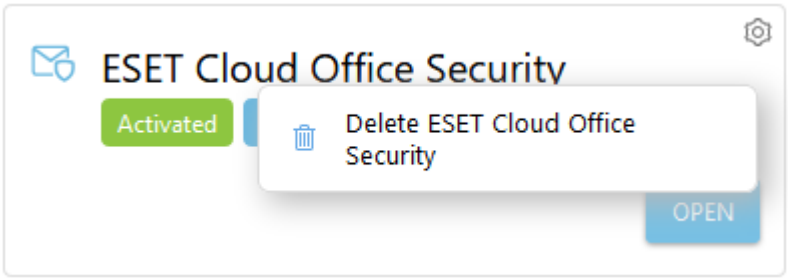
2. Proteger a los usuarios. Si pulsa **Omitir**, puede proteger a los usuarios o las empresas más adelante con la Administración de licencias de ESET Cloud Office Security.



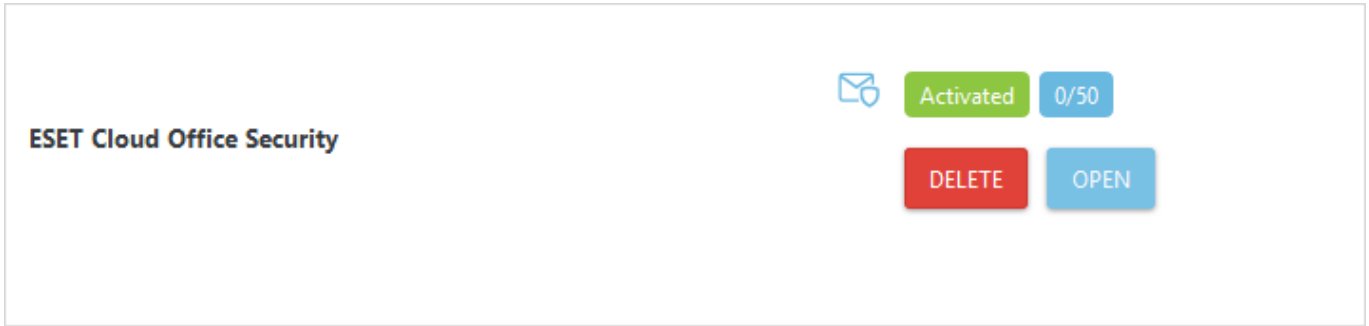
Desactivar ESET Cloud Office Security

1. Inicie sesión en ESET Business Account o ESET MSP Administrator y localice la ventana ESET Cloud Office Security ventana en el **Panel**.

2. Haga clic en el icono del engranaje en la esquina superior derecha de la ventana de ESET Cloud Office Security y seleccione **Eliminar ESET Cloud Office Security**.

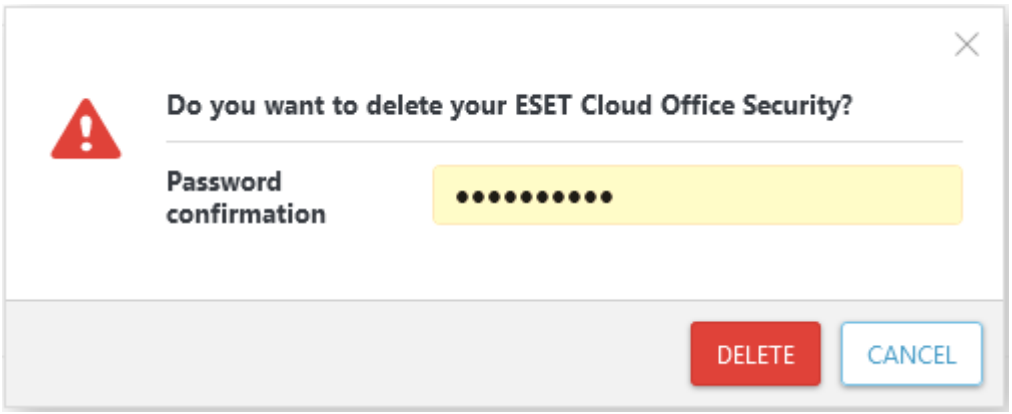


3. También puede ir a la sección **Detalles** y hacer clic en **Eliminar**.



4. Aparece una ventana emergente de advertencia en la que se le avisa de que se van a quitar todos los datos. Introduzca su contraseña de ESET Business Account para confirmar y haga clic en **Eliminar**.

La eliminación de ESET Cloud Office Security es permanente. Los datos eliminados no se pueden restaurar.



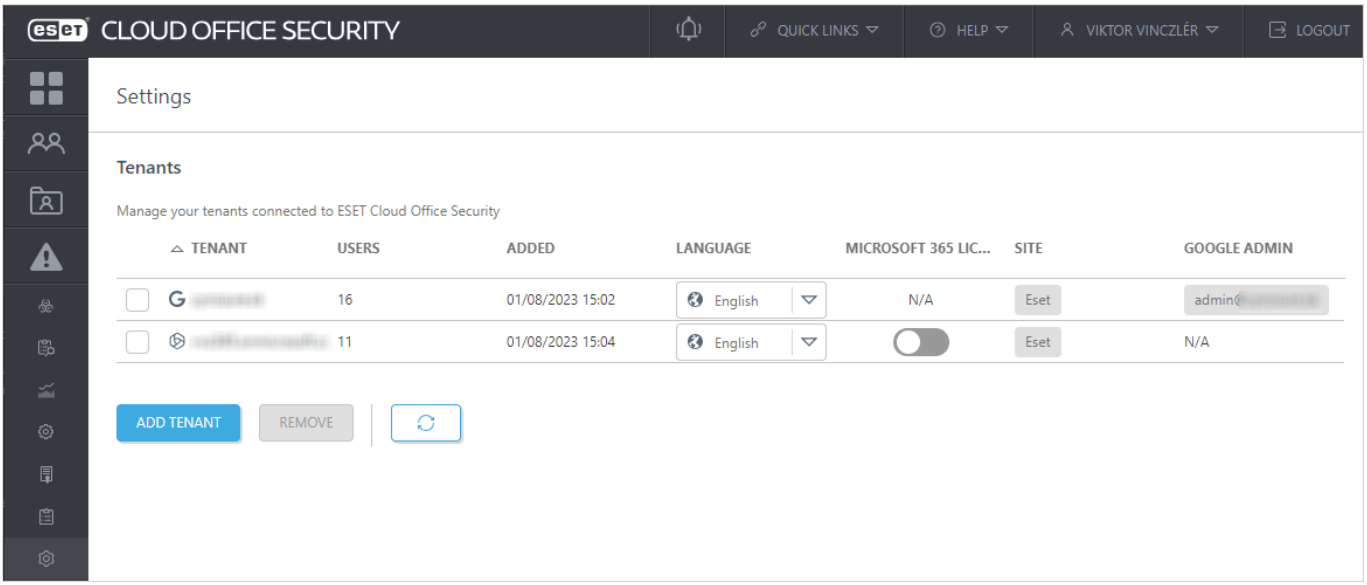
A continuación, la instancia de ESET Cloud Office Security se elimina y la ventana del producto ESET Cloud Office Security vuelve al estado **No activado**. También recibirá un correo electrónico de confirmación de ESET Business Account.

Administrar los inquilinos en Configuración

Administre los inquilinos conectados a ESET Cloud Office Security. Puede ver todos los inquilinos registrados en la tabla con detalles para cada inquilino. Utilice el botón Actualizar para volver a cargar la tabla con inquilinos.

Si desea agregar un inquilino nuevo, haga clic en Agregar inquilino y elija Microsoft 365 o Google Workspace según la plataforma en la nube que desee proteger. Una vez finalizado el proceso de registro de inquilinos, Microsoft 365 o Google Workspace estarán protegidos por ESET Cloud Office Security.

Después de agregar el inquilino, la pantalla cambia y se muestra la lista de inquilinos asociados a un sitio. Puede gestionar los inquilinos o agregar más inquilinos. En la tabla se muestra el nombre del inquilino, el número de usuarios, cuándo se agregó el inquilino, la configuración de idioma, los usuarios con licencia de Microsoft 365, el nombre del sitio y el administrador de Google.



Idioma

Este ajuste determina el idioma de los mensajes de notificación de correo electrónico a los miembros del inquilino. Puede definir el idioma de cada inquilino por separado, por ejemplo, para las necesidades de un MSP que administra varias empresas.

Para eliminar un inquilino de ESET Cloud Office Security, seleccione el inquilino correspondiente y haga clic en Quitar. Aparecerá una ventana de confirmación para que tome una decisión final. Una vez eliminado, todos los datos del usuario se quitarán transcurridos 30 días.

Usuarios con licencia de Microsoft 365

Esta opción está activada de forma predeterminada. Equivale a una lista de usuarios del centro de administración de Microsoft 365 en **Usuarios** > **Usuarios activos** > Filtrar: **Usuarios con licencia**.

Si se desactiva esta opción, ESET Cloud Office Security mostrará todos los usuarios, incluidos los usuarios sin una licencia de Microsoft 365 (por ejemplo, buzones de correo compartidos). Si está utilizando la protección automática para el grupo o el inquilino que contiene usuarios sin una licencia de Microsoft 365, estos usuarios pasarán a estar visibles, estarán protegidos y consumirán unidades de licencia ESET Cloud Office Security. El estado de protección de los nuevos usuarios visibles puede ser **Pendiente** durante un periodo de hasta 1 hora. Una vez completado el proceso de protección automática, el estado de protección cambiará a **Protegido** u otro Estado posible en la sección Usuarios.

> Si su inquilino o grupo con protección automática contiene un usuario sin un buzón de correo y OneDrive, este usuario consumirá una unidad de licencia ESET Cloud Office Security. Verá el estado de protección **Advertencia** para este usuario.

Si vuelve a activar Usuarios con licencia de Microsoft 365, solo se mostrarán los usuarios que tengan una licencia de Microsoft 365. Si había protegido automáticamente a algunos usuarios sin una licencia de Microsoft 365, estos usuarios desaparecerán de la sección Usuarios y se liberarán las unidades de licencia de ESET Cloud Office Security. El cambio puede tardar hasta 1 hora en realizarse.

> Si tiene usuarios protegidos de forma manual que no disponen de una licencia de Microsoft 365 (mientras estaba desactivado el ajuste **Usuarios con licencia de Microsoft 365**), estos usuarios permanecerán visibles y protegidos incluso después de activar la opción **Usuarios con licencia de Microsoft 365** (hasta que los usuarios dejen de estar protegidos).

Sitio

Si desea cambiar el sitio al que está asociado el inquilino, haga clic en el nombre del sitio para abrir la ventana **Seleccione un sitio para protegerlo** y realice los cambios necesarios.

Administrador de Google

El administrador de Google debe corresponder a una dirección correo electrónico activa del administrador de Google Workspace.

> Si la función o la dirección de correo electrónico del administrador están a punto de cambiar, haga clic en la información del administrador de Google para actualizarla. Hágalo con antelación para garantizar la funcionalidad del inquilino y la protección del sitio.

Actualizar consentimiento

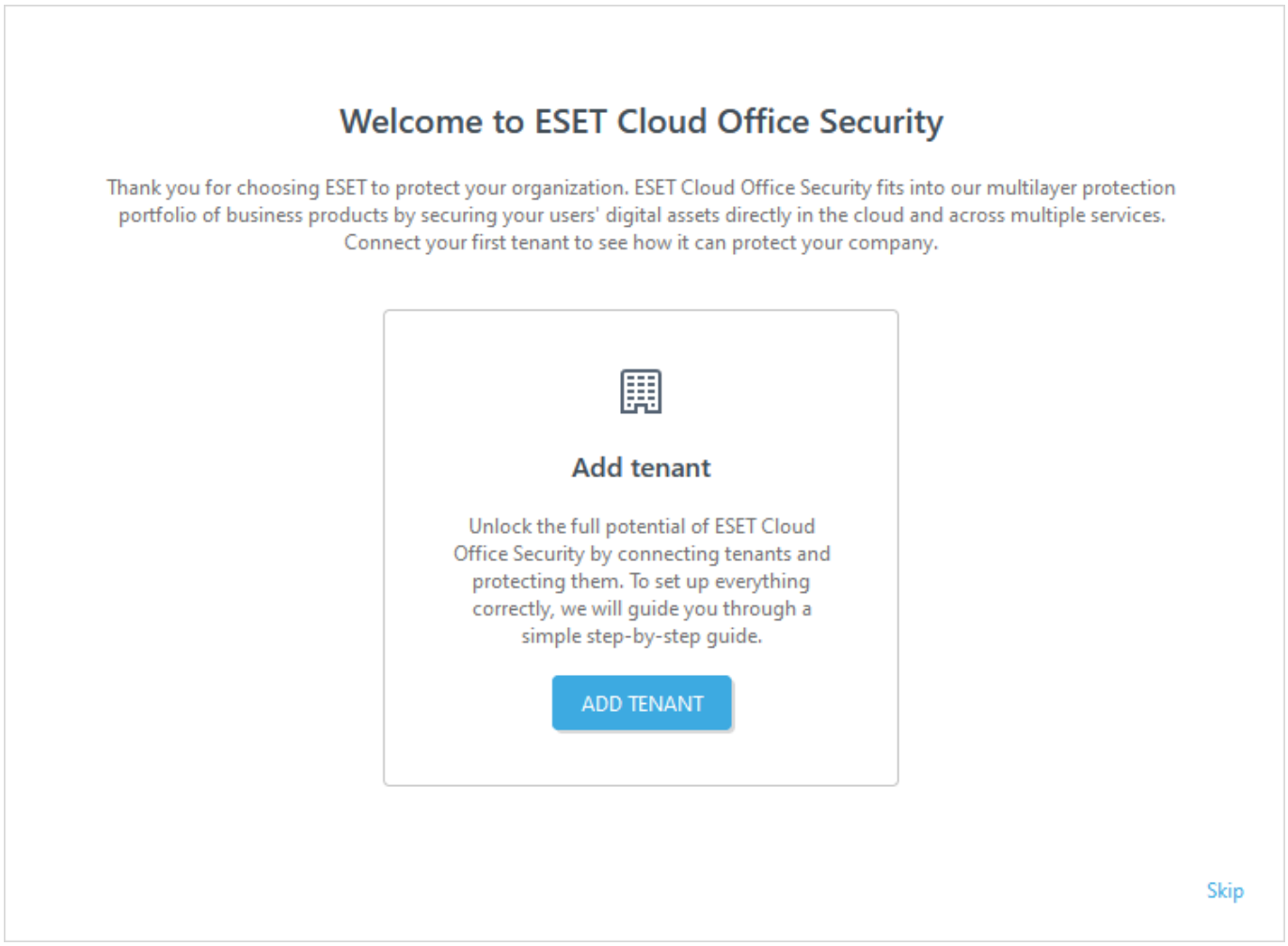
Si se muestra un botón amarillo, puede actualizar su consentimiento. La actualización del consentimiento para el inquilino existente amplía los permisos de ESET Cloud Office Security a su cuenta de Microsoft 365. Esto activa una función para proporcionar información sobre el tipo de usuario. El tipo de usuario se define en Azure Active Directory y se muestra en una columna específica de la sección Usuarios. Por ejemplo, puede filtrar los usuarios de Microsoft 365 por tipo si solo desea ver los buzones compartidos.

Haga clic en el botón **Actualizar** con cada inquilino para el que desee habilitar esta característica. La actualización del tipo de usuario de Azure AD puede tardar hasta 24 horas.

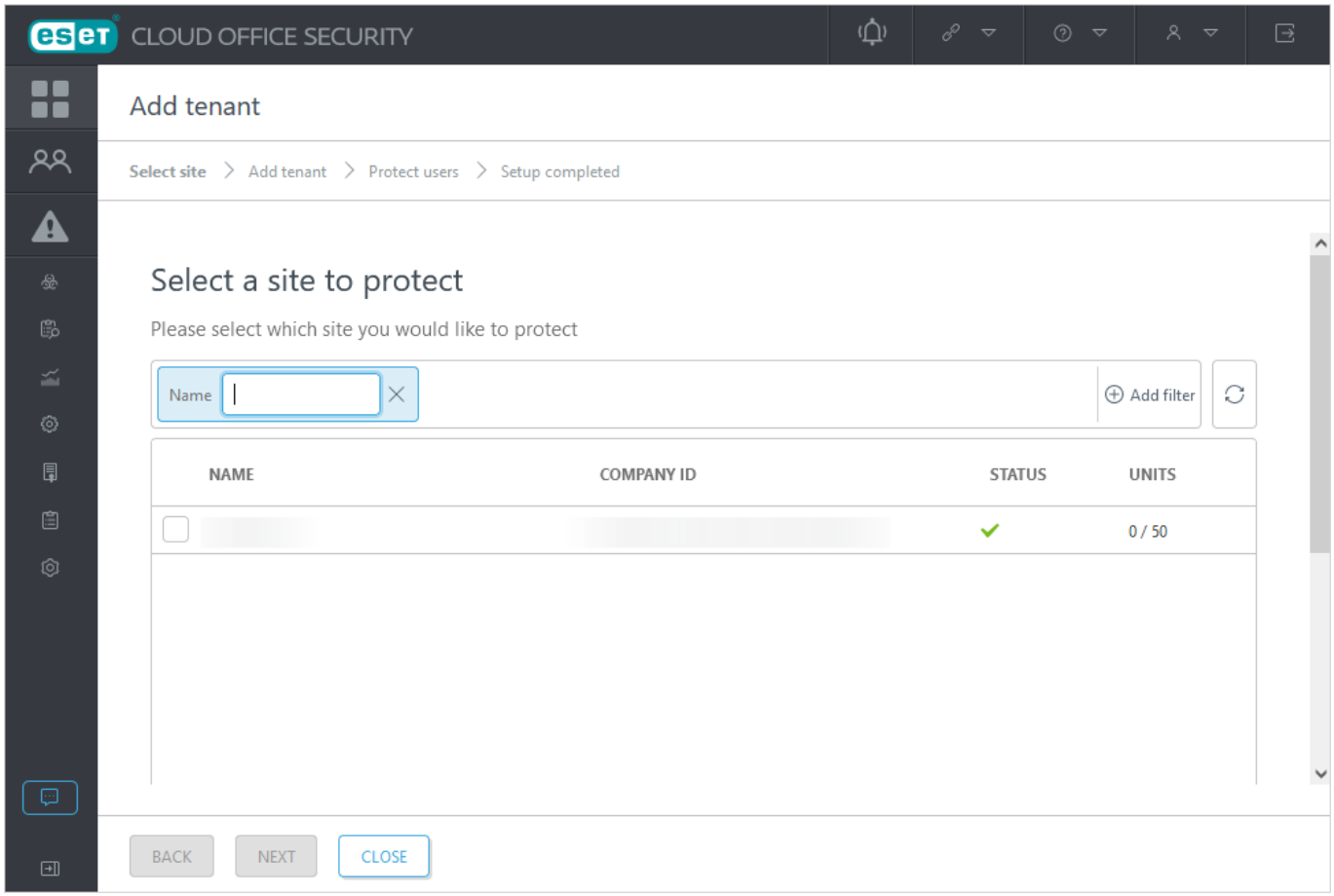
Si se muestra un botón rojo, significa que se ha revocado el consentimiento o que se ha realizado otro cambio que afectó a la integración del inquilino con ESET Cloud Office Security. Haga clic en el botón **Actualizar** si desea seguir protegiendo a los usuarios.

Agregue su primer inquilino

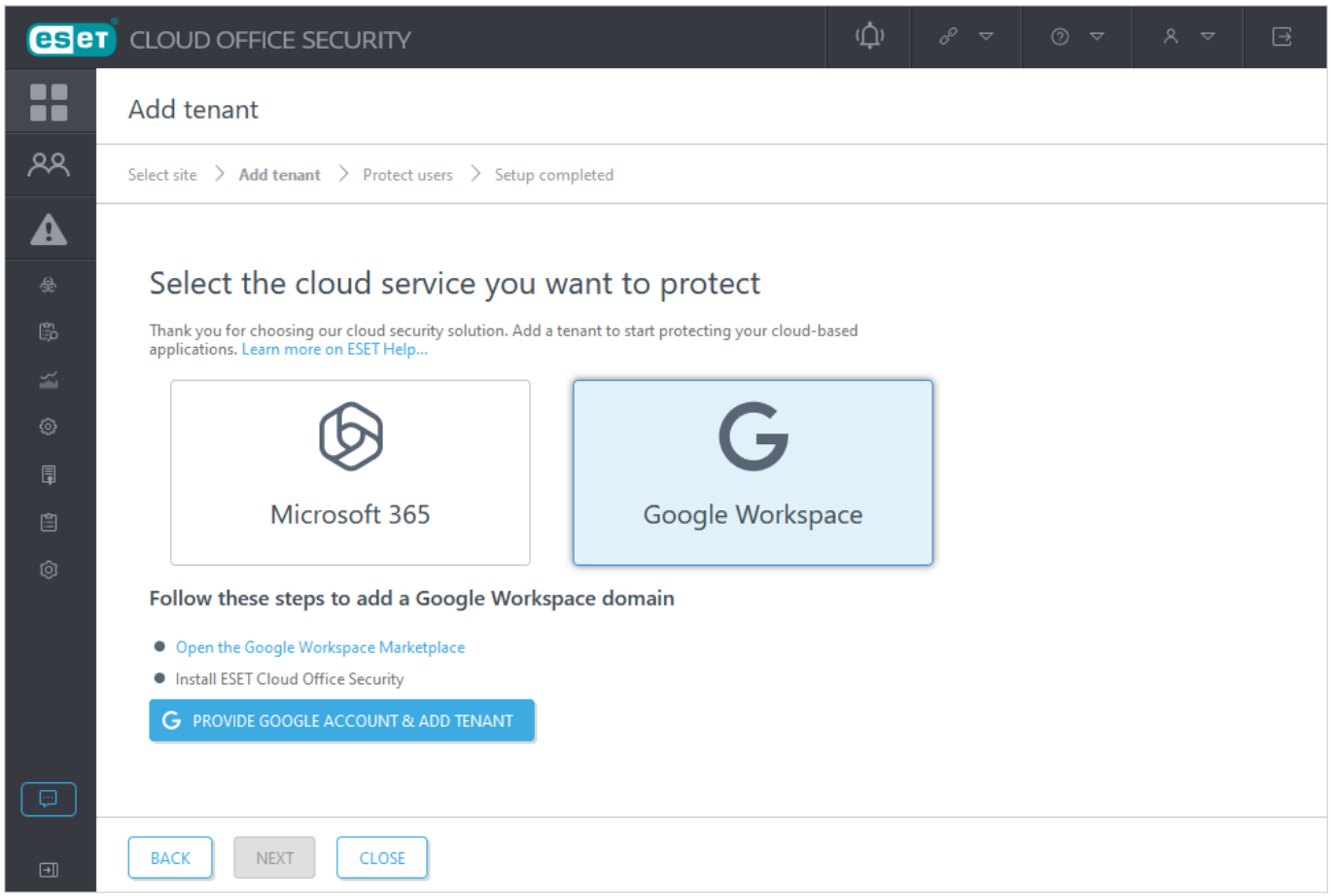
Para proteger la plataforma en la nube, haga clic en **Agregar inquilino** y conecte el sitio de Microsoft 365 o Google Workspace a ESET Cloud Office Security.



Debería ver una lista de los sitios disponibles en la ventana **Seleccionar un sitio para protegerlo**. Use la casilla para seleccionar el sitio que desea asociar a un inquilino y haga clic en **Siguiente**.



Haga clic en el icono de Microsoft 365 o Google Workspace en la ventana **Seleccione el servicio en la nube que desea proteger** y siga los pasos de las viñetas:



Inquilino de Microsoft 365

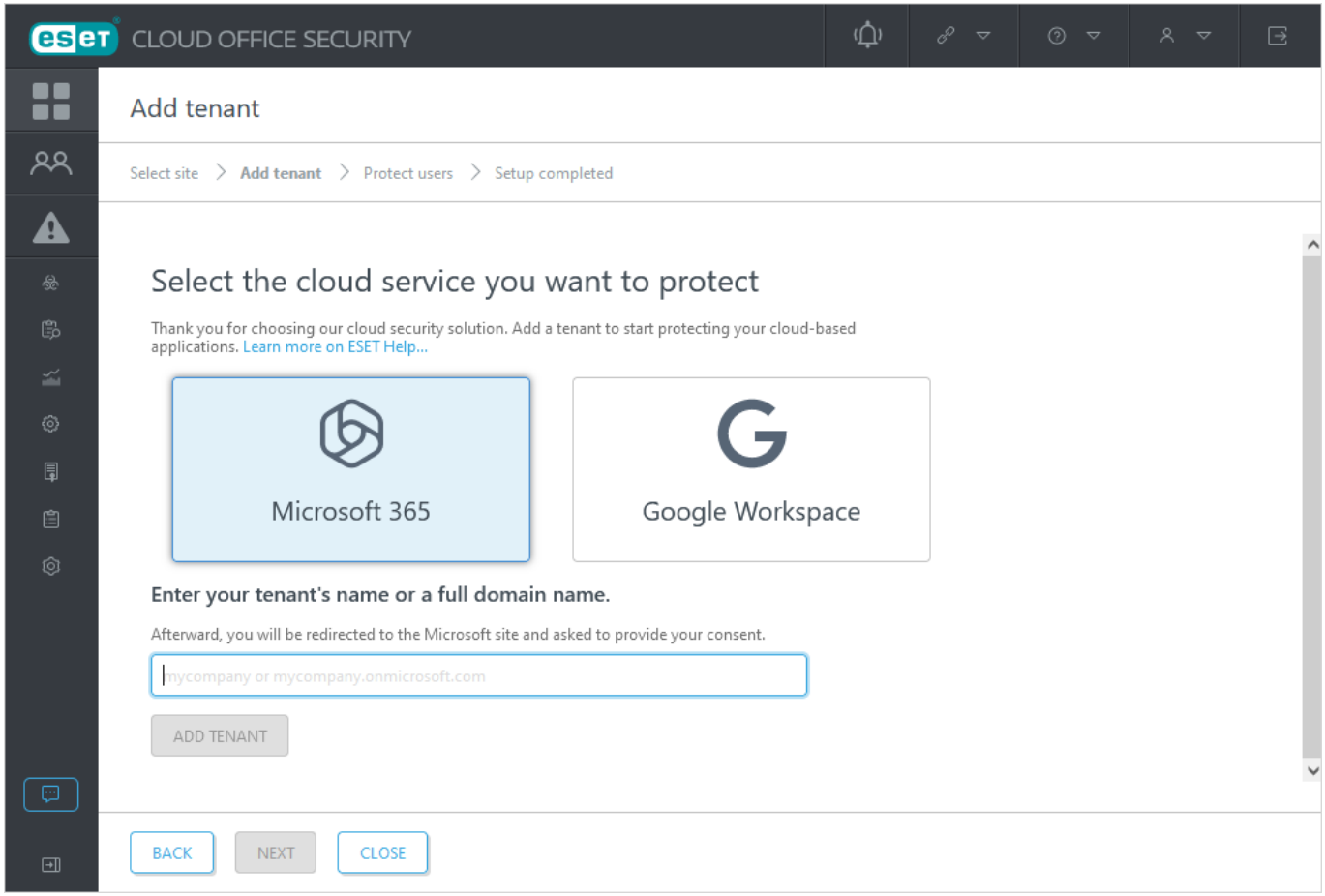
Azure Active Directory (Azure AD) organiza objetos como usuarios y aplicaciones en grupos denominados inquilinos. Una forma habitual de identificar a un inquilino es utilizar un nombre de dominio. Si varios usuarios comparten un nombre de dominio, estos usuarios forman parte del mismo inquilino. Los inquilinos le permiten establecer políticas sobre los usuarios y las aplicaciones de su organización para cumplir las políticas de seguridad y operativas. Puede proteger y administrar varios inquilinos de Microsoft 365 desde una consola ESET Cloud Office Security.

Si desea obtener más información, consulte el artículo de Microsoft sobre Inquilinos en Azure Active Directory.

Agregar inquilino

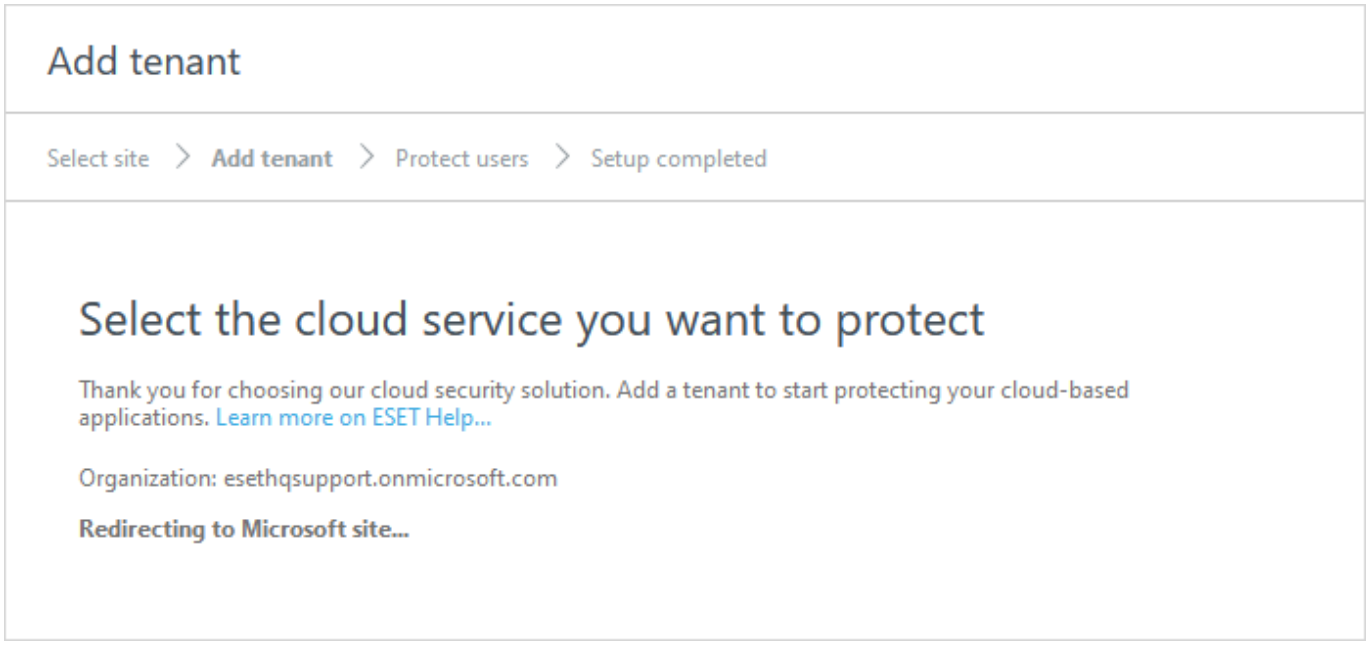
1. Vaya a **Configuración** y haga clic en **Agregar inquilino** (o en cualquier lugar donde vea el botón **Agregar inquilino**).

2. Haga clic en el icono de **Microsoft 365**.

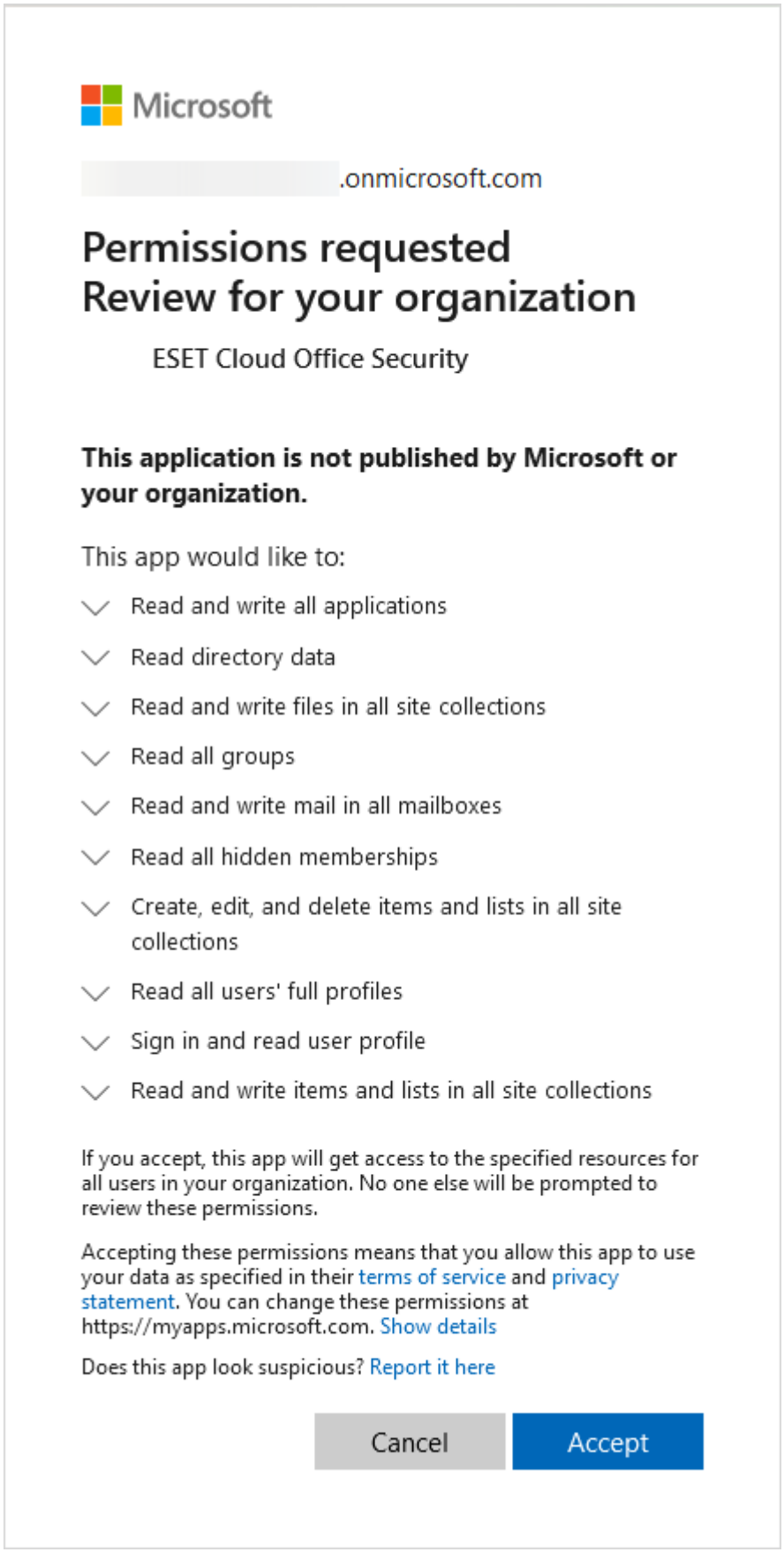


3. Escriba el nombre del inquilino de Microsoft 365 o el nombre de dominio completo y haga clic en **Agregar inquilino**.

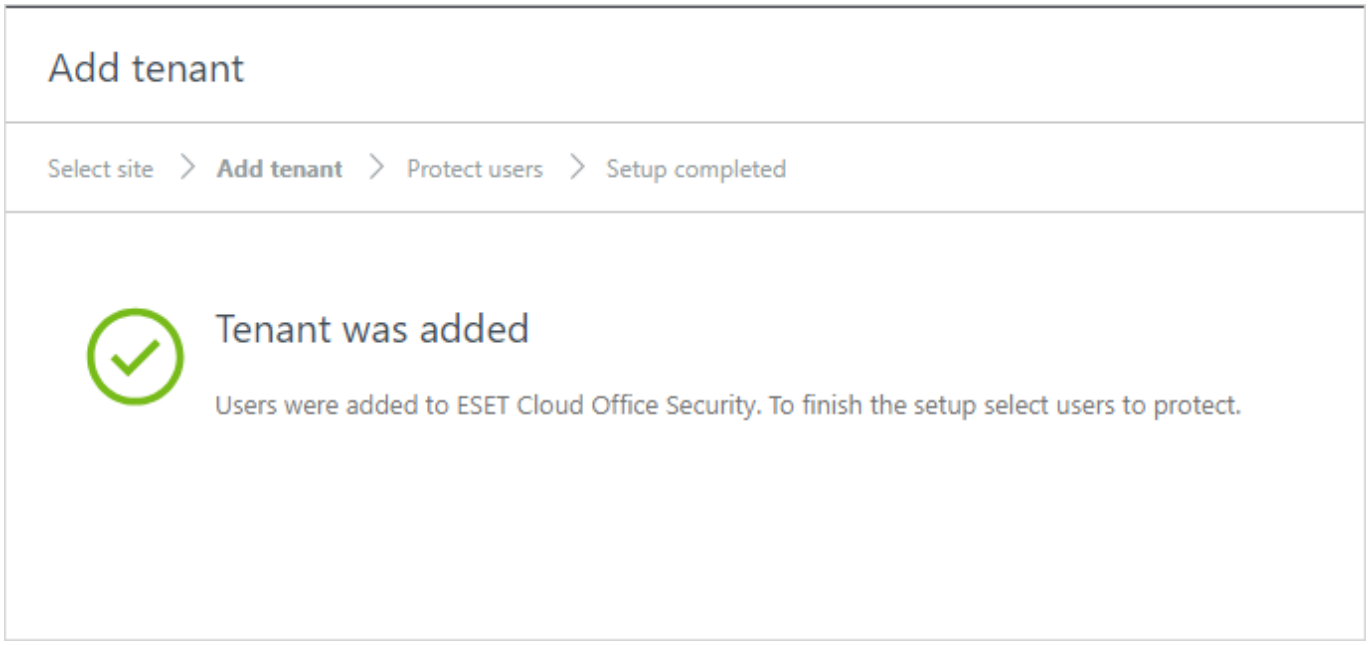
4. Se le redirigirá a la página de consentimiento en línea de Microsoft, en la que se muestra una lista de los permisos que necesita ESET Cloud Office Security.



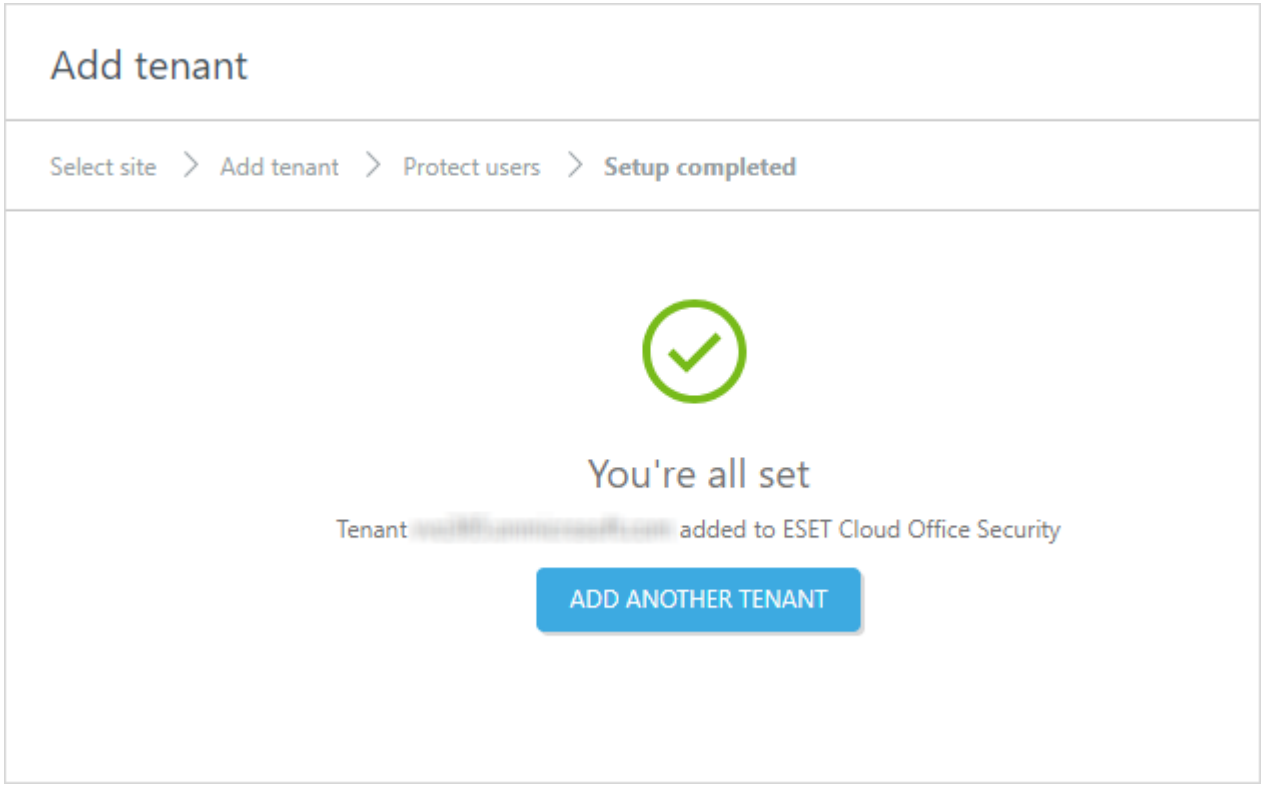
5. Introduzca las credenciales de su cuenta de administrador de Microsoft 365 para permitir el acceso de ESET Cloud Office Security a los datos de su cuenta de Microsoft y haga clic en **Aceptar**.



6. Se agregó el inquilino de Microsoft 365, incluidos los usuarios.



7. Para finalizar la configuración, haga clic en **Siguiente** y seleccione los usuarios que desea **Proteger**.



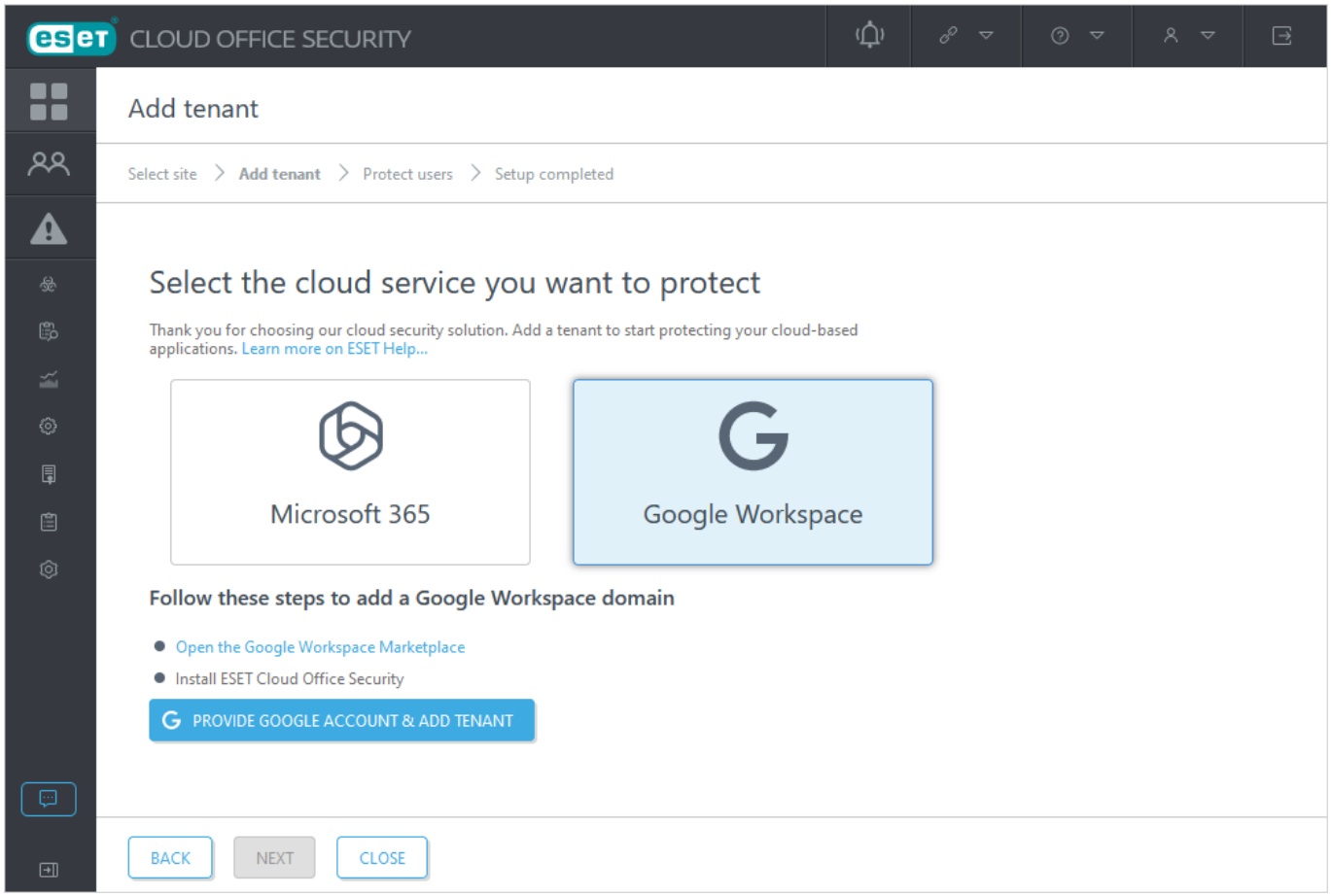
Inquilino de Google Workspace

Integre su inquilino de Google Workspace con ESET Cloud Office Security para activar la protección de los usuarios de Google Workspace.

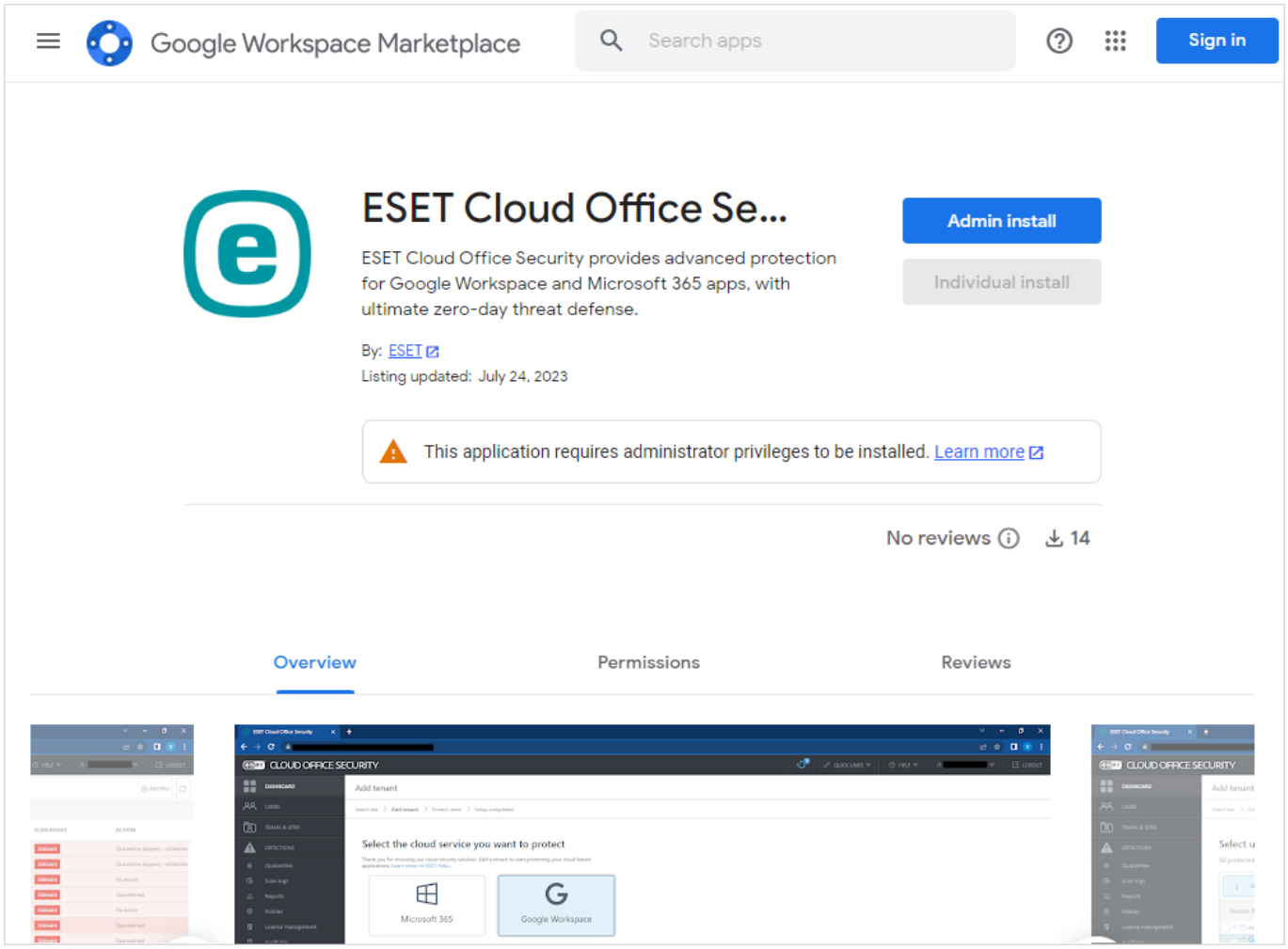
Agregar inquilino

1. Vaya a **Configuración** y haga clic en **Agregar inquilino** (o en cualquier lugar donde vea el botón **Agregar inquilino**).

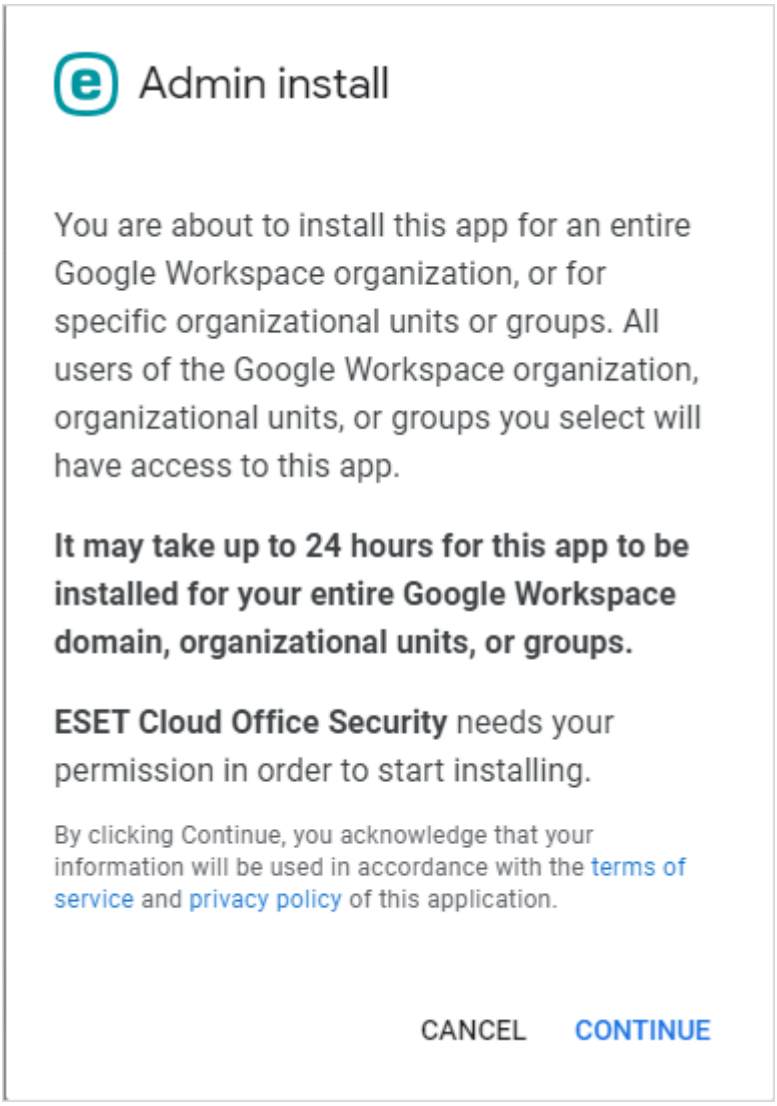
2. Haga clic en el icono de **Google Workspace**.



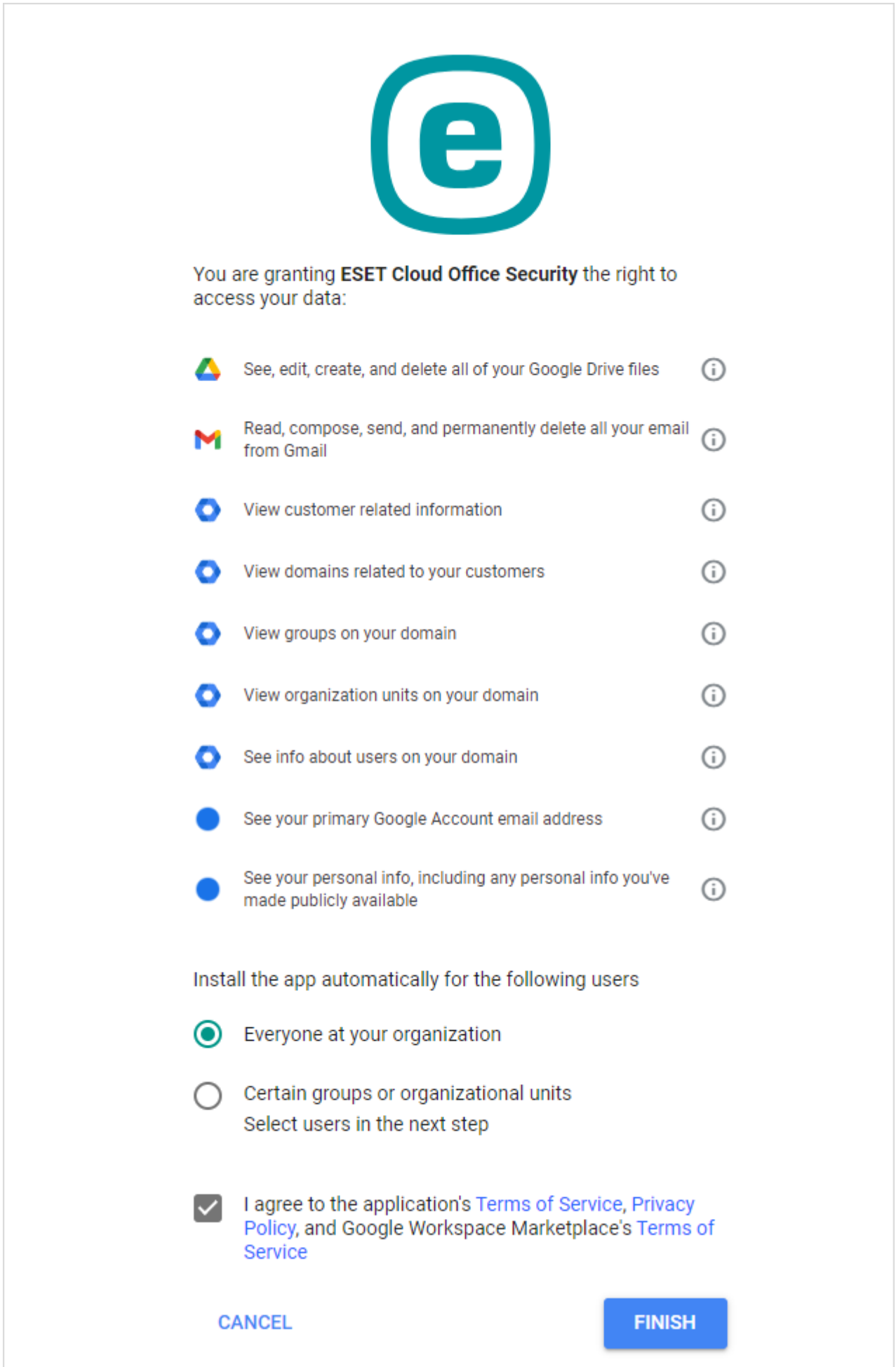
3. Haga clic en Abrir Google Workspace Marketplace e instale la aplicación de ESET Cloud Office Security con una cuenta de administrador. A día de hoy, la aplicación de ESET Cloud Office Security está disponible en Google Workspace Marketplace solo mediante el enlace directo de este asistente.



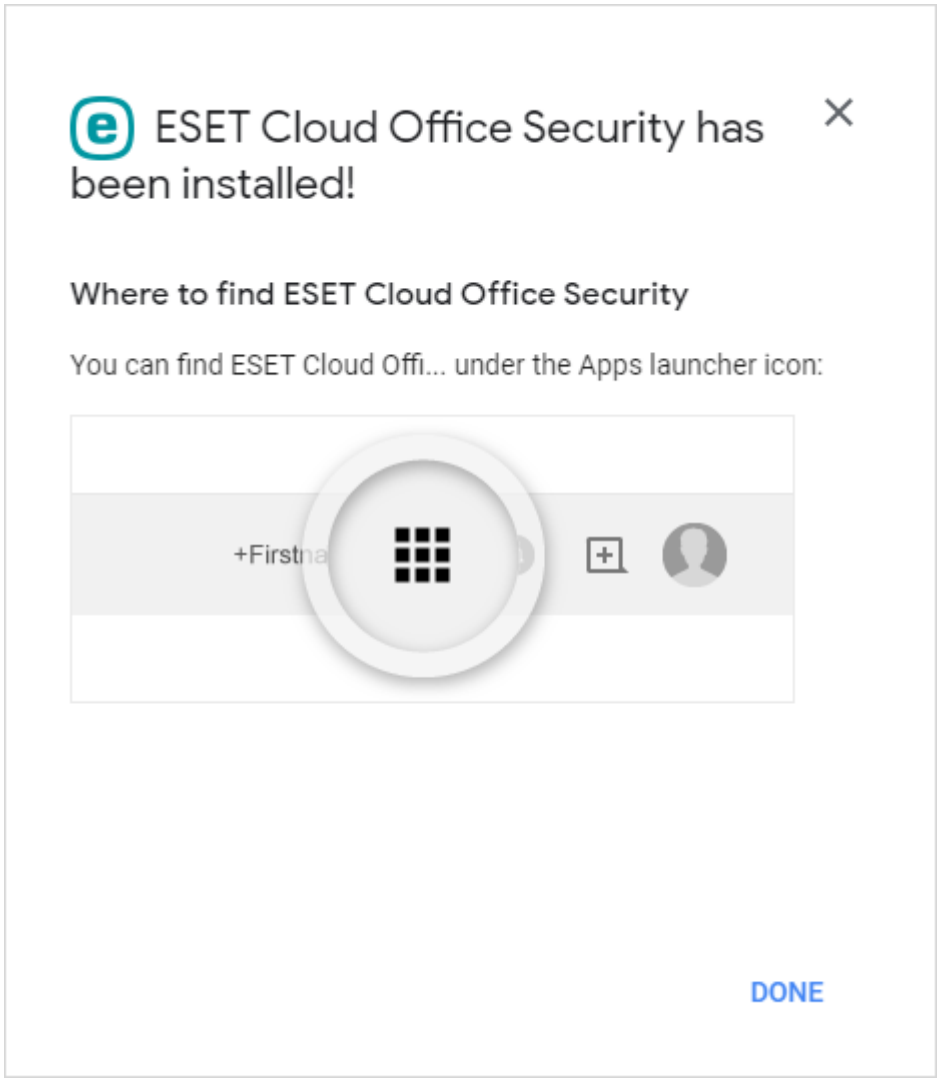
4. Haga clic en **Continue** (Continuar) en la pantalla **Admin install** (Instalación de administración).



5. Asegúrese de que la opción **Everyone at your organization** (Todos los miembros de la organización) está seleccionada en la pantalla de derechos de acceso. Además, las casillas Terms of service (Condiciones del servicio) y Privacy Policy (Política de privacidad) deben estar marcadas antes de hacer clic en **Finalizar**.

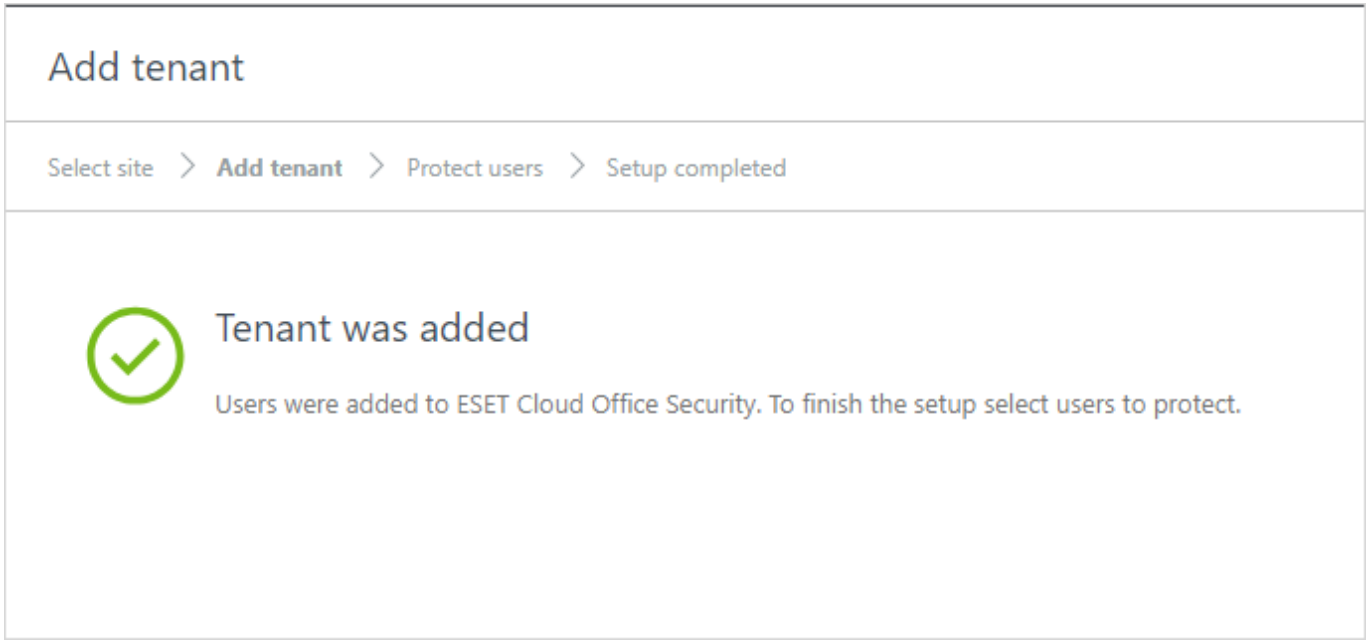

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your domain
View organization units on your domain
See info about users on your domain
See your primary Google Account email address
See your personal info, including any personal info you've made publicly available
Install the app automatically for the following users
Everyone at your organization
Certain groups or organizational units
Select users in the next step
I agree to the application's Terms of Service, Privacy Policy, and Google Workspace Marketplace's Terms of Service
CANCEL
FINISH

6. La aplicación de ESET Cloud Office Security está instalada, haga clic en **Listo**.

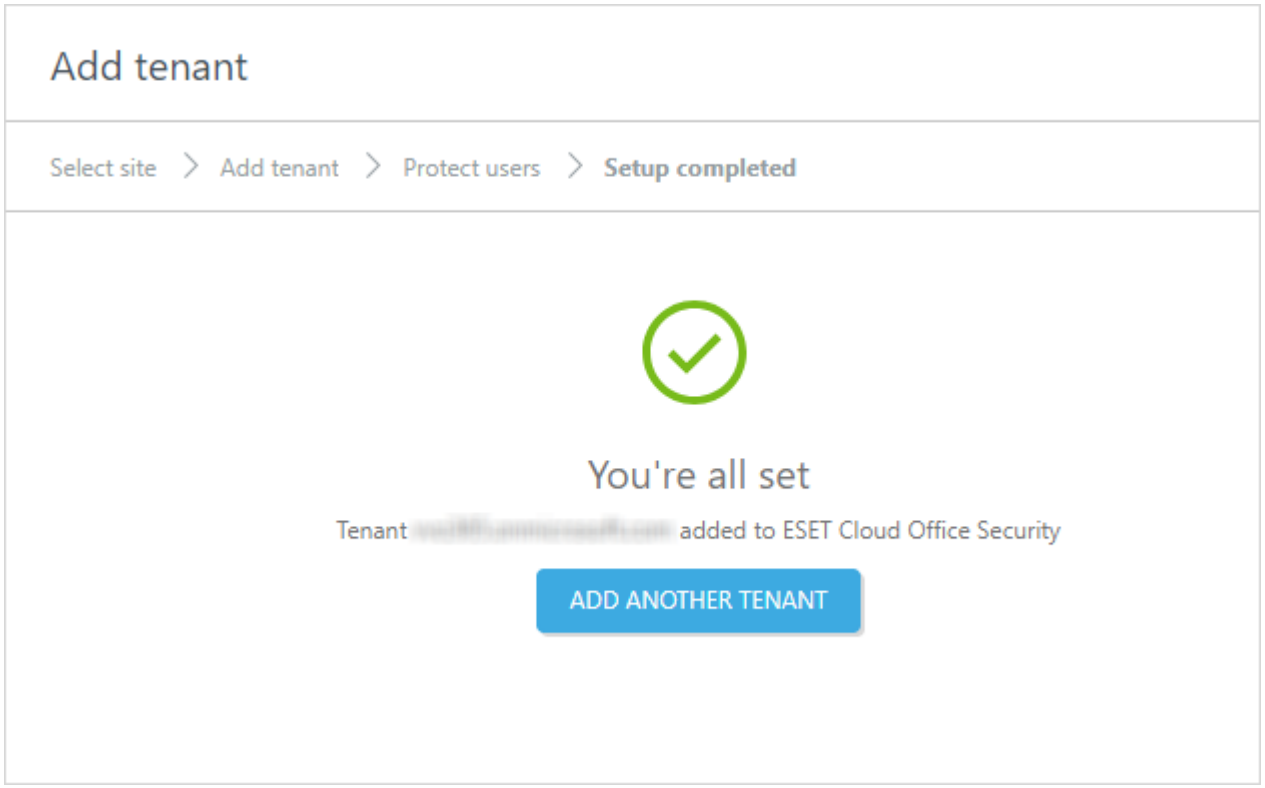


7. Una vez completada la aplicación ESET Cloud Office Security, vuelva a la consola ESET Cloud Office Security. Haga clic en **Proporcionar una cuenta de Google y agregar inquilino** para verificar la propiedad y continuar.

8. Se ha agregado el inquilino de Google Workspace, incluidos los usuarios.



9. Para finalizar la configuración, haga clic en **Siguiente** y seleccione los usuarios que desea **Proteger**. Ya lo tiene todo listo.

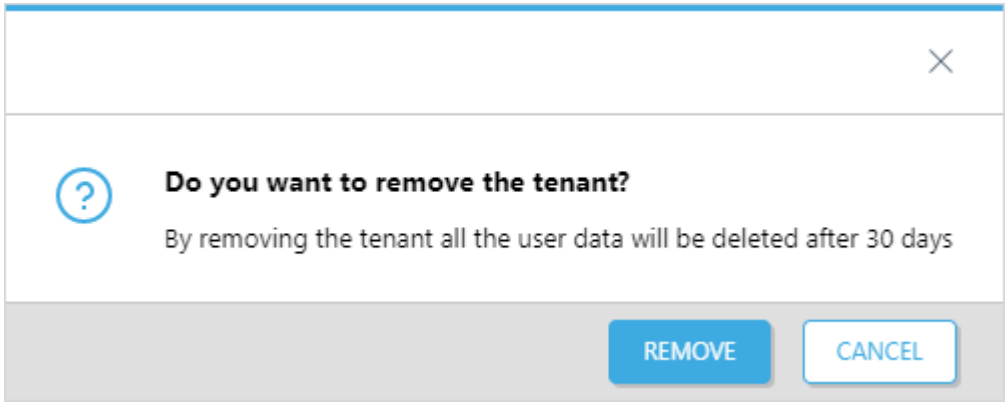


Eliminar inquilino de ESET Cloud Office Security

1. Seleccione **Configuración**.

2. Seleccione el inquilino correspondiente y haga clic en **Quitar**.

3. En una ventana de notificación se advierte de que este proceso eliminará datos como se describe en la Política de retención de datos y limitaciones y de que los usuarios perderán la protección. Haga clic en **Eliminar** para confirmar la eliminación.



Cuando elimina un inquilino de la consola ESET Cloud Office Security, los datos del inquilino se conservan durante 30 días (la cuarentena, los registros del análisis y las estadísticas se eliminan a los 30 días). Si agrega el inquilino de nuevo en un plazo de 30 días, se restaurarán todos los datos. Los demás objetos (inquilinos, usuarios, grupos, sitios, informes y políticas) se eliminan de forma permanente a los 90 días. Para obtener más información, consulte la Política de limitaciones y retención de datos.

Quitar ESET Cloud Office Security del portal de Azure

1. Inicie sesión en el portal de Azure con una cuenta de administrador.

Para eliminar una aplicación, debe figurar como propietario de la aplicación o tener privilegios de administrador.

2. Desplácese hasta el servicio **Azure Active Directory** y seleccione **Aplicaciones empresariales**.

3. Busque la aplicación **ESET Cloud Office Security** y haga clic en ella en la página de información general. Diríjase a **propiedades** y haga clic en **Eliminar**.

Navegar por ESET Cloud Office Security

Descubra cómo navegar por la interfaz de ESET Cloud Office Security. Pronto conocerá los elementos y herramientas de navegación de ESET Cloud Office Security. Son intuitivos, fáciles de usar e interactivos.

Utilice la barra de navegación del lado izquierdo para cambiar entre distintas partes de la consola de ESET Cloud Office Security:

- Usuarios
- Equipos y sitios
- Detecciones
- Cuarentena
- Registros del análisis
- Informes
- Políticas
- Administración de licencias
- Registro de auditoría
- Configuración

Colapsar: despliegue y colapse el menú de navegación. El colapso del panel ofrece más espacio en la pantalla del Panel. Para desplegar el panel de navegación, haga clic en el icono .

La barra de herramientas de la parte superior está disponible en todo momento:

Navegador de productos: acceso rápido a las consolas de ESET y otros enlaces útiles. (los productos que puede ver dependen de la licencia y los derechos de acceso).

ESET Business Account y **ESET MSP Administrator** (cuenta de licencias híbrida): si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede alternar entre la vista de ESET Business Account y la de ESET MSP Administrator.

Mostrar notificaciones: para ver todas las notificaciones, haga clic en el icono de la campana de la barra superior.

Vínculos rápidos: permite acceder fácilmente a Agregar inquilino, Nueva política, ESET Business Account o ESET MSP Administrator.

Ayuda: el primer enlace de este menú siempre remite a la ayuda en línea de la pantalla en la que se encuentra. Si no puede resolver un problema, realice una búsqueda en la Base de conocimiento de ESET o en el Foro de soporte técnico. También puede enviar comentarios o **enviar una muestra para su análisis**. Abra la página Acerca de, que contiene información detallada sobre la versión de ESET Cloud Office Security y vínculos a documentos legales.

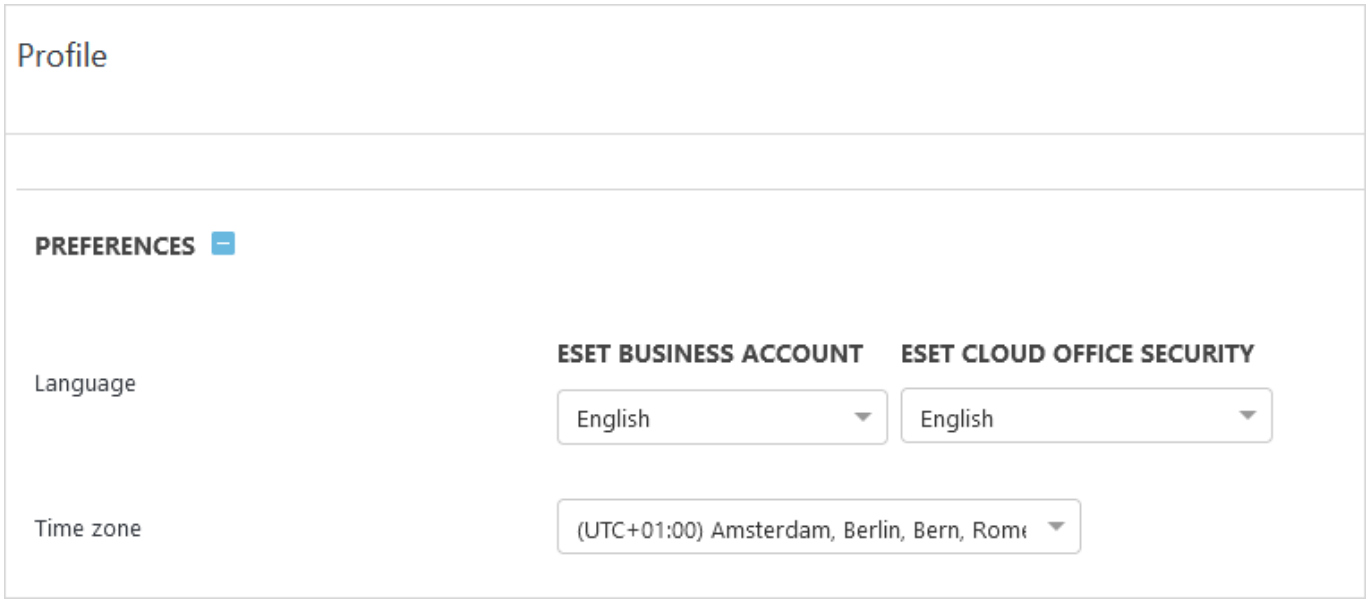
Usuario (sesión actual) – Muestra el nombre de usuario. Haga clic en **Establecer tema** y seleccione el tema que quiera en el menú desplegable:

- **Tema predeterminado (claro)**: ESET Cloud Office Security utilizará un esquema de colores claro (estándar).
- **Tema oscuro**: ESET Cloud Office Security utilizará un esquema de colores oscuro (modo oscuro).
- **Tema del sistema operativo**: el esquema de colores de ESET Cloud Office Security se basa en la configuración del sistema operativo.

Salir de sesión: para salir de la consola de ESET Cloud Office Security, pulse este pictograma omnipresente.

Cambiar idioma en el portal de ESET Cloud Office Security

Inicie sesión en ESET Business Account o ESET MSP Administrator, vaya a **Administración de usuarios** y **Modificar** usuario. Busque la configuración de idioma de ESET Cloud Office Security, cambie al idioma que desee y haga clic en **Guardar** antes de salir de la pantalla **Perfil**.



ESET LiveGuard Advanced

ESET LiveGuard Advanced ofrece otra capa de seguridad al utilizar tecnología avanzada basada en la nube de ESET para detectar nuevos tipos de amenazas nunca vistos. ESET LiveGuard Advanced le ofrece la ventaja de estar protegido frente a las posibles consecuencias de las nuevas amenazas. Si ESET LiveGuard Advanced detecta un código o comportamiento sospechoso, evita que se produzcan amenazas futuras al ponerlas temporalmente en cuarentena.

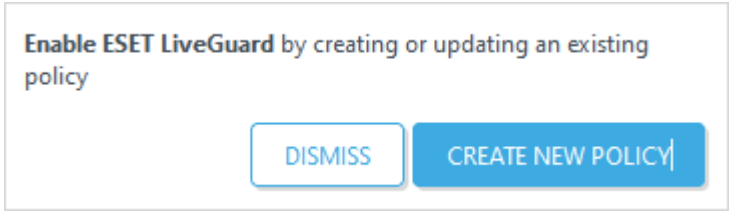
Las muestras sospechosas (archivo o mensaje de correo electrónico) se envían automáticamente a la nube de ESET, donde el servidor de ESET LiveGuard Advanced analiza la muestra con sus avanzados motores de detección de malware. Mientras los archivos o los correos electrónicos están en cuarentena, ESET Cloud Office Security espera los resultados del servidor de ESET LiveGuard Advanced.

Una vez finalizado el análisis, su ESET Cloud Office Security recibe un informe con un resumen del comportamiento observado de la muestra. Si la muestra resulta inofensiva, se libera de la cuarentena. De lo contrario, se mantiene en cuarentena.

Los resultados de ESET LiveGuard Advanced de las muestras de los mensajes de correo electrónico suelen llegar en cuestión de minutos. Sin embargo, el intervalo de espera predeterminado está establecido en 5 minutos. En casos raros, si los resultados de ESET LiveGuard Advanced no llegan en el plazo establecido, el mensaje se liberará. Puede cambiar el intervalo a su tiempo preferido (cualquier opción entre 5-60 minutos, en incrementos de un minuto).

La licencia de ESET Cloud Office Security le permite usar la característica ESET LiveGuard Advanced sin tener que pagar más. Verá la etiqueta de ELG junto al ID de licencia en Administración de licencias.

Cuando aparezca una pequeña ventana emergente, podrá activar ESET LiveGuard Advanced mediante la creación de una política nueva o la actualización de una existente.



Para obtener información más detallada sobre ESET LiveGuard Advanced, consulte Cómo funcionan las capas de detección de ESET LiveGuard Advanced .

Panel

El Panel es un conjunto de widgets que proporcionan información general sobre las actividades de seguridad de Microsoft 365. El Panel contiene información esencial en cada una de sus pestañas de información general (Información general/Exchange Online/OneDrive/Grupos del equipo/Sitios de SharePoint, Gmail, Google Drive y ESET LiveGuard Advanced). **Información general** es la pantalla principal del Panel que ve cada vez que inicia sesión en la consola de ESET Cloud Office Security. Muestra información general y estadísticas.

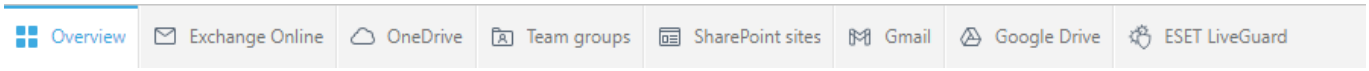
> El intervalo de actualización del Panel es de 10 minutos. Si no ve la información más reciente en el Panel, pulse **F5** para actualizarlo manualmente.

Si desea ver las estadísticas del Panel, utilice los filtros de la parte superior para elegir el **Periodo de tiempo**

(Últimas 24 horas, Últimos 7 días, Últimos 30 días o Últimos 90 días) y el **Inquilino** aplicables. En las pestañas de información general **Exchange Online**, **OneDrive**, **Grupos del equipo Sitios de SharePoint**, **Gmail**, **Google Drive** y **ESET LiveGuard Advanced** se pueden ver estadísticas y gráficos de detección adicionales. Se trata de estadísticas como el número de correos electrónicos y archivos analizados y el número de spam/phishing/malware detectado. Los gráficos muestran el tráfico de cada tipo de detección: spam, malware y phishing.

Ocasionalmente, es posible que aparezca la barra de anuncio. Los colores indican el tipo de anuncio (azul = noticias, amarillo = conocimiento, rojo = advertencia).

Utilice las pestañas del Panel para cambiar de panel de vista:



Visión general

indica
• número de inquilinos y uso de licencias
• estadísticas por cada inquilino:
oNúmero total de usuarios/Usuarios sin protección
oPrincipales destinatarios de correo no deseado/phishing/malware
oPrincipales cuentas sospechosas de OneDrive
oGrupos del equipo más sospechosos
oSitios de SharePoint más sospechosos
profundizar
• haga clic en la ventana Número total de usuarios para abrir la sección Usuarios
• haga clic en un usuario de la sección de estadísticas (spam/phishing/malware/OneDrive) para ver las detecciones pertinentes o haga clic en un grupo o sitio para ver detecciones y más información sobre el grupo del equipo o el sitio de SharePoint sospechosos.

Exchange Online

muestra
• número total de correos electrónicos analizados
• estadísticas de correos electrónicos de spam, malware y phishing detectados
• gráficos en los que cada uno representa el tráfico de spam, malware y phishing
Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

OneDrive

muestra
• el número de usuarios protegidos
• número total de archivos analizados
• estadísticas de malware detectado
• un gráfico que representa el tráfico de malware
Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

Grupos del equipo

muestra
- el número de grupos protegidos
- número total de archivos analizados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

Sitios de SharePoint

muestra
- el número de sitios protegidos
- número total de archivos analizados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

Gmail

muestra
- número total de correos electrónicos analizados
- estadísticas de correos electrónicos de spam, malware y phishing detectados
- gráficos en los que cada uno representa el tráfico de spam, malware y phishing

Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

Google Drive

muestra
- el número de usuarios protegidos
- número total de archivos analizados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

ESET LiveGuard Advanced

muestra
- archivos enviados (el recuento incluye duplicados y el número puede ser mayor que los archivos únicos)
- número de detecciones
- tiempo medio de análisis
- un gráfico que representa los archivos enviados
- principales propietarios de archivos enviados
- tipos de archivo enviados

Las ventanas son interactivas. Haga clic en una ventana de su interés y acceda a la sección correspondiente de la consola de ESET Cloud Office Security. Por ejemplo, se abre la sección Registros del análisis con las entradas del registro pertinentes.

Usuarios

La entidad central que protege ESET Cloud Office Security es la cuenta de usuario. Haga doble clic en un usuario para ver información útil como, por ejemplo, la información general, la configuración definida por las políticas, la lista de políticas asignadas al usuario y las detecciones de Gmail, Google Drive, Exchange Online y OneDrive. También puede elegir qué usuarios se protegerán o no. Los usuarios se clasifican en grupos, y cada grupo es un inquilino de Microsoft 365 que contiene sus usuarios. Para facilitar la búsqueda de un usuario determinado dentro de un grupo, puede utilizar varios criterios para filtrar.

> No se mostrarán en la consola de ESET Cloud Office Security los usuarios sin una licencia de Microsoft 365 válida y activa. Esto incluye buzones de correo compartidos sin una licencia de Microsoft 365.
> Si desea ver y administrar todos los usuarios de Microsoft 365, diríjase a Configuración y active Usuarios con licencia de Microsoft 365.

Estado de protección:

Estado	Descripción
Sin protección	Un usuario no está protegido actualmente.
Protegido automáticamente	Usuario protegido con protección automática.
Pendiente	Estado de transición que tiene lugar durante el proceso de protección de un usuario. Cuando finalice, el estado del usuario cambiará a Protegido.
Protegido	El buzón y el OneDrive del usuario están protegidos por la política predeterminada o por una política personalizada.
Advertencia de	El proceso de protección de un usuario ha fallado. Es posible que se haya producido un error en uno de los recursos, buzones de correo o OneDrive. Es probable que ninguno de los dos recursos estén disponibles para el usuario. Compruebe si el usuario tiene una licencia de Microsoft 365 válida asignada.

Desplácese por el árbol para ver los usuarios de un inquilino o grupo determinados. Para ver todos los usuarios de todos los inquilinos y grupos, haga clic en **Todo**.

Para obtener información más detallada, haga doble clic en un usuario o haga clic en el icono y seleccione una acción (**Mostrar detalles**, **Proteger** o **Quitar protección**). Haga clic en un usuario para abrir la ventana **Mostrar detalles**, que consta de cuatro partes:

Acción	Uso
Visión general	Muestra información básica sobre el usuario cargado desde Microsoft 365 (correo electrónico, grupo, perfil de trabajo, etc.). También se muestra el estado de protección actual del buzón y OneDrive.
Configuración	Contiene una lista de solo lectura de la Configuración y las Políticas asignadas a este usuario. Cambie entre las pestañas para ver la configuración o una lista de las políticas asignadas. No puede modificar la configuración ni asignar políticas a usuarios; vaya a la sección Políticas.
Detecciones	Mostrar todas las detecciones de esta cuenta de usuario (Gmail, Google Drive, Exchange Online o OneDrive).
Cuarentena	Muestre todos los archivos y los correos electrónicos en cuarentena almacenados de este usuario. También puede utilizar una de las siguientes acciones: Liberar, Descargar o Eliminar los archivos o los correos electrónicos en cuarentena.

Puede filtrar los usuarios en función de varios criterios. Haga clic en **Agregar filtro** y seleccione un tipo de filtro en

el menú desplegable o escriba una cadena (repetir al combinar varios criterios):

Agregar filtro	Uso
Estado de protección	Seleccione el estado Protegido, Sin protección, Advertencia o Pendiente de un usuario.
Protegido automáticamente	Mostrar solo los usuarios protegidos automáticamente.
Nombre	Escriba un nombre de usuario válido.
Correo electrónico	Escriba un correo electrónico de usuario válido.
Escribir	Seleccione el tipo de usuario (Desconocido, Usuario, Vinculado, Buzón compartido, Sala, Equipo u Otros).

Proteger a los usuarios

1. Seleccione los **Usuarios** que se protegerán y haga clic en **Proteger**.
2. Seleccione el **Grupo de licencias** cargado desde ESET Business Account y haga clic en **Aceptar**. La política predeterminada protege ahora a los usuarios seleccionados.
3. Si es necesario, especifique una política personalizada para los usuarios en la sección Políticas.

Quitar protección a los usuarios

Seleccione los **Usuarios** que se desprotegerán y haga clic en **Quitar protección**.

Equipos y sitios

ESET Cloud Office Security ofrece protección para grupos del equipo o sitios de SharePoint.

Cambie entre las pestañas Grupos del equipo y Sitios de SharePoint. Muestra una lista de grupos del equipo o sitios de SharePoint para cada inquilino.

Grupos del equipo

Muestra objetos que son tipos de grupo de Microsoft 365, incluidos el sitio predeterminado de SharePoint del equipo y OneDrive:

- nombre
- status
- en el mensaje
- inquilino

Para proteger a los grupos del equipo, asegúrese de que al menos un miembro es un usuario protegido por ESET Cloud Office Security. Cada grupo de Microsoft 365 tiene un sitio predeterminado de SharePoint del equipo y OneDrive, que también están protegidos.

Sitios de SharePoint

Muestra todos los sitios raíz de SharePoint que no están asociados al grupo de Microsoft 365:

- nombre
- status

- URL
- inquilino

Los sitios de SharePoint están protegidos automáticamente, incluyendo sus subsitios (no mostrados).

Para obtener información más detallada, haga clic en un grupo del equipo o en un sitio de SharePoint para abrir la ventana **Mostrar detalles**, que consta de cuatro partes:

Acción	Uso
Visión general	Muestra la información necesaria sobre los grupos del equipo o sitios de SharePoint cargados desde Microsoft 365 (correo electrónico, propietario, miembros, autor, URL, etc.). También se muestra el estado de protección actual del grupo del equipo o el sitio de SharePoint.
Configuración	Contiene una lista de solo lectura de la Configuración y las Políticas asignadas. Cambie entre las pestañas para ver la configuración o una lista de las políticas asignadas. No puede modificar la configuración ni asignar políticas; vaya a la sección Políticas.
Detecciones	Muestre todas las detecciones del grupo del equipo o el sitio de SharePoint.
Cuarentena	Muestre todos los archivos en cuarentena. También puede utilizar una de las siguientes acciones: Libere, descargue o elimine los archivos en cuarentena.

Haga clic en **Agregar filtro** para filtrar grupos del equipo o sitios de SharePoint.

Detecciones

Muestra todas las detecciones realizadas por ESET Cloud Office Security. Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint utilizando las pestañas. Muestra información de cada detección, por ejemplo, los archivos detectados que se han cargado en un grupo del equipo se mostrarán en la pestaña Grupos del equipo.

Haga clic en el icono para abrir una barra lateral con un resumen de una entrada de registro específica (detección). Para obtener información más detallada, haga clic en el icono y seleccione **Mostrar detalles**.

Desplácese por el árbol para ver solo las detecciones de un determinado inquilino o grupo. Para ver todas las detecciones de cada inquilino y grupo, haga clic en **Todo**. Para facilitar la búsqueda de una determinada detección, puede utilizar varios criterios para filtrar. Haga clic en **Agregar filtro** y seleccione el tipo de filtro en el menú desplegable o escriba una cadena (repetir cuando se combinen criterios):

Agregar filtro	Uso
Ocurrido desde	Especifique el rango de "fecha de inicio".
Ocurrido hasta	Especifique el rango de "fecha de fin".
Asunto	Se aplica a los mensajes que contienen o no contienen una cadena concreta (o una expresión regular) en el asunto.
ID del mensaje	Filtra los mensajes de correo electrónico por ID exclusivo del mensaje al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o varios intentos de entrega.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtre los mensajes por destinatarios.
Buzón	Se aplica a los mensajes situados en un buzón concreto.

Agregar filtro	Uso
Resultado del análisis	Seleccione una de las siguientes opciones: Malware, Malware (detectado por ESET LiveGuard Advanced), Phishing o Spam.
Acción	Seleccione una de las acciones disponibles.
Equipo	Escriba el nombre de equipo válido.
Sitio	Escriba el nombre de sitio válido.
Objeto	Escriba un nombre de objeto válido.
Detección	Escriba un nombre de detección válido.
Hash	Escriba un hash de detección válido.

Cuando haga clic en el icono , se mostrará la opción **Quitar elemento de lista blanca** si antes ha añadido a la lista blanca un archivo quitándolo de la Cuarentena para el mismo usuario. Utilice esta opción para quitar un archivo de la lista blanca. Todos los futuros archivos de este tipo se pondrán en cuarentena.

> El periodo de retención de las detecciones es de 90 días. Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente.

Informe de falsos positivos (FP)/falso negativo (FN)

Puede informar de forma manual de las detecciones falsos positivos y falsos negativos de spam, phishing o malware mediante el envío de una muestra a los laboratorios de ESET para su análisis. Direcciones de correo electrónico a las que enviar las muestras:

Spam: envíe un mensaje de correo electrónico a nospam_ecos@eset.com para los mensajes de correo electrónico incorrectamente marcados como spam o a spam_ecos@eset.com para los mensajes de spam no detectados con el mensaje original como archivo adjunto en formato *.eml* o *.msg*.

Phishing: para informar de un falso positivo o falso negativo de clasificación de phishing, envíe un mensaje de correo electrónico a Samples@eset.com con el asunto *'phishing email'* e incluya el correo electrónico de phishing como archivo adjunto en formato *.eml* o *.msg*.

Malware: para informar de un falso positivo o falso positivo de clasificación de malware, envíe un mensaje de correo electrónico Samples@eset.com con el asunto *'False positive'* o *'Suspected infection'* e incluya los archivos comprimidos en formato *.zip .rar* como archivo adjunto.

Informes

Los informes de ESET Cloud Office Security le mantienen informado con una descripción general de las estadísticas de protección de ESET Cloud Office Security. Puede elegir entre dos tipos de informes: informes estadísticos o informes de Cuarentena de correo electrónico.

Los informes estadísticos contienen la siguiente información para la protección de Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint: el número de correos electrónicos y archivos analizados, así como el malware, phishing y spam detectados durante el periodo especificado. Los informes se pueden generar y descargar manualmente en formato *PDF* o *CSV*, o programarlos y enviarlos por correo electrónico a los destinatarios seleccionados. El formato de salida *PDF* presenta los datos en un gráfico, muestra la media a largo plazo para compararlas e incluye información sobre el tráfico de cada tipo de protección y los principales destinatarios de malware, phishing y spam.

El informe de Cuarentena de correo electrónico contiene una lista de los objetos que se han puesto en

cuarentena recientemente. El informe se envía por correo electrónico a los destinatarios seleccionados. Los destinatarios pueden liberar los mensajes de spam (si se consideran seguros o legítimos) haciendo clic en el vínculo **Liberar**. Solo se aplica al spam; no se pueden liberar otros tipos de objetos en cuarentena.

Puede acceder a las estadísticas por correo electrónico sin necesidad de iniciar sesión en la consola de ESET Cloud Office Security. Configure y programe informes recurrentes y especifique destinatarios de correos electrónicos. Además, puede generar estadísticas de informes inmediatamente desde la consola de ESET Cloud Office Security. Seleccione un informe existente (también puede ser un informe programado) y haga clic en **Generar & Descargar.** Hacer clic con el botón derecho del ratón en el menú desplegable también funciona. Puede crear fácilmente una nueva plantilla de informe con una configuración personalizada.

Nuevo informe

Haga clic en Nuevo informe para abrir el asistente de plantilla de informe y especificar los ajustes personalizados. Escriba el nombre y la descripción del informe.

Idioma

Elija el idioma que desee en el menú desplegable. El informe se generará en el idioma seleccionado.

Escribir

Seleccione el tipo que desea incluir en las estadísticas.

Informes estadísticos

Cree informes programados o a petición que contengan información según las opciones que elija.

Informes de Cuarentena de correo electrónico

Para informar a los usuarios sobre los mensajes de correo electrónico que han puesto en cuarentena recientemente, envíe correos electrónicos de notificación a los usuarios seleccionados. Puede asignar uno o varios destinatarios, o un grupo. Elija un intervalo para los informes y la fecha y la hora de inicio. Si se trata de un informe repetido, elija cuándo debe finalizar (en una fecha, después de varias ocurrencias o nunca). El informe de Cuarentena de correo electrónico solo se desencadena cuando hay elementos nuevos. Los destinatarios del informe pueden liberar los mensajes de spam (si se consideran seguros o legítimos) haciendo clic en el vínculo Liberar (se abre una ventana nueva en un navegador web). El mensaje de spam liberado se entrega en un correo electrónico independiente como archivo adjunto.

Inquilino

Esta opción está disponible para un entorno multiinquilino. Puede seleccionar varios inquilinos para los que generar estadísticas. El informe se generará para cada inquilino por separado, y se enviará en un mensaje de correo electrónico de informe de ESET Cloud Office Security con varios archivos adjuntos.

Período de tiempo

Defina el periodo de tiempo para el que desea que se muestren los resultados (últimas 24 horas, semana, mes). Si selecciona Personalizar, puede especificar un intervalo (Fecha de inicio y Fecha de fin).

Salida

Seleccione el formato de archivo adecuado. Puede elegir *PDF* o *CSV*. El formato *PDF* incluye datos recogidos en gráficos. El formato *CSV* es apropiado para datos sin procesar. Los informes se recopilarán de acuerdo con las

opciones especificadas. Si seleccionó Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo o sitios de SharePoint, el archivo de salida sería un archivo comprimido en formato ZIP que contiene archivos de informes en formato *PDF* o *CSV*.

Marca blanca

Active esta característica si necesita que el logotipo de su empresa aparezca en el informe. Tiene la opción de usar el encabezado del informe de marca conjunta que muestra su logotipo junto con el logotipo de ESET o solo su logotipo. Cargue el logotipo en formato *PNG* o *JPEG*.

Programado

Utilice las tareas programadas para que los informes se generen en una fecha y una hora especificadas, también como evento recurrente. Los informes programados se entregan a destinatarios seleccionados, que recibirán el mensaje de correo electrónico del informe de ESET Cloud Office Security con archivos adjuntos.

Repetir

Elija si desea que el informe se genere una o varias veces:

- **Una vez**: el informe se realizará solo una vez.
- **Diariamente:** el informe se generará y entregará reiteradamente todos los días (a menos que defina la opción finalizar después de ocurrencias).
- **Semanalmente:** el informe se generará y entregará reiteradamente los días seleccionados de la semana.
- **Mensualmente:** el informe se generará y entregará una vez al mes el día seleccionado.

Inicio desde

Elija la fecha de inicio de los informes.

Termina

Seleccione cuándo finaliza el intervalo de repetición.

Destinatarios

Especifique la dirección de correo electrónico del destinatario del informe y pulse Entrar para confirmar. Repita el procedimiento para agregar varios destinatarios.

Para ver información o acciones detalladas, haga clic en el icono y seleccione una acción:

Acción	Uso
Mostrar detalles	Muestra información detallada sobre un informe.
Generar & Descargar	Haga clic en Generar & Descargar y elija *PDF* o *CSV*. El formato *PDF* incluye datos recogidos en gráficos. El formato *CSV* es apropiado para datos sin procesar. Los informes se recopilarán de acuerdo con las opciones especificadas. Si seleccionó Exchange Online, OneDrive, grupos del equipo o sitios de SharePoint, el archivo de salida sería un archivo comprimido en formato *ZIP* que contiene archivos de informes en formato PDF o *CSV*.
Modificar	Edite la configuración de un informe existente.
Eliminar	Elimine el informe seleccionado por completo.

Para filtrar los informes, haga clic en **Agregar filtro** y seleccione un tipo de filtro en el menú desplegable o escriba una cadena (repetir al combinar varios criterios):

Agregar filtro	Uso
Nombre	Escriba el nombre parcial o completo del informe.
Programado	Seleccione No programado, Una vez, Diariamente, Semanalmente o Mensualmente.
Datos	Seleccione Exchange Online, OneDrive, Grupos del equipo o Sitios de SharePoint para filtrar por datos.

Cuarentena

Una sencilla administración de objetos (mensajes de correo electrónico y archivos) que ha puesto en cuarentena ESET Cloud Office Security. Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint utilizando las pestañas. Puede ver información importante sobre cada objeto.

Haga clic en el icono para abrir una barra lateral con un resumen de un objeto específico. Para obtener información más detallada, haga clic en el icono y seleccione **Mostrar detalles**.

Desplácese por el árbol para ver solo las detecciones de un determinado inquilino o grupo. Para ver todas las detecciones de cada inquilino y grupo, haga clic en **Todo**.

Inspeccione archivos o mensajes de correo electrónico puestos en cuarentena y realice una acción (**Eliminar** o **Liberar**). También puede **Descargar** el archivo original o el archivo de almacenamiento con protección por contraseña en formato *.zip*.

> Si considera que una detección no es maliciosa (falso positivo), puede **Liberar** un archivo de la cuarentena. El archivo liberado se coloca automáticamente en una lista blanca, en función del hash. Todas las instancias futuras del mismo archivo, para el mismo usuario, no se detectarán como sospechosas y no se pondrán en cuarentena. La lista blanca se realiza automáticamente por usuario. Para otros usuarios, el mismo archivo se sigue detectando como sospechoso y puesto en cuarentena.
> Puede quitar un archivo de la lista blanca de Detecciones mediante la opción **Quitar elemento de lista blanca**.

Haga clic en el icono y seleccione una acción:

Acción	Uso
Mostrar detalles	Muestra información más detallada sobre el mensaje de correo electrónico puesto en cuarentena.
Liberar (mensajes de correo electrónico o archivos)	Libera el correo electrónico y lo envía a sus destinatarios originales en forma de correo electrónico de notificación de la cuarentena con el mensaje original como archivo adjunto. Si se trata de un elemento de OneDrive, el archivo se cargará en su ubicación original en el OneDrive del usuario. Al liberar un archivo de un grupo del equipo o un sitio de SharePoint, el archivo aparecerá de nuevo en su ubicación original. El archivo liberado se coloca automáticamente en una lista blanca, en función del hash. Esto impide que el archivo se vuelva a poner en cuarentena.
Eliminar	Elimina el elemento de la cuarentena.
Descargar archivo original	Descargue el archivo no protegido en su forma original.
Descargar archivo de almacenamiento con protección por contraseña	Descargue el archivo comprimido protegido con una contraseña.

Acción	Uso
Enviar muestra	El cuadro de diálogo de envío de muestras le permite enviar un archivo o spam a ESET para que lo analicen. En el menú desplegable, elija el Motivo del envío para indicar por qué quiere enviar la muestra.

Para facilitar la búsqueda de un objeto en cuarentena determinado, puede utilizar varios criterios para filtrar. Haga clic en **Agregar filtro** y seleccione el tipo de filtro en el menú desplegable o escriba una cadena (repetir cuando se combinen criterios):

Agregar filtro	Uso
Ocurrido desde	Especifique el rango de "fecha de inicio".
Ocurrido hasta	Especifique el rango de "fecha de fin".
Asunto	Se aplica a los mensajes que contienen o no contienen una cadena concreta (o una expresión regular) en el asunto.
ID del mensaje	Filtra los mensajes de correo electrónico por ID exclusivo del mensaje al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o varios intentos de entrega.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtre los mensajes por destinatarios.
Buzón	Se aplica a los mensajes situados en un buzón concreto.
Resultado del análisis	Seleccione una de las siguientes opciones: Malware, Malware (detectado por ESET LiveGuard Advanced), Phishing o Spam.
Equipo	Escriba el nombre de equipo válido.
Objeto	Escriba un nombre de objeto válido.
Sitio	Escriba un nombre de sitio válido.

> El periodo de retención de los objetos en cuarentena es de 30 días. Los objetos con una antigüedad superior a los 30 días se eliminarán de la cuarentena de forma permanente.

Registros del análisis

Muestra todos los resultados de análisis obtenidos por ESET Cloud Office Security. Los registros son similares a las Detecciones, pero, además, puede incluir en la lista objetos sin limpiar (active la opción Registrar todos los objetos en las políticas). Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, Grupos del equipo, Sitios de SharePoint y Archivos enviados con las pestañas. Puede ver una cantidad importante de información para cada detección. La lista Archivos enviados enumera los archivos enviados a ESET LiveGuard Advanced para su análisis.

Haga clic en el icono para abrir una barra lateral con un resumen de una entrada de registro concreta. Para obtener información más detallada, haga clic en el icono y seleccione **Mostrar detalles**.

Desplácese por el árbol para ver solo las entradas de registro de un determinado inquilino o grupo. Para ver todas las detecciones de cada inquilino y grupo, haga clic en **Todo**.

> Si el resultado del análisis es **No analizado**, el motivo puede variar. Consulte las limitaciones para obtener más información.

Cuando hace clic en el icono del engranaje situado en la esquina superior derecha para acceder a **Exportar a CSV** desde el menú contextual, puede exportar la tabla con cuadrícula a formato *CSV* y utilizarla en otras

aplicaciones para trabajar con la lista.

Para facilitar la búsqueda de una determinada entrada de registro, puede utilizar varios criterios para filtrar. Haga clic en **Agregar filtro** y seleccione el tipo de filtro en el menú desplegable o escriba una cadena (repetir cuando se combinen criterios):

Agregar filtro	Uso
Ocurrido desde	Especifique el rango de "fecha de inicio".
Ocurrido hasta	Especifique el rango de "fecha de fin".
Origen de datos	Seleccione una de las siguientes opciones: Exchange Online, OneDrive, Grupo del equipo y Sitio de SharePoint.
Buzón	Se aplica a los mensajes situados en un buzón concreto.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtre los mensajes por destinatarios.
Asunto	Se aplica a los mensajes que contienen o no contienen una cadena específica en el asunto.
ID del mensaje	Filtra los mensajes de correo electrónico por ID exclusivo del mensaje al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o varios intentos de entrega.
Resultado del análisis	Seleccione una de las siguientes opciones: Malware, Malware (detectado por ESET LiveGuard Advanced), Phishing, Spam, Desinfectado, No analizado, Error o Desactivado.
Acción	Seleccione una de las acciones disponibles.
Propietarios	Escriba el nombre de propietario válido.
Objeto	Escriba un nombre de objeto válido.
Detección	Escriba un nombre de detección válido.
Hash	Escriba un hash de detección válido.
Equipo	Escriba un nombre de equipo válido.
Sitio	Escriba un nombre de sitio válido.

Hay un periodo de retención de 90 días para los registros. Los registros con una antigüedad superior a 90 días se eliminarán de forma permanente. Si tiene una política que utiliza **Registrar todos los objetos**, la retención de las entradas de registro con un resultado de análisis de **Desinfectado** es de 3 días. Los resultados de análisis de Desinfectado con una antigüedad superior a los 3 días se eliminarán de forma permanente.

Políticas

Las organizaciones de mayor tamaño suelen tener varios departamentos y desean configurar diferentes ajustes de protección para cada unidad organizativa. ESET Cloud Office Security ofrece ajustes de protección basados en políticas que puede personalizar y asignar a los usuarios, grupos de usuarios, inquilinos, grupos del equipo o sitios de SharePoint seleccionados.

Para agregar criterios de filtrado, haga clic en **Agregar filtro**, seleccione el **Nombre** del elemento aplicable y escriba el nombre de la política válido. El árbol de políticas muestra los inquilinos y sus grupos de usuarios, grupos del equipo o sitios de SharePoint, incluido un grupo **No asignado** que contiene políticas personalizadas que no están asignadas a ningún destino.

Puede agregar una nueva política o modificar una política existente y su configuración:

1. Haga clic en **Políticas** > **Nueva política**.

2. Escriba el **Nombre** y la **Descripción** de una política nueva.

3. Seleccione un destino y configure una política para:

   • **Inquilinos** – Configurar la protección de Gmail, Google Drive, Exchange Online, OneDrive, sitios de SharePoint y grupos del equipo y asignarla a los inquilinos seleccionados

   • **Usuarios**: protección de Gmail, Google Drive, Exchange Online y OneDrive, y asígnela a los usuarios o grupos de usuarios seleccionados

   • **Grupos del equipo** – Configurar la protección de los grupos del equipo y asignarla a los grupos del equipo seleccionados

   • **Sitios de SharePoint** – Configurar la protección de los sitios de SharePoint y asignarla a los sitios seleccionados

4. Personalice la **configuración** de protección para Exchange Online, Gmail, OneDrive, Google Drive, Grupos del equipo, Sitios de SharePoint o ESET LiveGuard Advanced y haga clic en **Siguiente**.

5. Haga clic en **Asignar** y elija el destino al que desee asignar la política.

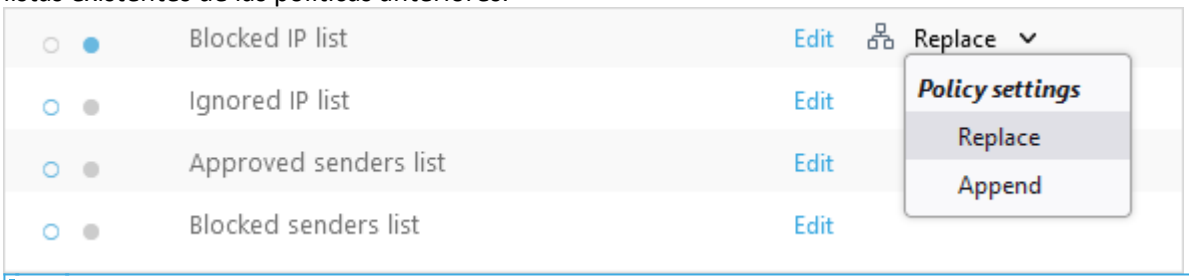
6. Haga clic en **Guardar cambios** para guardar la configuración de la política.

Principios de la política

Política predeterminada • Se aplica a todos los usuarios (protegidos y no protegidos) • No se puede modificar ni eliminar
La política personalizada puede asignarse a: • **Usuarios:** se aplica a usuarios concretos seleccionados manualmente • **Grupos:** se aplica a todos los miembros del grupo de usuarios • **Inquilinos:** la política se aplica a todas las entidades del inquilino • **Grupos del equipo:** se aplica a un grupo del equipo • **Sitios de SharePoint:** se aplica a un sitio de SharePoint
La política personalizada asignada a un **Inquilino** o un **Grupo** se fusiona con la política predeterminada. La **Política de inquilino**, la **Política de grupo**, la **Política de grupos del equipo** o la **Política de sitios de SharePoint** personalizadas tienen prioridad sobre la política predeterminada. La política personalizada asignada a un **usuario** se fusiona con las políticas de **inquilino, grupo**, **grupos del equipo**, **sitios de SharePoint** y la política predeterminada. Una política de **usuario** personalizada tiene prioridad sobre una política de inquilino o grupo y una política predeterminada. No obstante, cuando un usuario carga un archivo en un grupo del equipo o un sitio de SharePoint, se aplica la política para el grupo del equipo o el sitio de SharePoint.
A los usuarios e inquilinos pueden asignárseles varias **políticas personalizadas**, pero la política efectiva se calcula según la prioridad (orden).

Configuración de listas antispam al fusionar políticas

La opción de fusión se aplica a la configuración de Listas antispam y de Notificar al administrador (direcciones para correos electrónicos de notificación de Antimalware y Antiphishing).
Si tiene varias políticas con listas antispam (listas de direcciones IP, dominios o direcciones de correo electrónico aprobadas, bloqueadas e ignoradas) o direcciones de administrador de Antimalware y Antiphishing para correos electrónicos de notificación, elija la estrategia de fusión:
Sustituir: mantenga solo las nuevas entradas de las listas (opción predeterminada). Las nuevas entradas de las listas de la política actual sustituyen a las listas de las políticas anteriores.
Anexar: amplíe las listas de las políticas anteriores anexando nuevas entradas. Fusione las listas de las políticas anteriores con nuevas entradas de la política actual. Las nuevas entradas se colocan al final (parte inferior) de las listas existentes de las políticas anteriores.



Antes de que la opción de fusión estuviera disponible, el comportamiento predeterminado era **Sustituir**. Si ya utiliza políticas con listas antispam específicas, puede mantener la opción predeterminada **Sustituir** o cambiar a **Anexar** si lo prefiere.

Cree una nueva política con una lista antispam definida y seleccione la opción de fusión (si hay políticas existentes con listas antispam).
1. Haga clic en **Políticas** > **Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Inquilinos** como destino y haga clic en **Siguiente**.
3. Expanda **Antispam de Exchange Online** y haga clic en **Editar** junto a la lista IP bloqueadas.
4. Haga clic en **Agregar**, escriba la dirección IP, pulse la tecla **Entrar** para completar la acción (también puede importar la lista desde un archivo) y haga clic en **Guardar cambios**.
5. Elija **Anexar** como opción de fusión en el menú desplegable y haga clic en **Siguiente**.
6. Haga clic en **Asignar**, elija **Asignar a inquilinos** en el menú desplegable, marque la casilla de verificación situada junto al inquilino y haga clic en **Aceptar**.
7. Haga clic en **Guardar cambios** para finalizar el proceso.

Para reorganizar la prioridad de las políticas, haga clic en **Cambiar orden**. Seleccione una política o varias políticas y haga clic en **Aplicar antes** o en **Aplicar más tarde** para cambiar su prioridad. Las políticas se aplican de forma global (independientemente de la asignación: inquilino, grupo o usuario) en el orden especificado, de arriba abajo. La política predeterminada siempre se aplica primero.

Para realizar las siguientes acciones, seleccione la política y haga clic en el icono :

Acción	Uso
Mostrar detalles	Muestre información detallada sobre una política creada, ajustes y a quién están asignadas las políticas.
Modificar	Modificar la configuración de una política existente.
Asignar	Seleccione los usuarios, los inquilinos, los grupos del equipo o los sitios de SharePoint a los que se aplica la política.
Duplicar	Cree una política nueva basada en la plantilla seleccionada. Se necesitará un nombre nuevo para la política duplicada.
Eliminar	Elimine por completo la política seleccionada.

Cree una política de inquilino personalizada para ver todos los resultados del análisis (incluidos los archivos desinfectados) en Registros del análisis. La política de inquilino se aplica a todos los usuarios (protegidos y no protegidos).

1. Haga clic en **Políticas** > **Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Inquilinos** como destino y haga clic en **Siguiente**.
3. Expanda **Configuración general de Exchange Online** y haga clic en el interruptor para activar **Registrar todos los objetos**.
4. Expanda **Configuración general de OneDrive** y haga clic en el interruptor para activar **Registrar todos los objetos**.
5. Expanda **Configuración general de grupos del equipo** y haga clic en el interruptor para activar **Registrar todos los objetos**.
6. Expanda **Configuración general de sitios de Sharepoint**, haga clic en el interruptor para activar **Registrar todos los objetos** y haga clic en **Siguiente**.
7. Haga clic en **Asignar**, marque la casilla de verificación situada junto al inquilino y, a continuación, haga clic en **Aceptar**.
8. Haga clic en **Guardar cambios** para finalizar el proceso.

Cree una política personalizada para usuarios específicos con ajustes avanzados que afecten al modo de tratar el malware, el spam y el phishing. Con esta política, los archivos adjuntos de correo electrónico que contienen malware se eliminarán, los mensajes de spam se moverán a la carpeta de correo no deseado del usuario, se marcará el asunto de los correos electrónicos de phishing, que se pondrán en cuarentena, y el contenido de los archivos de malware ubicados en OneDrive se sustituirá por texto sin formato para evitar que cause daños.

1. Haga clic en **Políticas** > **Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Usuarios** como destino y haga clic en **Siguiente**.
3. Expanda **Antimalware de Exchange Online** y utilice el menú desplegable situado junto a **Cuando se informa de elementos** para seleccionar **Eliminar archivo adjunto**.
4. Expanda **Antispam de Exchange Online** y utilice el menú desplegable situado junto a **Cuando se informa de elementos** para seleccionar **Mover a correo no deseado**.
5. Expanda **Antiphishing de Exchange Online** y haga clic en el interruptor para activar **Etiquetar asunto**. También puede cambiar **Etiquetar texto del asunto** para personalizarlo.
6. Expanda **Antimalware de OneDrive Online**, utilice el menú desplegable situado junto a **Cuando se informa de elementos** para seleccionar **Sustituir** y haga clic en **Siguiente**.
7. Haga clic en **Asignar**, marque las casillas de verificación situadas junto a los usuarios a los que desee aplicar la política y haga clic en **Aceptar**. Si un usuario tiene una política personalizada existente aplicada, se sobrescribirá con la nueva.
8. Haga clic en **Guardar cambios** para finalizar el proceso.

Configuración de la protección de Exchange Online

En esta sección se proporciona información sobre cómo cambiar la configuración general, antimalware, antispam o antiphishing de Exchange Online, así como las diferentes opciones.

Configuración general de Exchange Online

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre ESET LiveGrid® en el glosario .
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de conservación para los resultados del análisis de desinfección es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de Exchange Online

Activar Antimalware de Exchange Online
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el correo electrónico se envía al destinatario
- **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
- **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
- **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
- **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.
- **Eliminar archivo adjunto**: el archivo adjunto del mensaje se elimina, y el mensaje se entrega al destinatario sin el archivo adjunto.
- **Sustituir archivo adjunto**: sustituye el archivo adjunto por un archivo de texto con información detallada sobre la acción que se ha realizado.
- **Archivos adjuntos en la cuarentena**: el archivo adjunto se elimina del correo electrónico y se coloca en la cuarentena de archivos.

Texto de reemplazo de archivo adjunto
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Notificar al propietario del buzón
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Idioma
Elija el idioma que desee en el menú desplegable. El propietario del buzón recibirá correos electrónicos de notificación en el idioma seleccionado cuando se libere un objeto de la cuarentena de Exchange Online. Esta opción anula el idioma predeterminado del inquilino en configuración.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Antispam de Exchange Online

Activar Antispam de Exchange Online
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el correo electrónico se envía al destinatario
- **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
- **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
- **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
- **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.

Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Puede configurar las listas de **Aprobado**, **Bloqueado** e **Ignorado** especificando criterios como direcciones IP o intervalos de direcciones IP, nombres de dominio, etc. Si desea añadir, modificar o eliminar criterios, haga clic en **Editar** en la lista que quiera gestionar. Si quiere importar la lista personalizada de un archivo en lugar de agregar las entradas manualmente, haga clic en **Importar** y busque el archivo (*.txt*) que contiene las entradas que quiere agregar a la lista. Del mismo modo, si quiere exportar la lista existente a un archivo (*.txt*), seleccione **Exportar** en el menú contextual.

Lista de IP autorizadas	Añade automáticamente a la lista blanca los correos electrónicos que tienen su origen en las direcciones IP especificadas. El contenido del correo electrónico no se comprobará.
Lista de IP bloqueadas	Bloquea automáticamente los correos electrónicos que tienen su origen en las direcciones IP especificadas.
Lista de IP ignoradas	Lista de direcciones IP que se ignorarán durante la clasificación. Se comprobará el contenido del correo electrónico.
Lista de remitentes autorizados	Agregar a la lista blanca los correos electrónicos procedentes de un remitente o dominio concretos. Para la verificación solo se utiliza una dirección de remitente o un dominio completo. Se sigue el orden de prioridad siguiente: 1.Dirección "MAIL FROM" SMTP 2.Campo del encabezado de correo electrónico "Return-Path:" 3.Campo del encabezado de correo electrónico "X-Env-Sender:" 4.Campo del encabezado de correo electrónico "From:" 5.Campo del encabezado de correo electrónico "Sender:" 6.Campo del encabezado de correo electrónico "X-Apparently-From:"
Lista de remitentes bloqueados	Bloquea los correos electrónicos procedentes de un remitente o dominio concretos. Para la verificación se utilizan todas las direcciones de remitentes identificadas o todos los dominios: Dirección "MAIL FROM" SMTP Campo del encabezado de correo electrónico "Return-Path:" Campo del encabezado de correo electrónico "X-Env-Sender:" Campo del encabezado de correo electrónico "From:" Campo del encabezado de correo electrónico "Sender:" Campo del encabezado de correo electrónico "X-Apparently-From:"

Antiphishing de Exchange Online

Activar Antiphishing de Exchange Online
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Cuando se informa de elementos
• **Sin accion**: no se realiza ninguna acción y se envía al destinatario un correo electrónico con un archivo adjunto malicioso.
• **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
• **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
• **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
• **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.
Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Notificar al propietario del buzón
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección para cualquier usuario de Exchange Online.

Ajustes de protección de Gmail

En esta sección se proporciona información sobre cómo cambiar la configuración general, antimalware, antispam o antiphishing de Gmail, así como las diferentes opciones.

Generalidades de Gmail

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre ESET LiveGrid® en el glosario .
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de conservación para los resultados del análisis de desinfección es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de Gmail

Activar antimalware de Gmail
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el correo electrónico se envía al destinatario
- **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
- **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
- **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
- **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.
- **Eliminar archivo adjunto**: el archivo adjunto del mensaje se elimina, y el mensaje se entrega al destinatario sin el archivo adjunto.
- **Sustituir archivo adjunto**: sustituye el archivo adjunto por un archivo de texto con información detallada sobre la acción que se ha realizado.
- **Archivos adjuntos en la cuarentena**: el archivo adjunto se elimina del correo electrónico y se coloca en la cuarentena de archivos.

Texto de reemplazo de archivo adjunto
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Notificar al propietario del buzón
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Idioma
Elija el idioma que desee en el menú desplegable. El propietario del buzón recibirá correos electrónicos de notificación en el idioma seleccionado cuando se libere un objeto de la cuarentena. Esta opción anula el idioma predeterminado del inquilino en configuración.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Antispam de Gmail

Activar antispam de Gmail
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el correo electrónico se envía al destinatario
- **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
- **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
- **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
- **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.

Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Puede configurar las listas de **Aprobado**, **Bloqueado** e **Ignorado** especificando criterios como direcciones IP o intervalos de direcciones IP, nombres de dominio, etc. Si desea añadir, modificar o eliminar criterios, haga clic en **Editar** junto a la lista que quiera gestionar. Si quiere importar la lista personalizada de un archivo en lugar de agregar las entradas manualmente, haga clic en **Importar** y busque el archivo (*.txt*) que contiene las entradas que quiere agregar a la lista. Del mismo modo, si quiere exportar la lista existente a un archivo (*.txt*), seleccione **Exportar** en el menú contextual.

Lista de IP autorizadas	Añade automáticamente a la lista blanca los correos electrónicos que tienen su origen en las direcciones IP especificadas. El contenido del correo electrónico no se comprobará.
Lista de IP bloqueadas	Bloquea automáticamente los correos electrónicos que tienen su origen en las direcciones IP especificadas.
Lista de IP ignoradas	Lista de direcciones IP que se ignorarán durante la clasificación. Se comprobará el contenido del correo electrónico.
Lista de remitentes autorizados	Agregar a la lista blanca los correos electrónicos procedentes de un remitente o dominio concretos. Para la verificación solo se utiliza una dirección de remitente o un dominio completo. Se sigue el orden de prioridad siguiente: 1.Dirección "MAIL FROM" SMTP 2.Campo del encabezado de correo electrónico "Return-Path:" 3.Campo del encabezado de correo electrónico "X-Env-Sender:" 4.Campo del encabezado de correo electrónico "From:" 5.Campo del encabezado de correo electrónico "Sender:" 6.Campo del encabezado de correo electrónico "X-Apparently-From:"
Lista de remitentes bloqueados	Bloquea los correos electrónicos procedentes de un remitente o dominio concretos. Para la verificación se utilizan todas las direcciones de remitentes identificadas o todos los dominios: Dirección "MAIL FROM" SMTP Campo del encabezado de correo electrónico "Return-Path:" Campo del encabezado de correo electrónico "X-Env-Sender:" Campo del encabezado de correo electrónico "From:" Campo del encabezado de correo electrónico "Sender:" Campo del encabezado de correo electrónico "X-Apparently-From:"

Antiphishing de Gmail

Activar Gmail Anti-Phishing
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Cuando se informa de elementos
• **Sin accion**: no se realiza ninguna acción y se envía al destinatario un correo electrónico con un archivo adjunto malicioso.
• **Mover a correo no deseado**: el correo electrónico se mueve a la carpeta de correo no deseado.
• **Mover a la papelera**: el correo electrónico se mueve a la carpeta Papelera.
• **Eliminar mensaje**: se elimina el mensaje de correo electrónico.
• **Mensaje en cuarentena**: se elimina el correo electrónico original y se almacena una copia del correo electrónico en la cuarentena. Si decide liberar el correo electrónico de la cuarentena, se enviará como archivo adjunto en un correo electrónico nuevo y se entregará al destinatario.
Etiquetar asunto
Cuando esta opción está activada, puede modificar las plantillas agregadas al asunto de mensajes infectados.
Etiquetar texto del asunto
Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.
Notificar al propietario del buzón
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Configuración de la protección de OneDrive

En esta sección se proporciona información sobre cómo cambiar la configuración general de OneDrive o la configuración antimalware de OneDrive, así como las diferentes opciones.

Configuración general de OneDrive

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre estas aplicaciones en el glosario.
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de conservación para los resultados del análisis de desinfección es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de OneDrive

Antimalware de OneDrive
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el archivo permanece en OneDrive
- **Mover a la papelera**: el archivo se mueve a la papelera de reciclaje.
- **Sustituir**: el contenido del archivo original se sustituye por el texto definido a continuación en la ventana "Texto de reemplazo del archivo"
- **Cuarentena:** el archivo original se mueve a la papelera de reciclaje y se copia en la cuarentena. Cuando se libera el archivo, el archivo eliminado anteriormente se mantiene en la papelera y se carga una nueva copia en la carpeta de OneDrive original.

Texto de reemplazo del archivo
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Notificar al propietario
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Configuración de la protección de Google Drive

Esta sección contiene información sobre cómo cambiar la configuración general de Google Drive o la configuración antimalware de Google Drive, así como las diferentes opciones.

General de Google Drive

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre estas aplicaciones en el glosario.
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de conservación para los resultados del análisis de desinfección es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de Google Drive

Antimalware de Google Drive
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción y el archivo permanece en Google Drive
- **Mover a la papelera**: el archivo se mueve a la papelera de reciclaje.
- **Sustituir**: el contenido del archivo original se sustituye por el texto definido a continuación en la ventana "Texto de reemplazo del archivo".
- **Cuarentena:** el archivo original se mueve a la papelera de reciclaje y se copia en la cuarentena.
- **Eliminar**: el archivo original se elimina permanentemente de Google Drive.

Texto de reemplazo del archivo
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Notificar al propietario
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Configuración de la protección de Grupos del equipo

En esta sección se proporciona información sobre cómo cambiar la configuración general de Grupos del equipo o la configuración antimalware de Grupos del equipo, así como las diferentes opciones.

Configuración general de grupos del equipo

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de retención de los resultados de análisis de Desinfectado es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de grupos del equipo

Antimalware de grupos del equipo
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción, el archivo permanece intacto.
- **Mover a la papelera**: el archivo se mueve a la papelera de reciclaje del equipo.
- **Sustituir**: el contenido del archivo original se sustituye por el texto definido a continuación en la ventana "Texto de reemplazo del archivo"
- **Cuarentena**: el archivo original se mueve a la papelera de reciclaje del equipo. y se copia en cuarentena.

Cuando se libera el archivo, el archivo eliminado anteriormente se mantiene en la papelera de reciclaje y se carga una nueva copia en la ubicación original.
Texto de reemplazo del archivo
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Notificar al propietario
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Configuración de la protección de sitios de SharePoint

En esta sección se proporciona información sobre cómo cambiar la configuración general de Sitios de SharePoint o la configuración antimalware de Sitios de SharePoint, así como las diferentes opciones.

Configuración general de sitios de Sharepoint

ESET LiveGrid®Comentarios sobre
Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
Registrar todos los objetos
Si se selecciona esta opción, se mostrarán en los Registros del análisis todos los resultados de análisis (incluidos los elementos desinfectados). La política de retención de los resultados de análisis de Desinfectado es de tres días. Los resultados de análisis con una antigüedad superior a los tres días se eliminarán de forma permanente.

Antimalware de sitios de Sharepoint

Antimalware de sitios de Sharepoint
Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.
Protección de informes y aprendizaje automático
El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) para las categorías de informe.
Cuando se informa de elementos
- **Sin acción**: no se realiza ninguna acción, el archivo permanece intacto.
- **Mover a la papelera**: el archivo se mueve a la papelera de reciclaje de SharePoint.
- **Sustituir**: el contenido del archivo original se sustituye por el texto definido a continuación en la ventana "Texto de reemplazo del archivo"
- **Cuarentena**: el archivo original se mueve a la papelera de reciclaje de SharePoint y se copia en cuarentena. Cuando se libera el archivo, el archivo eliminado anteriormente se mantiene en la papelera de reciclaje y se carga una nueva copia en la ubicación original.

Texto de reemplazo del archivo
Sustituye los archivos adjuntos por un archivo de texto que contiene información detallada sobre una acción realizada.
Notificar al propietario
Cuando esta opción está activada, el usuario recibe un mensaje de correo electrónico de notificación cuando se produce una detección.
Notificar al administrador
Especifique la dirección de correo electrónico (pulse Entrar para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se produzca una detección.

Ajustes de protección de ESET LiveGuard Advanced

Para utilizar la característica ESET LiveGuard Advanced, configure una política que permita el análisis de ESET LiveGuard Advanced. Los usuarios o grupos a los que se haya asignado esta política tendrán protección adicional. Los archivos enviados a ESET LiveGuard Advanced para su análisis se muestran en la pestaña Archivos enviados; esto se aplica a las muestras sospechosas desconocidas (nunca vistas). Los archivos maliciosos conocidos (basados en hash) no se envían para el análisis por parte de ESET LiveGuard Advanced.

Verá los resultados de ESET LiveGuard Advanced en los Registros del análisis (Exchange Online, OneDrive, Grupos del equipo o Sitios de SharePoint) marcados como malware.

ESET LiveGuard Advanced

Cuando se selecciona esta función, se activa y podrá configurar opciones detalladas.

> ESET LiveGuard Advanced activará automáticamente la respuesta de ESET LiveGrid®. Los datos se enviarán al ESET Research Lab para su posterior análisis. Puede obtener más información sobre ESET LiveGrid® en el glosario .

Umbral de detección

Los resultados con el nivel umbral seleccionado y superiores se considerarán amenazas.

Envío automático de muestras sospechosas (menú desplegable)

Este ajuste está relacionado con ESET LiveGrid® y permite las siguientes acciones: Todos, Todo excepto documentos, Ninguno.

Envío automático de muestras sospechosas (controles deslizantes)

Elija qué tipos de archivo se envían a ESET LiveGuard Advanced si contienen código sospechoso de ser una amenaza, o presentan un comportamiento o características inusuales:

- **Ejecutables** – .exe, .dll, .sys
- **Archivos comprimidos** – .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Scripts** – .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Otros** – .jar, .reg, .msi, .swf, .lnk

Eliminar muestras sospechosas de los servidores de ESET

Elija cuándo desea eliminar las muestras enviadas a analizar. Eliminar muestras de la nube de ESET LiveGuard Advanced: Nunca, Después de 30 días, Inmediatamente después del análisis.

Documentos

Utilice el control deslizante para permitir el envío de documentos de Microsoft Office, PDF y otros tipos de documentos a ESET LiveGuard Advanced para su análisis.

Eliminar documentos de los servidores de ESET

Eliminar muestras en formato de archivo de documento de la nube de ESET LiveGuard Advanced: Nunca, Después de 30 días, Inmediatamente después del análisis.

Protección de informes y aprendizaje automático

El motor de detección protege contra ataques maliciosos al sistema mediante el análisis de los archivos, los correos electrónicos y la comunicación de red. Si se detecta un objeto clasificado como malware, se iniciará la corrección. El motor de detección puede eliminarlo bloqueándolo primero y, a continuación, emprendiendo acciones como la desinfección, la eliminación o la puesta en cuarentena.

Protección en tiempo real y de aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como capa de protección avanzada, que mejora la detección. Puede obtener más información sobre este tipo de protección en el glosario. Puede configurar niveles de información para las siguientes categorías:

Malware

Un virus informático es un fragmento de código malicioso que antecede o sigue a los archivos existentes en el ordenador. Sin embargo, el término "virus" suele utilizarse de forma inadecuada. "Malware" (software malicioso) es un término más exacto. La detección de malware la realiza el módulo del motor de detección en combinación con el componente de aprendizaje automático. Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente indeseables (PUA)

Una aplicación potencialmente indeseable es un software con una intención que no es inequívocamente malintencionada. Pero que puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades no aprobadas o esperadas por el usuario, o que tiene otros objetivos que

no son claros.
En esta categoría se incluyen el software de visualización de publicidad, los contenedores de descarga, diversas herramientas barras de herramientas para el navegador, software con comportamiento engañoso, software agrupado, software de seguimiento.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente sospechosas

Es un software comprimido con empaquetadores o protectores que normalmente se utilizan para impedir la ingeniería inversa u ocultar el contenido del archivo ejecutable (por ejemplo para ocultar la presencia de malware) con métodos privados de compresión o cifrado.
En esta categoría se incluyen todas las aplicaciones desconocidas comprimidas con un empaquetador o protector que se suelen usar para comprimir malware.

Aplicaciones potencialmente peligrosas

Esta clasificación se ofrece para programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Por aplicaciones potencialmente peligrosas se entienden programas de software comercial legítimo que tienen el potencial de usarse con fines maliciosos.
En esta categoría se incluyen herramientas de descifrado, generadores de claves de licencia, herramientas de ataques informáticos, herramientas de control o acceso remoto aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran todas las teclas que pulsa un usuario). Esta opción está desactivada de forma predeterminada.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

Informe

Los informes los realizan el motor de detección y el componente de aprendizaje automático. Puede establecer el umbral de elaboración de informes como mejor se adapte a su entorno y a sus necesidades. No hay una sola configuración correcta. Por ello, le recomendamos que supervise el comportamiento de su entorno y decida si es más adecuado un ajuste de Informe distinto.

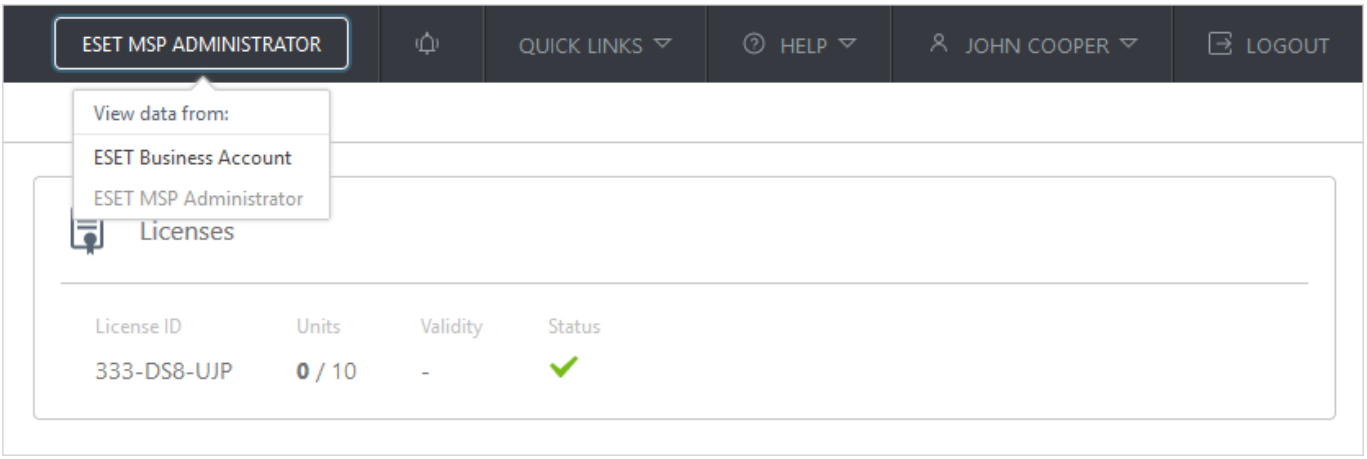
Los informes no llevan a cabo acciones con los objetos. Transfieren información a la capa de protección correspondiente y la capa de protección lleva a cabo la acción adecuada.

Agresivo	**Informe configurado con la máxima sensibilidad. Se informa de más detecciones. Aunque el ajuste Agresivo puede parecer el más seguro, suele ser demasiado sensible, lo que puede ser contraproducente.** El ajuste Agresivo puede identificar erróneamente objetos como maliciosos, y se realizará una acción con dichos objetos (en función de la configuración de la protección).
Equilibrado	Este ajuste tiene un equilibrio óptimo entre rendimiento, precisión de la detección y número de falsos positivos.
Precavido	Informe configurado para reducir al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la probabilidad es evidente y coincide con el comportamiento del malware.
Desactivado	El informe no está activo. Las detecciones no se producen, no se informa de ellas o no se desinfectan. Los informes de malware no se pueden desactivar; por lo tanto, el ajuste Desactivado no está disponible para el malware.

Administración de licencias

La ventana principal muestra una visión general de las licencias recuperadas de ESET Business Account o ESET MSP Administrator. Puede ver todos los grupos de licencias, sitios o empresas disponibles en el portal de ESET Business Account o ESET MSP Administrator. La administración de licencias le permite proteger o desproteger a los usuarios.

Si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede alternar entre la vista de ESET Business Account y la de ESET MSP Administrator (cuenta de licencias híbridas).



La licencia de ESET Cloud Office Security le permite utilizar la función ESET LiveGuard Advanced sin coste adicional. Verá la etiqueta de ELG junto al ID de licencia.

Administración de licencias con ESET Business Account

Muestra información sobre la licencia y el uso (nombre del grupo de licencias, ID de licencia, unidades, validez y estado). Las licencias y los grupos de licencias se cargan desde ESET Business Account. Los grupos de licencias solo están disponibles si tiene sitios en ESET Business Account (los sitios son útiles para la categorización). Una unidad representa la protección que realiza ESET Cloud Office Security de un solo usuario para Exchange Online y OneDrive.

> Cada usuario protegido consume una unidad de licencia. Esto es así con independencia de los servicios de Microsoft 365 que se utilicen. Un usuario con Exchange Online o OneDrive (o ambos) siempre consume una unidad de licencia.
> Los grupos de Teams y los sitios de SharePoint no consumen unidades de licencia.

Todos los usuarios nuevos aparecerán en la sección Usuarios como Sin protección. Si utiliza la protección automática por inquilino o grupo, los nuevos usuarios se protegen automáticamente y aparecerán como Protegido.
Cuando protege a los usuarios, tiene dos opciones:

- **Protección automática por inquilino o grupo (recomendada)**: no hay mantenimiento; cualquier usuario recién agregado que esté en un grupo de Azure AD o pertenezca a un inquilino se protege automáticamente. Consulte la siguiente nota si desea obtener más información.
- **Protección de usuarios individuales**: requiere administración; debe proteger manualmente a cada nuevo usuario.

Proteger a los usuarios (sin grupo de licencias)

1. Haga clic en **Proteger**.
2. Seleccione el inquilino o el grupo para la protección automática del usuario y haga clic en **Proteger**. Para la protección individual del usuario, seleccione los usuarios que quiera proteger y haga clic en **Proteger**. La política predeterminada protege ahora a los usuarios.
3. Si es necesario, especifique una política personalizada para los usuarios en la sección Políticas.

Proteger a los usuarios (con el grupo de licencias)

1. Seleccione el grupo de licencias y haga clic en el icono de tres puntos > **Mostrar detalles** junto al grupo de licencias.
2. Haga clic en **Proteger**.
3. Seleccione el inquilino o el grupo para la protección automática del usuario y haga clic en **Proteger**. Para la protección individual del usuario, seleccione los usuarios que quiera proteger y haga clic en **Proteger**. La política predeterminada protege ahora a los usuarios.
4. Si es necesario, especifique una política personalizada para los usuarios en la sección Políticas.

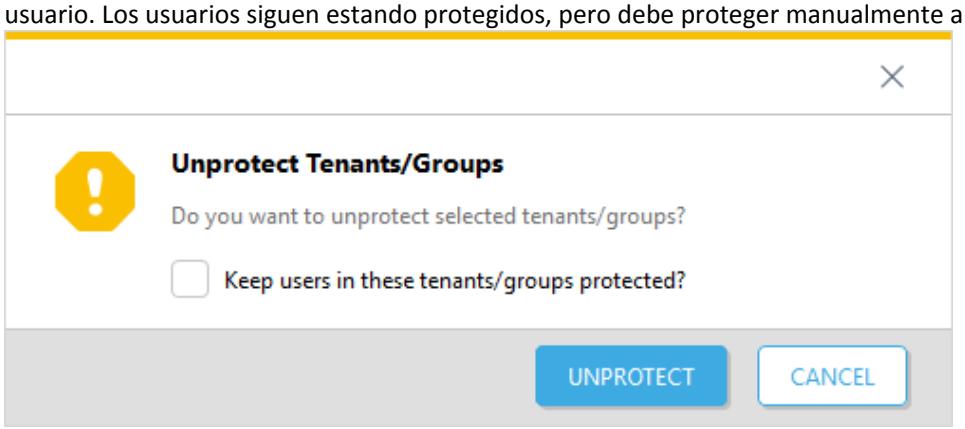
> Asegúrese de tener suficientes unidades de licencia, especialmente si la protección automática está activada y se aumenta el número de usuarios. Una vez se consuman todas las unidades de licencia, los nuevos usuarios que se hagan miembros de un inquilino o grupo no estarán protegidos. La protección de los usuarios existentes no se ve afectada.
> Si carece temporalmente de suficientes unidades de licencia y desea especificar los usuarios que va a proteger, utilice grupos no protegidos (no utilice la protección automática) y proteja manualmente a los usuarios. Cuando amplíe los grupos de licencias con más unidades, podrá volver a activar la protección automática para facilitar la administración.

Mover

Para mover los usuarios entre grupos de licencias y para realizar operaciones más avanzadas con licencias, haga clic en Abrir ESET Business Account .

Quitar protección

1. Seleccione usuarios individuales, un inquilino o un grupo y haga clic en **Desproteger**.
2. Al quitar la protección automática de inquilino o grupo, se le preguntará **¿Desea mantener protegidos a los usuarios de estos inquilinos o grupos?** Si opta por no utilizar esta opción, los usuarios se desprotegerán. Si selecciona la casilla de verificación, la protección automática de inquilinos o grupos se desactivará y cambiará a la protección individual del usuario. Los usuarios siguen estando protegidos, pero debe proteger manualmente a los usuarios recién agregados.



Muestra información y uso de la licencia (empresa del cliente, ID de la licencia, unidades y estado).

> Cada usuario protegido consume una unidad de licencia. Esto es así con independencia de los servicios de Microsoft 365 que se utilicen. Un usuario con Exchange Online o OneDrive (o ambos) siempre consume una unidad de licencia.
> Los grupos de Teams y los sitios de SharePoint no consumen unidades de licencia.

Todos los usuarios nuevos aparecerán en la sección Usuarios como **Sin protección**. Si utiliza la protección automática por inquilino o grupo, los nuevos usuarios se protegen automáticamente y aparecerán como **Protegido**.

Cuando protege a los usuarios, tiene dos opciones:

- **Protección automática por inquilino o grupo (recomendada)**: no hay mantenimiento, cualquier usuario recién agregado que sea miembro del grupo de Azure AD o pertenezca a un inquilino se protege automáticamente. Consulte la siguiente nota si desea obtener más información.
- **Protección de usuarios individuales**: requiere administración; debe proteger manualmente a cada nuevo usuario.

Proteger a los usuarios

1. Haga clic en **Proteger**.
2. Seleccione el inquilino o el grupo para la protección automática del usuario y haga clic en **Proteger**. Para la protección individual del usuario, seleccione los usuarios que quiera proteger y haga clic en **Proteger**. La política predeterminada protege ahora a los usuarios.
3. Si es necesario, especifique una política personalizada para los usuarios en la sección Políticas.

> Asegúrese de tener suficientes unidades de licencia, especialmente si la protección automática está activada y se aumenta el número de usuarios. Una vez se consuman todas las unidades de licencia, los nuevos usuarios que se hagan miembros de un inquilino o grupo no estarán protegidos. La protección de los usuarios existentes no se ve afectada.
> Si carece temporalmente de suficientes unidades de licencia y desea especificar los usuarios que va a proteger, utilice grupos no protegidos (no utilice la protección automática) y proteja manualmente a los usuarios. Cuando amplíe los grupos de licencias con más unidades, podrá volver a activar la protección automática para facilitar la administración.

Quitar protección

1. Seleccione usuarios individuales, un inquilino o un grupo y haga clic en **Desproteger**.
2. Al quitar la protección automática de inquilino o grupo, se le preguntará **¿Desea mantener protegidos a los usuarios de estos inquilinos o grupos?** Si opta por no utilizar esta opción, los usuarios se desprotegerán. Si selecciona la casilla de verificación, la protección automática de inquilinos o grupos se desactivará y cambiará a la protección individual del usuario. Los usuarios siguen estando protegidos, pero debe proteger manualmente a los usuarios recién agregados.

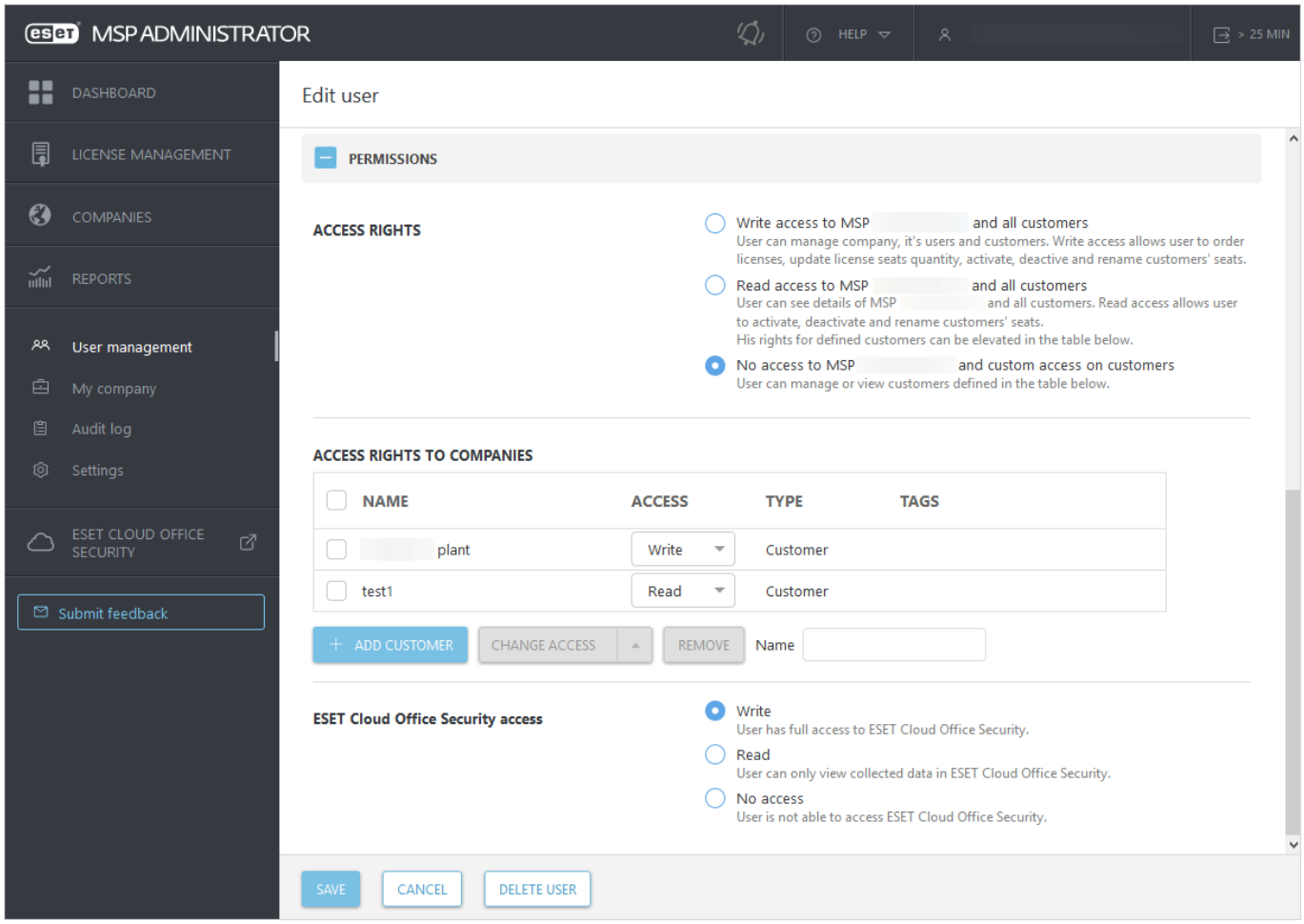
Acceso de usuario de ESET Cloud Office Security a una empresa concreta

En un entorno con varios inquilinos, puede proporcionar a un usuario acceso a ESET Cloud Office Security para permitir que el usuario solo vea una empresa específica (con permiso de lectura o escritura). Esto suelen utilizarlo los MSP.

Configure los derechos de acceso del usuario en ESET MSP Administrator mediante la asignación a una empresa de permiso de **Escritura** y acceso de **Lectura** a ESET Cloud Office Security:

1. Inicie sesión en ESET MSP Administrator como administrador.
2. Edite un usuario, configure los **Derechos de acceso a empresas** desde Permisos y seleccione acceso de **Escritura**. El usuario solo puede ver la empresa asignada con su grupo de licencias.

3. Seleccione acceso de **Escritura** a ESET Cloud Office Security para que el usuario pueda proteger una empresa agregando un inquilino. Un usuario con acceso de Lectura no puede agregar ni quitar un inquilino.



Solo se puede configurar un tipo de acceso a ESET Cloud Office Security como ajuste global, y se aplica a todas las empresas (si a un usuario se le asignan varias empresas).

Registro de auditoría

Realiza un seguimiento de los cambios en la configuración o protección de ESET Cloud Office Security. Las entradas del registro de auditoría muestran las actividades y la secuencia en la que se realizaron. Los registros de auditoría almacenan información sobre la operación o el evento específicos. Los registros de auditoría se generan siempre que se crea o modifica un objeto ESET Cloud Office Security (grupo de licencias, usuario, política, informe o elemento de cuarentena como datos adjuntos).

Cuando hace clic en el icono del engranaje situado en la esquina superior derecha para acceder a **Exportar a CSV** desde el menú contextual, puede exportar la tabla con cuadrícula a formato *CSV* y utilizarla en otras aplicaciones para trabajar con la lista.

Haga clic en el icono para abrir una barra lateral con un resumen de una entrada de Registro de auditoría concreta. Para obtener información más detallada, haga clic en el icono y seleccione **Mostrar detalles**.

Mosaico	Detalle
Información básica	Muestra los datos generales del registro de auditoría (sucesos, acción, gravedad, resultado y sección).

Mosaico	Detalle
Usuario	Muestra información sobre el usuario que realizó una acción o un cambio, lo que incluye el correo electrónico y la dirección IP del usuario.
Cambios	Detalles sobre los cambios realizados.
Configuración antigua	Muestra la configuración de política anterior.
Nueva configuración	Muestra la configuración de la política actual.
Objetos	Muestra los objetos afectados por el cambio o la acción (usuario, política, datos adjuntos, etc.).

Puede filtrar los usuarios en función de varios criterios. Haga clic en **Agregar filtro** y seleccione un tipo de filtro en el menú desplegable o escriba una cadena (repetir al combinar varios criterios):

Agregar filtro	Uso
Acción	Seleccione una de las acciones disponibles.
Objeto	Escriba un nombre de objeto válido.
Estado	Seleccione una de las siguientes opciones: Correcto, Error, Iniciado o Parcialmente correcto
Usuario	Escriba el usuario que realizó los cambios.
Nivel de registro	Seleccione el nivel de gravedad: Baja, Media o Alta
Ocurrió desde/Ocurrió hasta	Filtrado por hora del suceso. Utilice Ocurrió desde y haga clic en la fecha para mostrar solo las entradas posteriores a la fecha especificada. Utilice Ocurrió hasta para mostrar las entradas anteriores. o bien utilice ambos para definir el intervalo de tiempo deseado.
Sistema iniciado	Filtra los registros realizados por el sistema.

Enviar opinión

Para enviar sus comentarios, en la consola ESET Cloud Office Security, use la barra de herramientas de la esquina superior derecha, coloque el cursor del ratón sobre **Ayuda** y haga clic en **Enviar comentarios**. A continuación, elija **Háganos saber lo que piensa** (para compartir ideas y experiencias) o **Informar de un problema o error**.

Soporte técnico

Utilice los siguientes vínculos con información de soporte que le ayudará a solucionar los problemas que se encuentre:

Buscar en la base de conocimientos de ESET

Base de conocimiento de ESET Contiene respuestas a las preguntas más frecuentes y posibles soluciones a diferentes problemas. La actualización periódica por parte de los especialistas técnicos de ESET convierte esta base de conocimiento en la herramienta más potente para resolver diversos problemas.

Visite el foro de seguridad de ESET

Foro de soporte técnico El foro de ESET proporciona a los usuarios de ESET una manera fácil de obtener ayuda y ayudar a otros. Puede publicar cualquier problema o pregunta relacionada con sus productos ESET.

Ponerse en contacto con el servicio de soporte técnico

Formulario de soporte técnico de ESET Rellene el formulario para proporcionar sus datos, incluida la descripción del problema.

Póngase en contacto con su socio local de ESET para obtener asistencia técnica.

Comuníquese con su soporte local de ESET Localice la información de contacto de soporte para el soporte de ESET en su región en su correo electrónico de licencia de ESET.

Enviar opinión

Enviar opinión Envíenos su opinión (compartir ideas y experiencias) o informe de un problema o fallo.

Sugerir mejoras en la Ayuda en línea

Puede publicar su calificación y proporcionar comentarios sobre un tema específico en Ayuda en línea al hacer clic en el vínculo **¿Le ha resultado útil esta información?** debajo de la página de ayuda. Háganos saber si el contenido ayudó o cómo cree que el redactor técnico puede mejorarlo.

Disponibilidad de los servicios

El Portal de estado de ESET muestra el estado actual de los servicios en la nube de ESET, las interrupciones programadas y los incidentes pasados. Si tiene un problema con un servicio de ESET compatible y no lo ve incluido en el Portal de estado, póngase en contacto con el Soporte técnico de ESET.

Los equipos de supervisión verifican los posibles problemas internamente, y los incidentes confirmados se publican y actualizan manualmente para mantener la credibilidad y la precisión. Por lo tanto, aparecen en el Portal de estado con un ligero retraso. Es posible que no publiquemos incidentes breves si se resuelven antes de ser confirmados manualmente.

Security for ESET Cloud Office Security

Introducción

La finalidad de este documento es resumir los controles y prácticas de seguridad que se aplican en ESET Cloud Office Security. Los controles y prácticas de seguridad están diseñados para proteger la confidencialidad, integridad y disponibilidad de la información del cliente. Tenga en cuenta que los controles y prácticas de seguridad pueden cambiar.

Alcance

En este documento se resumen los controles y prácticas de seguridad para la infraestructura, organización, personal y procesos operativos de ESET Dynamic Threat Defense, ESET Business Account (en adelante, "EBA"), ESET Data Framework, ESET LiveGrid, las actualizaciones, la protección antispam, y la infraestructura de ESET Cloud Office Security. Entre los controles y prácticas de seguridad se incluyen los siguientes:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información

3. Seguridad de recursos humanos
4. Administración de activos
5. Control de acceso
6. Cifrado
7. Seguridad física y ambiental
8. Seguridad de las operaciones
9. Seguridad de la comunicación
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relación con proveedores
12. Gestión de incidentes de seguridad de la información
13. Aspectos de seguridad de la información de la gestión de la continuidad de la actividad
14. Cumplimiento

Concepto de seguridad

La empresa ESET s.r.o. cuenta con la certificación ISO 27001:2013, con un alcance del sistema de administración integrado que abarca explícitamente los servicios de ESET Cloud Office Security y EBA, entre otros.

Por lo tanto, el concepto de seguridad de la información utiliza el marco de ISO 27001 para implementar una estrategia de seguridad por capas al aplicar controles de seguridad en las capas de red, sistemas operativos, bases de datos, aplicaciones, personal y procesos operativos. El objetivo de los controles y las prácticas de seguridad aplicables es superponerse y complementarse entre sí.

Controles y prácticas de seguridad

1. Políticas de seguridad de la información

ESET utiliza políticas de seguridad de la información para cumplir todos los aspectos de la norma ISO 27001, incluidos los controles y prácticas de seguridad, así como la gobernanza de la seguridad de la información. Las políticas se revisan anualmente y se actualizan tras cambios importantes para garantizar su conveniencia, adecuación y eficacia continuas.

ESET efectúa revisiones anuales de esta política y comprobaciones de seguridad interna para garantizar la coherencia con esta. El incumplimiento de las políticas de seguridad de la información puede acarrear medidas disciplinarias para los empleados de ESET y sanciones contractuales, incluida la rescisión del contrato, en el caso de los proveedores.

2. Organización de la seguridad de la información

La organización de la seguridad de la información de ESET Cloud Office Security se compone de varios equipos y personas implicados en la seguridad de la información y la TI, entre otros los siguientes:

- Administración ejecutiva de ESET
- Equipos de seguridad interna de ESET
- Equipos de TI de aplicaciones empresariales
- Otros equipos de apoyo

Las responsabilidades de seguridad de la información se asignan de acuerdo con las políticas de seguridad de la información establecidas. Los procesos internos se identifican y evalúan para determinar si hay riesgo de uso indebido o modificación no autorizada o involuntaria de los activos de ESET. Las actividades riesgosas o delicadas de los procesos internos adoptan el principio de segregación de controles para mitigar el riesgo.

El equipo jurídico de ESET es responsable de la comunicación con las autoridades gubernamentales, incluidas las entidades reguladoras eslovacas dedicadas a la seguridad informática y la protección de datos personales. El equipo de seguridad interna de ESET es responsable de la comunicación con grupos de interés especiales, como ISACA. El equipo del laboratorio de investigación de ESET es responsable de la comunicación con otras empresas de seguridad y la comunidad de seguridad informática en general.

La seguridad de la información se integra en la gestión de proyectos mediante el marco de gestión de proyectos aplicado desde la concepción hasta la finalización del proyecto.

El teletrabajo se asegura mediante una política implementada en los dispositivos móviles que incluye protección de datos mediante cifrado seguro al atravesar redes que no son de confianza. Los controles de seguridad de los dispositivos móviles están diseñados para funcionar independientemente de los sistemas internos y las redes internas de ESET.

3. Seguridad de recursos humanos

ESET utiliza prácticas estándar de recursos humanas, como políticas diseñadas para proteger la seguridad de la información. Estas prácticas abarcan todo el ciclo de vida de los empleados y se aplican a todos los equipos que acceden al entorno de ESET Cloud Office Security.

4. Administración de activos

La infraestructura de ESET Cloud Office Security está incluida en los inventarios de activos de ESET con estrictos controles de propiedad y reglas que se aplican según el tipo y la sensibilidad del activo. ESET tiene un esquema de clasificación interno definido. Todos los datos y configuraciones de ESET Cloud Office Security se clasifican como confidenciales.

5. Control de acceso

El acceso a ESET Cloud Office Security se rige por la política de control de acceso de ESET. El control de acceso se establece en la infraestructura, los servicios de red, el sistema operativo, la base de datos y el nivel de la aplicación. La administración del acceso total de los usuarios a nivel de la aplicación es autónoma. El inicio de sesión único de ESET Cloud Office Security y ESET Business Account se rige por un proveedor de identidad central, que garantiza que un usuario solo pueda acceder al inquilino autorizado. La aplicación utiliza permisos de ESET Cloud Office Security estándar para aplicar control de acceso basado en roles para el inquilino.

El acceso al backend de ESET está estrictamente limitado a las personas y roles autorizados. Los procesos estándar de ESET para el (des)registro, (des)aprovisionamiento, administración de privilegios y revisión de derechos de acceso de los usuarios se utilizan para administrar el acceso de los empleados de ESET a la infraestructura y las redes de ESET Cloud Office Security.

Existe una autenticación segura para proteger el acceso a todos los datos de ESET Cloud Office Security.

6. Cifrado

Con el fin de proteger los datos de ESET Cloud Office Security, se utiliza un cifrado seguro para cifrar los datos en reposo y en tránsito. Por lo general, la autoridad certificadora de confianza se utiliza para emitir certificados para servicios públicos. La infraestructura de clave pública de ESET interna se utiliza para administrar las claves de la infraestructura de ESET Cloud Office Security. Los datos almacenados en la base de datos están protegidos por claves de cifrado generadas en la nube. Todos los datos de copia de seguridad están protegidos por claves administradas de ESET.

7. Seguridad física y ambiental

Dado que ESET Cloud Office Security y ESET Business Account están basados en la nube, utilizamos Microsoft Azure para la seguridad física y ambiental. Microsoft Azure utiliza centros de datos certificados con estrictas medidas de seguridad física. La ubicación física del centro de datos depende de la región seleccionada por el cliente.

8. Seguridad de las operaciones

El servicio de ESET Cloud Office Security se presta por medios automatizados basados en estrictos procedimientos operativos y plantillas de configuración. Todos los cambios, como los cambios de configuración y la implementación de nuevos paquetes, se aprueban y prueban en un entorno de pruebas específico antes de la implementación en producción. Los entornos de desarrollo, pruebas y producción se separan entre sí. Los datos de ESET Cloud Office Security se ubican solo en el entorno de producción.

El entorno de ESET Cloud Office Security se somete a supervisión operativa para identificar rápidamente los problemas y proporcionar suficiente capacidad a todos los servicios de la red y los niveles de host.

Todos los datos de configuración se almacenan en nuestros repositorios con copia de seguridad periódica para garantizar la recuperación automática de la configuración de un entorno. Las copias de seguridad de los datos de ESET Cloud Office Security se almacenan tanto en el sitio como fuera del sitio.

Las copias de seguridad se cifran y se someten a pruebas periódicas de recuperabilidad como parte de las pruebas de continuidad de la actividad.

La auditoría de los sistemas se lleva a cabo de conformidad con las normas y directrices internas. Se recopilan de forma continuada los registros y eventos de la infraestructura, el sistema operativo, la base de datos, los servidores de aplicaciones y los controles de seguridad. Los equipos de TI y seguridad interna procesan los registros para identificar anomalías operativas y de seguridad, e incidentes de seguridad de la información.

ESET utiliza un proceso general de administración de vulnerabilidades técnicas para gestionar la aparición de vulnerabilidades en la infraestructura de ESET, incluida la de ESET Cloud Office Security y otros productos de ESET. Este proceso incluye un análisis proactivo de vulnerabilidades y pruebas reiteradas de penetración de la infraestructura, los productos y las aplicaciones.

ESET establece directrices internas para la seguridad de la infraestructura interna, las redes, los sistemas operativos, las bases de datos, los servidores de aplicaciones y las aplicaciones. Estas directrices se verifican mediante la supervisión del cumplimiento técnico y nuestro programa interno de auditoría de seguridad de la información.

9. Seguridad de la comunicación

El entorno de ESET Cloud Office Security se somete a segmentación nativa de la nube, con acceso a la red limitado solo a los servicios necesarios entre los segmentos de red. La disponibilidad de los servicios de red se consigue mediante controles nativos de la nube, como zonas de disponibilidad, equilibrio de carga y redundancia. Se implementan componentes específicos de equilibrio de carga a fin de proporcionar equipos concretos para el enrutamiento de instancias de ESET Cloud Office Security que exijan la autorización del tráfico y el equilibrio de carga. El tráfico de red se supervisa continuamente para detectar anomalías operativas y de seguridad. Los posibles ataques se pueden resolver mediante controles nativos de la nube o soluciones de seguridad implementadas. Todas las comunicaciones de red se cifran mediante técnicas generalmente disponibles, como IPsec y TLS.

10. Adquisición, desarrollo y mantenimiento de sistemas

El desarrollo de los sistemas de ESET Cloud Office Security se realiza de conformidad con la política de desarrollo de software seguro de ESET. Los equipos de seguridad interna se incluyen en el proyecto de desarrollo de ESET Cloud Office Security desde la fase inicial y supervisan todas las actividades de desarrollo y mantenimiento. El equipo de seguridad interna define y verifica el cumplimiento de los requisitos de seguridad en diferentes etapas del desarrollo de software. Todos los servicios, incluidos los que se han desarrollado recientemente, se someten a pruebas de seguridad continuas tras su lanzamiento.

11. Relación con proveedores

Las relaciones con proveedores relevantes se desarrollan de conformidad con las directrices válidas de ESET, que abarcan la gestión de toda la relación y los requisitos contractuales desde la perspectiva de la privacidad y la seguridad de la información. La calidad y seguridad de los servicios prestados por el proveedor de servicios críticos se evalúan periódicamente.

12. Administración de seguridad de la información

La gestión de incidentes de seguridad de la información en ESET Cloud Office Security es similar a la de otras infraestructuras de ESET y se basa en procedimientos de respuesta a incidentes definidos. En la respuesta a incidentes, se definen y asignan funciones en múltiples equipos, como el jurídico, así como los de TI, seguridad, recursos humanos, relaciones públicas y administración ejecutiva. El equipo de respuesta a incidentes se establece función de la clasificación del incidente determinada por el equipo de seguridad interna. Este equipo estará a cargo de la coordinación del resto de equipos que gestionen el incidente. El equipo de seguridad interna también es responsable de la recopilación de pruebas y las lecciones aprendidas. Se notifica a las partes afectadas cuando ocurre el incidente y cuando se resuelve. El equipo jurídico de ESET es responsable de notificar a los organismos normativos en caso necesario de acuerdo con el Regulación General de Protección de Datos (RGPD) y la Ley de seguridad informática, por la que se transpone la Directiva de seguridad de las redes y la información (NIS).

13. Aspectos de seguridad de la información de la gestión de la continuidad de la actividad

La continuidad de la actividad del servicio de ESET Cloud Office Security está codificada en la sólida arquitectura utilizada para maximizar la disponibilidad de los servicios proporcionados. Es posible restaurar totalmente componentes de ESET Cloud Office Security o el servicio de ESET Cloud Office Security a partir de datos de configuración y copia de seguridad fuera del sitio en caso de fallo catastrófico de todos los nodos redundantes. El proceso de restauración se prueba periódicamente.

14. Cumplimiento

El cumplimiento de los requisitos normativos y contractuales de ESET Cloud Office Security se evalúa y revisa con regularidad, al igual que otros procesos e infraestructuras de ESET, y se toman las medidas necesarias para garantizar dicho cumplimiento en todo momento. ESET está registrado como proveedor de servicios digitales de informática en la nube y presta múltiples servicios, entre otros, ESET Cloud Office Security. Tenga en cuenta que las actividades de cumplimiento de ESET no están destinadas a satisfacer los requisitos generales de cumplimiento de los clientes.

Términos de uso

Fecha de entrada en vigor: 23 de octubre de 2023 | Consulte una versión anterior de los Términos de uso | Comparar cambios

El presente Acuerdo de ESET Cloud Office Security (en adelante, "Términos") constituyen un acuerdo especial entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrita en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, sección Sro, entrada n.º 3586/B, número de registro de la empresa 31333532 (en adelante, "ESET" o " Proveedor") y usted, persona física o jurídica (en adelante, "Usted" o "Usuario") que accede a una cuenta para la administración, ESET Cloud Office Security y que accede al portal web controlado por ESET (en adelante, "Cuenta") para utilizar ESET Cloud Office Security. Si utiliza la Cuenta y ESET Cloud Office Security (en adelante, el "Producto") en nombre de una organización, acepta estos Términos en nombre de dicha organización y garantiza que tiene autoridad para someter a la organización a estos Términos. Es ese caso, "Usted" y el "Usuario" se referirán a esa organización. Lea estos Términos detenidamente: se refieren también a los servicios prestados por ESET a través del Producto o en relación con él. Las condiciones específicas de uso de servicios concretos no incluidas en estos Términos se indican con cada servicio, y su aceptación forma parte del proceso de activación del servicio. Los anexos adjuntos complementan estos Términos.

Seguridad y protección de datos

La Cuenta permite acceder a los servicios prestados por ESET. El nombre completo del usuario, el nombre de la empresa, la dirección de correo electrónico válida, el número de teléfono, los datos de licencias y las estadísticas son necesarios para el registro y el uso de la Cuenta y a efectos de la prestación y el mantenimiento de los servicios a los que se accede a través de la Cuenta. Acepta la recopilación de los datos y su transferencia a los servidores del Proveedor o de sus socios: los únicos fines de lo anterior son garantizar la funcionalidad y la autorización de uso del Software y la protección de los derechos del Proveedor. Cuando estos Términos dejen de estar en vigor, el Proveedor y sus socios podrán transferir, procesar y almacenar datos esenciales que lo identifiquen para fines relacionados con la asistencia y el cumplimiento de estos Términos. Solo está autorizado para utilizar la Cuenta con los fines y la forma que se mencionan en estos Términos, en los términos de servicio correspondientes y en la documentación.

Usted es el responsable de la seguridad de su Cuenta y las credenciales necesarias para iniciar sesión. ESET no es responsable de pérdidas o daños derivados del incumplimiento de esta obligación de garantizar la seguridad. El Usuario también es responsable de todas las actividades relacionadas con el uso de la Cuenta, autorizadas o no. Si la seguridad de la Cuenta se ve comprometida, debe informar al Proveedor inmediatamente.

Para proporcionar el servicio de administración de la Cuenta, es necesaria la recopilación de los datos relativos a los datos administrados junto con la información de administración (en lo sucesivo "Datos"). Usted proporciona los Datos con el único fin de recibir el servicio de administración de la Cuenta. Los Datos se proporcionarán y almacenarán de conformidad con las políticas y prácticas de seguridad de ESET, además de con la Política de privacidad.

Puede obtener información detallada sobre la privacidad, la protección de los datos personales y sus derechos como persona interesada en la Política de privacidad.

Directiva de uso correcto

El usuario está obligado a cumplir las limitaciones técnicas estipuladas en la documentación. Acepta que solo utilizará la Cuenta y sus funciones de manera que no se limiten las posibilidades de otros Usuarios de acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance de los servicios prestados a Usuarios concretos a fin de permitir que la máxima cantidad posible de Usuarios pueda utilizar los servicios. Limitar el alcance de los servicios significa también poner fin por completo a la posibilidad de utilizar cualquiera de las funciones de la Cuenta y eliminar datos e información.

En Limitaciones puede encontrar información detallada sobre las limitaciones técnicas.

Ubicación

El Proveedor puede permitirle elegir una de las ubicaciones host disponibles para la Cuenta, incluida la ubicación recomendada elegida por el Proveedor. Reconoce que, si elige una ubicación distinta de la recomendada, su experiencia de Usuario puede verse afectada. En función de la ubicación elegida, podrían ser de aplicación el Acuerdo de protección de datos incluido en el Anexo n.º 2 de este Acuerdo y las Cláusulas contractuales tipo incluidas en el Anexo n.º 3 de este Acuerdo. ESET se reserva el derecho a cambiar la ubicación específica en cualquier momento sin previo aviso para mejorar los servicios prestados por ESET de acuerdo con sus preferencias de ubicación (p. ej., Unión Europea).

Software

ESET o sus proveedores tienen los derechos de autor o los ejercen en lo que respecta a todo el software disponible como parte del Producto (en adelante, el "Software"). El Software solo puede utilizarse de conformidad con el Acuerdo de licencia para el usuario final incluido en el Anexo n.º 1 de este Acuerdo. Encontrará más información sobre licencias, derechos de autor, documentación y marcas comerciales en la Información legal.

Restricciones

No puede copiar ni distribuir la Cuenta, ni extraer componentes o crear obras derivadas de ella. El uso de la Cuenta software está sujeto a las siguientes restricciones:

(a) No puede utilizar, modificar, traducir ni reproducir la Cuenta ni transferir los derechos de uso de la Cuenta o sus componentes de ninguna forma que no se haya establecido expresamente en estos Términos.

(b) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar la Cuenta, ni utilizarla para prestar servicios comerciales.

(c) No puede aplicar la ingeniería inversa, descompilar ni desmontar la Cuenta, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

(d) Acepta que el uso de la Cuenta se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

Descargo de responsabilidad

COMO USUARIO, RECONOCE POR LA PRESENTE QUE LA CUENTA Y LOS SERVICIOS SE OFRECEN "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, HASTA DONDE LO PERMITA LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, NI SUS LICENCIADORES O FILIALES NI LOS TITULARES DE LOS DERECHOS DE AUTOR DECLARAN NI GARANTIZAN NADA, NI EXPLÍCITA NI IMPLÍCITAMENTE, LO QUE INCLUYE, ENTRE OTRAS COSAS, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN A UN PROPÓSITO ESPECÍFICO O QUE LA CUENTA O LOS SERVICIOS RESPETEN LAS PATENTES, LOS DERECHOS DE AUTOR, LAS MARCAS U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LA CUENTA O LOS SERVICIOS CUMPLAN SUS REQUISITOS NI QUE EN EL FUNCIONAMIENTO DE LA CUENTA O LOS SERVICIOS NO HAYA INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN Y EL USO DE LA CUENTA Y LOS SERVICIOS PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LOS RESULTADOS OBTENIDOS.

Estos Términos no crean más obligaciones al Proveedor ni a sus licenciadores que las expuestas específicamente en este documento.

Limitación de responsabilidad

HASTA DONDE LO PERMITA LA LEGISLACIÓN APLICABLE, NI EL PROVEEDOR, NI SUS EMPLEADOS NI SUS CONTRATISTAS SERÁN RESPONSABLES EN NINGÚN CASO DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE GASTOS POR ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, DAÑOS MATERIALES, DAÑOS PERSONALES, INTERRUPCIÓN COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, INCIDENTALES, ECONÓMICOS, DE COBERTURA, PUNITIVOS O CONSECUENTES, SEA CUAL SEA SU CAUSA Y TANTO SI SE DERIVAN DE UN CONTRATO, UN ACUERDO EXTRACONTRACTUAL, UNA NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD, PROVOCADOS POR EL USO DE LA CUENTA O LA INCAPACIDAD DE UTILIZARLA, AUNQUE EL PROVEEDOR O SUS CONTRATISTAS O FILIALES CONOZCAN LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, SUS CONTRATISTAS O SUS AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR EL SERVICIO O LA CUENTA EN CUESTIÓN.

Cumplimiento de las normas de control comercial

(a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo ("Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen:

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud de estos Términos o en el que ESET o cualquiera de sus Filiales estén registradas u operen y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud de estos Términos o en el que ESET o cualquiera de sus Filiales estén registradas u operen (los actos jurídicos a los que se hace referencia en los puntos i e ii. anteriores se denominan, conjuntamente, "Leyes de control comercial").

(b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en la sección (a) de esta cláusula de Cumplimiento de las normas de control comercial, o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud de estos Términos podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

(c) Ninguna disposición de estos Términos tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe

interpretarse en ese sentido.

Legislación aplicable e idioma

Estos Términos se regirán e interpretarán de conformidad con la legislación eslovaca. El Usuario final y el Proveedor acuerdan que no se aplicarán las disposiciones relativas a conflictos de leyes de la legislación aplicable y la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Si es un consumidor con domicilio habitual en la UE, también se le concede protección adicional mediante disposiciones legales obligatorias aplicables en su país de residencia.

Acepta explícitamente que la jurisdicción exclusiva en caso de reclamaciones o disputas con el Proveedor, relacionadas de cualquier forma con su uso del Software, la Cuenta o los Servicios o derivadas de estos Términos o Términos especiales (en su caso), corresponde al tribunal de distrito de Bratislava I (Eslovaquia); además, acepta y consiente explícitamente el ejercicio de la jurisdicción personal en el tribunal de distrito de Bratislava I en relación con dichas reclamaciones o disputas. Si es consumidor y tiene un domicilio habitual en la UE, también puede presentar una reclamación para exigir que se cumplan sus derechos de consumidor en el lugar de la jurisdicción exclusiva o en el país de la UE en el que vive. También puede utilizar una plataforma de resolución de disputas en línea, a la que se puede acceder aquí: https://ec.europa.eu/consumers/odr/. No obstante, puede ponerse en contacto con nosotros en primer lugar antes de realizar cualquier reclamación de forma oficial.

Si existen discrepancias entre las versiones en diferentes idiomas de estos Términos, siempre prevalecerá la versión en inglés, disponible aquí.

Disposiciones generales

ESET se reserva el derecho de revisar estos Términos y esta documentación o cualquier parte de ellos en cualquier momento; se limitará a actualizar el documento correspondiente para reflejar cambios de la legislación o cambios de la Cuenta. Se le notificará cualquier revisión de estos Términos mediante la Cuenta. Si no acepta los cambios de estos Términos, puede cancelar su Cuenta. A menos que cancele su Cuenta tras recibir la notificación de los cambios, las modificaciones y las revisiones de estos Términos serán vinculantes para Usted. Le recomendamos que visite esta página periódicamente para consultar los Términos aplicables a su uso de la Cuenta.

Avisos

Todos los avisos deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Anexo n.º 1

Acuerdo de licencia para el usuario final

Anexo n.º 2

Acuerdo de procesamiento de datos

Anexo n.º 3

Cláusulas contractuales tipo

Acuerdo de licencia para el usuario final

IMPORTANTE: Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final (en adelante, "Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 (en adelante, "ESET" o "Proveedor") y usted, una persona física o jurídica (en adelante, "Usted" o "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto…" durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo. Si no acepta todos los términos y condiciones de este Acuerdo, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo (de aquí en adelante, la "Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. **Instalación, Ordenador y una Clave de licencia**. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el

Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (en adelante denominados "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (de aquí en adelante, “un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíqueselo inmediatamente al Proveedor.

c) **Business Edition.** Debe obtener una versión Business Edition del software para poder utilizarlo en servidores, transmisores y pasarelas de correo, así como en pasarelas de Internet.

d) **Vigencia de la licencia**. Tiene derecho a utilizar el software durante un período de tiempo limitado.

e) **Software OEM**. El software OEM solo se puede utilizar en el ordenador con el que se le proporcionó. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR**. El software clasificado como "No para la reventa", NFR o VERSIÓN DE PRUEBA no se puede vender y únicamente se debe utilizar para demostraciones o para comprobar las características del software.

g) **Terminación de la licencia**. La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la licencia, el usuario debe eliminar, destruir o devolver (a sus expensas) el software y todas las copias de seguridad del mismo a ESET o al lugar donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4.**Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El proveedor podrá publicar ocasionalmente actualizaciones del software ("actualizaciones"), aunque no está obligado a ello. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para suministrar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

b) Envío de amenazas e información al proveedor. El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet (de aquí en adelante "amenazas") y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el Ordenador o la plataforma en la que el Software está instalado e información sobre las operaciones y las funciones del Software (en adelante "Información"). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados. La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La información y las amenazas pueden recogerse mediante las siguientes funciones del software:
i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador. Por la presente acepta recibir notificaciones y mensajes, lo que incluye, entre otros elementos, información de marketing.

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.

5. **Ejercicio de los derechos de usuario final**. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los

Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes ni crear versiones derivadas del software. El uso del software está sujeto a las siguientes restricciones:

a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.

c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.

d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. **Copyright**. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. **Reserva de derechos**. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. **Versiones en varios idiomas, software en soporte dual, varias copias**. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. **Comienzo y rescisión del Acuerdo**. Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. **No existe ninguna otra obligación**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE LAS PÉRDIDAS DE BENEFICIOS, INGRESOS, VENTAS, DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, CONDUCTA INADECUADA INTENCIONADA, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO A LA UTILIZACIÓN O LA INCAPACIDAD DE UTILIZACIÓN DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR O SUS PROVEEDORES DE LICENCIAS HAYAN SIDO NOTIFICADOS DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. **Soporte técnico**. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. **Transferencia de la licencia**. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software**. El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. **Licencia para organismos públicos y gubernamentales de EE.UU.**. UU. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. **Cumplimiento de las normas de control comercial**.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo (en adelante, las "Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes de control de las exportaciones") y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes sancionadoras").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en el Artículo 19.a del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. **Avisos**. Los avisos y el Software y la Documentación devueltos deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Legislación aplicable**. Este acuerdo se regirá e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. En caso de discrepancia entre las versiones de este acuerdo en diferentes idiomas, prevalecerá la versión en inglés. Este acuerdo solo se puede modificar por escrito y con la firma de un representante autorizado del proveedor o una persona autorizada expresamente para este fin mediante un poder notarial.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

De acuerdo con los requisitos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, "RGPD"), el Proveedor (en adelante, "Encargado del tratamiento") y Usted (en adelante, "Responsable del tratamiento") establecen una relación contractual sobre tratamiento de datos para definir los términos y condiciones del tratamiento de datos personales, la forma de proteger esos datos y otros derechos y obligaciones de ambas partes respecto al tratamiento de datos personales de los interesados en nombre del Responsable del tratamiento con respecto al objeto de estos Términos como contrato principal.

1. **Tratamiento de datos personales.** Entre los servicios prestados de acuerdo con estos Términos, se puede incluir el tratamiento de información relativa a una persona física identificada o identificable indicada en la Política de privacidad (en adelante, "Datos personales").

2. **Autorización.** El Responsable del tratamiento autoriza al Encargado del tratamiento a tratar los Datos personales, incluidas las siguientes instrucciones:

(i) "Finalidad del tratamiento" es la prestación de servicios de acuerdo con estos Términos. El Encargado del tratamiento solo puede procesar los Datos personales en nombre del Responsable del tratamiento en relación con la prestación de servicios solicitada por este. Toda la información recopilada con fines adicionales se procesa fuera de la relación contractual Controlador-Encargado del tratamiento.

(ii) Período de tratamiento es el período comprendido entre el inicio de la cooperación mutua de acuerdo con estos Términos y la finalización de los servicios.

(iii) Alcance y categorías de los datos personales. Los Servicios están diseñados únicamente para el tratamiento de datos personales generales. Sin embargo, el Responsable del tratamiento es el único responsable de la determinación del alcance de los datos personales.

(iv) "Interesado" es la persona física en tanto usuario autorizado de los dispositivos del Responsable del tratamiento.

(v) Operaciones de tratamiento son todas las operaciones necesarias para el tratamiento.

(vi) "Instrucciones documentadas" son las instrucciones descritas en estos Términos, sus Anexos, la Política de privacidad y la documentación del servicio. El Responsable del tratamiento se encargará de la legalización del tratamiento de los Datos personales por parte del Encargado del tratamiento en relación con las correspondientes disposiciones aplicables de la ley de protección de datos.

3. **Obligaciones del Encargado del tratamiento**. El Encargado del tratamiento está obligado a:

(i) Procesar los Datos personales solo de acuerdo con las instrucciones documentadas y con el fin definido en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio.

(ii) Dar instrucciones a las personas autorizadas para tratar los Datos personales (en adelante, las "Personas autorizadas") sobre sus derechos y obligaciones en virtud del RGPD, sobre su responsabilidad en caso de infracción, y a garantizar que las Personas autorizadas se han comprometido a mantener la confidencialidad y seguir las instrucciones Documentadas.

(iii) Implementar y seguir las medidas descritas en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio.

(iv) Ayudar al Responsable del tratamiento a responder a las solicitudes de los Interesados relacionadas con sus derechos. El Encargado del tratamiento no corregirá, eliminará ni restringirá el tratamiento de los Datos personales sin las instrucciones del Responsable del tratamiento. Todas las solicitudes del Interesado relacionadas con los Datos personales procesados en nombre del Responsable del tratamiento se remitirán al Responsable del tratamiento sin demora.

(v) Ayudar al Responsable del tratamiento en la notificación de una infracción de los Datos personales a la autoridad supervisora y al Interesado. El Encargado del tratamiento debe informar al Responsable del tratamiento de cualquier infracción del tratamiento de los Datos personales o de la seguridad de los datos personales inmediatamente después de tener constancia de dicha infracción. El Encargado del tratamiento deberá colaborar, en la medida de lo posible, en la investigación y corrección de dicha infracción, y adoptará medidas razonables para limitar otras implicaciones negativas.

(vi) Según decida el Responsable del tratamiento, eliminar o devolver todos los Datos personales al Responsable del tratamiento una vez que finalice el Periodo de tratamiento. El Responsable del tratamiento se compromete a informar al Encargado del tratamiento de su decisión en el plazo de diez (10) días después de la finalización del Periodo de tratamiento. Esta disposición no afectará al derecho del Encargado del tratamiento de mantener los Datos personales en la medida necesaria con fines de archivado por interés público, fines de investigación, con fines estadísticos o con fines de divulgación, ejercicio o defensa de procedimientos legales.

(vii) Mantener un registro actualizado de todas las categorías de actividades de tratamiento realizadas en nombre del Responsable del tratamiento.

(viii) Poner toda la información necesaria para demostrar el cumplimiento de los Términos, sus Anexos, la Política de privacidad y la documentación del servicio a disposición del Responsable del tratamiento. En caso de auditoría o control del tratamiento de los Datos personales por parte del Responsable del tratamiento, el Responsable del

tratamiento está obligado a informar al Encargado del tratamiento por escrito con una antelación mínima de treinta (30) días antes de la auditoría o el control planificados.

4. **Participación de otro Encargado del tratamiento.** El Encargado del tratamiento tiene derecho a solicitar la participación de otro Encargado del tratamiento para realizar actividades de tratamiento específicas, como proporcionar infraestructura y almacenamiento en la nube para el servicio de acuerdo con estos Términos, sus Anexos, la Política de privacidad y la documentación del servicio. Microsoft ofrece actualmente almacenamiento en la nube e infraestructura como parte de Azure Cloud Service. Incluso en este caso, el Encargado del tratamiento seguirá siendo el único punto de contacto y la parte responsable del cumplimiento de la normativa. Por la presente, el Encargado del tratamiento se compromete a informar al Responsable del tratamiento de posibles adiciones o sustituciones de otro encargado del tratamiento, por si decidiera oponerse a dicho cambio.

5. **Territorio del tratamiento.** El Encargado del tratamiento garantiza que el tratamiento tiene lugar en el Espacio Económico Europeo o en un país considerado seguro por la Comisión Europea de acuerdo con la decisión del Responsable del tratamiento. En caso de transferencias y tratamiento que tengan lugar fuera del Espacio Económico Europeo o de un país considerado seguro por la Comisión Europea a petición del Responsable del tratamiento, se aplican las cláusulas contractuales tipo.

6. **Seguridad.** El Encargado del tratamiento cuenta con la certificación ISO 27001:2013 y usa el marco de referencia ISO 27001 para implementar una estrategia de seguridad por capas al aplicar controles de seguridad en las capas de red, sistemas operativos, bases de datos, aplicaciones, personal y procesos operativos. El cumplimiento de los requisitos normativos y contractuales se evalúa y revisa con regularidad, de forma similar a lo que sucede con otras operaciones e infraestructuras del Encargado del tratamiento, y se dan los pasos necesarios para garantizar dicho cumplimiento en todo momento. El Encargado del tratamiento ha organizado la seguridad de los datos mediante ISMS según la norma ISO 27001. La documentación de seguridad incluye principalmente documentos de políticas sobre seguridad de la información, seguridad física y seguridad del equipo, gestión de incidentes, gestión de filtraciones de datos e incidentes de seguridad, etc.

7. **Medidas técnicas y organizativas**. El Encargado del tratamiento protegerá los Datos personales contra daños y destrucción, pérdidas, cambios, acceso y revelación no autorizadas de los Datos personales. A tal fin, el Encargado del tratamiento deberá adoptar las medidas técnicas y organizativas adecuadas correspondientes al modo de tratamiento y al riesgo que presenta el tratamiento para los derechos de los Interesados, de acuerdo con los requisitos que marca el RGPD. En la Política de seguridad se expone una descripción detallada de las medidas técnicas y organizativas.

8. **Datos de contacto del Encargado del tratamiento.** Todas las notificaciones, solicitudes, demandas y demás comunicaciones relativas a la protección de Datos personales deben dirigirse a ESET, spol. s.r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECCIÓN I

Cláusula 1 Finalidad y ámbito de aplicación

a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos(1) (Reglamento general de protección de datos), exige para la transferencia de datos personales a un tercer país.

b) Las Partes:

i) la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «exportador de datos»), y

ii) la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «importador de datos»),

han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas»).

c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.

d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del pliego.

Cláusula 2 Efecto e invariabilidad de las cláusulas

a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados, de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3 Tercero beneficiario

a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.

Cláusulas 1, 2, 3, 6 y 7.

ii) Cláusula 8: [módulo uno] cláusula 8.5, letra e), y cláusula 8.9, letra b); [módulo dos] cláusula 8.1, letra b), y cláusula 8.9, letras a), c), d) y e); [módulo tres] cláusula 8.1, letras a), c) y d), y cláusula 8.9, letras a), c), d), e), f) y g); [módulo cuatro] cláusula 8.1, letra b), y cláusula 8.3, letra b).

iii) Cláusula 9: [módulo dos] cláusula 9, letras a), c), d) y e); [módulo tres] cláusula 9, letras a), c), d) y e).

iv) Cláusula 12: [módulo uno] cláusula 12, letras a) y d); [módulos dos y tres] cláusula 12, letras a), d) y f).

v) Cláusula 13

vi) Cláusula 15.1, letras c), d) y e).

vii) Cláusula 16, letra e).

viii) Cláusula 18: [módulos uno, dos y tres] cláusula 18, letras a) y b); [módulo cuatro] cláusula 18.

b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4 Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.

b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.

c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5 Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6 Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

Cláusula 7 (opcional) Cláusula de incorporación

a) Cualquier entidad que no sea parte en el presente pliego de cláusulas podrá, previo consentimiento de todas las partes, adherirse al presente pliego de cláusulas en cualquier momento, ya sea como exportador de datos o como importador de datos, cumplimentando el apéndice y firmando el anexo I.A.

b) Una vez haya cumplimentado el apéndice y firmado el anexo I.A, la entidad que se adhiera se considerará parte en el presente pliego de cláusulas y tendrá los derechos y obligaciones de un exportador de datos o un importador de datos, según la categoría en la que se haya inscrito en el anexo I.A.

c) La entidad que se adhiera no adquirirá derechos y obligaciones del presente pliego de cláusulas derivados del período anterior a la adhesión.

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8 Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas.

MÓDULO UNO: transferencia de responsable a responsable

8.1. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B. Solo podrá tratar los datos personales con otros fines:

i) cuando haya recabado el consentimiento previo del interesado;

ii) cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

iii) cuando el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

8.2. Transparencia

a) A fin de que los interesados puedan ejercer de forma eficaz los derechos que les otorga la cláusula 10, el importador de datos les informará, directamente o a través del exportador de datos:

i) de su identidad y datos de contacto;

ii) de las categorías de datos personales tratados;

iii) del derecho a solicitar una copia del presente pliego de cláusulas;

iv) cuando tenga la intención de realizar transferencias ulteriores de los datos personales a terceros, del destinatario o de las categorías de destinatarios (según proceda con el fin de proporcionar información significativa), la finalidad de dicha transferencia ulterior y el motivo de la misma con arreglo a la cláusula 8.7.

b) Lo dispuesto en la letra a) no será de aplicación cuando el interesado ya disponga de la información (por ejemplo, si el exportador de datos ya ha proporcionado dicha información) o cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado para el importador de datos. En este último caso, el importador de datos hará pública la información en la medida de lo posible.

c) Previa solicitud, las partes pondrán gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, las partes podrán expurgar el texto del apéndice antes de compartir una copia, pero deberán aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada.

d) Lo dispuesto en las letras a) a c) se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.3. Exactitud y minimización de datos

a) Cada parte se asegurará de que los datos personales sean exactos y, cuando proceda, estén actualizados. El importador de datos adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

b) Si una de las partes tiene conocimiento de que los datos personales que ha transferido o recibido son inexactos o han quedado obsoletos, informará de ello a la otra parte sin dilación indebida.

c) El importador de datos se asegurará de que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento.

8.4. Limitación del plazo de conservación

El importador de datos no conservará los datos personales más tiempo del necesario para los fines para los que se traten. Establecerá las medidas técnicas u organizativas adecuadas para garantizar el cumplimiento de esta obligación, como la supresión o anonimización (2) de los datos y de todas las copias de seguridad al finalizar el período de conservación.

8.5. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para el interesado. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento.

b) Las partes han pactado las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

c) El importador de datos garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

d) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los posibles efectos negativos.

e) En caso de violación de la seguridad de los datos personales que sea probable que entrañe un riesgo para los derechos y libertades de las personas físicas, el importador de datos lo notificará sin dilación indebida tanto al exportador de datos como a la autoridad de control competente con arreglo a la cláusula 13. Dicha notificación contendrá i) una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), ii) las consecuencias probables, iii) las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad y iv) los datos de un punto de contacto en el que pueda obtenerse más información. En la medida en que el importador de datos no pueda proporcionar toda la información al mismo tiempo, podrá hacerlo por fases sin más dilaciones indebidas.

f) En caso de violación de la seguridad de los datos personales que sea probable que entrañe un riesgo elevado para los derechos y libertades de las personas físicas, el importador de datos también notificará sin dilación indebida a los interesados la violación de la seguridad de los datos personales y su naturaleza —en caso necesario con la colaboración del exportador de datos— junto con la información a que se refiere la letra e), incisos ii) a iv), a menos que dicha notificación suponga un esfuerzo desproporcionado o que el importador de datos haya aplicado medidas para reducir significativamente el riesgo para los derechos o libertades de las personas físicas. En este último caso, el importador de datos realizará una comunicación pública o adoptará una medida semejante para informar al público de la violación de la seguridad de los datos personales.

g) El importador de datos documentará todos los hechos pertinentes relacionados con la violación de la seguridad de los datos personales, como sus efectos y las medidas correctivas adoptadas, y llevará un registro de las mismas.

8.6. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas o infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará restricciones específicas y/o garantías adicionales adaptadas a la naturaleza específica de los datos y el riesgo de que se trate. Una de estas puede ser, por ejemplo, la reducción del personal autorizado a acceder a los datos personales, medidas de seguridad adicionales (como la seudonimización) y/o restricciones adicionales con respecto a la comunicación ulterior.

8.7. Transferencias ulteriores

El importador de datos no comunicará los datos personales a terceros situados fuera de la Unión Europea (3) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») a menos que el tercero esté vinculado por el presente pliego de cláusulas o consienta a someterse a este, con elección del módulo correspondiente. De no ser así, el importador de datos solo podrá efectuar una transferencia ulterior si:

i) esta va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;

iii) el tercero suscribe un instrumento vinculante con el importador de datos que garantice el mismo nivel de protección de datos que el del presente pliego de cláusulas, y el importador de datos entrega una copia de estas garantías al exportador de datos;

iv) si es necesario para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

v) si es necesario para proteger intereses vitales del interesado o de otra persona física; o

vi) de no concurrir las demás condiciones, el importador de datos ha recabado el consentimiento expreso del interesado para una transferencia ulterior en una situación específica, tras haberle informado de su finalidad, de la identidad del destinatario y de los posibles riesgos de dicha transferencia para el interesado debido a la falta de garantías adecuadas en materia de protección de datos. En este caso, el importador de datos informará al exportador de datos y, a petición de este, le remitirá una copia de la información proporcionada al interesado.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.8. Tratamiento bajo la autoridad del importador de datos

El importador de datos se asegurará de que las personas que actúen bajo su autoridad, especialmente el encargado, solo trate los datos siguiendo instrucciones del importador de datos.

8.9. Documentación y cumplimiento

a) Las partes deberán poder demostrar el cumplimiento de las obligaciones derivadas del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen bajo su responsabilidad.

b) El importador de datos pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud.

MÓDULO DOS: transferencia de responsable a encargado

8.1. Instrucciones

a) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del exportador de datos. El exportador de datos podrá dar dichas instrucciones durante todo el período de vigencia del contrato.

b) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones.

8.2. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del exportador de datos.

8.3. Transparencia

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como las medidas descritas en el anexo II y datos personales, el exportador de datos podrá expurgar el texto del apéndice del presente pliego de cláusulas antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada. La presente cláusula se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del exportador de datos y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la

comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

b) El importador de datos solo concederá acceso a los datos personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también lo notificará al exportador de datos sin dilación indebida una vez tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente, en su caso, medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del exportador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea (4) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;

iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o

iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del exportador de datos.

c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y, a instancia del exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.

d) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.

e) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

MÓDULO TRES: transferencia de encargado a encargado

8.1. Instrucciones

a) El exportador de datos ha informado al importador de datos de que actúa como encargado del tratamiento siguiendo las instrucciones de su responsable o responsables, que el exportador de datos deberá poner a disposición del importador de datos antes del tratamiento.

b) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del responsable del tratamiento, comunicadas al importador por el exportador de datos, así como instrucciones documentadas adicionales del exportador de datos. Dichas instrucciones adicionales no podrán estar en conflicto con las instrucciones del responsable. El responsable o el exportador de datos podrán dar instrucciones documentadas adicionales sobre el tratamiento de datos durante todo el período de vigencia del contrato.

c) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones. Si el importador de datos no puede seguir las instrucciones del responsable, el exportador de datos lo notificará inmediatamente al responsable.

d) El exportador de datos asegura que ha impuesto al importador de datos las obligaciones en materia de protección de datos establecidas en el contrato u otro acto jurídico con arreglo al Derecho de la Unión o del

Estado miembro entre el responsable y el exportador de datos (5).

8.2. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del responsable, comunicadas al importador de datos por el exportador de datos, o del exportador de datos.

8.3. Transparencia

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el exportador de datos podrá expurgar el texto del apéndice antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del responsable y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para el interesado. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos o del responsable. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles

periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

b) El importador de datos solo concederá acceso a los datos a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también notificará sin dilación indebida al exportador de datos y, cuando proceda y sea viable, al responsable cuando tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación al responsable para que este luego lo notifique a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del responsable, tal y como las haya comunicado el exportador de datos al importador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea (6) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;

ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679;

iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o

iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos o del responsable relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del responsable.

c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente pliego de cláusulas; el exportador de datos luego la proporcionará al responsable.

d) El importador de datos permitirá y contribuirá a las auditorías que realice el exportador de datos sobre las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Lo mismo se aplicará cuando el exportador de datos solicite una auditoría siguiendo instrucciones del responsable. Al decidir si se realiza una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.

e) Cuando la auditoría se realice siguiendo instrucciones del responsable del tratamiento, el exportador de datos pondrá los resultados a disposición del responsable.

f) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.

g) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

MÓDULO CUATRO: transferencia de encargado a responsable

8.1. Instrucciones

a) El exportador de datos solo tratará los datos personales siguiendo instrucciones documentadas del importador de datos que actúe como su responsable.

b) El exportador de datos informará inmediatamente al importador de datos si no puede seguir dichas instrucciones, especialmente si dichas instrucciones infringen el Reglamento (UE) 2016/679 u otro instrumento normativo del Derecho de la Unión o del Estado miembro en materia de protección de datos.

c) El importador de datos no obrará de forma que pueda impedir al exportador de datos cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679 y, en particular, en el marco del subtratamiento o de la cooperación con las autoridades de control competentes.

d) Una vez se hayan prestado los servicios de tratamiento, el exportador de datos suprimirá, a petición del importador de datos, todos los datos personales tratados por cuenta del importador de datos y acreditará al importador de datos que lo ha hecho, o devolverá al importador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes.

8.2. Seguridad del tratamiento

a) Las partes aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, especialmente durante la transferencia; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza de los datos personales (7), la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados, y considerarán, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento.

b) El exportador de datos ayudará al importador de datos a garantizar una seguridad adecuada de los datos de conformidad con la letra a). En caso de violación de la seguridad de los datos personales tratados por el exportador de datos en virtud del presente pliego de cláusulas, el exportador de datos lo notificará sin dilación indebida al importador de datos, una vez que tenga conocimiento de ello, y le ayudará a poner remedio a la violación de la seguridad.

c) El exportador de datos garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

8.3. Documentación y cumplimiento

Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

b) El exportador de datos pondrá a disposición del importador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones que le atribuye el presente pliego de cláusulas y permitirá y contribuirá a las auditorías.

Cláusula 9 Recurso a subencargados

MÓDULO DOS: transferencia de responsable a encargado

a) El importador de datos cuenta con una autorización general del exportador de datos para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al exportador de datos específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el exportador de datos tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeción.

b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios. (8) Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

c) El importador de datos proporcionará al exportador de datos, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.

d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.

e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

MÓDULO TRES: transferencia de encargado a encargado

a) El importador de datos cuenta con una autorización general del responsable para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al responsable específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el responsable tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al responsable la información necesaria para que pueda ejercer su derecho a formular objeción. El importador de datos informará al exportador de datos de la contratación del subencargado o subencargados.

b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del responsable), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios. (9) Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

c) El importador de datos proporcionará al exportador de datos o al responsable, a instancia del exportador de datos o el responsable, respectivamente, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.

d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.

e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

Cláusula 10 Derechos del interesado

MÓDULO UNO: transferencia de responsable a responsable

a) El importador de datos, en su caso con la asistencia del exportador de datos, tramitará, sin dilación indebida y como tarde en un plazo de un mes desde la recepción de la consulta o solicitud, las consultas y solicitudes que reciba de interesados en relación con el tratamiento de sus datos personales y el ejercicio de los derechos que les otorga el presente pliego de cláusulas. (10) El importador de datos adoptará medidas adecuadas para facilitar dichas consultas y solicitudes y el ejercicio de los derechos de los interesados. Toda la información que se

proporcione a los interesados deberá ser inteligible y de fácil acceso, con un lenguaje claro y sencillo.

b) En particular, el importador de datos deberá, a petición del interesado y de forma gratuita:

i) confirmar al interesado si se están tratando datos personales que le conciernan y, en su caso, proporcionar una copia de los datos que le conciernan, así como la información que figura en el anexo I; si los datos personales han sido o serán ulteriormente transferidos, información sobre los destinatarios o las categorías de destinatarios (según proceda, con vistas a proporcionar información significativa) a los que se haya realizado o vaya realizarse la transferencia ulterior de los datos personales, la finalidad de dichas transferencias ulteriores y su motivo de conformidad con la cláusula 8.7; e información sobre el derecho a presentar una reclamación ante una autoridad de control en virtud de la cláusula 12, letra c), inciso i);

ii) rectificar los datos inexactos o incompletos relativos al interesado;

iii) suprimir los datos personales relativos al interesado si dichos datos se están tratando o han sido tratados en contravención de cualquiera de las cláusulas que garantizan los derechos de terceros beneficiarios o si el interesado retira el consentimiento en que se basa el tratamiento.

c) Cuando el importador de datos trate los datos personales con fines de mercadotecnia directa, dejará de tratarlos para tales fines si el interesado se opone a ello.

d) El importador de datos no tomará una decisión, basándose únicamente en el tratamiento automatizado de los datos personales transferidos («decisión automatizada»), que produzca efectos jurídicos para el interesado o le afecte de forma igualmente significativa, salvo con el consentimiento expreso del interesado o si así lo autoriza el Derecho del país de destino, siempre que dicho Derecho disponga medidas adecuadas para garantizar los intereses legítimos y los derechos del interesado. En este caso, el importador de datos, con la colaboración del exportador de datos cuando sea necesario:

i) informará al interesado de la decisión automatizada prevista y de las consecuencias previstas, así como de la lógica aplicada; y

ii) aplicará garantías adecuadas, como mínimo permitiendo al interesado impugnar la decisión, expresar su punto de vista y solicitar una revisión por parte de un ser humano.

e) Cuando las solicitudes de un interesado sean excesivas, especialmente debido a su carácter repetitivo, el importador de datos podrá establecer una tasa razonable en función del coste administrativo que implique la concesión de la solicitud o negarse a actuar respecto de la solicitud.

f) El importador de datos podrá denegar la solicitud de un interesado cuando ello esté permitido con arreglo al Derecho del país de destino y sea necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

g) Si el importador de datos pretende denegar la solicitud de un interesado, le informará de los motivos de la denegación y de la posibilidad de presentar una reclamación ante la autoridad de control competente o de ejercitar una acción judicial.

MÓDULO DOS: transferencia de responsable a encargado

a) El importador de datos notificará con presteza al exportador de datos las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el exportador de datos le haya autorizado a hacerlo.

b) El importador de datos ayudará al exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 atribuye a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del

tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del exportador de datos.

MÓDULO TRES: transferencia de encargado a encargado

a) El importador de datos notificará con presteza al exportador de datos y, en su caso, al responsable toda solicitud que reciba de un interesado, sin responder a dicha solicitud, a menos que haya sido autorizado a hacerlo por el responsable.

b) El importador de datos ayudará al exportador de datos, cuando proceda con la colaboración del exportador de datos, a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725 atribuyen a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del responsable, comunicadas por el exportador de datos.

MÓDULO CUATRO: transferencia de encargado a responsable

Las partes se prestarán ayuda recíproca para responder a las consultas y solicitudes de los interesados en virtud del Derecho doméstico aplicable al importador de datos o, respecto del tratamiento de datos por parte del exportador de datos en la Unión, en virtud del Reglamento (UE) 2016/679.

Cláusula 11 Reparación

a) El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

b) En caso de litigio entre un interesado y una de las partes en relación con el cumplimiento del presente pliego de cláusulas, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán para resolverlos.

c) El importador de datos se compromete a aceptar, cuando el interesado invoque un derecho de tercero beneficiario con arreglo a la cláusula 3, la decisión del interesado de:

i) presentar una reclamación ante la autoridad de control del Estado miembro de su residencia habitual o su lugar de trabajo o ante la autoridad de control competente con arreglo a la cláusula 13;

ii) ejercitar una acción judicial en el sentido de la cláusula 18.

d) Las partes aceptan que el interesado pueda estar representado por una entidad, organización o asociación sin ánimo de lucro en las condiciones establecidas en el artículo 80, apartado 1, del Reglamento (UE) 2016/679.

e) El importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo al Derecho aplicable de la UE o del Estado miembro de que se trate.

f) El importador de datos acepta que la elección del interesado no menoscabe sus derechos sustantivos y procesales a obtener reparación de conformidad con el Derecho aplicable.

Cláusula 12 Responsabilidad

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO CUATRO: transferencia de encargado a responsable

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

b) Cada parte será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que la parte ocasione al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Ello se entiende sin perjuicio de la responsabilidad que le atribuye el Reglamento (UE) 2016/679 al exportador de datos.

c) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

d) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra c), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

e) El importador de datos no puede alegar la conducta de un encargado o subencargado del tratamiento para eludir su propia responsabilidad.

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

b) El importador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el importador de datos o su subencargado ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas.

c) A pesar de lo dispuesto en la letra b), el exportador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el exportador de datos o el importador de datos (o su subencargado) ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Lo anterior se entiende sin perjuicio de la responsabilidad del exportador de datos y, cuando el exportador de datos sea un encargado que actúe por cuenta de un responsable, de la responsabilidad del responsable con arreglo al Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725, según cuál sea de aplicación.

d) Las partes acuerdan que, si el exportador de datos es considerado responsable, de conformidad con la letra c), de los daños o perjuicios causados por el importador de datos (o su subencargado), estará legitimado para exigir

al importador de datos la parte de la indemnización que sea responsabilidad del importador de los datos.

e) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

f) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra e), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

g) El importador de datos no puede alegar la conducta de un subencargado del tratamiento para eludir su propia responsabilidad.

Cláusula 13 Supervisión

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) [Cuando el exportador de datos esté establecido en un Estado miembro de la UE:] La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679:] La autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión:] La autoridad de control de uno de los Estado miembros en que estén situados los interesados cuyos datos personales se transfieran en virtud del presente pliego de cláusulas en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, indicada en el anexo I.C, actuará como autoridad de control competente.

b) El importador de datos da su consentimiento a someterse a la jurisdicción de la autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14 Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: Transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:

i) las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;

ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables (12);

iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.

d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a). [Módulo tres: El exportador de datos notificará al responsable.]

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres:, si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).

Cláusula 15 Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: Transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

15.1. Notificación

a) El importador de datos se compromete a notificar con presteza al exportador de datos y, cuando sea posible, al interesado (de ser necesario, con la ayuda del exportador de datos) si:

i) recibe una solicitud jurídicamente vinculante de comunicación de datos personales transferidos con arreglo al presente pliego de cláusulas presentada por una autoridad pública (sobre todo, judicial) en virtud del Derecho del país de destino; dicha notificación contendrá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada; o

ii) tiene conocimiento de que las autoridades públicas han tenido acceso directo a los datos personales transferidos con arreglo al presente pliego de cláusulas en virtud del Derecho del país de destino; dicha notificación incluirá toda la información de que disponga el importador de datos.

[Módulo tres: El exportador de datos notificará al responsable.]

b) Si se prohíbe al importador de datos enviar la notificación al exportador de datos y/o al interesado en virtud del Derecho del país de destino, el importador de datos se compromete a hacer todo lo posible para obtener una dispensa de la prohibición, con el fin de comunicar toda la información disponible y lo antes posible. El importador de datos se compromete a documentar las actuaciones que realice a tal fin para poder justificar su diligencia si se lo pide el exportador de datos.

c) En la medida en que lo permita el Derecho del país de destino, el importador de datos se compromete a proporcionar al exportador de datos, a intervalos regulares durante el período de vigencia del contrato, la mayor cantidad posible de información pertinente sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o autoridades solicitantes, la impugnación de las solicitudes, el resultado

de tales impugnaciones, etc.). [Módulo tres: El exportador de datos remitirá la información al responsable.]

d) El importador de datos se compromete a conservar la información a que se refieren las letras a) a c) durante el período de vigencia del contrato y a ponerla a disposición de la autoridad de control competente previa solicitud.

e) Las letras a) a c) se entenderán sin perjuicio de la obligación del importador de datos, contemplada en la cláusula 14, letra e), y en la cláusula 16, de informar con presteza al exportador de datos cuando no pueda dar cumplimiento al presente pliego de cláusulas.

15.2. Control de la legalidad y minimización de datos

a) El importador de datos se compromete a controlar la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, así como a impugnar la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del Derecho internacional y los principios de cortesía internacional. El importador de datos agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, el importador de datos instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable. Estos requisitos se entienden sin perjuicio de las obligaciones que la cláusula 14, letra e), atribuye al importador de datos.

b) El importador de datos se compromete a documentar sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y a poner dicha documentación a disposición del exportador de datos en la medida en que lo permita el Derecho del país de destino. También pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud. [Módulo tres: El exportador de datos pondrá la valoración a disposición del responsable.]

c) El importador de datos se compromete a proporcionar la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16 Incumplimiento de las cláusulas y resolución del contrato

a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

i) el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

ii) el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o

iii) el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

En este supuesto, informará a la autoridad de supervisión competente [módulo tres: y al responsable] de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

d) [Módulos uno, dos y tres: Los datos personales que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán, a elección del exportador de datos, devolverse inmediatamente al exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos.] [Módulo cuatro: Los datos personales recopilados por el exportador de datos en la UE que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán destruirse en su totalidad inmediatamente, así como cualquier copia de estos.] El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

e) Ninguna de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si: i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17 Ley aplicable

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

El presente pliego de cláusulas se regirá por el Derecho de uno de los Estados miembros de la Unión Europea, siempre que dicho Derecho admita la existencia de derechos de los terceros beneficiarios. Las Partes acuerdan que esta es la ley según está definida en los Términos.

MÓDULO CUATRO: transferencia de encargado a responsable

El presente pliego de cláusulas se regirá por el Derecho de un país que contemple los derechos de los terceros beneficiarios. Las Partes acuerdan que esta es la ley según está definida en los Términos.

Cláusula 18 Elección del foro y jurisdicción

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

a) Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en un Estado miembro de la Unión Europea.

(b) Las Partes acuerdan que estos serán los tribunales según están definidos en los Términos.

c) Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el importador de datos en el Estado miembro en el que el interesado tenga su residencia habitual.

d) Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro.

MÓDULO CUATRO: transferencia de encargado a responsable

Cualquier disputa derivada de estas Cláusulas deberá ser resuelta por los tribunales según están definidos en los Términos.

APÉNDICE

NOTA ACLARATORIA: Se debe poder distinguir claramente la información aplicable a cada transferencia o categoría de transferencias y, por tanto, determinar la función o funciones respectivas de las partes en cuanto exportador(as) de datos y/o importador(as) de datos. No es imprescindible cumplimentar y firmar apéndices separados por cada transferencia o categoría de transferencias y/o relación contractual si se puede lograr un nivel de transparencia equivalente cumplimentando un solo apéndice. No obstante, cuando sea necesario para garantizar claridad suficiente, deben utilizarse apéndices separados.

ANEXO I

A. LISTA DE PARTES

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable

Exportador(es) de datos: [Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, del delegado de protección de datos de este o estos y/o del representante en la Unión Europea]

1. Responsable del tratamiento según está definido en el Acuerdo de tratamiento de datos

2. Encargado del tratamiento según está definido en el Acuerdo de tratamiento de datos

(según el flujo de datos)

Importador(es) de datos: [Identidad y datos de contacto del importador o importadores de datos, incluida cualquier persona de contacto responsable de la protección de los datos]

1. Responsable del tratamiento según está definido en el Acuerdo de tratamiento de datos

2. Encargado del tratamiento según está definido en el Acuerdo de tratamiento de datos

(según el flujo de datos)

B. DESCRIPCIÓN DE LA TRANSFERENCIA

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable

Categorías de interesados cuyos datos personales se transfieren: según están definidas en el Acuerdo de tratamiento de datos.

Categorías de datos personales transferidos: según están definidas en el Acuerdo de tratamiento de datos y la Política de privacidad.

Datos sensibles transferidos (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales. según están definidas en el Acuerdo de tratamiento de datos y la Política de privacidad.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de una vez o de forma periódica): de forma continua.

Naturaleza del tratamiento: automatizado.

Finalidad(es) de la transferencia y posterior tratamiento de los datos: prestación del servicio según está definida en los Términos, sus Anexos, su Política de privacidad y la documentación del servicio.

El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo: según están definidas en el Acuerdo de tratamiento de datos.

En caso de transferencia a (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento: según están definidas en el Acuerdo de tratamiento de datos.

C. AUTORIDAD DE CONTROL COMPETENTE

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

Indíquese la autoridad o autoridades de control competentes de conformidad con la cláusula 13: según están definidas en la Política de privacidad

ANEXO II: MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

MÓDULO UNO: transferencia de responsable a responsable

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

NOTA ACLARATORIA: Las medidas técnicas y organizativas deben describirse de manera concreta y no de manera genérica. Véase también el comentario general de la primera página del apéndice, especialmente en cuanto a la necesidad de indicar claramente qué medidas se aplican a cada transferencia o conjunto de transferencias.

Descripción de las medidas técnicas y organizativas aplicadas por los importadores de datos (inclusive las certificaciones pertinentes) para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas: según están definidas en la Política de seguridad

En el caso de las transferencias a (sub)encargados, descríbanse también las medidas técnicas y organizativas específicas que deberá adoptar el (sub)encargado para poder prestar ayudar al responsable y, en el caso de transferencias de un encargado a un subencargado, al exportador de datos.

ANEXO III: LISTA DE SUBENCARGADOS DEL TRATAMIENTO

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

NOTA ACLARATORIA: Debe cumplimentarse este anexo respecto de los módulos dos y tres cuando sea necesaria la autorización específica de uno o más subencargados [cláusula 9, letra a), opción 1].

El responsable ha autorizado que se recurra a los subencargados siguientes: según está definido en el Acuerdo de tratamiento de datos

Referencias:

(1) Cuando el exportador de datos sea un encargado del tratamiento sujeto al Reglamento (UE) 2016/679 que actúe por cuenta de una institución u organismo de la Unión como responsable del tratamiento, se considera que la utilización del presente pliego de cláusulas al recurrir a otro encargado (subtratamiento) no sujeto al Reglamento (UE) 2016/679 también garantiza el cumplimento del artículo 29, apartado 4, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. o 45/2001 y la Decisión n. o 1247/2002/CE (DO L295 de 21.11.2018, p. 39), en la medida en que estén armonizados el presente pliego de cláusulas y las obligaciones en materia de protección de datos que imponga el contrato u otro acto jurídico celebrado entre el responsable y el encargado con arreglo al artículo 29, apartado 3, del Reglamento (UE) 2018/1725. Este será el caso, en particular, cuando el responsable y el encargado del tratamiento se basen en las cláusulas contractuales tipo incluidas en la Decisión 2021/915.

(2) Para ello es necesario anonimizar los datos de tal manera que nadie pueda identificar a la persona, de conformidad con el considerando 26 del Reglamento (UE) 2016/679, y que este proceso sea irreversible.

(3) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(4) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación

de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(5) Véase el artículo 28, apartado 4, del Reglamento (UE) 2016/679 y, cuando el responsable sea una institución u organismo de la UE, el artículo 29, apartado 4, del Reglamento (UE) 2018/1725.

(6) El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(7) En concreto, si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales.

(8) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(9) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(10) Dicho plazo podrá prorrogarse por un máximo de dos meses adicionales en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El importador de datos informará debidamente y con prontitud al interesado de cualquier prórroga de este tipo.

(11) El importador de datos solo podrá ofrecer una resolución independiente de los litigios a través de un órgano de arbitraje si está establecido en un país que haya ratificado el Convenio de Nueva York sobre la ejecución de laudos arbitrales.

(12) Por lo que se refiere al efecto de dicho Derecho y prácticas en el cumplimiento del presente pliego de cláusulas, a la hora de realizar una valoración integral de esta cuestión pueden tenerse en cuenta distintos aspectos. Uno de estos aspectos puede ser que haya experiencia práctica pertinente y documentada en casos anteriores de solicitudes de comunicación por parte de las autoridades públicas, o la ausencia de tales solicitudes, en un período suficientemente representativo. Con esto se quiere decir, en particular, los registros internos u otra documentación elaborados de forma continua con la diligencia debida y certificados en los niveles más altos de la dirección siempre que esta información pueda compartirse legalmente con terceros. Cuando se use esta experiencia práctica para llegar a la conclusión de que el importador de datos no tendrá impedimento para cumplir el presente pliego de cláusulas, deberá estar respaldada por otros elementos pertinentes y objetivos; corresponde a las partes valorar minuciosamente si la suma de estos factores es suficientemente determinante, en términos de fiabilidad y representatividad, para respaldar esta conclusión. En particular, las partes deben tener en cuenta si su experiencia práctica está corroborada y no se ve desmentida, por información que sea fiable y de dominio público o accesible de cualquier otro modo acerca de la existencia o ausencia de solicitudes en el mismo sector o acerca de la aplicación de la normativa de que se trate en la práctica, como jurisprudencia e informes de organismos de supervisión independientes.

Política de privacidad

Fecha de entrada en vigor: 21 de marzo de 2023 | Consulte una versión anterior de la Política de Privacidad | Comparar cambios

La protección de los datos personales es muy importante para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, n.º de registro de la empresa: 31333532 como Responsable del tratamiento ("ESET"). Cumplimos con el requisito de transparencia que se estipula en el Reglamento general de protección de datos de la UE ("RGPD"). Para lograr este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes ("Usuario final" o "Usted") sobre los siguientes temas de protección de datos personales:

- Fundamento jurídico del tratamiento de datos personales
- Intercambio y confidencialidad de datos
- Seguridad de datos
- Sus derechos como interesado
- Tratamiento de sus datos personales
- Información de contacto.

Fundamento jurídico del tratamiento de datos personales

Solo hay varias disposiciones jurídicas para el tratamiento de datos que usamos de acuerdo con el marco jurídico aplicable a la protección de los datos personales. El tratamiento de los datos personales en ESET es necesario para la ejecución del Términos de uso ("Términos") con el Usuario final (artículo 6 1] b] del RGPD), que se aplica a la prestación de servicios o productos de ESET a menos que se indique explícitamente lo contrario, por ejemplo:

- El fundamento jurídico de interés legítimo (artículo 6 1] b] del RGPD), que nos permite tratar los datos sobre el uso que los clientes hacen de nuestros Servicios y su satisfacción para ofrecer a los usuarios los mejores niveles de protección, asistencia y experiencia que sea posible. Incluso el marketing es reconocido por la legislación aplicable como un interés legítimo, por lo que nos basamos en ese concepto para las comunicaciones de marketing con nuestros clientes.
- El consentimiento (artículo 6 1] b] del RGPD), que podemos solicitarle en situaciones concretas en las que consideramos que este fundamento jurídico es el más adecuado o si la ley lo requiere.
- El cumplimiento de una obligación legal (artículo 6 1] b] del RGPD), por ejemplo, estipulando los requisitos de comunicación electrónica o retención de facturas o documentos de facturación.

Intercambio y confidencialidad de datos

No compartimos sus datos con terceros. Sin embargo, ESET es una empresa que opera en todo el mundo a través de empresas o socios que forman parte de su red de ventas, servicio y asistencia. La información de licencias, facturación y asistencia técnica tratada por ESET puede transferirse entre filiales o socios para cumplir el EULA en aspectos como la prestación de servicios o la asistencia.

ESET prefiere procesar sus datos en la Unión Europea (UE). No obstante, en función de su ubicación (uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transferir sus datos a un país fuera de la UE. Por ejemplo, utilizamos servicios de terceros para prestar servicios de informática en la nube. En estos casos, seleccionamos cuidadosamente a los proveedores de servicios y ofrecemos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por lo general, aceptamos las cláusulas contractuales tipo de la UE con la normativa contractual aplicable si es necesario.

En algunos países de fuera de la UE, como el Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos comparable. Gracias al nivel de protección de datos, la transferencia de datos a estos países no requiere ninguna autorización o acuerdo especial.

Nos basamos en servicios de terceros relacionados con la informática en la nube proporcionados por Microsoft como proveedor de servicios en la nube.

Seguridad de datos

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar la confidencialidad, la integridad, la disponibilidad y la resistencia de los sistemas y los servicios de procesamiento. En caso de filtración de datos que pongan en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora correspondiente y a los usuarios finales en calidad de interesados.

Derechos del titular de los datos.

Los derechos de los usuarios finales son importantes para nosotros, sean de un país de la UE o de fuera de la UE. Por lo tanto, en ESET les garantizamos los derechos siguientes. Para ejercer los derechos de los interesados, puede ponerse en contacto con nosotros a través del formulario de asistencia o por correo electrónico en la dirección dpo@eset.sk. Le pediremos la información siguiente con fines de identificación: Nombre, dirección de correo electrónico y, si procede, clave de licencia o número de cliente y empresa. No nos envíe otros datos personales, como la fecha de nacimiento. Cabe destacar que trataremos sus datos personales con fines de identificación y procesamiento de solicitudes.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento solo se aplica si se tratan los datos con su consentimiento previo. Si nos da su consentimiento para tratar sus datos personales, podrá retirarlo en cualquier momento sin explicar los motivos. La retirada del consentimiento solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite.

Derecho de objeción. El derecho a oponerse al tratamiento se aplica si el tratamiento se basa en el interés legítimo de ESET o terceros. Si tratamos sus datos personales para proteger un interés legítimo, puede oponerse a dicho interés legítimo y al tratamiento de sus datos personales en cualquier momento. La oposición solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite. Si tratamos sus datos personales con fines de marketing directo, no es necesario explicar los motivos por los que se opone. Esto también se aplica a la creación de perfiles, ya que está relacionada con el marketing directo. En el resto de casos, debe enviarnos las quejas que tenga en relación con el interés legítimo de ESET para tratar sus datos personales.

En algunos casos, a pesar de su consentimiento, podemos seguir tratando sus datos personales sobre la base de otro fundamento jurídico (como la ejecución de un contrato).

Derecho de acceso. Como interesado, puede solicitar información sobre los datos personales que ESET almacena en cualquier momento sin coste alguno.

Derecho de rectificación. Si tratamos datos personales incorrectos de manera involuntaria, puede pedir que se corrija esta información.

Derecho a eliminar y restringir el tratamiento de datos personales. Como interesado, puede solicitar la eliminación o restricción del tratamiento de sus datos personales. Por ejemplo, si tratamos datos personales con su consentimiento y lo retira sin otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. Sus datos personales también se eliminarán cuando dejen de ser necesarios para los fines indicados

al finalizar el periodo de retención.

Si solo utilizamos sus datos personales con fines de marketing directo y revoca su consentimiento o se opone al interés legítimo de ESET, restringiremos el tratamiento una vez que incluyamos sus datos de contacto en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales se eliminarán.

Puede que estemos obligados a almacenar sus datos hasta que expiren las obligaciones de retención y los periodos emitidos por el organismo de legislación o las autoridades supervisoras. También pueden surgir periodos u obligaciones de retención porque la legislación eslovaca así lo exija. En ese caso, los datos correspondientes se eliminarán de forma rutinaria a partir de ese momento.

Derecho a la portabilidad de datos. Dado que es un interesado, le proporcionamos los datos personales que trata ESET en formato XLS.

Derecho a presentar una queja. Como interesado, puede presentar una reclamación ante una autoridad supervisora en cualquier momento. ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. La autoridad supervisora que gestiona cuestiones de datos es la Oficina de protección de datos personales de Eslovaquia, situada en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Tratamiento de sus datos personales

Los servicios prestados por ESET implementados en su producto web se prestan de acuerdo con los Términos de uso ("Términos"), pero algunos pueden requerir atención especial. Queremos proporcionarle más detalles sobre el tratamiento de los datos relacionado con la prestación de nuestros productos y servicios. Prestamos distintos servicios descritos en el Términos y la documentación del documentación. Para que todo funcione, debemos recopilar la siguiente información:

Datos de licencias y facturación. ESET recopila y trata el nombre, la dirección de correo electrónico, la clave de licencia y, si procede, la dirección, la afiliación y los pagos de la empresa para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios de caducidad, las solicitudes de asistencia, la verificación de autenticidad de la licencia, la prestación de nuestros servicios y otras notificaciones (como mensajes de marketing) en virtud de la legislación aplicable o su consentimiento. Aunque ESET debe retener la información de facturación durante un periodo de 10 años, la información de la licencia se anonimizará en un plazo máximo de 12 meses una vez que la licencia caduque.

Actualizaciones y otras estadísticas. Los datos tratados abarcan información relativa al proceso de instalación y a su ordenador, incluidas la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos (como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto). Todo ello se trata en el marco de los servicios de actualización con fines de mantenimiento, seguridad y mejora de la infraestructura de backend.

Estos datos se retienen junto con la información de identificación necesaria para las licencias y la facturación, ya que no es necesario identificar al Usuario final. El periodo de retención asciende a cuatro años.

Sistema de Reputación **ESET LiveGrid®.** Trata algoritmos hash unidireccionales relativos a infiltraciones para ejecutar el Sistema de Reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones antimalware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube. Durante este proceso no se identifica al Usuario final.

Sistema de Respuesta **ESET LiveGrid®.** Muestras sospechosas y metadatos que forman parte del sistema de

respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe

- Infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;
- Archivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

La información obtenida y tratada con el Sistema de Respuesta ESET LiveGrid® se debe utilizar sin identificar al Usuario final.

Soporte técnico. La información de contacto o licencia y los datos contenidos en sus solicitudes de asistencia pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Podemos pedirle que nos facilite otra información para facilitar el servicio de asistencia. Los datos tratados para ofrecer asistencia técnica se almacenan durante cuatro años.

Si la persona que utiliza nuestros productos o servicios no es el Usuario final que ha adquirido el producto o servicio ni ejecutado los Términos con ESET (como un empleado o familiar del Usuario final o una persona autorizada por este para utilizar el producto o servicio en virtud de los Términos, el tratamiento de los datos se llevará a cabo según el interés legítimo de ESET conforme al artículo 6 1) f) del RGPD. De este modo, la persona autorizada por el Usuario final podrá utilizar nuestros productos y servicios en virtud de los Términos.

Información de contacto

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk