Guía de Seguridad de las TIC
CCN-STIC 885G

Guía de configuración segura para Microsoft Defender para Office 365

JUNIO 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.07.23 13:10:22 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-252-8
Fecha de Edición: junio de 2024

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. MICROSOFT DEFENDER PARA OFFICE 365

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración segura y despliegue de *Microsoft Defender para Office 365* cumpliendo con los requisitos *Esquema Nacional de Seguridad*.

1.2 DEFINICIÓN DE LA SOLUCIÓN

Microsoft Defender para Office 365 forma parte de la suite de seguridad integrada Microsoft Defender XDR (anteriormente Microsoft 365 Defender).

Microsoft Defender para Office 365 protege la organización contra las amenazas malintencionadas que suponen los mensajes de correo electrónico, los vínculos (URL) y las herramientas de colaboración. También proporciona funcionalidades de investigación, búsqueda y corrección para identificar, priorizar, investigar y responder amenazas de forme eficaz.

Microsoft Defender para Office 365 ofrece:

- **Directivas de protección contra amenazas:** definir directivas de protección contra amenazas para establecer el nivel de protección adecuado para la organización.
- **Informes:** ver informes en tiempo real para supervisar el rendimiento de Microsoft Defender XDR para Office 365 en la organización.
- **Investigación y respuesta de amenazas:** usar las herramientas más avanzadas para investigar, entender, simular y evitar las amenazas.
- **Investigación automatizada y funcionalidades de respuesta:** ahorrar tiempo y esfuerzo al investigar y mitigar las amenazas.

1.2.1 DIRECTIVAS DE PROTECCIÓN CONTRA AMENAZAS

Las directivas definidas por la organización determinan el comportamiento y el nivel de protección para las amenazas predefinidas. Las opciones de directivas son muy flexibles. Por ejemplo, el equipo de seguridad de la organización puede establecer protección contra amenazas específica para el nivel de usuario, organización, destinatario y dominio.

- **Archivos adjuntos seguros**: proporciona protección de día cero para proteger los sistemas de mensajería, comprobando si los archivos adjuntos del correo electrónico contienen contenido malicioso. Dirige todos los mensajes y datos adjuntos que no tienen una firma de virus o malware a un entorno especial y, a continuación, utiliza técnicas de aprendizaje automático y análisis para detectar fines malintencionados. Si no se encuentra ninguna actividad sospechosa, el mensaje se reenvía al buzón.

- **Vínculos seguros**: proporciona verificación del tiempo de clic de las URL, por ejemplo, en mensajes de correo electrónico y archivos de Office. La protección es continua y se aplica en las aplicaciones de Microsoft 365 tanto en Windows como en Mac. Con cada clic los vínculos maliciosos se bloquean de forma dinámica mientras que los vínculos seguros seguirán siendo accesibles.
- **Documentos seguros**: permite examinar documentos de Office abiertos en una vista protegida o también denominada protección de aplicaciones para Office. Protege contra malware y virus desconocidos, proporcionando protección cero tanto en aplicaciones de Microsoft Office 365 como en versiones Office 2004(12730.x) o superior
- **Protección para SharePoint, OneDrive y Microsoft Teams**: protege la organización de Microsoft Office 365 cuando los usuarios colaboran y comparten archivos, identificando y bloqueando archivos maliciosos en sitios de equipo y bibliotecas de documentos.
- **Directivas de protección contra phishing en Microsoft Defender para Office 365**: detecta los intentos de suplantar la identidad de sus usuarios y dominios internos o personalizados. Aplica modelos de aprendizaje automático y algoritmos avanzados de detección de suplantación para evitar ataques de suplantación de identidad.

1.2.2 INFORMES

Los informes se actualizan en tiempo real y proporcionan los detalles más recientes. Estos informes también proporcionan recomendaciones y avisan de amenazas inminentes, permitiendo centrarse en los problemas de alta prioridad.

Los informes predefinidos incluyen:

- Informe de eliminación de mensajes de datos adjuntos seguros
- Informe de estado de protección contra amenazas
- Informe de protección e URL.

Se puede acceder a los informes en el portal de Microsoft Defender XDR https://security.microsoft.com en Informes > Correo electrónico y colaboración > Informes de correo electrónico y colaboración o directamente en https://security.microsoft.com/emailandcollabreport.

1.2.3 INVESTIGACIÓN Y RESPUESTA DE AMENAZAS

El Plan 2 de Microsoft Defender para Office 365 incluye las mejores herramientas de investigación y respuesta de amenazas. Con ellas, el equipo de seguridad de la organización puede anticiparse a ataques malintencionados, entenderlos y evitarlos.

- **Los incidentes** proporcionan información sobre los problemas de ciberseguridad existentes. Por ejemplo, puede verse información sobre el malware más reciente, realizar un seguimiento y ejecutar correcciones.

- **Explorador de amenazas** (o detecciones en tiempo real) es un informe en tiempo real que permite identificar y analizar amenazas recientes. Se puede configurar el Explorador para mostrar los datos de períodos personalizados. Siendo el punto de partida de cualquier analista de seguridad
- **El aprendizaje del simulador de ataques** permite ejecutar escenarios de ataque realistas en la organización para identificar vulnerabilidades. Están disponibles simulaciones de diferentes tipos: cosecha de credenciales, datos adjuntos de malware, vínculos a malware, etc.
- **Investigación y respuesta de amenazas** proporcionan funcionalidades automatizadas de investigación y respuesta para ahorrar tiempo y esfuerzo para correlacionar amenazas de usuarios en riesgo, datos y dispositivos. Se desencadenan cuando se producen ciertas alertas o cuando el equipo de operaciones de seguridad las inicia.

1.3 PROTECCIÓN DEL PUESTO DE TRABAJO

Microsoft Defender XDR (anteriormente Microsoft 365 Defender), es un conjunto de defensa empresarial unificado previo y posterior a la vulneración.

Este sistema coordina de forma nativa la detección, prevención, investigación y respuesta entre puntos de conexión, identidades, correo electrónico y aplicaciones para proporcionar protección integrada contra ataques sofisticados.

Con la solución Microsoft Defender XDR integrada, los profesionales de seguridad pueden unir las señales de amenaza que cada uno de estos productos recibe y determinar el alcance completo y el impacto de la amenaza; cómo entró en el entorno, lo que está afectado y cómo está afectando actualmente a la organización. Microsoft Defender XDR realiza acciones automáticas para evitar o detener el ataque y auto sanar los buzones, workloads, puntos de conexión e identidades de usuario afectados.

El conjunto de servicios de *Microsoft Defender XDR* protege:

- **Puntos de Conexión** con *Microsoft Defender for Endpoint*: Microsoft Defender for Endpoint es una plataforma de extremo unificada para la protección preventiva, la detección posterior a la infracción, la investigación automatizada y la respuesta.
- **Correo electrónico y colaboración** con *Microsoft Defender para Office 365*: protege la organización contra las amenazas malintencionadas que suponen los mensajes de correo electrónico, los vínculos (URL) y las herramientas de colaboración.
- **Identidades** con *Microsoft Defender for Identity y Protección de Microsoft Entra ID*: Microsoft Defender for Identity es una solución de seguridad basada en la nube que aprovecha las señales del Active Directory local, para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a su organización. Protección de Microsoft Entra ID ayuda a las organizaciones a detectar, investigar y corregir los riesgos relacionados con las identidades, que pueden ser utilizados posteriormente en herramientas como Acceso condicional para tomar decisiones de acceso o

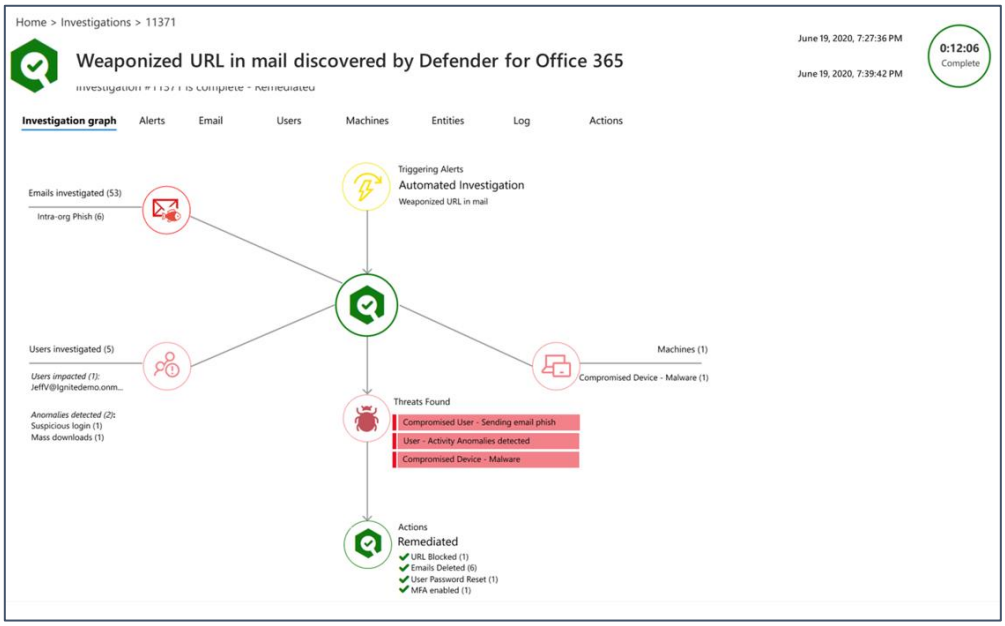
alimentar una herramienta de administración de eventos e información de seguridad (SIEM) para realizar una investigación más detallada.

- **Aplicaciones** con seguridad de *Microsoft Cloud App*: la seguridad de Microsoft Cloud App es una solución completa entre SaaS que ofrece una visibilidad profunda, controles de datos sólidos y una protección contra amenazas mejorada para las aplicaciones en la nube.
- **Administración de vulnerabilidades** ofrece visibilidad continua de los recursos, evaluaciones inteligentes basadas en riesgos y herramientas de corrección integradas para ayudar a los equipos de TI y seguridad a priorizar y abordar vulnerabilidades críticas y configuraciones incorrectas en toda la organización.

Microsoft Sentinel como SIEM/SOAR, es una plataforma de administración de eventos e información de seguridad (SIEM) nativa de la nube que utiliza IA integrada para ayudar a analizar grandes volúmenes de datos en toda una empresa, rápidamente. Microsoft Sentinel agrega datos de todas las fuentes, incluidos usuarios, aplicaciones, servidores y dispositivos que se ejecutan en la infraestructura local o en cualquier nube, lo que te permite razonar sobre millones de registros en unos segundos, permitiendo crear construir playbooks para dar una respuesta efectiva e inmediata.

1.3.1 INTEGRACIÓN CON MICROSOFT DEFENDER XDR

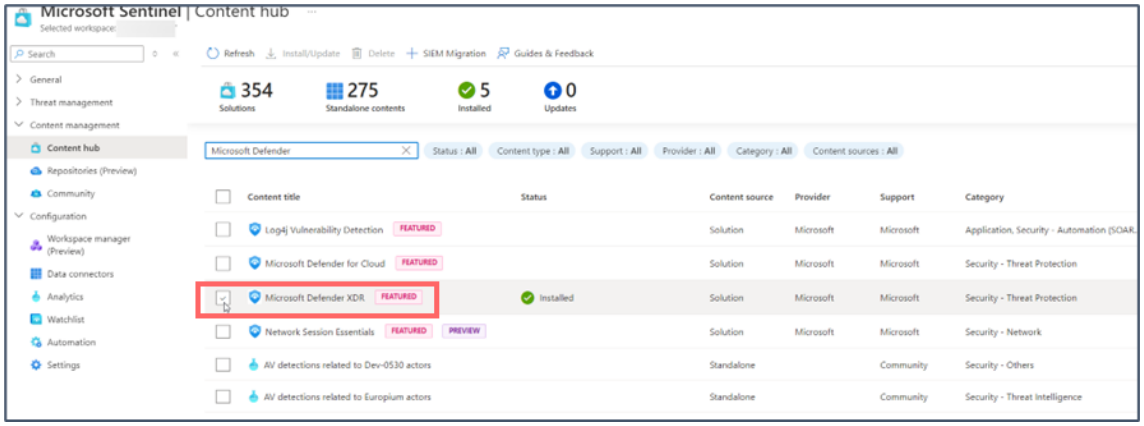
La integración de *Microsoft Defender para Office 365* con *Microsoft Defender XDR* ayuda al equipo de operaciones de seguridad a supervisar y tomar medidas rápidamente cuando los dispositivos de los usuarios estén en riesgo. Por ejemplo, se podrán ver los dispositivos potencialmente afectados por un incidente en un mensaje de correo electrónico, así como cuántas alertas recientes se generaron para esos dispositivos en *Microsoft Defender for Endpoint*.



* En este ejemplo, puede verse como la integración de todas las soluciones de Microsoft Defender XDR se correlacionan entre sí, ante varias alertas que se integran en un único incidente. Identificando tanto las identidades y los dispositivos ante una amenaza detectada en Microsoft Defender para Office 365.

1.3.2 INTEGRACIÓN CON MICROSOFT SENTINEL

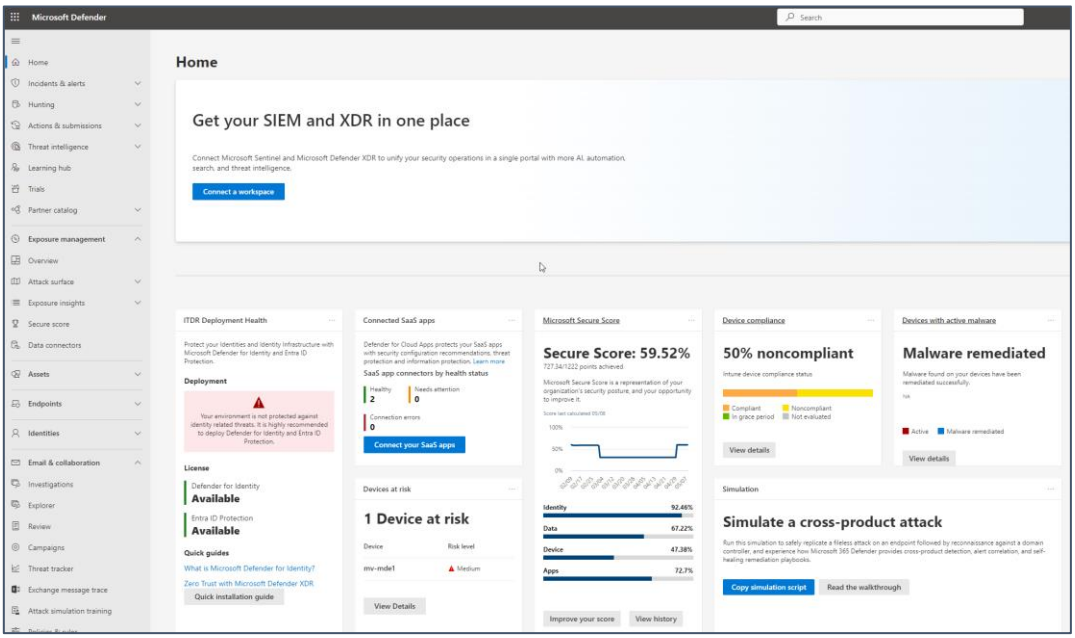
A través del centro de contenido (Content hub), **Microsoft Sentinel** genera la integración con **Microsoft Defender XDR** (M365XDR) permitiendo transmitir todos los incidentes y alertas de M365XDR a Microsoft Sentinel y manteniendo todos los incidentes sincronizados entre ambos portales. Los incidentes de M365XDR incluyen todas sus alertas, entidades y otra información relevante de todos los servicios que lo componen.



* Consultar: [CCN-STIC- 884E- Guía de configuración segura para Azure Sentinel].

1.4 FUNCIONALIDADES DEL PORTAL

El acceso a las funcionalidades de Microsoft Defender para Office 365 se realiza desde el portal mejorado de seguridad de Microsoft Defender XDR, accediendo a la siguiente URL:https://security.microsoft.com/

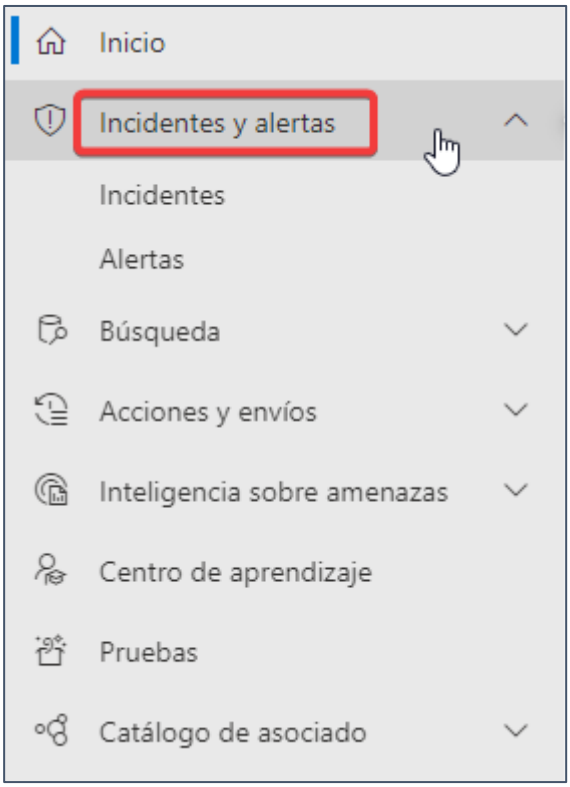


El nuevo portal de *Microsoft Defender XDR*, reúne las funcionalidades que solían estar en portales independientes en un solo lugar, de modo que pueda protegerse de una manera más sencilla y centralizada de cualquier tipo de amenaza.

Desde un punto de vista genérico, en este portal puede realizarse distintas acciones relacionadas con la defensa empresarial (detección, prevención, investigación y respuesta entre *endpoints*, identidades, correo electrónico, workloads y aplicaciones) e integrase con Microsoft Sentinel y Microsoft Defender for Cloud.

1.4.1 INVESTIGAR INCIDENTES Y RESPONDER A AMENAZAS

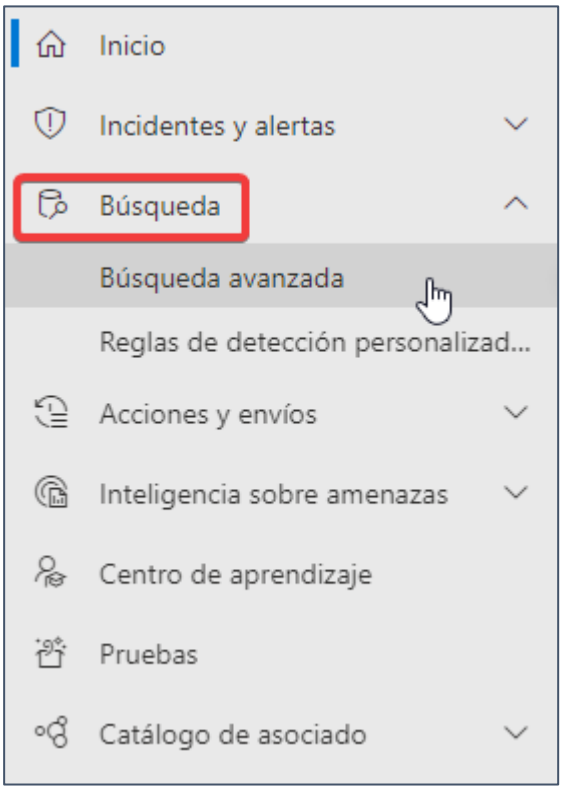
Las alertas están categorizadas, combinadas y correlacionadas en incidentes completos.



- **Incidentes:** Muestra una lista de incidentes de seguridad, con opciones para investigar, clasificar y resolver cada incidente.
- **Alertas**: Proporciona una lista detallada de alertas individuales. Se visualiza la fuente de la alerta, la descripción y tomar acciones como la investigación adicional o la resolución.

1.4.2 BUSCAR AMENAZAS DE MANERA PROACTIVA

Mediante la creación de consultas avanzadas se permite buscar amenazas en correos electrónicos y elementos de colaboración.



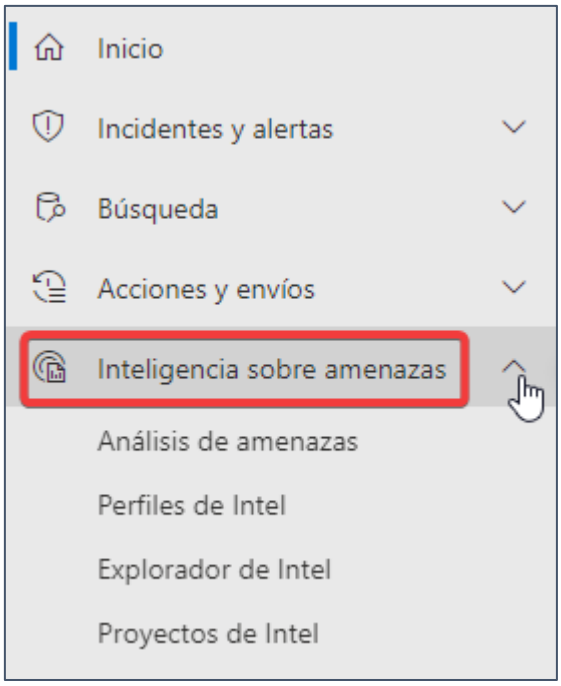
- **Busqueda avanzada:** herramienta que permite crear consultas personalizadas utilizando un lenguaje de consulta avanzado para buscar indicadores de compromiso (IOC) y actividades sospechosas en los datos recopilados por la plataforma.

1.4.3 REALIZAR UN SEGUIMIENTO Y RESPONDER A LAS AMENAZAS EMERGENTES

Microsoft Defender Threat Intelligence (Defender TI) permite acceder a la información sobre amenazas desde el portal de Microsoft Defender.

Microsoft Defender TI ayuda a agilizar el triaje de los analistas de seguridad, la respuesta a incidentes, la caza de amenazas y los flujos de trabajo de gestión de vulnerabilidades. Defender TI agrega y enriquece la información crítica sobre amenazas en una interfaz fácil de usar.

Este cambio introduce un nuevo menú de navegación dentro del portal de Microsoft Defender denominado Inteligencia de amenazas.

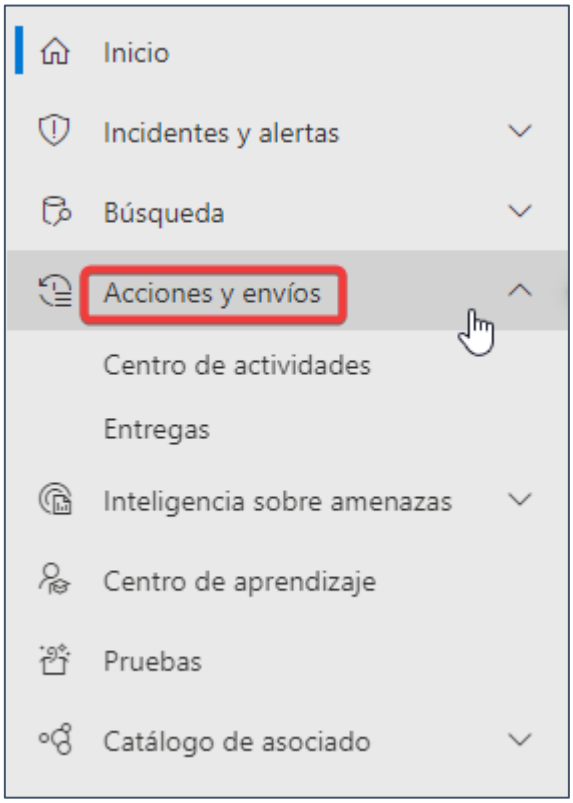


En el menú de Inteligencia de amenazas existe la función **Análisis de amenazas** que está diseñado para ayudar a los equipos de seguridad a ser más eficientes y dos nuevas funcionalidades:

- **Perfiles Intel:** una nueva característica que facilita información sobre contenido de actores de amenazas, sus herramientas y vulnerabilidades conocidas.
- **Explorador de Intel**: proporciona la experiencia existente de búsqueda e investigación de contenidos de TI de Defender.

1.4.4 SUPERVISAR LAS ACCIONES Y EL ESTADO DE INVESTIGACIÓN

Está enfocado en la gestión de acciones de seguridad y la administración de archivos o elementos sospechosos que han sido enviados para su análisis. Aquí se describen las principales funciones y submenús que típicamente se encuentran en esta sección:



- **Actions(Acciones):** esta sección se encarga de gestionar las acciones recomendadas y las tareas de respuesta a incidentes de seguridad. Incluye:
  - **Pending Actions (Acciones Pendientes):** muestra una lista de todas las acciones de seguridad recomendadas que aún no se han completado. Estas acciones pueden incluir tareas como aislar un dispositivo, ejecutar un análisis completo, aplicar parches de seguridad, o eliminar software malicioso. Cada acción pendiente suele incluir detalles como el tipo de amenaza, el dispositivo afectado, y la urgencia de la acción recomendada.
  - **Completed Actions (Acciones Completadas):** registra todas las acciones que han sido llevadas a cabo en respuesta a alertas o recomendaciones. Esto permite a los administradores de seguridad revisar qué medidas se han tomado y verificar que las respuestas adecuadas se han implementado correctamente.

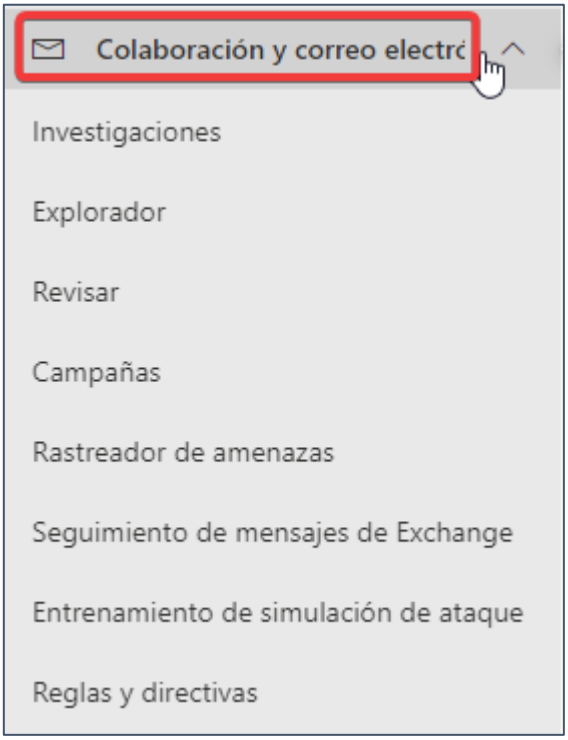
- **Submissions(envios):** permite a los usuarios enviar archivos sospechosos o URLs para un análisis más profundo por parte de Microsoft. Esta función es

crucial para gestionar posibles falsos positivos y obtener una comprensión más clara de las amenazas detectadas.

- **File Submissions (Envío de Archivos):** los usuarios envían archivos sospechosos directamente a Microsoft para su análisis detallado. Esto puede ser útil cuando hay dudas sobre si un archivo es realmente malicioso o no. Microsoft proporciona un análisis detallado y una respuesta sobre la naturaleza del archivo enviado.
- **URL Submissions (Envío de URLs):** similar a los envíos de archivos, esta función permite enviar URLs sospechosas para su análisis. Esto ayuda a identificar si una URL conduce a un sitio web malicioso o a un posible ataque de phishing.
- **Submission History (Historial de Envíos):** proporciona un registro de todos los archivos y URLs que se han enviado para análisis, junto con el estado y los resultados de esos análisis. Esto ayuda a los equipos de seguridad a mantener un seguimiento de lo que se ha revisado y las conclusiones obtenidas

1.4.5 PROTEGER OFFICE 365

Ofrece herramientas y recursos para gestionar la seguridad del correo electrónico y la colaboración. Los administradores pueden investigar incidentes, explorar datos, revisar alertas e incidentes, y gestionar políticas y reglas de seguridad.



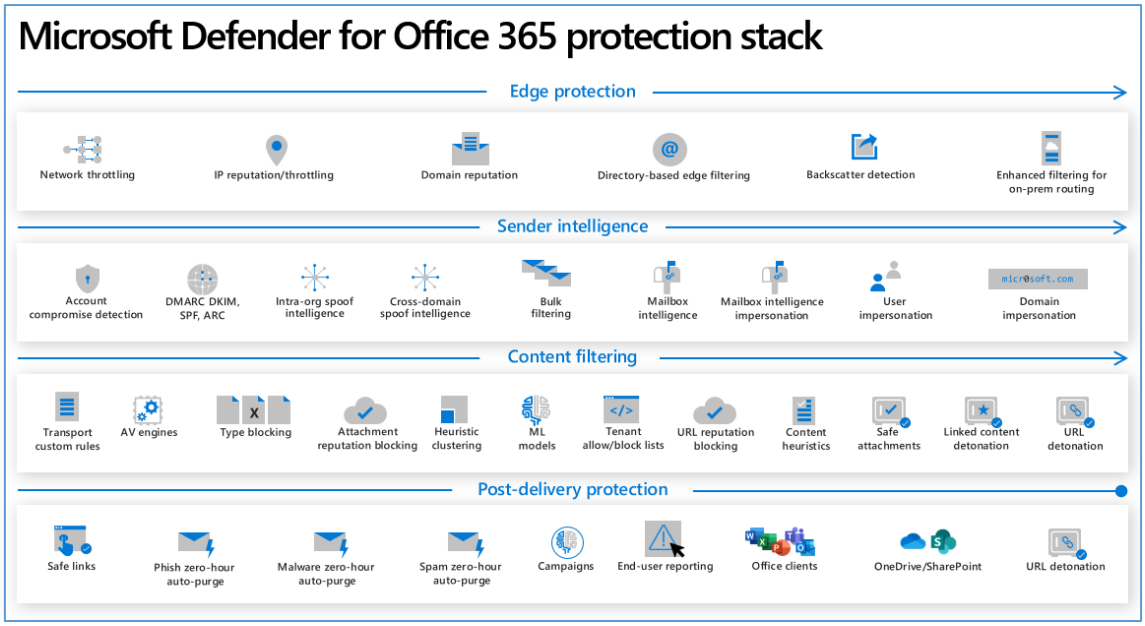
- **Investigations (Investigaciones):** proporciona detalles sobre incidentes detectados, permite analizar la cadena de eventos, identificar usuarios afectados, y documentar las acciones de respuesta tomadas.

- **Explorer (Explorador):** busca y visualiza eventos de seguridad relacionados con correos electrónicos y colaboración, filtrar por diferentes criterios y obtener detalles específicos sobre amenazas detectadas.
- **Review (Revisión):** lugar centralizado para revisar correos electrónicos y actividades de colaboración marcadas como sospechosas, facilitando la evaluación y toma de decisiones sobre las acciones a seguir.
- **Campaigns (Campañas):** detalla las campañas de phishing, malware y otras amenazas dirigidas a la organización, incluyendo objetivos, métodos de ataque y alcance de la campaña.
- **Threat Tracker (Rastreador de Amenazas):** proporciona actualizaciones y seguimientos sobre amenazas activas, permitiendo a los equipos de seguridad mantenerse informados sobre las amenazas emergentes y en curso.
- **Exchange Message Trace (Rastreo de Mensajes de Exchange):** rastrea el flujo de correos electrónicos dentro de la organización, desde el remitente hasta el destinatario, identificando posibles problemas de entrega y actividades sospechosas.
- **Attack Simulation Training (Entrenamiento de Simulación de Ataques):** crea y ejecuta simulaciones de ataques de phishing y otros vectores de amenazas para entrenar a los empleados y mejorar la conciencia de seguridad dentro de la organización.
- **Policies & Rules (Políticas y Reglas):** permite definir, aplicar y gestionar políticas de seguridad específicas para correo electrónico y plataformas de colaboración, estableciendo reglas para detectar y responder a amenazas.

1.5 FASES DE PROTECCIÓN DE MICROSOFT DEFENDER PARA OFFICE 365

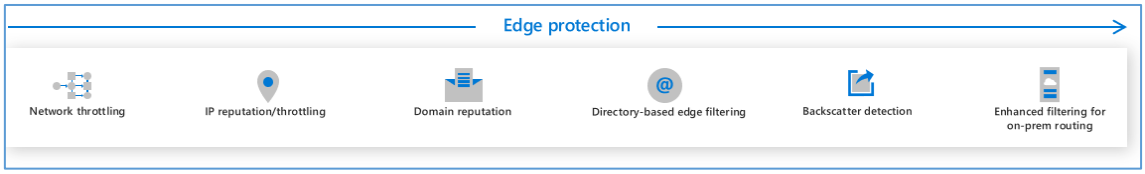
En esta sección se verá como la pila de protección de *Microsoft Defender para Office 365*, puede proteger la organización frente amenazas de seguridad. Esta pila de protección puede dividirse en 4 fases. En general, el correo entrante pasa a través de todas estas fases antes de la entrega.

* Esta información que a continuación se describe es útil para entender la configuración de las medidas de seguridad reflejadas en el apartado [3.1.2.1 Protección frente a código dañino].



* En las siguientes secciones se explican los distintos componentes con su terminología en inglés para no perder la referencia de los tecnicismos utilizados en la documentación de Microsoft.

FASE 1: PROTECCIÓN PERIMETRAL



Desafortunadamente, los bloques perimetrales que antes eran cruciales ahora son relativamente sencillos de superar. Con el tiempo, se bloquea menos tráfico aquí, pero sigue siendo una parte importante de la pila de protección.

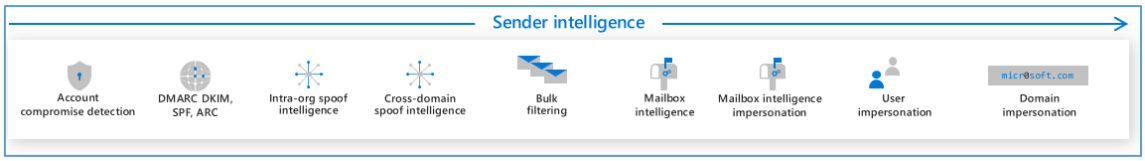
Los bloques perimetrales están diseñados para ser automáticos. En el caso de falso positivo, se notificará a los remitentes y se les indicará cómo solucionar su problema.

- **Network throttling**. La limitación de red protege la infraestructura de Office 365 infraestructura y clientes de ataques por denegación de servicio (DOS)

limitando el número de mensajes que puede enviar un conjunto específico de infraestructura.

- **IP reputation and throttling**. La reputación y la limitación de IP bloquearán los mensajes que se envían desde direcciones IP de conexión no válidas conocidas. Si una dirección IP específica envía muchos mensajes en un breve período de tiempo, se limitarán.
- **Domain reputation**. La reputación del dominio bloqueará los mensajes que se envíen desde un dominio sospechoso.
- **Directory-based edge filtering**. El filtro perimetral basado en directorios bloquea los intentos de recopilar información de directorio de una organización a través de SMTP.
- **Backscatter detection.** Detección de devolución impide que una organización sea atacada a través de informes de "no entregados" (NDR) no válidos.
- **Enhanced filtering for connectors.** El filtrado mejorado para conectores conserva la información de autenticación incluso cuando el tráfico pasa a través de otro dispositivo antes de que llegue a Office 365. Esto mejora la precisión de la pila de filtrado, incluso en escenarios de enrutamiento complejos o híbridos.

FASE 2: INTELIGENCIA DE REMITENTE

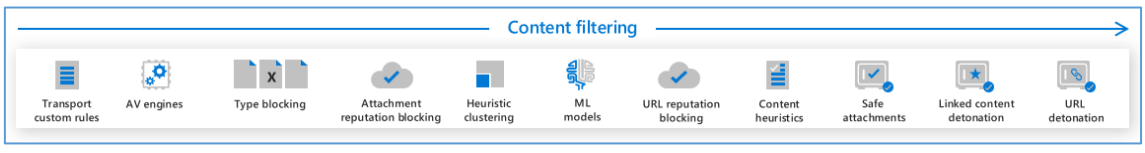


Las características de la *inteligencia de remitente* son fundamentales para capturar mensajes de correo no deseado, masivos, y de suplantación. La mayoría de estas características se pueden configurar individualmente.

- **Account compromise detection.** Los disparadores y alertas de detección de cuentas comprometidas se desencadenan cuando una cuenta tiene un comportamiento anómalo que puede llevar a una situación de riesgo. En algunos casos, la cuenta de usuario se bloquea e impide enviar más mensajes de correo electrónico hasta que el equipo de operaciones de seguridad de la organización resuelva el problema.
- **Email Authentication. La autenticación de correo electrónico involucra métodos** configurados en el cliente y métodos configurados en la nube, destinados a garantizar que los remitentes sean remitentes autorizados y auténticos. Estos métodos resisten la suplantación.
    - **SPF** puede rechazar correos basados en registros TXT DNS que listan direcciones IP y servidores permitidos para enviar correo en nombre de la organización.
    - **DKIM** proporciona una firma cifrada que autentica al remitente.
    - **DMARC** permite a los administradores marcar SPF y DKIM según sea necesario en su dominio y fuerza la alineación entre los resultados de estas dos tecnologías.

  - **ARC** no está configurado por el cliente, pero se basa en DMARC para trabajar con el reenvío en listas de correo, mientras se registra una cadena de autenticación.
- **Spoof intelligence**. La inteligencia suplantación de identidad es capaz de filtrar aquellos emails de remitentes malintencionados que imitan dominios externos conocidos u organizaciones. Separa el correo legítimo "en nombre de" de los remitentes que suplantan la identidad para entregar mensajes de *spam* o *phishing*.
- **Intra-org spoof intelligence**. Inteligencia contra la suplantación de identidad dentro de la organización detecta y bloquea los intentos de suplantación de identidad de un dominio dentro de la organización.
- **Cross-domain spoof intelligence**. Inteligencia contra la suplantación de identidad entre dominios detecta y bloquea los intentos de suplantación de identidad de un dominio fuera de la organización.
- **Bulk filtering**. El filtrado masivo permite a los administradores configurar un nivel de confianza masivo (BCL) que indica si el mensaje se envió desde un remitente masivo. Los administradores pueden usar el control deslizante masivo en la directiva contra correo no deseado para decidir qué nivel de correo masivo tratar como correo no deseado.
- **Mailbox intelligence**. Inteligencia de buzones aprende del comportamiento estándar del correo electrónico del usuario. Aprovecha el flujo de comunicación de un usuario para detectar cuándo un remitente parece ser alguien con el que el usuario suele comunicarse, pero en realidad es malintencionado.
- **Mailbox intelligence impersonation**. La suplantación de inteligencia de buzones habilita o deshabilita los resultados de suplantación mejorados en función del mapa de remitentes individuales de un usuario.
- **User impersonation**. La suplantación de usuario permite a un administrador crear una lista de objetivos de alto valor estratégico susceptibles de ser suplantados. Si llega un correo donde el remitente parece tener el mismo nombre y dirección que la cuenta de valor protegida, el correo se marca o etiqueta. (Por ejemplo, trαcye@contoso.com para tracye@contoso.com).
- **Domain impersonation**. La suplantación de dominio detecta dominios que son similares al dominio del destinatario y que intentan parecer un dominio interno. Por ejemplo, tracye@liwαre.com para tracye@litware.com.

FASE 3: FILTRADO DE CONTENIDO



En esta fase, la pila de filtrado comienza a controlar el contenido específico del correo, incluidos sus hipervínculos y datos adjuntos.

- **Transport rules**. Las reglas de transporte (también conocidas como reglas de flujo de correo o reglas de transporte Exchange) permiten que un

administrador lleve a cabo una amplia variedad de acciones cuando se cumple una amplia gama de condiciones para un mensaje. Todos los mensajes que fluyen a través de la organización se evalúan con las reglas de flujo de correo /reglas de transporte habilitadas.

- **Microsoft Defender Antivirus** junto con un motor de antivirus de terceros se usan para detectar todo el malware conocido en los datos adjuntos. Los motores antivirus (**AV engines**) pueden bloquear datos adjuntos de los tipos especificados por el administrador. Para obtener la lista de tipos de archivo admitidos, puede consultar el siguiente enlace: https://learn.microsoft.com/es-es/defender-office-365/anti-malware-protection-about#true-type-matching-in-the-common-attachments-filter
- Siempre que Microsoft Defender para Office 365 detecta datos adjuntos malintencionados, el hash del archivo y un hash de su contenido activo se agregan a la reputación de Exchange Online Protection (EOP). El bloqueo de reputación de datos adjuntos (**attachment reputation blocking**) bloqueará ese archivo en todo Office 365, y en los puntos de conexión.
- **Heuristic clustering**. La agrupación heurística puede determinar que un archivo es sospechoso en función de la heurística de entrega. Cuando se encuentra un archivo adjunto sospechoso, toda la campaña se pausa y el archivo se aísla. Si se encuentra que el archivo es malintencionado, se bloquea toda la campaña.
- **Machine learning models**. Modelo de aprendizaje automático actúa sobre el encabezado, el contenido del cuerpo y las direcciones URL de un mensaje para detectar intentos de suplantación de identidad.
- Microsoft utiliza la reputación de esas URL aisladas, así como la reputación de URL de terceras fuentes en el bloqueo de reputación de direcciones URL (**URL reputation blocking**), para bloquear cualquier mensaje con una dirección URL malintencionada conocida.
- **Content heuristics**. Los heurísticos de contenido pueden detectar mensajes sospechosos en función de la estructura y la frecuencia de palabras dentro del cuerpo del mensaje, mediante modelos de aprendizaje automático.
- **Safe Attachments** aísla los datos adjuntos de los clientes de Microsoft Defender para Office 365, usando análisis dinámico para detectar amenazas nunca vistas.
- **Linked content detonation**. Detonación de contenido vinculado trata todas las direcciones URL que se vinculan a un archivo de un correo electrónico como datos adjuntos, creando de forma asincrónica un espacio aislado en el archivo en el momento de la entrega.
- **URL Detonation**. La detonación de URL se produce cuando la tecnología antiphishing detecta que un mensaje o una dirección URL son sospechosos, y aísla las direcciones URL del mensaje en el momento de la entrega.

FASE 4: PROTECCIÓN POSTERIOR A LA ENTREGA

La última fase tiene lugar después de la entrega de correo o archivo, actuando en correos que se encuentran en distintos buzones, o archivos y vínculos que aparecen en clientes tales como Microsoft Teams.

- **Safe Links**. Vínculos seguros es la protección de tiempo de hacer clic (time-of-click) de Microsoft Defender para Office 365. Cada dirección URL de cada mensaje se ajusta para apuntar a servidores de vínculos seguros de Microsoft (Microsoft Safe Links servers). Cuando se hace clic en una dirección URL, se comprueba con la reputación más reciente del destino, antes de redirigir al usuario.
- **Zero-hour auto purge (ZAP) for phishing**. La purga automática de hora cero (ZAP) para la suplantación de identidad (phishing) detecta y neutraliza de forma retroactiva los mensajes de suplantación de identidad malintencionados que ya se han entregado Exchange Online buzones de correo.
- **ZAP for malware**. ZAP para malware detecta y neutraliza de forma retroactiva los mensajes malintencionados de malware que ya se han entregado a buzones de Exchange Online.
- **ZAP for phishing**. ZAP para la suplantación de identidad (phishing) detecta y neutraliza de forma retroactiva los mensajes de correo no deseado malintencionados que ya se han entregado a los buzones de Exchange Online.
- **Campaign Views**. Las vistas de campañas permiten a los administradores ver la imagen general de un ataque, de manera más rápida y completa de lo que cualquier equipo podría sin automatización. Microsoft aprovecha las grandes cantidades de datos contra suplantación de identidad (phishing), antispam y antimalware en todo el servicio para ayudar a identificar las campañas y, a continuación, permite a los administradores investigarlas de principio a fin, incluidos los destinos, los impactos y los flujos.
- **The Report Message add-ins**. Los complementos de mensaje de informe permiten a los usuarios notificar fácilmente falsos positivos (correo electrónico válido marcado erróneamente como negativo) o falsos negativos (correo electrónico erróneo marcado como bueno) a Microsoft para su análisis posterior.
- **Safe Links for Office clients**. Vínculos seguros para clientes de Office ofrece de forma nativa la misma protección de tiempo de clic que “Safe Links”, dentro de clientes de Office como Word, PowerPoint y Excel.
- **Protection for OneDrive, SharePoint, and Teams**. La protección para OneDrive, SharePoint y Teams ofrece la misma protección de datos adjuntos seguros, de forma nativa, dentro de OneDrive, SharePoint y Microsoft Teams.

- **Cuando** una URL que apunta a un fichero se selecciona, después de la entrega, la detonación de contenido vinculado (**linked content detonation**) muestra una página de advertencia hasta que se completa el aislamiento del archivo y se encuentra que la dirección URL es segura.

1.6 PLANIFICACIÓN DE LA SEGURIDAD

Desde el punto de vista de la planificación, pueden seguirse distintas estrategias de seguridad, por ejemplo, utilizando las políticas por defecto y usando la protección standard o la estricta de forma sencilla, o bien configurando de manera más personalizada las distintas opciones de seguridad en este portal. Una manera lógica de abordar esta segunda estrategia podría ser:

- Configurar todo con "anti" en el nombre.
  - **Antimalware**
  - **Anti-phishing**
  - **Anti-spam** (protección contra correo electrónico no deseado)
- Configurar todo con "seguro" en el nombre.
  - **Vínculos seguros**
  - **Archivos adjuntos seguros**
- Securizar *workloads* (ej. SharePoint Online, OneDrive y Teams)
- Proteger con purga automática de hora cero (ZAP – *zero hour auto purge*).

Para obtener más información sobre dicha configuración consultar la sección [1.5 Fases de protección de Microsoft Defender para Office 365] donde se explican las distintas fases de la pila de protección de Microsoft Defender para Office 365, y la sección [3.1.2.1 Protección frente a código dañino] donde se configuran las opciones más relevantes para una configuración *estricta* de la seguridad.

Microsoft facilita una guía de onboarding para Microsoft Defender para Office 365 en el siguiente enlace

https://admin.microsoft.com/Adminportal/Home?Q=ADG#/modernonboarding/office365advancedthreatprotectionadvisor

1.7 LICENCIAMIENTO Y PLANES

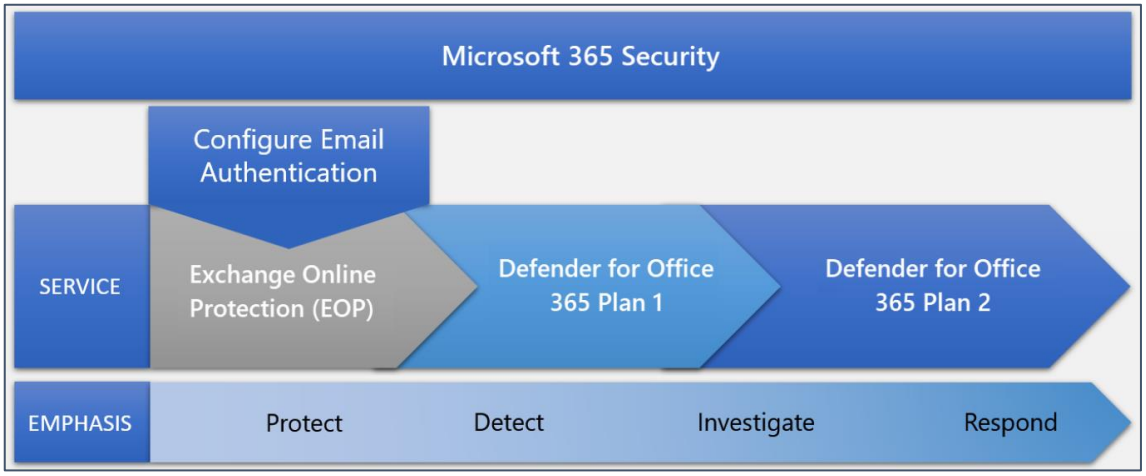
Todas las suscripciones de Microsoft 365 cuentan con funcionalidades de seguridad. Los objetivos y acciones que puede realizar dependen del foco de las diferentes suscripciones. En Microsoft Defender para Office 365, existen tres servicios (o productos) de seguridad principales vinculados al tipo de suscripción:

a) Exchange Online Protection (EOP)
b) Microsoft Defender para Office 365 Plan 1
c) Microsoft Defender para Office 365 Plan 2

Microsoft Defender para Office 365 se fundamenta sobre las principales protecciones que ofrece EOP. EOP siempre está presente en todas las suscripciones de Microsoft Defender para Office 365.

EOP	Microsoft Defender para Office 365 Plan 1	Microsoft Defender para Office 365 Plan 2
Evita ataques generales conocidos basados en el volumen.	Protege al correo electrónico y a la colaboración de la vulnerabilidad de día cero contra los ataques de malware y suplantación de identidad (phishing) que ponen en peligro al correo electrónico empresarial.	Agrega investigación, búsqueda y respuesta después de la vulneración, así como automatización y simulación (para el aprendizaje).

El núcleo de la seguridad de Microsoft 365 es la protección EOP. Microsoft Defender para Office 365 Plan 1 contiene EOP. Microsoft Defender para Office 365 Plan 2 contiene Plan 1 y EOP. La estructura es acumulativa. Es por ello por lo que, al configurar este producto, se debería empezar con EOP y continuar hasta Microsoft Defender para Office 365.



En cuanto al licenciamiento:

- EOP se incluye con cualquier suscripción que incluya Exchange Online y como suscripción independiente para proteger entornos de correo electrónico locales.
- Microsoft Defender para Office 365 plan 1 se ofrece de manera independiente a través de un complemento o con otro tipo de licenciamiento como por ejemplo puede ser Microsoft 365 Business o Microsoft 365 Enterprise E3.
- Microsoft Defender para Office 365 plan 2, también se ofrece de manera independiente a través de un complemento y en determinadas suscripciones

que incorporan medidas de seguridad más avanzadas, como pueden ser Microsoft 365 E5 o Microsoft 365 A5.

La siguiente tabla es un resumen de lo que se incluye en cada plan:

Funcionalidades segun licenciamiento		
EOP	**Plan 1 de Microsoft Defender para Office 365**	**Plan 2 de Microsoft Defender para Office 365**

Prevención y detección:
• Protección contra malware, correo no deseado, correo electrónico masivo y suplantación de identidad
• Protección contra correo no deseado
• Filtrado de conexión y de correo no deseado
• Directivas de cuarentena
• Detección de falsos positivos
• Lista de permitidos y bloqueados según:
  ○ Dominios
  ○ Direcciones de correo
  ○ URLs
  ○ Archivos
Investigación y respuesta:
• Informes y auditoria de seguridad
• Seguimiento de mensajes
• Purga automática hora cero (ZAP),
• Refinamiento de listas permitidos y bloqueados
	Capacidades EOP
	--- **además** ---
	
	Prevención y detección:
	• Directivas contra suplantación de identidad con protección contra suplantación y umbrales avanzados de suplantación de identidad
	• Datos adjuntos seguros, incluidos los datos adjuntos seguros para SharePoint, OneDrive y Microsoft Teams
	• Vínculos seguros
	Investigación y respuesta:
	• Detecciones en tiempo real
	• Entidad de correo electrónico
		Capacidades del Plan 1 de Microsoft Defender para Office 365
		--- **además** ---
		Prevención y detección:
		• Aprendizaje de simulación de ataque
		
		Investigación y respuesta:
		• Rastreadores de amenazas
		• Explorador de amenazas
		• AIRE
		• Búsqueda proactiva de amenazas con la búsqueda avanzada en Microsoft Defender XDR
		• Investigación de incidentes en Microsoft Defender XDR
		• Investigación de alertas en Microsoft Defender XDR

2. CONFIGURACIÓN SEGURA PARA MICROSOFT DEFENDER PARA OFFICE 365

2.1 MARCO OPERACIONAL

2.1.1 CONTROL DE ACCESO

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

2.1.1.1 IDENTIFICACION

La gestión de identidades de Microsoft Entra ID es común para el acceso a todas las funcionalidades de todo Microsoft 365, lo que también incluye Microsoft Defender para Office 365 y se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

2.1.1.2 REQUISITOS DE ACCESO

Según el ENS, los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Además, todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

El ENS recomienda bloquear recursos para personas que no necesiten utilizarlo, reduciendo así la superficie de exposición. La mayoría de los ataques en la actualidad están relacionados con el phishing, y las cuentas de menor privilegio suelen ser comprometidas con mayor facilidad, por lo que si esas cuentas tuvieran privilegios de administración supondrían un importante agujero de seguridad. De ahí que se deba utilizar el principio de *menor privilegio* y el Just In Time mediante la opción de Microsoft Entra Privileged Identity Managament que proporciona la opción de obtener los privilegios, única y exclusivamente en el momento que verdaderamente se necesiten

Los permisos del portal de Microsoft Defender XDR se basan en el modelo de permisos de control de acceso basado en roles (RBAC) proporcionando una única experiencia de administración de permisos en una ubicación central. RBAC es el mismo modelo de permisos que se usa en la mayoría de los servicios de Microsoft 365, por lo que sí está familiarizado con la estructura de permisos de estos servicios, le resultará sencillo conceder permisos en el portal de Microsoft Defender XDR.

* Más información en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

Para obtener acceso a las características de *Microsoft Defender para Office 365*, se debe tener asignado el rol adecuado. En la tabla siguiente se incluyen algunos ejemplos:

Roles necesarios para usar las características de Microsft Defender para Office 365	
Role o grupo de roles	**Descripción**
Administrador global	Acceso a todas las características administrativas en todos los servicios de Microsoft 365. Los administradores globales son los únicos que pueden asignar otros roles de administrador. Para más información, consultar Administrador global / Administrador de empresa.
Administrador de seguridad	Controla la seguridad global de la organización mediante la administración de directivas de seguridad, la revisión de análisis de seguridad y los informes en los productos de Microsoft 365, Para más información, consultar Administrador de seguridad.
Lector Global	La versión de solo lectura del rol de Administrador global. Ver todas las configuraciones e información administrativa en Microsoft 365. Para más información, consultar Lector global.
Administrador de simulación de ataques	Crea y administra todos los aspectos de la creación de simulación de ataques, el lanzamiento o la programación de la simulación y la revisión de los resultados de la misma. Para más información, consulte Administrador de simulación de ataque.
Administrador de datos de cumplimiento	Realizar un seguimiento de los datos de su organización a través de Microsoft 365, asegurarse de que están protegidos y obtener información sobre los problemas para ayudar a reducir los riesgos. Para obtener más información, consultar Administrador de datos de cumplimiento.

Para administrar permisos la cuenta debe ser de *administrador global en Microsoft Entra ID* o un miembro del grupo de roles de *Administración de la organización* en el portal de Microsoft defender XDR. En concreto, el rol de *Administración de roles* permite a los usuarios ver, crear y modificar grupos de roles en el portal de Microsoft Defender XDR y, de forma predeterminada, ese rol solo se asigna al grupo de roles Administración de la organización.

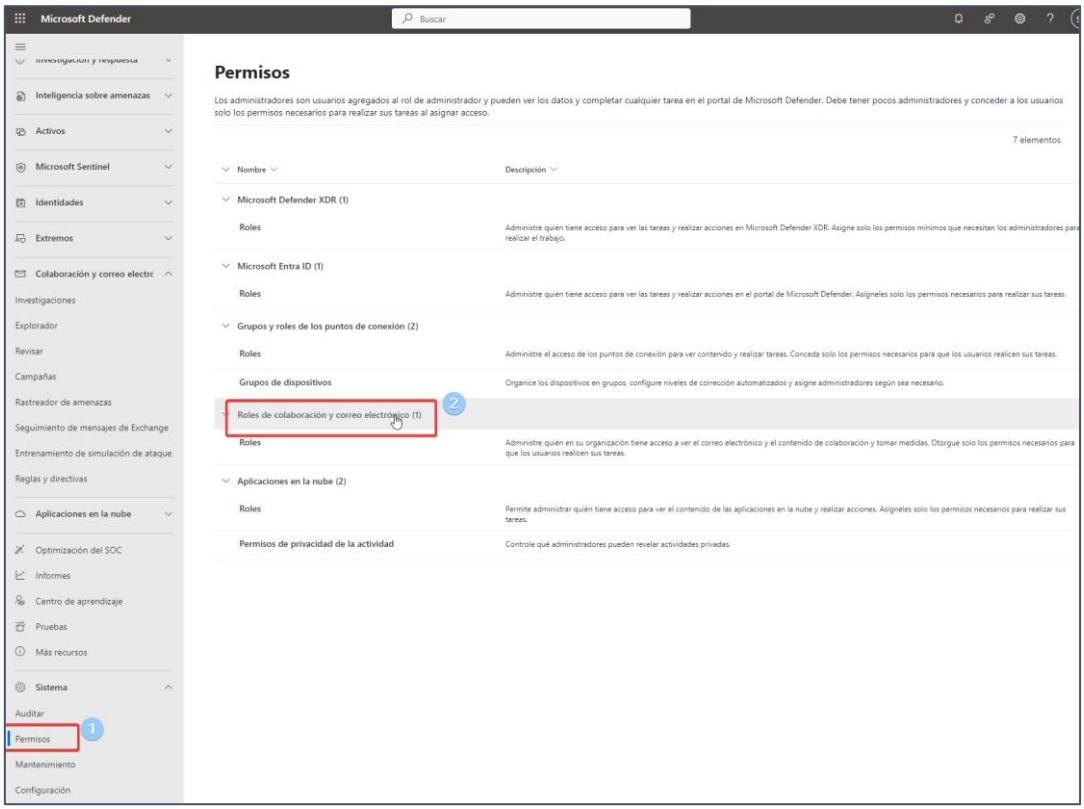
2.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Como determina el ENS, el sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.

Se necesita flexibilidad para dar permisos de administrador adecuados a las personas de la organización, para ello, desde el portal de Microsoft Defender XDR en https://security.microsoft.com se administran directamente permisos para los usuarios que realizan tareas de seguridad en Microsoft 365. Al usar el portal de Microsoft Defender XDR para administrar los permisos, se centralizan estas tareas relacionadas con la seguridad.

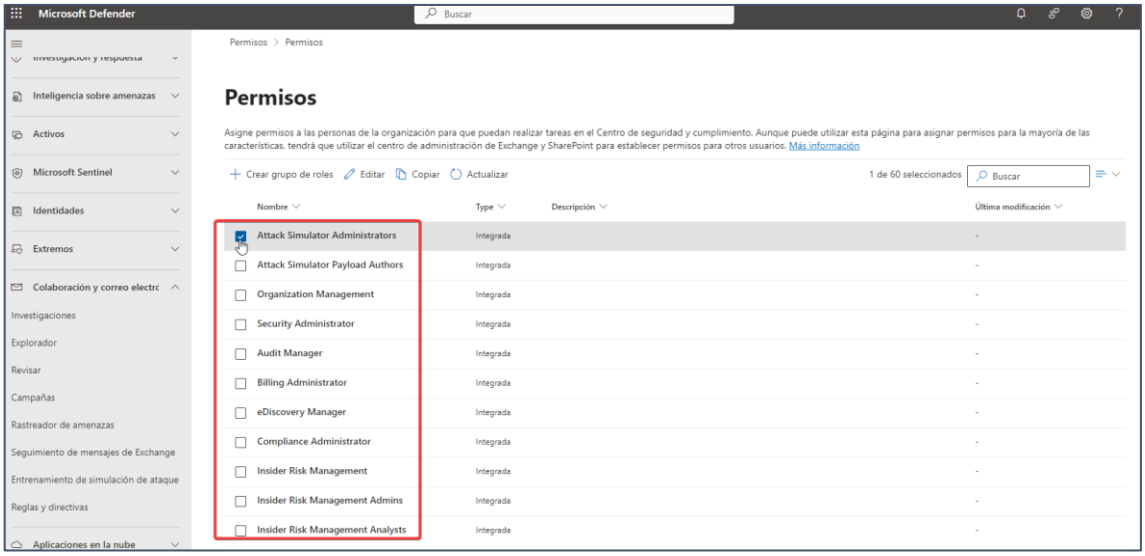
A continuación, se describe como asignar roles relacionados con *Microsoft Defender para Office 365* y el *Centro de Seguridad y Cumplimiento* de Microsoft 365.

1. Desde el portal de Microsoft Defender XDR, acceder a [Permisos], o accediendo al enlace: https://security.microsoft.com/securitypermissions



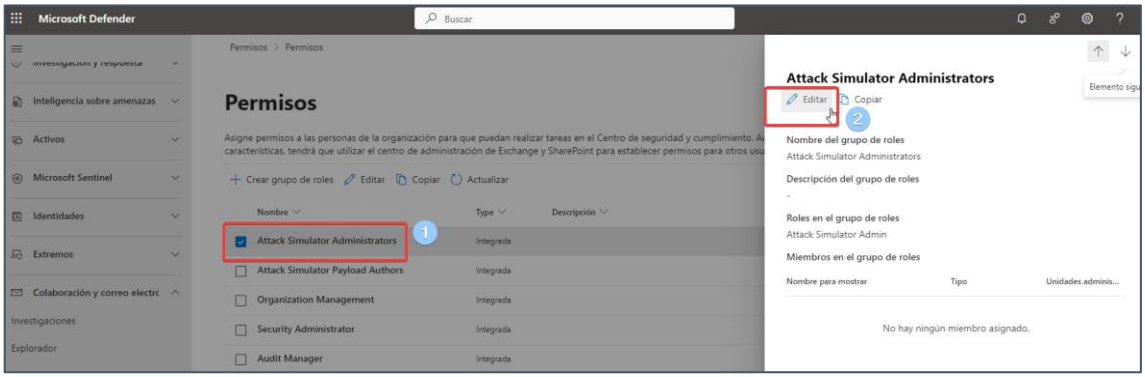
* Los *roles de Microsoft Entra ID* son roles centrales que asignan permisos para todos los servicios de Microsoft 365. Existen roles específicos para los servicios de Exchange y SharePoint, de tal manera que un administrador, podría ser administrador del servicio de Exchange y no de SharePoint y viceversa. Para la asignación de roles en los servicios específicos recomendamos usar los portales de administración de cada uno de ellos.

2. Seleccionar la opción [Roles de colaboración y correo electrónico]: son los mismos grupos de roles que están disponibles en el Centro de seguridad y cumplimiento, pero puede administrarse directamente desde este portal de Microsoft Defender XDR.

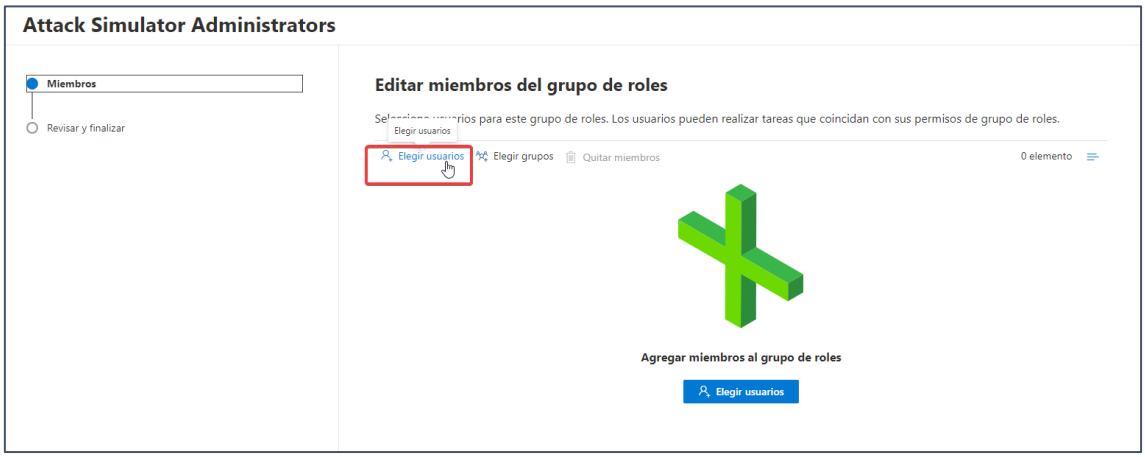


AÑADIR MIEMBROS O GRUPOS A DE ROLES DE ADMINISTRACIÓN

1. Para añadir miembros o un grupo a un *role de administración* basta con seleccionar el role y pulsar el botón [Editar]:



2. A continuación, elegir los integrantes (miembros o grupos):



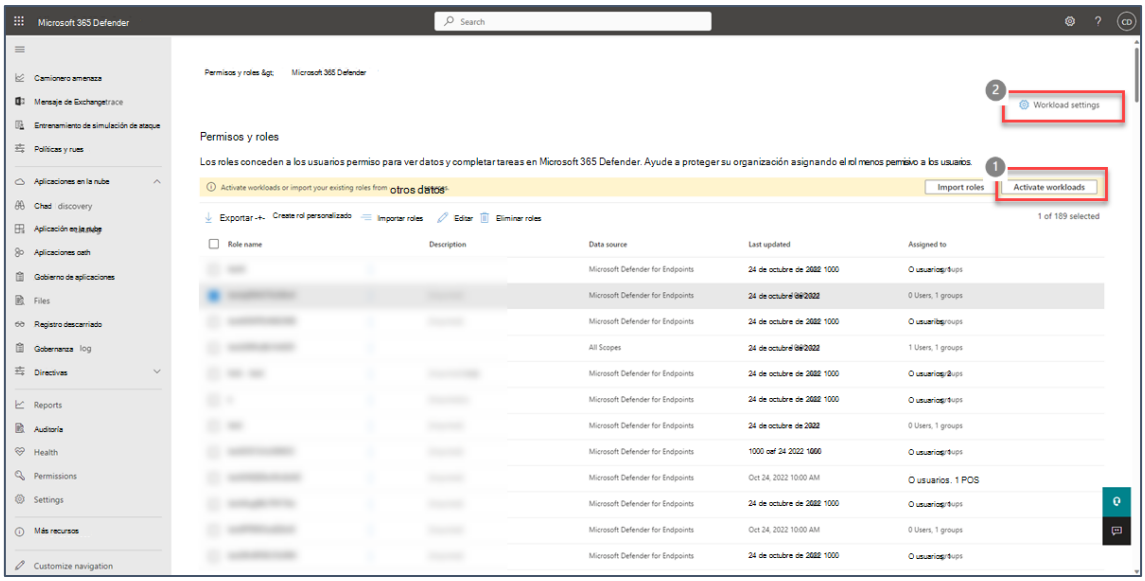
MICROSOFT DEFENDER XDR CONTROL DE ACCESO UNIFICADO

Microsoft Defender XDR proporciona protección contra amenazas integrada, detección y respuesta entre puntos de conexión, correo electrónico, identidades, aplicaciones y datos dentro de un único portal. Controlar los permisos de un usuario en torno a su acceso para ver datos o completar tareas es esencial para que las organizaciones minimicen los riesgos asociados al acceso no autorizado.

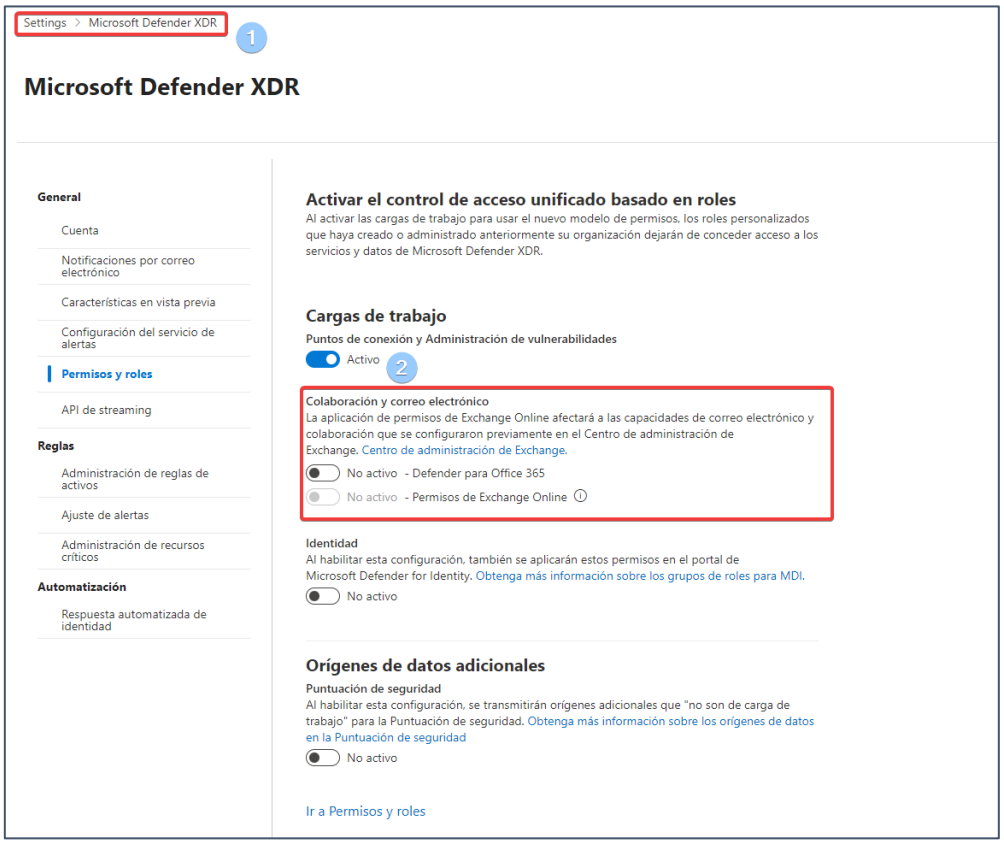
El modelo de control de acceso basado en rol unificado (RBAC) de Microsoft Defender XDR proporciona una única experiencia de administración de permisos que proporciona una ubicación central para que los administradores controlen los permisos de usuario en diferentes soluciones de seguridad.

Este modelo de segregación de roles, para Microsoft Defender para Office 365 solo está disponible para organizaciones con licencias de Microsoft Defender para Office 365 Plan 2.A continuación se describe como activar el modelo RBAC unificado de Microsoft Defender XDR. Existen dos maneras de activar las workloads desde la página de Permisos y roles:

Desde el portal https://security.microsoft.com/. En el panel de navegación, se selecciona [*Permisos* y Roles] en Microsoft Defender XDR.



1. Activación de workloads (carga de trabajo).
   - Seleccionar activar workloads en el banner situado encima de la lista de roles.
   - Esto da acceso directamente a la pantalla Activar workloads.
   - Activar cada workload una por una. Una vez que seleccione el botón de alternancia individual, se activará (o desactivará) ese workload.



2. Configuración de la carga de trabajo
   - Seleccionar configuración de la workload.
   - Esto da acceso a la página Permisos y roles de Microsoft Defender XDR.
   - Seleccionar el botón de alternancia de la workload que desea activar.
   - Seleccione Activar en el mensaje de confirmación.

Activar en la configuración de Microsoft Defender XDR

Con estos pasos se activar las workloads directamente en Microsoft Defender XDR configuración:

1. Iniciar sesión en el portal de Microsoft Defender.
2. En el panel de navegación, seleccionar **Configuración**.
3. Seleccionar **Microsoft Defender XDR**.
4. Seleccionar **Permisos y roles**. Esto da acceso a la página **Activar workloads**.
5. Seleccionar el botón de alternancia de la workload que desea activar.
6. Seleccionar Activar en el mensaje de confirmación.

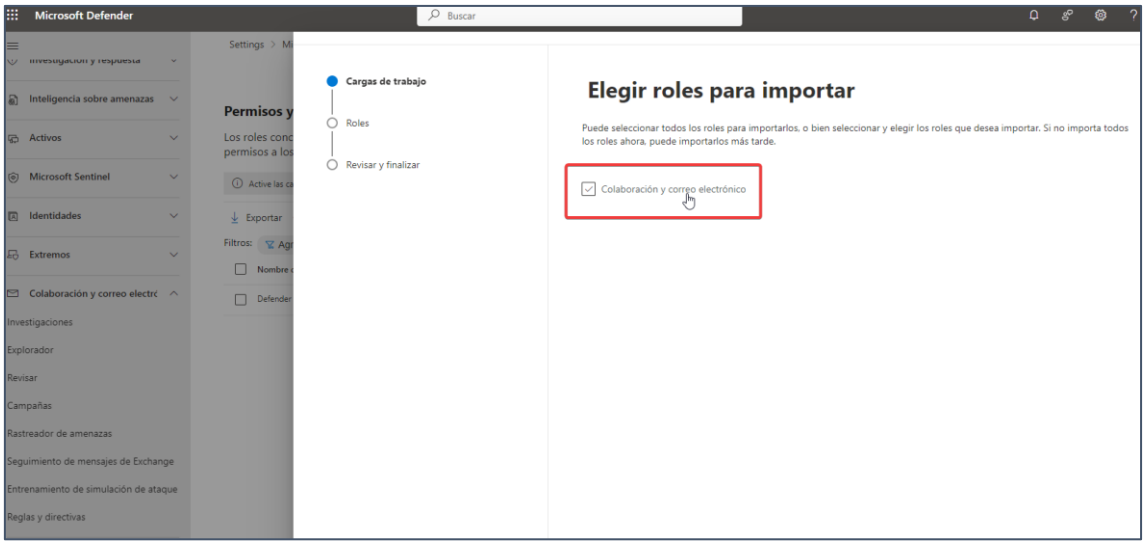
IMPORTAR ROLES CORREO Y COLABORACIÓN

Se pueden importar los roles existentes que se mantienen como parte de productos admitidos individualmente en Microsoft Defender XDR al modelo de RBAC unificado de Microsoft Defender XDR.

La importación de roles migrará y mantendrá los roles con paridad completa en relación con sus permisos y asignaciones de usuario en el modelo de RBAC unificado de Microsoft Defender XDR.

Los pasos siguientes guían sobre cómo importar roles en Microsoft Defender XDR RBAC unificado:

1. Iniciar sesión en el portal de Microsoft Defender.
2. En el panel de navegación, seleccionar **Permisos**.
3. Seleccionar **Roles** en Microsoft Defender XDR para acceder a la página Permisos y roles.
4. Seleccionar **Importar rol**.
5. Seleccionar los productos desde los que se importaran roles.



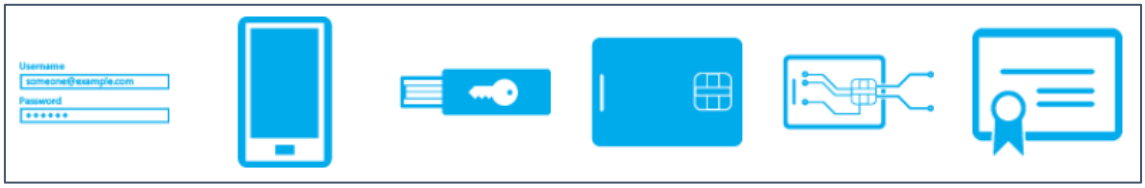
6. Seleccionar siguiente para elegir los roles que se van a importar. Es posible elegir todos los roles o seleccionar roles específicos de la lista.
7. Seleccionar los roles a importar y seleccione Siguiente.
8. Seleccionar Enviar.
9. En la página de confirmación, seleccionar Hecho.

En el siguiente enlace https://learn.microsoft.com/es-es/defender-xdr/compare-rbac-roles#map-defender-for-office-365-permissions-to-the-microsoft-defender-xdr-unified-rbac-permissions se puede ver la información sobre cómo se relacionan los roles de Microsoft Defender para Office 365 , con los nuevos permisos RBAC unificados de Microsoft Defender XDR. La asignación de estos roles se realiza de la misma forma que en el apartado [2.1.1.3.1 Añadir miembros o grupos a de roles de administración]

2.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.

Microsoft Entra ID ofrece una amplia gama de métodos de autenticación multifactorial flexibles, llamadas, datos biométricos y códigos de acceso únicos.



Si solo se usa una contraseña para autenticar a un usuario, se deja un vector desprotegido frente a los ataques. Al exigir una segunda forma de autenticación, aumenta la seguridad, ya que este factor adicional no es algo que resulte fácil de obtener o duplicar para un atacante.

Conviene evitar una mala práctica que suele producirse cuando se envía el código de MFA al mismo dispositivo donde se encuentra la cuenta que se quiere proteger, en este sentido se recomienda usar otro dispositivo. Más información en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

2.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

En el entorno empresarial actual, la identidad es el nuevo perímetro de seguridad. Si cada dispositivo, usuario, servidor, proceso y dispositivo IoT tiene una identidad única, estas identidades se convierten en el nuevo "perímetro", evitando el acceso no autorizado a los datos y sistemas.

La **autenticación** es **crucial** en este contexto de la identidad como nuevo perímetro de seguridad. Aquí hay algunas razones por las que la autenticación es de suma importancia:

- **Verificación de Identidad**: La autenticación garantiza que la persona o el dispositivo que intenta acceder a los recursos de la organización sea realmente quien dice ser. Esto ayuda a prevenir el acceso no autorizado y protege contra amenazas internas y externas.
- **Control de Acceso**: La autenticación permite a las organizaciones establecer políticas de acceso basadas en roles.
- **Prevención de Ataques de Fuerza Bruta**: La autenticación sólida dificulta que los atacantes adivinen o descifren las credenciales de acceso. La ausencia de contraseñas (passwordless), la autenticación multifactor (MFA) y otros métodos ayudan a prevenir ataques de fuerza bruta.
- **Protección contra Amenazas Emergentes**: A medida que las amenazas evolucionan, la autenticación también debe adaptarse. Las soluciones modernas, como la autenticación biométrica (huellas dactilares, reconocimiento facial), ayudan a mitigar riesgos emergentes.

En resumen, la autenticación es fundamental para garantizar que solo las personas y dispositivos autorizados tengan acceso a los recursos de la organización, especialmente en un mundo donde la identidad es el nuevo perímetro de seguridad.

Se requiere establecer un "doble factor de autenticación" (MFA) y tener una política adecuada de gestión de credenciales. Así mismo, se requiere un registro de intentos de accesos con éxito y fallidos al sistema. Adicionalmente se puede controlar el acceso al servicio mediante directivas de acceso condicional o reglas en ADFS.

El acceso a los portales de administración se puede realizar de forma descentralizada. Se recomienda reforzar la seguridad:

- Equipos administrados.
- Autenticación de doble factor.
- Conformidad de dispositivos.
- Ubicaciones de confianza.
- Evitar accesos de usuarios sin licenciamiento.
- Otras medidas a través de acceso condicional

Una configuración detallada puede consultarse en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

2.1.1.6 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Los mecanismos de autenticación que se utilizarán para proteger a los usuarios de la organización serán los mismos que los indicados en el punto anterior para los usuarios externos. Como se ha comentado, ahora el acceso a los recursos está descentralizado, siendo la identidad el nuevo perímetro de seguridad, y, por lo tanto, no se debería diferenciar entre tipos de usuarios en cuanto a las medidas de protección de acceso.

2.1.2 EXPLOTACIÓN

En esta sección se detallan aspectos relevantes de *Microsoft Defender para Office 365* en cuanto a la *explotación* de los recursos.

2.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

Las características de protección contra amenazas se incluyen en todas las suscripciones Microsoft 365; sin embargo, algunas suscripciones tienen características avanzadas. En la tabla siguiente se enumeran características de protección con los requisitos mínimos de suscripción:

Tipo de protección	Requisitos de suscripción
Registro de auditoría (para fines de informes)	Exchange Online
Protección contra malware	Exchange Online Protection (EOP)
Protección contra phishing	EOP
Protección contra correo no deseado	EOP
Protección contra direcciones URL malintencionadas y archivos en documentos Office correo electrónico	Microsoft Defender para Office 365

* Conviene recordar que Microsoft Defender para Office 365 contiene y se construye sobre EOP.

PROTECCIÓN ANTIMALWARE EN EOP

En organizaciones de Microsoft 365 con buzones de correo de Exchange Online u organizaciones independientes de Exchange Online Protection (EOP) sin buzones de Exchange Online, EOP protege automáticamente los mensajes de correo electrónico entrantes contra el malware. Algunas de las categorías principales de malware son:

- **Virus** que infectan otros programas y datos, y se propagan a través del equipo o red en busca de programas para infectar.
- **Spyware** que recopila información personal, como la información de inicio de sesión y los datos personales, y la envía de vuelta a su autor.
- **Ransomware** que cifra los datos y exige el pago para descifrarlos. El software antimalware no le ayuda a descifrar archivos cifrados, pero puede detectar la carga útil de malware asociada con el ransomware.

EOP ofrece protección contra malware multicapa diseñada para detectar todo el malware conocido en Windows, Linux y Mac que viaja dentro o fuera de una organización. Las opciones siguientes ayudan a proporcionar protección antimalware:

- **Defensas en capas contra malware:** varios motores de detección antimalware ayudan a protegerse contra amenazas conocidas y desconocidas. Dichos motores incluyen potente detección heurística que ofrece protección aún durante las primeras etapas de un ataque de malware.
- **Respuesta a amenazas en tiempo real:** durante algunas amenazas, el antimalware podría tener suficiente información sobre un virus u otra forma de malware para escribir reglas de directiva sofisticadas que detecten la amenaza. Esas reglas se publican en la red global cada 2 horas a fin de proporcionar a la organización una capa adicional de protección contra ataques.
- **Implementación rápida de definiciones antimalware:** el antimalware mantiene relaciones estrechas con otros asociados que desarrollan motores antimalware. Como resultado, el servicio puede recibir e integrar definiciones y revisiones de malware antes de que se lancen al público.

En EOP, los mensajes que contienen malware en los datos adjuntos se ponen en cuarentena. Las directivas de cuarentena controlan si los destinatarios pueden ver o interactuar con los mensajes en cuarentena. De forma predeterminada, los mensajes que se pusieron en cuarentena debido a malware solo pueden ser vistos y publicados por los administradores.

Microsoft 365 usa un motor de detección de virus común para examinar archivos que los usuarios cargan en SharePoint Online, OneDrive y Microsoft Teams. El motor de detección de virus de Microsoft 365 examina los archivos de forma asincrónica (en algún momento después de la carga). Si un usuario intenta descargar un archivo en un explorador web o desde Teams que no se ha examinado, se desencadena un examen antes de que se permita la descarga. Todos los tipos de archivo no se examinan automáticamente. La heurística determina los archivos que se van a examinar. Cuando se detecta que un archivo contiene un virus, el archivo se marcará como malware.

Esto es lo que sucede:

1. Un usuario carga un archivo en SharePoint Online.
2. SharePoint Online, como parte de sus procesos de detección de virus, determina más adelante si el archivo cumple los criterios para un examen.

3. Si el archivo cumple los criterios para un examen, el motor de detección de virus examina el archivo.
4. Si se encuentra un virus en el archivo examinado, el motor de virus establece una propiedad en el archivo que indica que el archivo está infectado.

De forma predeterminada, los usuarios pueden descargar archivos infectados desde SharePoint Online.

1. En un explorador web, un usuario intenta descargar un archivo de SharePoint Online que resulta estar infectado.
2. Al usuario se le muestra una advertencia de que se detectó un virus en el archivo. El usuario tiene la opción de continuar con la descarga e intentar limpiarla mediante software antivirus en su dispositivo.

Se recomienda cambiar este comportamiento para que los usuarios no puedan descargar archivos infectados. Los administradores pueden usar el pparámetro DisallowInfectedFileDownload en el cmdlet Set-SPOTenant en PowerShell de SharePoint Online. El valor $true para el parámetro DisallowInfectedFileDownload bloquea completamente el acceso a los archivos detectados o bloqueados para los usuarios.

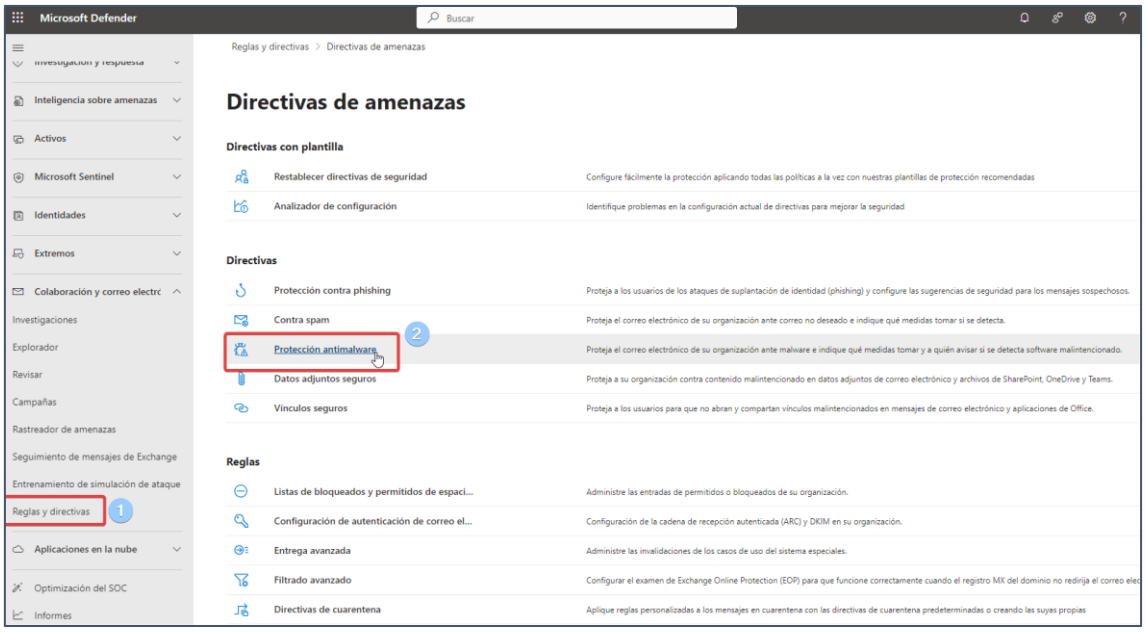
Los administradores de SharePoint y los administradores globales pueden realizar extracciones de archivos forenses de archivos infectados por malware en PowerShell de SharePoint Online con el cmdlet Get-SPOMalwareFileContent . Los administradores no necesitan acceso al sitio que hospeda el contenido infectado. Siempre que el archivo esté marcado como malware, los administradores pueden usar Get-SPOMalwareFileContent para extraer el archivo.

Las organizaciones de Microsoft 365 que tienen Microsoft Defender para Office 365 incluidas en su suscripción o compradas como complemento pueden habilitar datos adjuntos seguros para SharePoint, OneDrive y Microsoft Teams para la creación de informes y protección mejoradas

Para configurar las *políticas antimalware* para hacer frente a la amenaza de correos maliciosos:

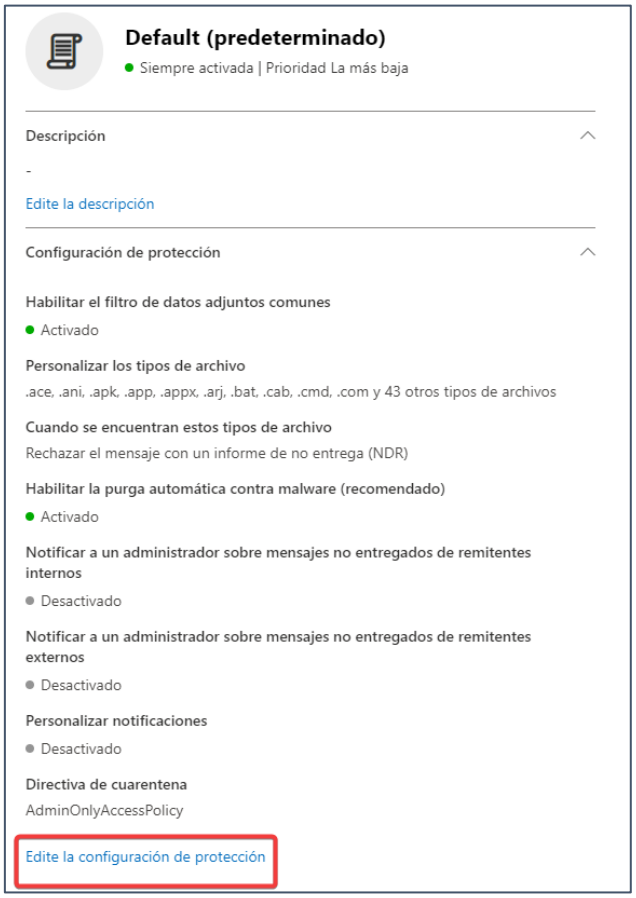
1. Entrar al portal se security.microsoft.com y a la opción [Reglas y directivas| Directivas de amenazas| protección antimalware] o bien mediante el vínculo:

https://security.microsoft.com/antimalwarev2



2. En la página Antimalware, seleccionar la directiva denominada *Default,* haciendo clic en el nombre.
3. En el control desplegable de detalles de directiva que se abre, hacer clic en "Editar configuración de protección":

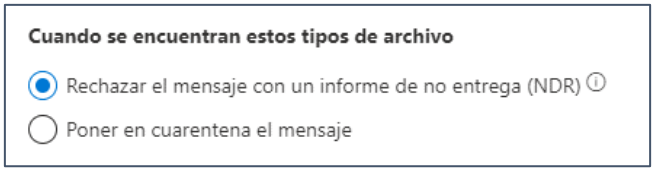
A continuación, configurar las siguientes opciones que se clasifican en secciones.



4. Configurar la sección “Configuración de la protección”:

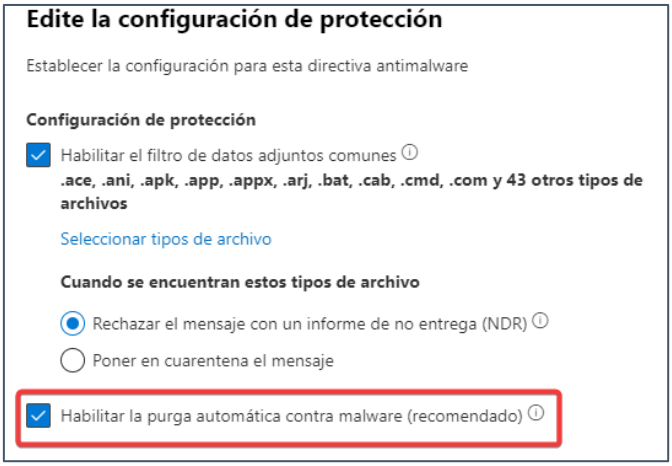
- Habilitar el filtro de datos adjuntos comunes: *seleccionar* (activar).
- Hacer clic en “seleccionar tipos de archivo” para agregar más tipos de archivo.

- Seleccionar el tipo de acción que se ejecutará cuando detecte ese tipo de ficheros:
  - Enviar un informe de no entrega (NDR)
  - Enviar el correo electrónico a cuarentena



* Los tipos de archivo especificados se consideran automáticamente como malware.

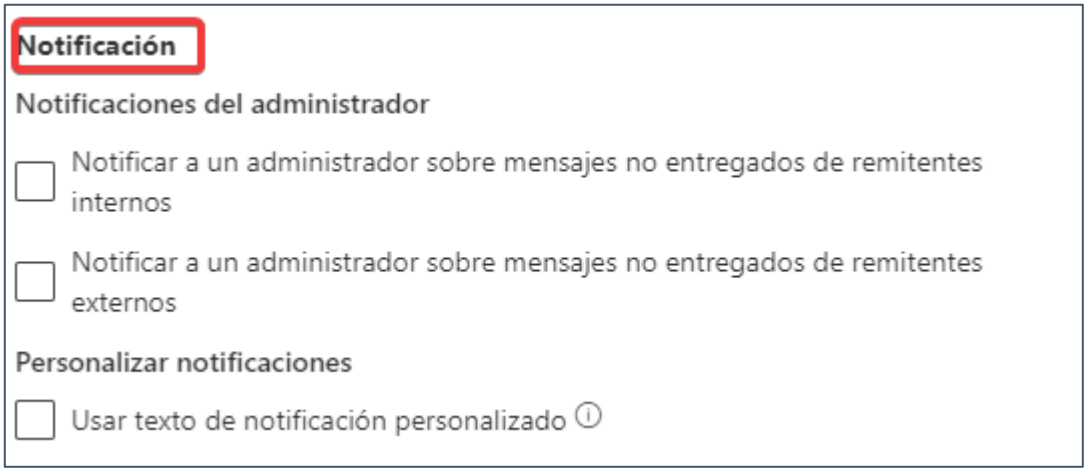
- Habilitar la *purga automática de hora cero para malware*: comprobar que esta configuración está seleccionada.



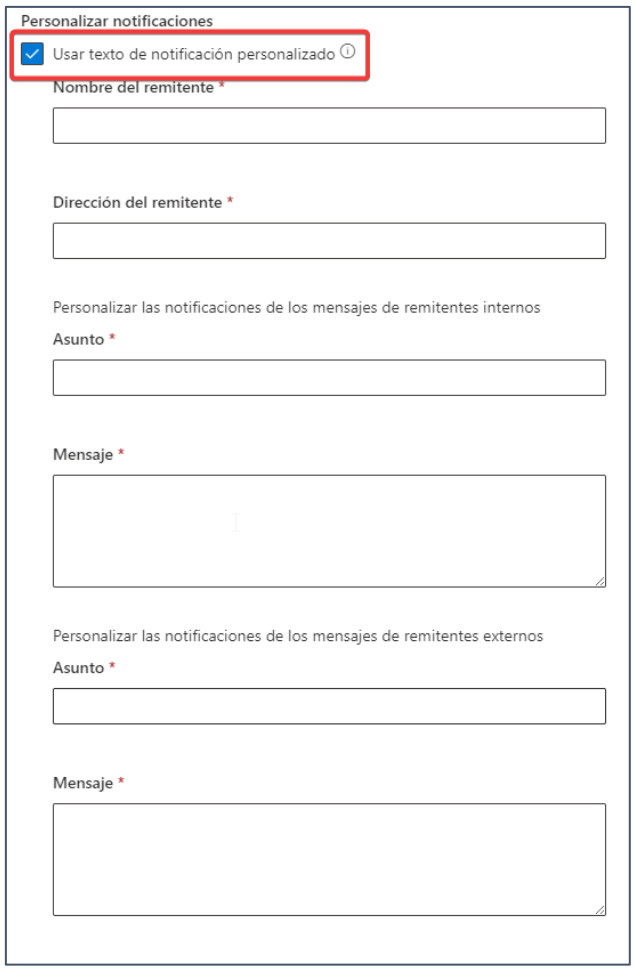
* Para los mensajes leídos o no leídos que contienen malware después de la entrega, ZAP pone en cuarentena el mensaje que contiene los datos adjuntos de malware. Se pueden crear diferentes directivas de cuarentena para definir quién debe acceder a ella y que acciones puede realizar de malware en cuarentena.

5. Configurar la sección de “Notificación”.

- Se recomienda activar las “Notificaciones del administrador”.



- Existe la posibilidad de personalizar la notificación, para modificar la que existe por defecto.



6. De nuevo en el control flotante de detalles de la directiva, hacer clic en Cerrar.

PROTECCIÓN ANTIPHISHING EN EOP Y MICROSOFT DEFENDER PARA OFFICE 365

Las organizaciones de Microsoft 365 con buzones en Exchange Online u organizaciones EOP independientes sin buzones de correo Exchange Online contienen las siguientes características que ayudan a proteger su organización frente a amenazas de suplantación de identidad (phishing):

- **Inteligencia de suplantación de identidad:** revisa los remitentes suplantados detectados en los mensajes de dominios externos e internos, y permitir o bloquear manualmente los remitentes detectados.
- **Directivas contra suplantación de identidad (phishing) en EOP**: permite activar o desactivar la inteligencia de suplantación de identidad, los indicadores de remitente no autenticados en Outlook y especificar la acción para los remitentes falsificados bloqueados.
- **Respetar la directiva DMARC del remitente cuando el mensaje se detecta como suplantación**: permite controlar lo que sucede con los mensajes en los que el remitente produce un error en las comprobaciones explícitas de DMARC y la directiva DMARC.
- **Permitir o bloquear remitentes suplantados en la lista de permitidos o bloqueados de inquilinos**: al invalidar el veredicto en la información de inteligencia de suplantación de identidad, el remitente suplantado se convierte en una entrada de bloqueo o permiso que solo aparecerá en la pestaña de **remitentes suplantados**. También es posible crear manualmente entradas de permiso o bloqueo para remitentes falsificados antes de que la inteligencia de suplantación de identidad las detecte.
- **Autenticación implícita de correo electrónico**: EOP mejora las comprobaciones de autenticación de correo electrónico estándar para el correo electrónico entrante (SPF, DKIM y DMARC con reputación del remitente, historial de remitentes, historial de destinatarios, análisis de comportamiento y otras técnicas avanzadas para ayudar a identificar remitentes falsificados. Para obtener más información, consulte Autenticación de correo electrónico de Microsoft 365.

Microsoft Defender para Office 365 contiene características contra phishing adicionales y más avanzadas:

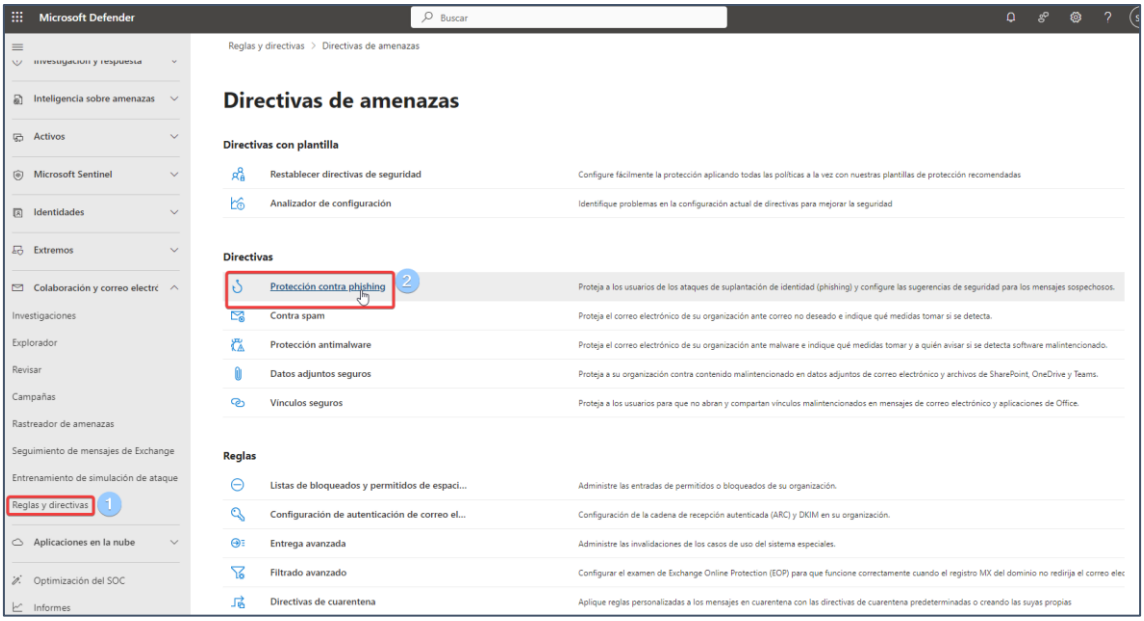
- **Directivas contra suplantación de identidad en Microsoft Defender para Office 365:** permite configuración de protección de suplantación para remitentes y dominios de remitente de mensajes específicos, opciones de inteligencia de buzones y umbrales de suplantación de identidad avanzados ajustables. Se muestran las diferencias de las características de EOP y Microsoft Defender para Office 365 en la siguiente imagen

Característica	Directivas de protección contra phishing en EOP	Directivas de protección contra phishing en Defender para Office 365
Directiva predeterminada creada automáticamente	✓	✓
Crear directivas personalizadas	✓	✓
Configuración de directiva común*	✓	✓
Configuración de suplantación de identidad	✓	✓
Primer consejo de seguridad de contacto	✓	✓
Configuración de suplantación		✓
Umbrales avanzados de phishing		✓

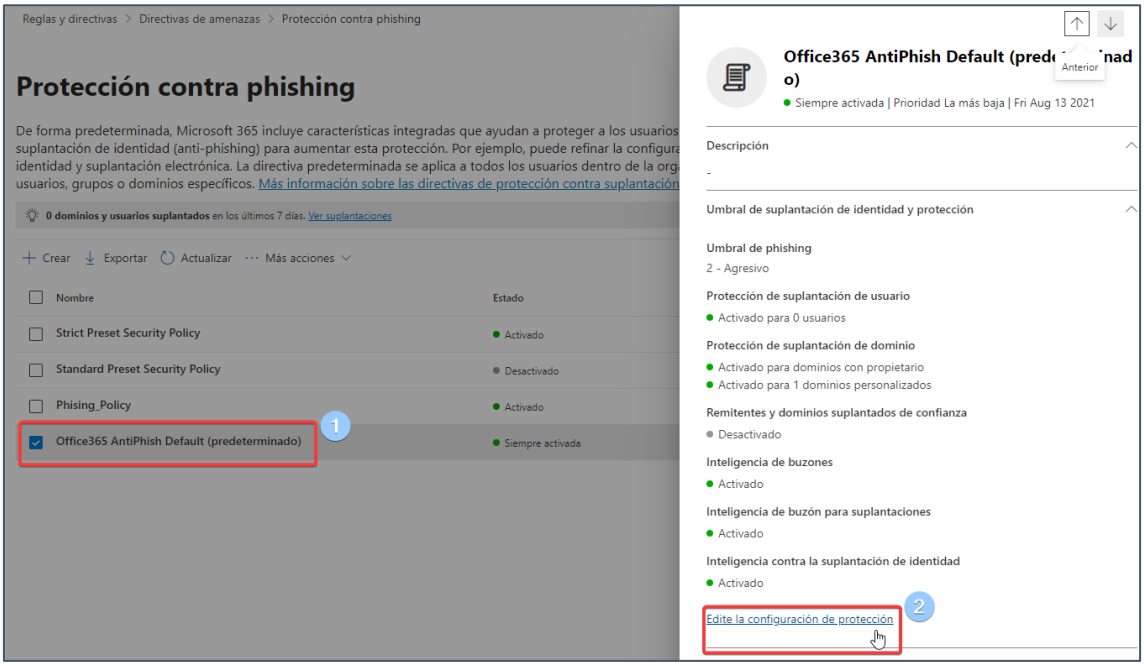
- **Vistas de campaña:** El aprendizaje automático y otras heurísticas identifican y analizan los mensajes implicados en ataques de suplantación de identidad (phishing) coordinados contra todo el servicio y la organización.
- **Entrenamiento de simulación de ataque:** Los administradores pueden crear mensajes de phishing falsos y enviarlos a usuarios internos como una herramienta de educación. Para obtener más información, consulte 3.1 Entrenamiento de simulación de ataque.

En el siguiente procedimiento se describe cómo configurar la directiva contra suplantación de identidad predeterminada:

1. Abrir la página Anti-phishing en el portal Microsoft Defender XDR en: https://security.microsoft.com/antiphishing o accediendo a [Reglas y directivas| Directivas de amenazas| protección contra phishing].

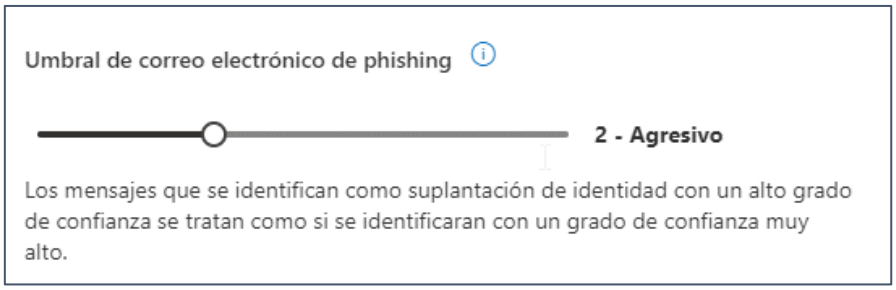


2. En la página Anti-phishing, seleccionar la directiva denominada “Office365 AntiPhish Default” (Valor predeterminado) haciendo clic en el nombre. En el control desplegable de detalles de directiva que se abre, hacer clic en “Editar configuración de protección”.



A continuación, configurar las siguientes opciones que se clasifican en secciones.

Umbral de correo electrónico de phishing



* Se recomienda aplicar como mínimo un grado 2 (agresivo), aunque este valor requerirá un estudio más detallado de la casuística de la organización.

La probabilidad de falsos positivos (mensajes buenos marcados como negativos) aumenta a medida que aumenta esta configuración.

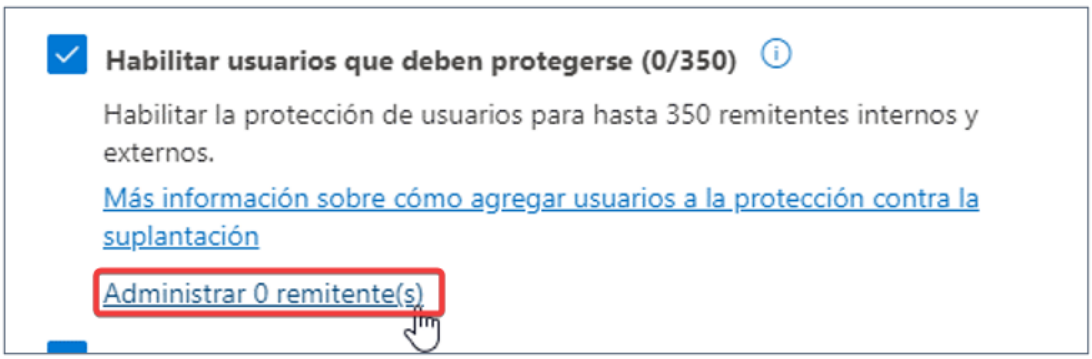
Los umbrales avanzados de suplantación de identidad solo están disponibles en las directivas contra suplantación de identidad en Microsoft Defender para Office 365. Estos umbrales controlan la confidencialidad para aplicar modelos de aprendizaje automático a los mensajes para determinar un veredicto de phishing.

Los distintos valores de este control son:

- **1 - Estándar**: este es el valor predeterminado. La severidad de la acción que se toma sobre el mensaje depende del grado de confianza de que el mensaje sea de *phishing* (confianza baja, mediana, alta o muy alta). Por ejemplo, los mensajes identificados como phishing con un grado de confianza muy alto tienen las acciones más graves aplicadas, mientras que los mensajes que se identifican como phishing con un bajo grado de confianza tienen acciones menos graves aplicadas.
- **2 - Agresivo**: los mensajes que se identifican como suplantación de identidad con un alto grado de confianza se tratan como si se identificaron con un grado de confianza muy alto.
- **3 - Más agresivo**: los mensajes que se identifican como suplantación de identidad con un grado de confianza medio o alto se tratan como si se identificaron con un grado de confianza muy alto.
- **4 - Más agresivo**: los mensajes que se identifican como suplantación de identidad con un grado de confianza bajo, medio o alto se tratan como si se identificaron con un grado de confianza muy alto.

Suplantación de usuarios que deben protegerse

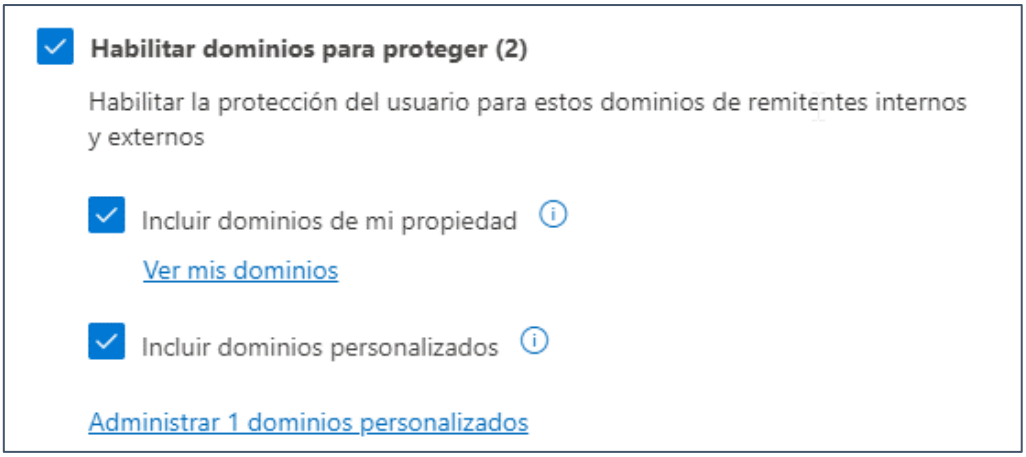
Para protegerse de la suplantación personas clave, como los miembros de la junta directiva de la organización, director general, director financiero y otros líderes.



Si se detecta suplantación en la dirección de correo electrónico del remitente, las acciones de protección de suplantación para los usuarios se aplican al mensaje (qué hacer con el mensaje, si se muestran sugerencias de seguridad de usuarios suplantados, etc.).

De forma predeterminada, ninguna dirección de correo electrónico del remitente está cubierta por la protección de suplantación, ya sea en la directiva predeterminada o en directivas personalizadas.

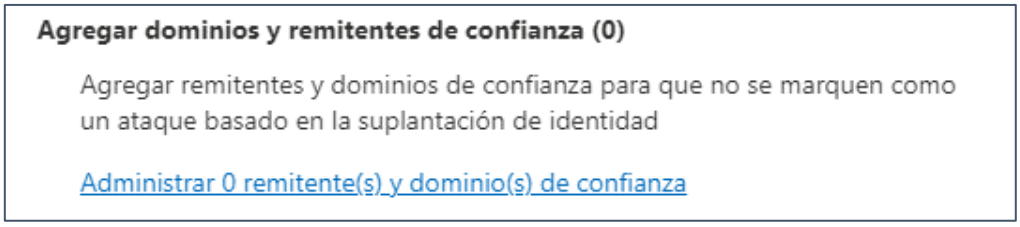
Suplantación de dominios para proteger



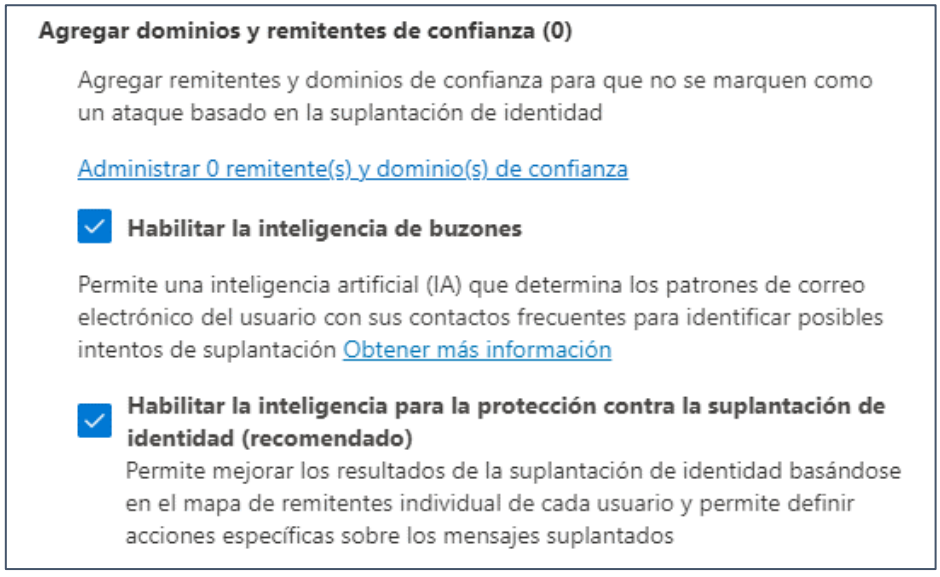
Evita que los dominios especificados se suplanten en el dominio del remitente del mensaje.

Remitentes y dominios de confianza

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

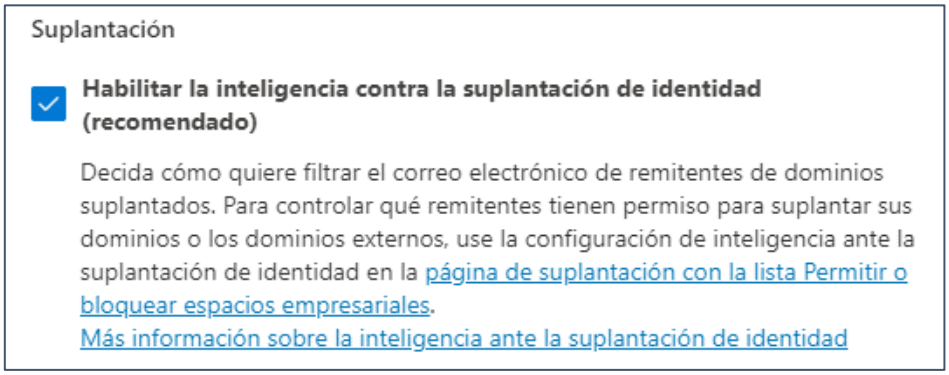


Inteligencia de buzones



Habilitar la inteligencia artificial (IA) que determina los patrones de correo electrónico del usuario con sus contactos frecuentes. Esta configuración ayuda a la IA a distinguir entre mensajes de remitentes legítimos y suplantados.

Inteligencia contra la suplantación de identidad



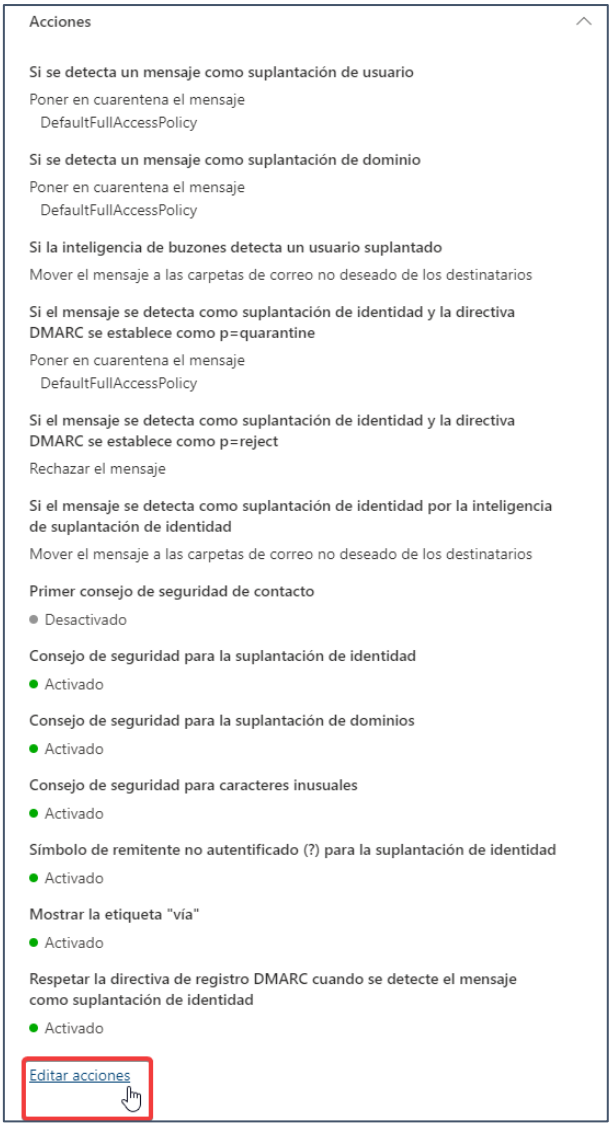
Activar esta configuración para especificar la acción que se debe realizar en los mensajes para las detecciones de suplantación:

- No aplicar ninguna acción.
- Redirigir el mensaje a otras direcciones de correo electrónico.
- Mover el mensaje a las carpetas de correo no deseado de los destinatarios.
- Poner en cuarentena el mensaje. Las directivas de cuarentena definen lo que los usuarios pueden hacer con los mensajes en cuarentena.
- Entregar el mensaje y agregar otras direcciones a la línea CCO.
- Eliminar el mensaje antes de entregarlo.

Para configurar la inteligencia ante la suplantación de identidad se proporciona un enlace a:
https://security.microsoft.com/tenantAllowBlockList?viewid=SpoofItem

Para más información consultar la página oficial de Microsoft:
https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365

3. En el control desplegable de detalles de directiva, hacer clic en “Editar acciones”.



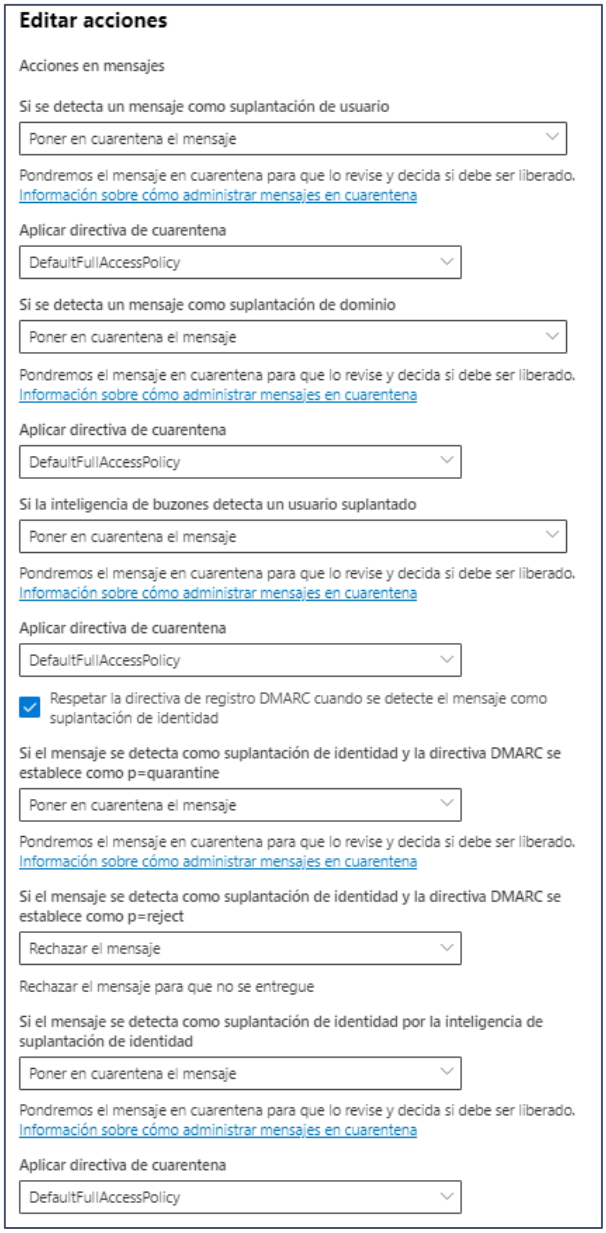
Acciones

A continuación, aparecen una serie de desplegables con la acción que se debe realizar en los mensajes entrantes que contienen intentos de suplantación contra los usuarios y los dominios protegidos de la directiva. Se puede especificar diferentes **acciones** para la suplantación de usuarios protegidos frente a la suplantación de dominios protegidos:

- No aplicar ninguna acción.
- Redirigir el mensaje a otras direcciones de correo electrónico: envía el mensaje a los destinatarios especificados en lugar de a los destinatarios previstos.
- Mover mensajes a las carpetas de correo no deseado de los destinatarios: el mensaje se entrega en el buzón y se mueve a la carpeta correo no deseado.
    - En Exchange Online, el mensaje se mueve a la carpeta Correo no deseado si la regla de correo no deseado está habilitada en el buzón (está habilitada de forma predeterminada).

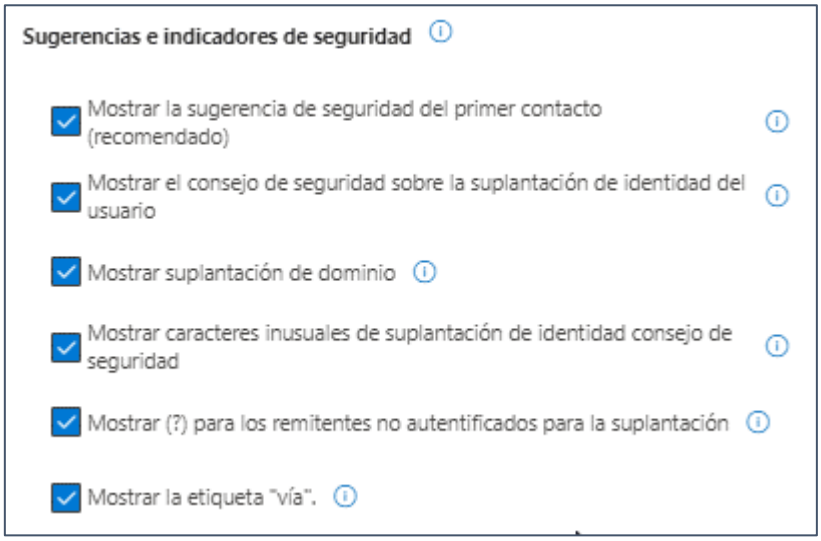
- Poner en cuarentena el mensaje: envía el mensaje a la cuarentena en lugar de los destinatarios previstos.
    - Las directivas de cuarentena definen lo que los usuarios pueden hacer con los mensajes en cuarentena.
- Entregar el mensaje y agregar otras direcciones a la línea CCO: entregar el mensaje a los destinatarios previstos y de forma silenciosa a los destinatarios especificados.
- Eliminar el mensaje antes de entregarlo: elimina silenciosamente todo el mensaje, incluidos todos los datos adjuntos.

Para las configuraciones de la política por defecto recomendamos "Poner en cuarentena el mensaje":



Sugerencias e indicadores de seguridad

Las sugerencias de seguridad son advertencias que se muestran a los destinatarios cuando se tiene algún tipo de sospecha sobre el correo entrante:



Más información:
https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365

Se recomienda activar todos los *checks*.

PROTECCIÓN ANTISPAM EN EOP

En organizaciones de Microsoft 365 con buzones de correo de Exchange Online u organizaciones independientes de Exchange Online Protection (EOP) sin buzones de Exchange Online, EOP protege automáticamente los mensajes de correo electrónico contra el spam (correo no deseado).

Para ayudar a reducir el correo electrónico no deseado, EOP incluye protección contra correo no deseado que usa tecnologías propietarias de filtrado de correo no deseado (también conocidas como *filtrado de contenido*) para identificar y separar el correo electrónico no deseado del correo electrónico legítimo. El filtrado de correo no deseado de EOP aprende de amenazas conocidas de spam y phishing y comentarios de los usuarios de nuestra plataforma de consumidores, Outlook.com. Los comentarios continuos de administradores y usuarios ayudan a garantizar que las tecnologías de EOP se entrene y mejore continuamente.

EOP usa los siguientes veredictos de filtrado de spam para clasificar los mensajes:

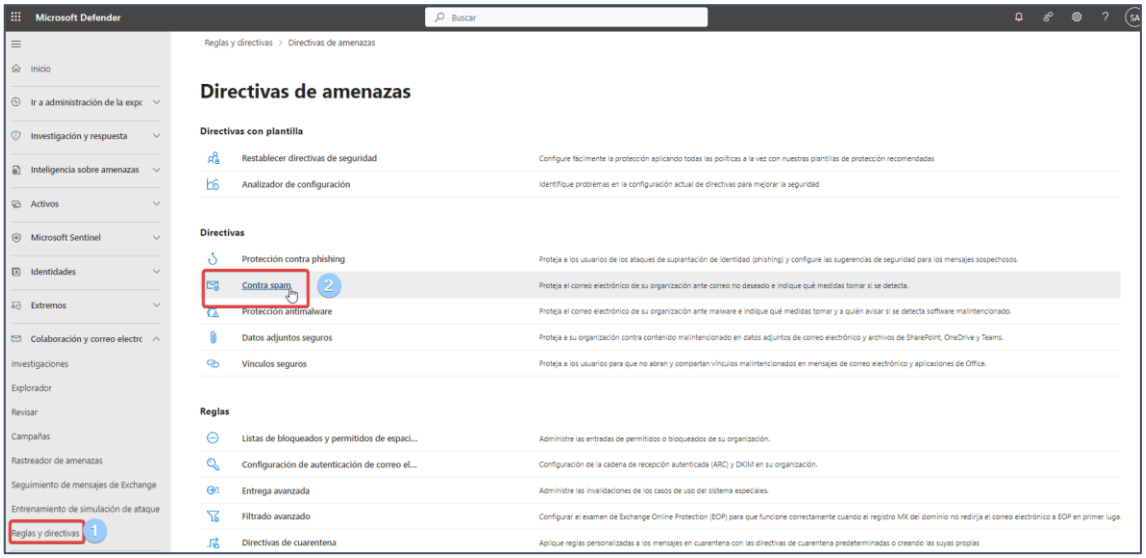
- **Correo no deseado:** el mensaje recibió un nivel de confianza de correo no deseado (SCL) de 5 o 6.
- **Spam de alta confianza:** el mensaje recibió una SCL de 7, 8 o 9.

- **Suplantación de identidad (phishing)**
- **Suplantación de identidad de alta confianza:** como parte de la seguridad de forma predeterminada, los mensajes que se identifican como suplantación de identidad de alta confianza siempre se ponen en cuarentena y los usuarios no pueden liberar sus propios mensajes de suplantación de identidad de alta confianza en cuarentena, independientemente de la configuración disponible que configuren los administradores.
- **En masa:** el origen del mensaje cumplió o superó el nivel de queja masiva (BCL) configurado. Umbral.

Para configurar las políticas *antispam* para frente a la recepción de correos no deseados:

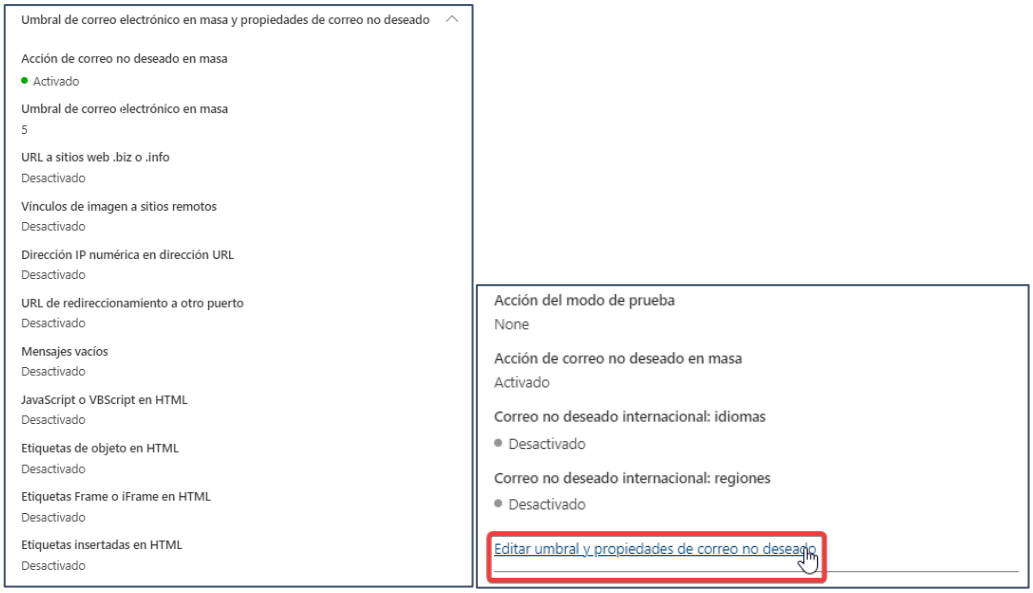
1. Entrar al portal se security.microsoft.com y a la opción [Reglas y directivas| Directivas de amenazas| protección antispam] o bien mediante el vínculo:

https://security.microsoft.com/antispam



2. En la página Antispam, seleccionar la directiva denominada “Directiva de entrada contra correo no deseado (Predeterminada)", haciendo clic en el nombre.
3. En el control desplegable de detalles de directiva que se abre, configurar las siguientes secciones:
   - Editar umbral y propiedades de correo no deseado
   - Editar acciones
   - Editar remitentes y dominios permitidos y bloqueado

Editar umbral y propiedades de correo no deseado

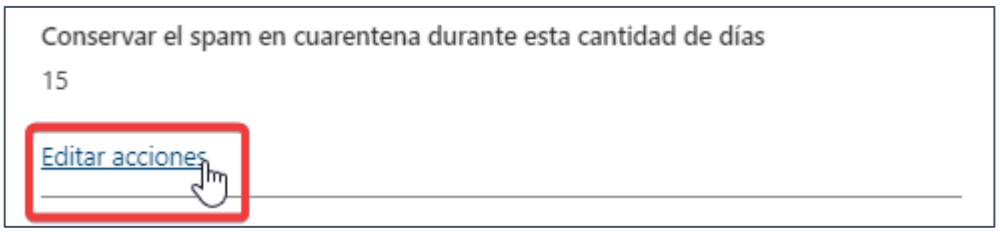


Recomendamos una configuración ***estricta*** para evitar que el correo no deseado llegue a la bandeja de entrada de los empleados en la mayoría de las situaciones.

Nombre de la característica de seguridad	Estándar	Estricta
Umbral de correo electrónico masivo & propiedades de correo no deseado		
Umbral de correo electrónico masivo (BulkThreshold)	6	5
Correo no deseado en masa (MarkAsSpamBulkMail)	(On)	(On)
Aumentar la configuración de puntuación de correo no deseado	Desactivado ($false y En blanco)	Desactivado ($false y En blanco)
Marcar como configuración de correo no deseado	Desactivado ($false y En blanco)	Desactivado ($false y En blanco)
Contiene idiomas específicos (EnableLanguageBlockList y LanguageBlockList)	Ninguna	Ninguna

Nombre de la característica de seguridad	Estándar	Estricta
De estos países (EnableRegionBlockList y RegionBlockList)	Desactivado ($false y En blanco)	Desactivado ($false y En blanco)
Modo de prueba (TestModeAction)	Desactivado ($false y En blanco)	Desactivado ($false y En blanco)

Editar acciones

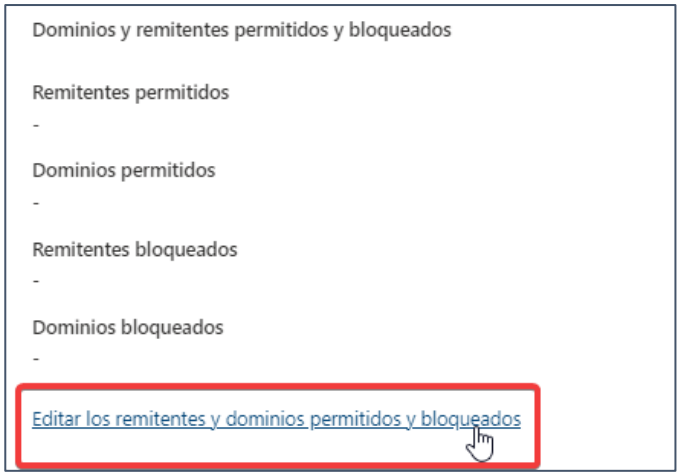


Se recomienda establecer la configuración estricta de parámetros:

Nombre de la característica de seguridad	Estándar	Estricta
El nivel de cumplimiento masivo (BCL) cumplió o superó la acción de detección (BulkSpamAction)	Mover el mensaje a la carpeta de correo electrónico no deseado (MoveToJmf)	Mover mensaje de cuarentena (Quarantine)
Acción de detección de correo no deseado (SpamAction)	Mover el mensaje a la carpeta de correo electrónico no deseado (MoveToJmf)	Mover mensaje de cuarentena (Quarantine)
Conservar el correo no deseado en cuarentena durante estos días QuarantineRetentionPeriod	15 días	30 días

* Donde quiera que seleccione mensaje de *cuarentena*, hay disponible un cuadro Seleccionar directiva de cuarentena. Las directivas de cuarentena definen lo que los usuarios pueden hacer en los mensajes en cuarentena.

Editar los remitentes y dominios permitidos y bloqueados

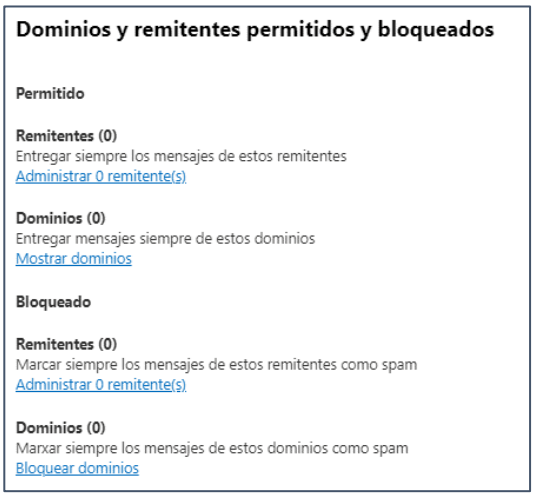


* No se recomienda agregar dominios a la lista de remitentes permitidos. Los atacantes podrían enviar un correo electrónico desde eso dominios permitidos que, de lo contrario, se filtraría. Se puede usar la información de *inteligencia de suplantación* (*spoof intelligence insight*) en el portal de Microsoft 365 XDR para identificar rápidamente a los remitentes falsificados que envían legítimamente correo electrónico no autenticado (mensajes de dominios que no pasan las comprobaciones de SPF, DKIM o DMARC) y permitir manualmente esos remitentes. Del mismo modo, se pueden revisar los remitentes falsificados que fueron permitidos por la "inteligencia de suplantación" y bloquear manualmente a esos remitentes desde "spoof intelligence insight":

  https://security.microsoft.com/tenantAllowBlockList?viewid=SpoofItem

  Más información en la documentación de Microsoft:

  https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide



Al pulsar sobre el enlace aparecen las distintas opciones de configuración. Se recomienda revisar o editar los remitentes y los dominios permitidos.

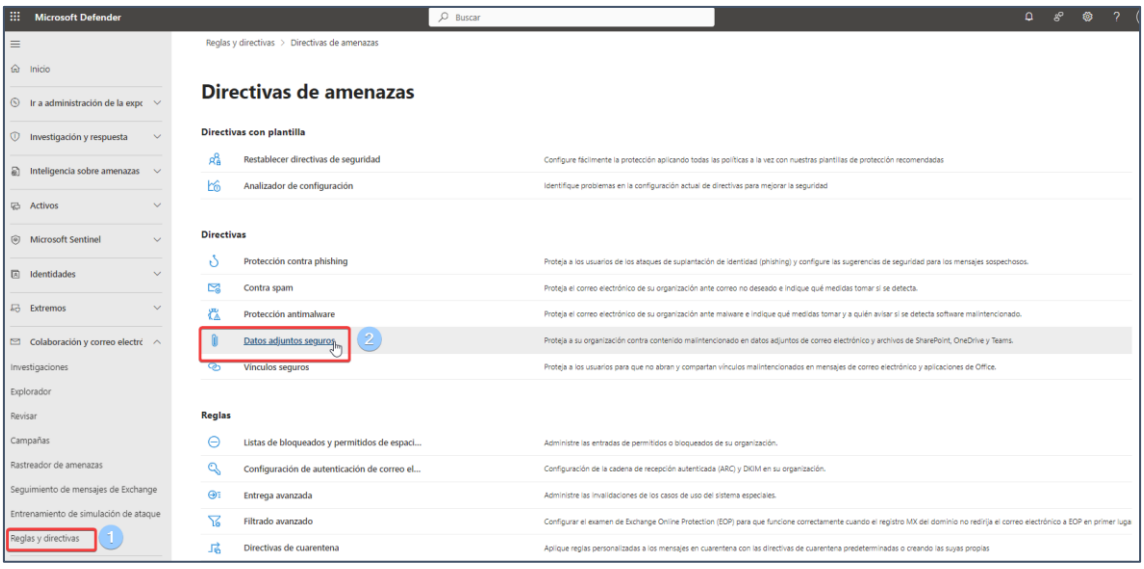
PROTECCIÓN DE ADJUNTOS SEGUROS (SAFE ATTACHMENTS) EN MICROSOFT DEFENDER PARAOFFICE 365

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

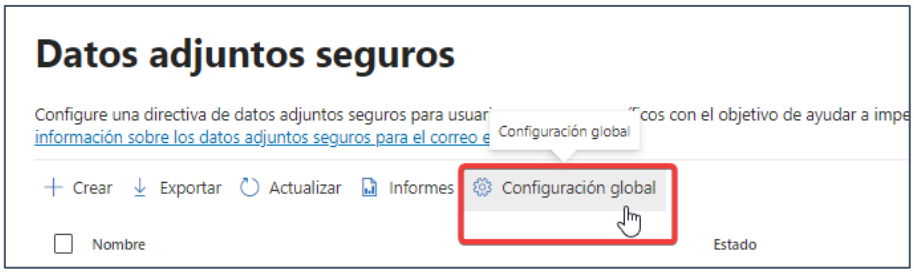
La protección de datos adjuntos seguros para mensajes de correo electrónico se controla mediante directivas de datos adjuntos seguros. Aunque no hay ninguna directiva de datos adjuntos seguros predeterminada, la directiva de seguridad preestablecida **de protección integrada** proporciona protección de datos adjuntos seguros a todos los destinatarios (usuarios que no están definidos en las directivas de seguridad preestablecidas estándar o estricta o en directivas de datos adjuntos seguros personalizadas).

Para configurar la protección de datos adjuntos seguros pueden seguirse los siguientes pasos:

1. Entrar al portal se security.microsoft.com y a la opción [Reglas y directivas| Directivas de amenazas| Datos adjuntos seguros] o bien mediante el vínculo: https://security.microsoft.com/safeattachmentv2



2. En la página “Datos adjuntos seguros”, hacer clic en “Configuración global” y, a continuación, configurar las siguientes opciones en el menú desplegable que aparece:



Se usará esta configuración para proteger a la organización del contenido malintencionado que haya en los datos adjuntos de correo electrónico y en los archivos de SharePoint, OneDrive y Microsoft Teams.

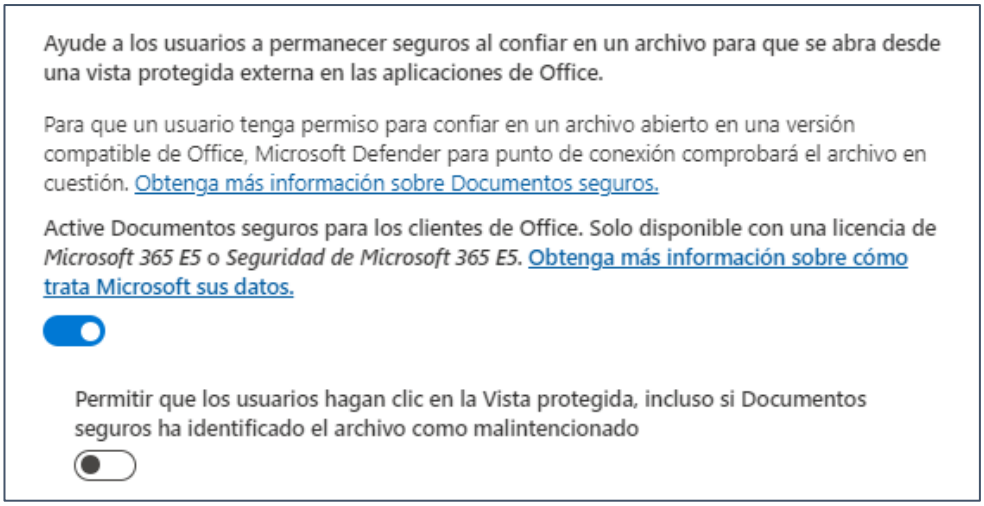
A continuación, se muestran los dos controles que se deben activar:

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

"Adjuntos Seguros" para SharePoint, OneDrive y Microsoft Teams en Microsoft Defender para Office 365 proporcionan una capa adicional de protección para los archivos que ya han sido examinados asincrónicamente por el motor de detección de virus común en Microsoft 365. "Adjuntos Seguros" ayuda a detectar y bloquear archivos existentes que se identifican como malintencionados en sitios de grupo y bibliotecas de documentos.

"Adjuntos Seguros" para SharePoint, OneDrive y Microsoft Teams no está habilitado de forma predeterminada. Hay que activarlo mediante el siguiente control deslizante:

Activar *documentos seguros* para los clientes de Office



* Solo disponible con una licencia de Microsoft 365 E5 o Seguridad de MS 365 E5.

3. En la página "Datos adjuntos seguros", hacer clic en "Crear" y, a continuación, configurar las siguientes opciones en el menú desplegable que aparece:

En esta sección se puede configurar lo siguiente:

- **Filtros de destinatarios**: condiciones y excepciones para identificar los destinatarios internos a los que se aplica la directiva. Se requiere al menos una condición. Donde están disponibles los siguientes filtros de destinatario para condiciones y excepciones:
  - **Usuarios**: uno o varios buzones de correo, usuarios de correo o contactos de correo de la organización.
  - **Grupos**:
    - Miembros de los grupos de distribución especificados o grupos de seguridad habilitados para correo (no se admiten grupos de distribución dinámicos).
    - Los Grupos de Microsoft 365 especificados.
    - **Dominios**: uno o varios de los dominios aceptados configurados en Microsoft 365. La dirección de correo electrónico principal del destinatario está en el dominio especificado.

Existe la opción de usar una condición o una excepción solo una vez, pero la condición o la excepción pueden contener varios valores:

- Varios **valores** de la **misma condición o excepción** usan lógica OR (por ejemplo, *<recipient1>* o *<recipient2>*):
  - **Condiciones**: si el destinatario coincide **con cualquiera** de los valores especificados, se le aplica la directiva.
  - **Excepciones**: si el destinatario coincide **con cualquiera** de los valores especificados, la directiva no se aplica a ellos.
- Los distintos **tipos de excepciones** usan lógica OR (por ejemplo, *<recipient1>* o *<miembro de group1>* o *<miembro de domain1>*). Si el destinatario coincide con **cualquiera** de los valores de excepción especificados, la directiva no se aplica a ellos.
- Los distintos **tipos de condiciones** usan lógica AND. El destinatario debe coincidir **con todas las** condiciones especificadas para que la directiva se aplique a ellos. Por ejemplo, configure una condición con los siguientes valores:
- Usuarios: "usuario"
- Grupos: "grupos

- **Respuesta de malware desconocida de datos adjuntos seguros:** esta configuración controla la acción para el análisis de malware de datos adjuntos seguros en los mensajes de correo electrónico.

* Para ampliar más información podemos consultar el siguiente enlace https://learn.microsoft.com/es-es/defender-office-365/safe-attachments-about?redirectSourcePath=%252fen-us%252farticle%252fSafe-attachments-in-Office-365-6e13311e-92ae-495e-a619-56d770199170#safe-attachments-policy-settings

PROTECCIÓN DE VÍNCULOS SEGUROS (SAFE LINKS)

En las organizaciones con Microsoft Defender para Office 365, el análisis de vínculos seguros protege a la organización frente a vínculos malintencionados que se usan en suplantación de identidad (phishing) y otros ataques. En concreto, vínculos seguros proporciona el examen de direcciones URL y la reescritura de mensajes de correo electrónico entrantes durante el flujo de correo, y la verificación de tiempo de clic de direcciones URL y vínculos en mensajes de correo electrónico, Teams y aplicaciones Office 365 compatibles. El análisis de vínculos seguros se produce además de la protección contra correo no deseado y antimalware normal.

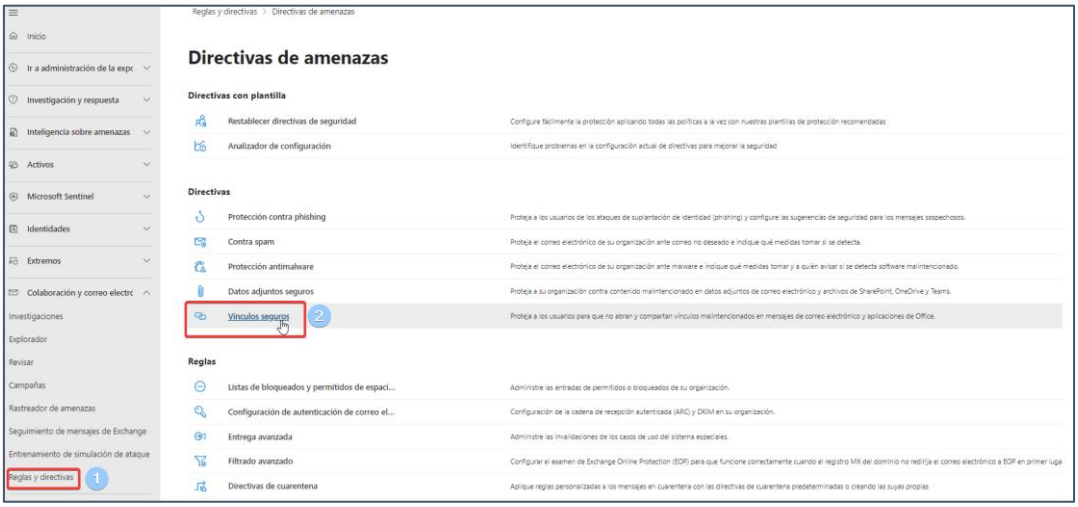
La protección de vínculos seguros mediante directivas de vínculos seguros está disponible en las siguientes ubicaciones:

- **Email mensajes:** Protección de vínculos seguros para vínculos en mensajes de correo electrónico.

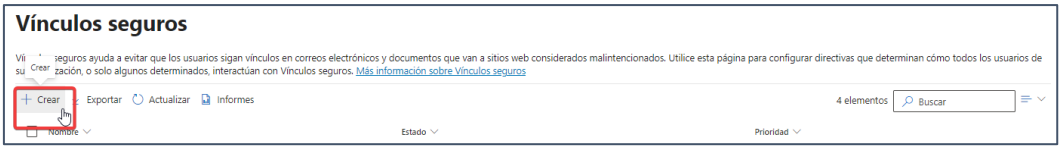
- **Microsoft Teams:** Protección de vínculos seguros para vínculos en conversaciones de Teams, chats de grupo o desde canales.
- **Aplicaciones de Office:** Protección de vínculos seguros para aplicaciones web, móviles y de escritorio de Office compatibles.

Para configurar la protección de *vínculos seguros* pueden seguirse los siguientes pasos:

1. Entrar al portal se security.microsoft.com y a la opción [Reglas y directivas| Directivas de amenazas| Vínculos seguros] o bien mediante el vínculo: https://security.microsoft.com/safelinksv2



2. En la página "Vínculos seguros", hacer clic en "Crear" y, a continuación, configurar las siguientes opciones en el menú desplegable que aparece:



- En la página **se asigna un nombre a la directiva**, configure estas opciones:
  - Nombre: Identificar un nombre único y descriptivo para la directiva.
  - Descripción: Descripción opcional para la directiva.

- En la página **Usuarios y dominios**, identificar los destinatarios internos a los que se aplica la directiva (condiciones de destinatario):
  - **Usuarios:** los buzones de correo, los usuarios de correo o los contactos de correo especificados.
  - **Grupos:**
    - Miembros de los grupos de distribución especificados (incluidos los grupos de seguridad no habilitados para correo dentro de los grupos de distribución) o grupos de seguridad habilitados para correo (no se admiten grupos de distribución dinámicos).
    - Los Grupos de Microsoft 365 especificados.

- **Dominios**: todos los destinatarios de la organización con una dirección de correo electrónico principal en el dominio aceptado especificado.

- En la página **Url & haga clic en Configuración de protección**, configure las siguientes opciones:
  - Email **sección:**
    - **Activado:** vínculos seguros comprueba una lista de vínculos conocidos y malintencionados cuando los usuarios hacen clic en vínculos de correo electrónico. Las direcciones URL se vuelven a escribir de forma predeterminada: se selecciona esta opción para activar la protección de vínculos seguros para vínculos en mensajes de correo electrónico (reescritura de direcciones URL y protección de la hora de clic). Estas opciones tienen disponible las siguientes configuraciones:
      - Aplicar vínculos seguros a los mensajes de correo electrónico enviados dentro de la organización
      - Aplicar el examen de direcciones URL en tiempo real en busca de vínculos sospechosos y vínculos que apunten a archivos
      - No vuelva a escribir direcciones URL, realice comprobaciones solo a través de safeLinks API:
      - No reescribir las siguientes direcciones URL en la sección de correo electrónico
  - **Sección de Teams**:
    - **Activado:** vínculos seguros comprueba una lista de vínculos conocidos y malintencionados cuando los usuarios hacen clic en vínculos en Microsoft Teams. Las direcciones URL no se reescriben.
  - **Office 365 sección aplicaciones:**
    - **Activado:** vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en aplicaciones de Microsoft Office. Las direcciones URL no se reescriben
  - **Configuración de protección**:
    - **Seguimiento de los clics del usuario:** esta opción seleccionada habilita los clics del usuario de seguimiento en las direcciones URL. Tiene disponibles las siguientes características:
      - Permitir que los usuarios hagan clic en la dirección URL original
      - Mostrar la personalización de marca de la organización en las páginas de notificación y advertencia.

* Para ampliar información de la configuración de los vínculos seguros, podemos consultar el siguiente enlace [Recomendaciones de Microsoft para la configuración de seguridad de EOP y Defender para Office 365 - Microsoft Defender for Office 365 | Microsoft Learn]

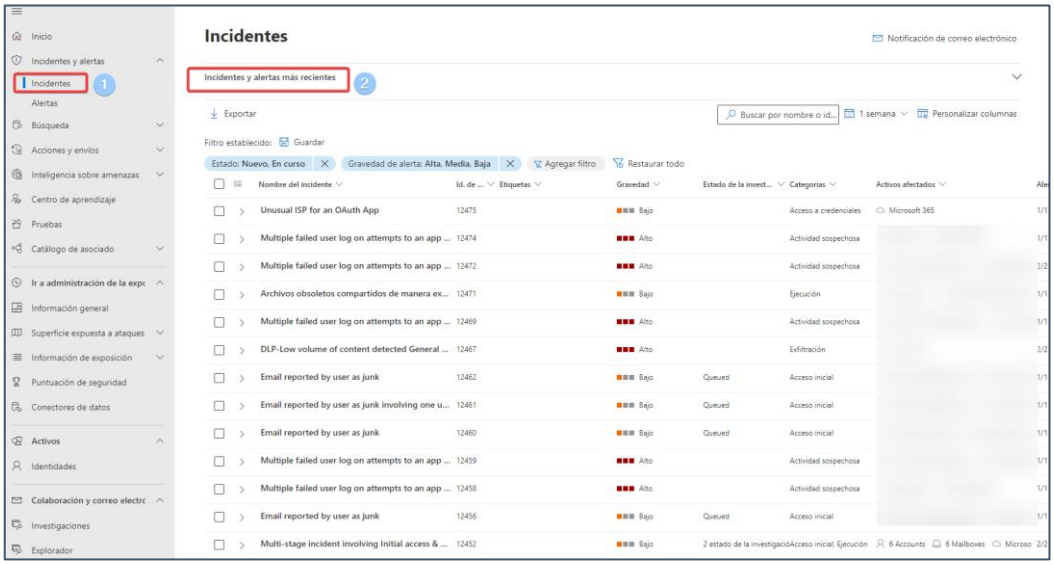
2.1.2.2 GESTIÓN DE INCIDENTES

En este apartado se describen las funcionalidades y capacidades que ofrece el servicio de Microsoft Defender para Office 365 respecto a los procedimientos de clasificación y reporte de incidentes que pudieran tener un impacto en la seguridad de la Organización.

Las capacidades mejoradas de investigación y respuesta de amenazas (*Threat investigation and response*) de Microsoft Defender XDR ayudan al equipo de seguridad a proteger a los usuarios de ataques a través de archivos, correos electrónicos. Desde dicho portal se supervisan señales y datos de distintos orígenes: actividad de usuario, autenticación, correo electrónico, equipos en peligro e incidentes de seguridad, que permiten a los responsables tomar medidas de prevención y respuesta a ciberataques.

Al ser un portal unificado, la gestión de incidentes permite obtener información de distintos orígenes del servicio: Microsoft Defender for Identity, Microsoft Defender for Endpoint y Microsoft Defender para Office 365, etc. A través de una única entrada unificada para la gestión.

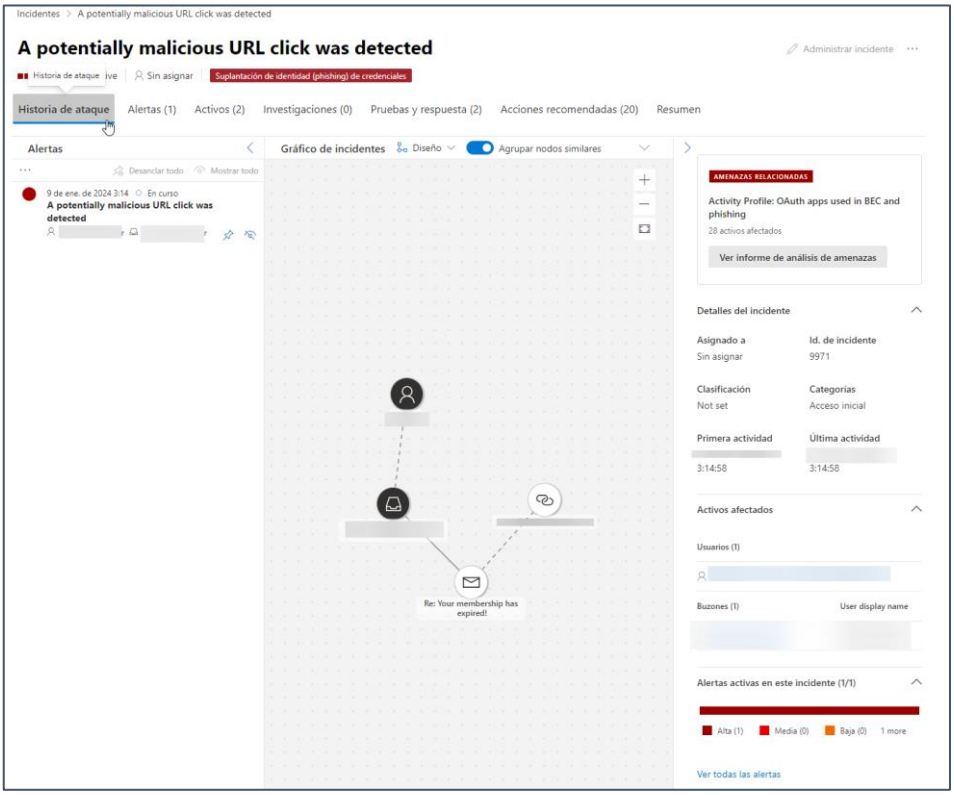
Los incidentes se administran desde La **investigación & respuesta > Incidentes & alertas >** incidentes en el inicio rápido del portal de Microsoft Defender.



Al seleccionar un nombre de incidente se muestra la página del incidente, empezando por todo el historial de ataques del incidente, incluidos:

- **Página de alertas dentro del incidente:** el ámbito de las alertas relacionadas con el incidente y su información en la misma pestaña.
- **Gráfico:** representación visual del ataque que conecta las distintas entidades sospechosas que forman parte del ataque con las entidades de recursos que componen los destinos del ataque, como usuarios, dispositivos, aplicaciones y buzones de correo.

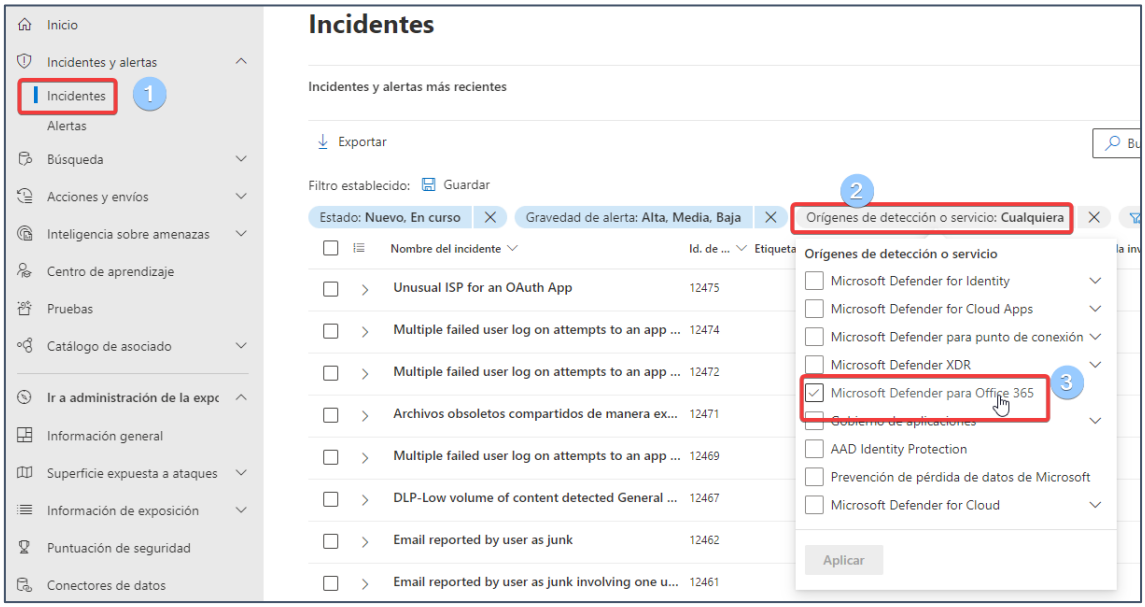
Un gráfico nos muestra el recurso y otros detalles de entidad directamente y permite actuar sobre ellos con opciones de respuesta, como deshabilitar una cuenta, eliminar un archivo o aislar un dispositivo.



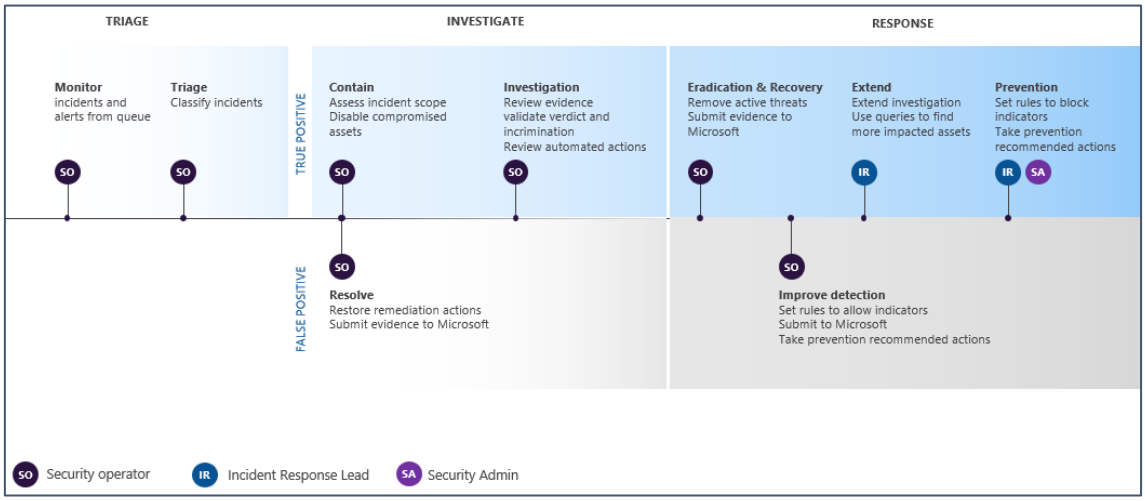
La página del incidente consta de las siguientes pestañas:

- **Historia de ataque:** Mencionada anteriormente, esta pestaña incluye la escala de tiempo del ataque, incluidas todas las alertas, entidades de recursos y acciones de corrección realizadas.
- **Alertas:** Todas las alertas relacionadas con el incidente, sus orígenes e información.
- **Activos:** Todos los recursos (entidades protegidas como dispositivos, usuarios, buzones, aplicaciones y recursos en la nube) que se han identificado para formar parte del incidente o estar relacionados con él.
- **Investigaciones:** Todas las investigaciones automatizadas desencadenadas por las alertas del incidente, incluido el estado de las investigaciones y sus resultados.
- **Evidencia y respuesta:** Todas las entidades sospechosas de las alertas del incidente, que constituyen pruebas que respaldan la historia del ataque. Estas entidades pueden incluir direcciones IP, archivos, procesos, direcciones URL, claves y valores del Registro, etc.
- **Resumen:** Información general rápida de los recursos afectados asociados a las alertas.

Para seleccionar únicamente los relacionados con el ámbito de esta guía, se debe aplicar un filtro especificando como origen del servicio: *Microsoft Defender para Office 365*.



Un ejemplo de una respuesta ante incidentes desde Microsoft Defender XDR, sería el siguiente:

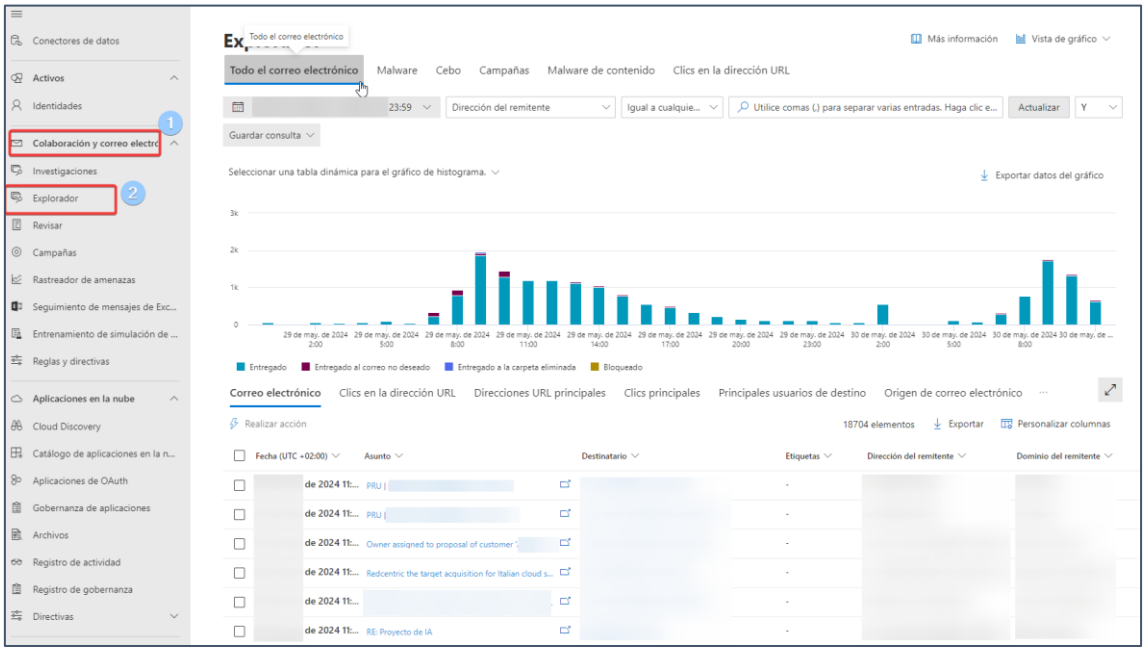


Otra herramienta eficaz para la gestión de incidentes relacionados con la colaboración y el correo electrónico es el “Explorador de amenazas”.

Explorador de amenazas y detecciones en tiempo real

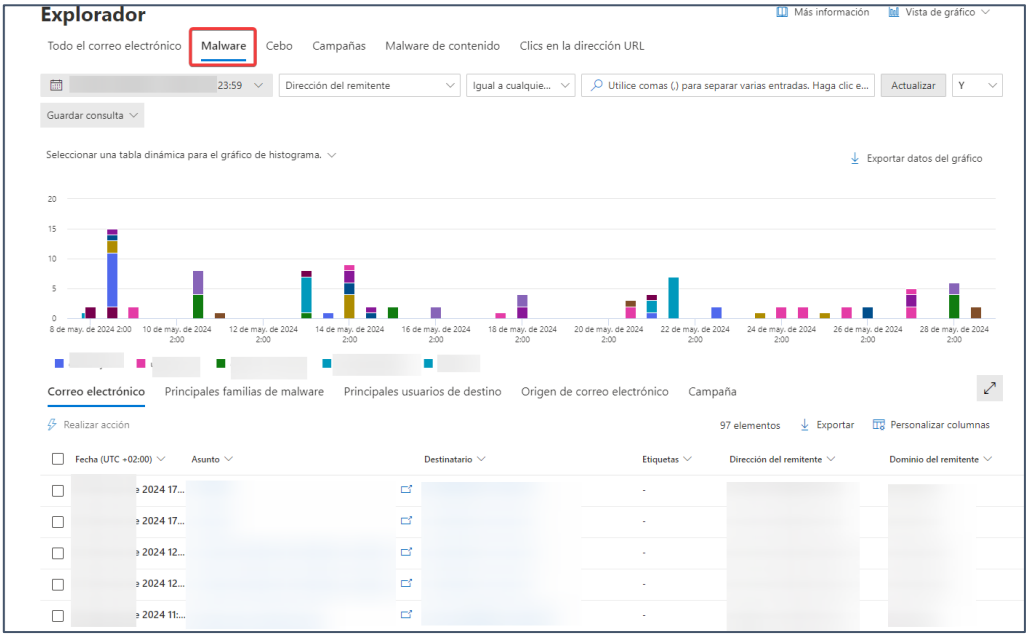
Explorador (también conocido como *Explorador de amenazas*) es otro punto de partida del trabajo de investigación de cualquier analista de seguridad. Desde aquí se pueden analizar amenazas, ver el volumen de ataques a lo largo del tiempo, analizar datos por familias de amenazas, infraestructura de atacantes, etc.

Se accede desde el portal security.microsoft.com y a la opción [Colaboración y correo electrónico| Explorador]:

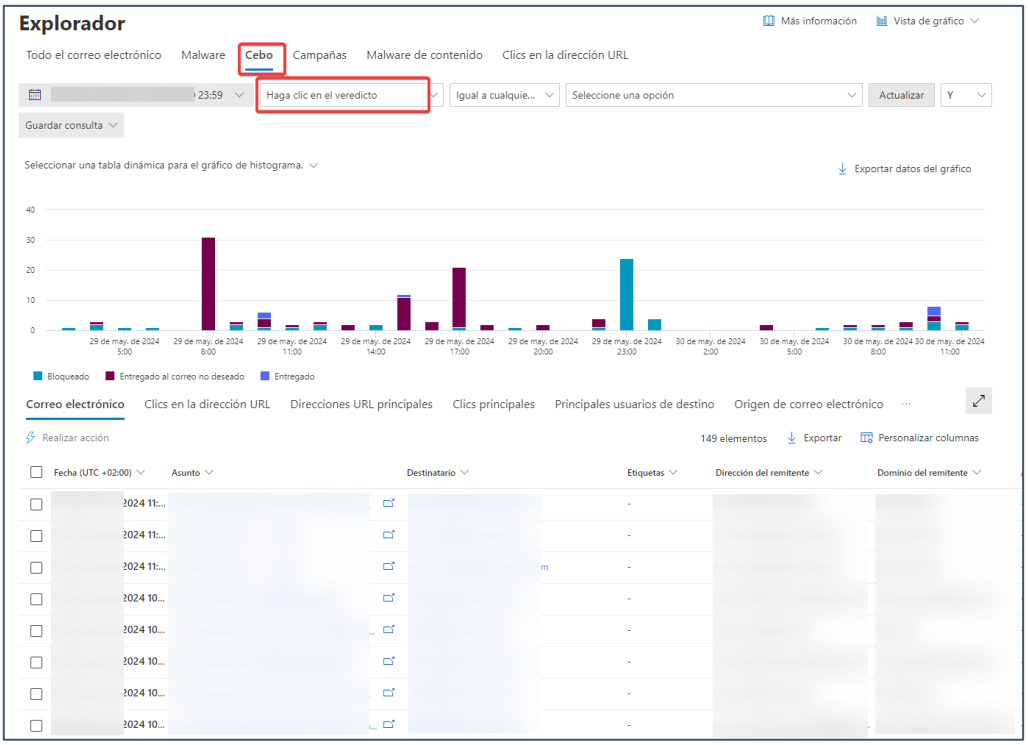


En primera instancia, puede seleccionar que tipo de amenazas visualizar clasificadas por All mail, Malware, Pish, Campaigns, Content Malware y URL clicks

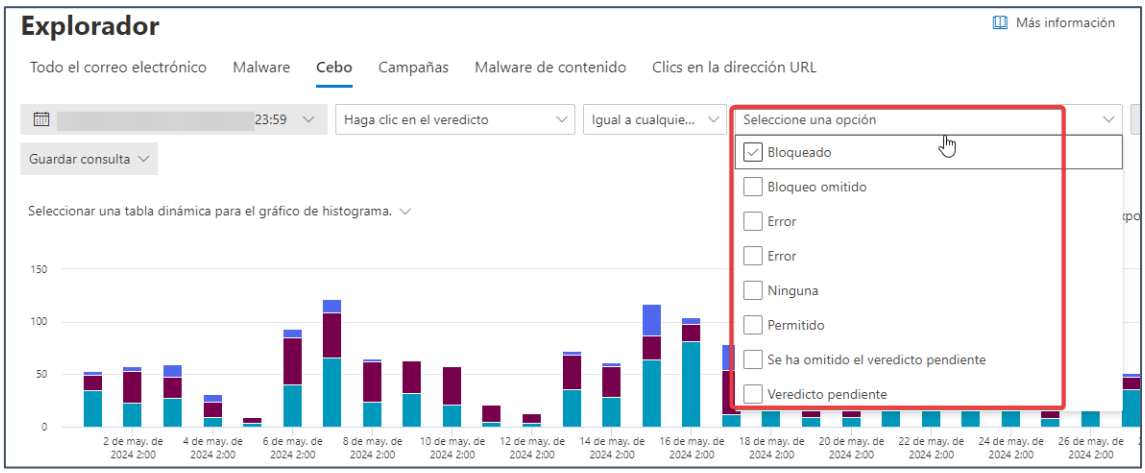
Una vez seleccionado este primer filtro, aparecen una serie de campos que, relacionados con la opción elegida, se puede filtrar aún más la información. Por ejemplo, si se ha seleccionado [**Malware**] aparece una vista donde se muestra información sobre el Top malware families, Email Orign, etc.



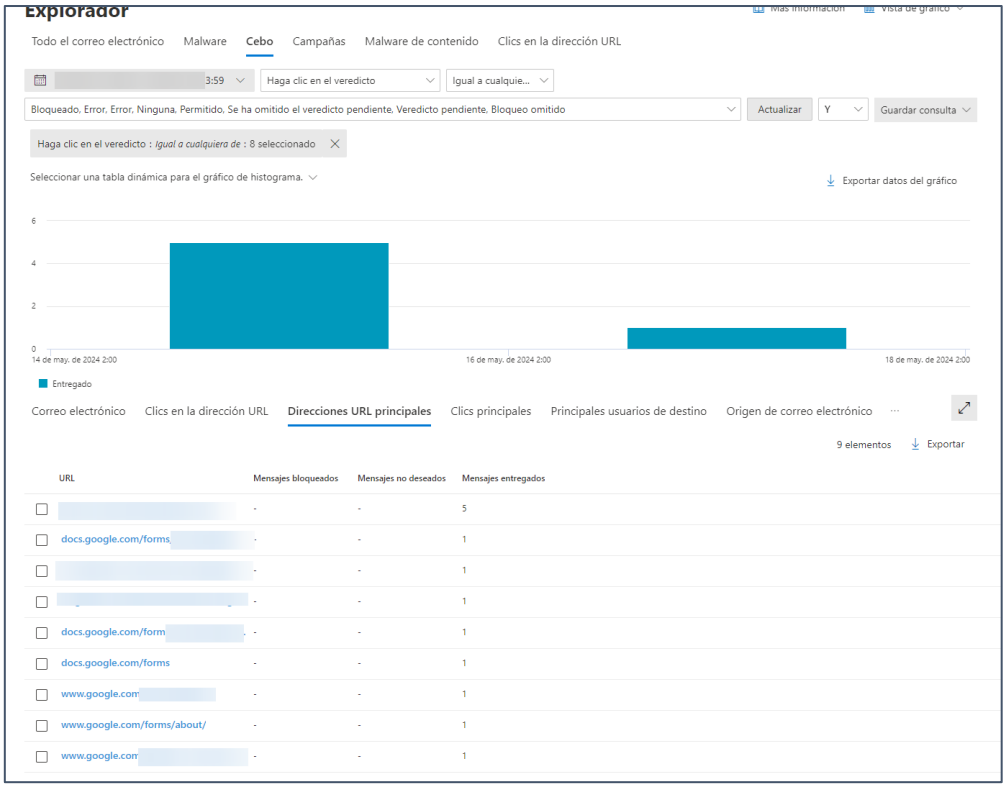
Otro ejemplo de filtrado de amenazas podría arrojar información sobre la dirección URL de suplantación de identidad (**phishing**), permitiéndose hacer clic en datos de veredicto.



En las opciones que aparecen, seleccionar una o más opciones, como Bloqueado y Bloquear invalidados y, a continuación, hacer clic en Actualizar (no actualizar la ventana del explorador).



El informe se actualiza para mostrar las direcciones URL principales en los mensajes de correo electrónico de suplantación de identidad por *acción de entrega* y *ubicación*. Las tablas muestran los clics de dirección URL bloqueados o visitados a pesar de una advertencia. Desde aquí, puede realizarse más análisis. Por ejemplo, debajo del gráfico pueden verse las direcciones URL principales de los mensajes de correo electrónico entregados o bloqueados en el entorno de la organización.



2.1.3 MONITORIZACIÓN DEL SISTEMA

Integración con Microsoft Sentinel

Desde el punto de vista de la monitorización del sistema, se recomienda la integración de Microsoft Defender para Office 365 con Azure Sentinel, que permita transmitir eventos de búsqueda avanzada a Azure Sentinel, tal y como se describe en la sección [1.3.1 Integración con Azure Sentinel].

Por otro lado, para ver los datos en los informes de protección contra amenazas, de seguridad de correo electrónico y poder explotar la herramienta *Explorador*, se debe *activar el registro de auditoría* ***(on)***.

* El registro de auditoría está disponible en suscripciones que incluyen Exchange Online. Para más información sobre cómo activar el registro de auditoría, consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

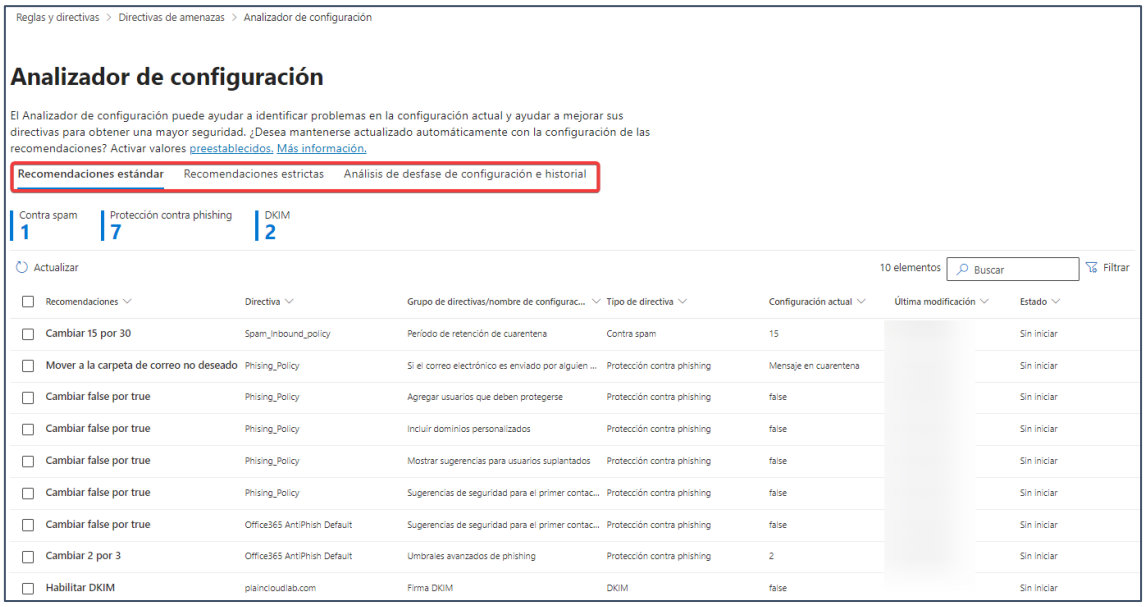
2.1.3.1 VIGILANCIA

En esta sección se detallan aspectos relevantes de *Microsoft Defender para Office 365* en cuanto a la *vigilancia* de los recursos.

Herramienta Analyzer

Configuration analyzer (Analizador de configuración), proporciona información del estado del entorno de Microsoft Defender para Office 365, equiparándolo con las medidas que se deben implementar de manera estándar o estricta. Para acceder esta herramienta. Se debe entrar al portal se security.microsoft.com y a la opción [Reglas y directivas| Directivas de amenazas|Configuration analyzer] o bien mediante el vínculo: https://security.microsoft.com/configurationAnalyzer

Una vez dentro del portal, muestra el estado actual de la configuración de la organización en referencia a las medidas estándar o estrictas recomendadas, así como un seguimiento de su implementación.



Campañas

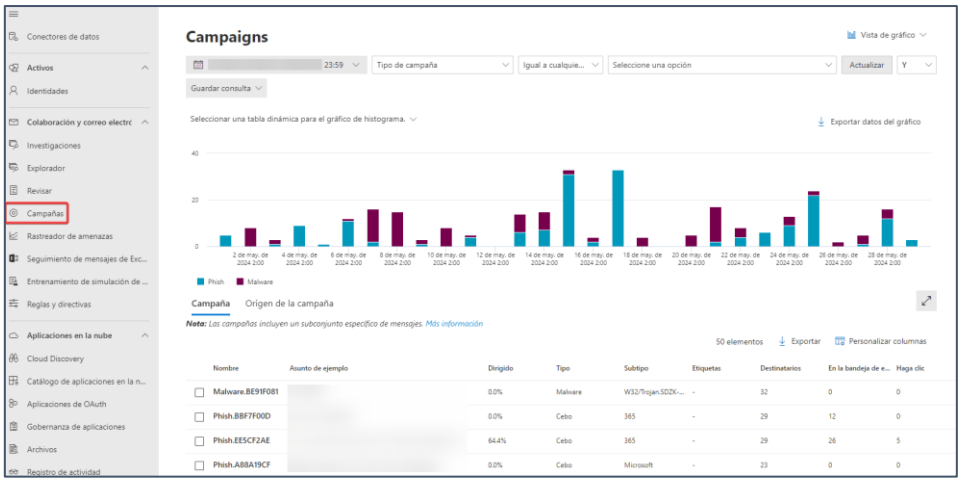
En las organizaciones de Microsoft 365 con Microsoft Defender para Office 365 Plan 2, la característica *campañas* identifica y clasifica los ataques coordinados de correo electrónico de phishing y malware.

Una campaña es un ataque coordinado por correo electrónico contra una o varias organizaciones. Los ataques por correo electrónico que roban credenciales y datos de la empresa son una industria grande y lucrativa. A medida que aumentan las tecnologías para detener los ataques, los atacantes modifican sus métodos para garantizar un éxito continuo.

Microsoft aplica las grandes cantidades de datos contra suplantación de identidad (phishing), correo electrónico no deseado y software (phishing) y antimalware de todo el servicio para identificar campañas. Analiza y clasifica la información del ataque en función de varios factores:

- **Origen del ataque:** las direcciones IP de origen y los dominios de correo electrónico del remitente.
- **Propiedades del mensaje:** el contenido, el estilo y el tono de los mensajes.
- **Destinatarios del mensaje:** cómo se relacionan los destinatarios. Por ejemplo, los dominios de los destinatarios, las funciones de trabajo de los destinatarios (administradores, ejecutivos, etc.), los tipos de empresas (grandes, pequeñas, públicas, privadas, etc.) y los sectores.
- **Carga de ataque:** vínculos, archivos adjuntos u otras cargas maliciosas en los mensajes

Para acceder esta herramienta. Se debe entrar al portal se security.microsoft.com y a la opción [Campañas]

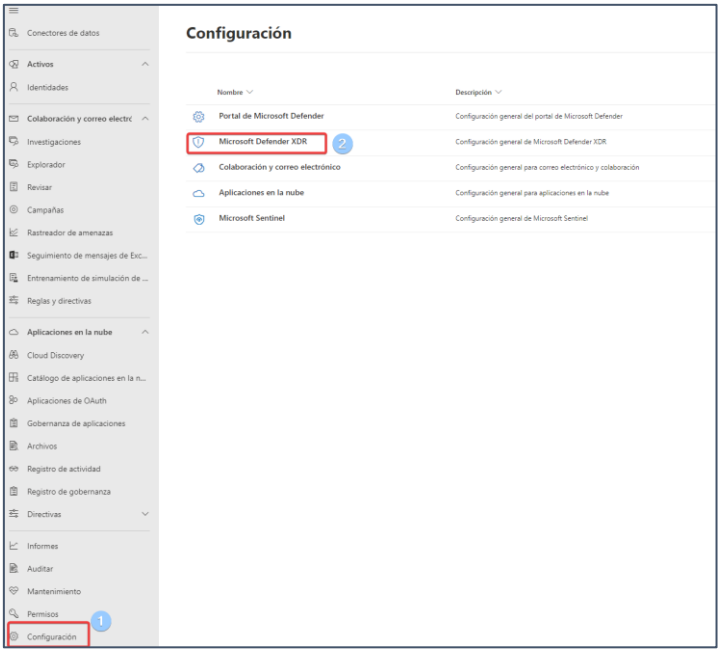


2.2 MEDIDAS DE PROTECCIÓN

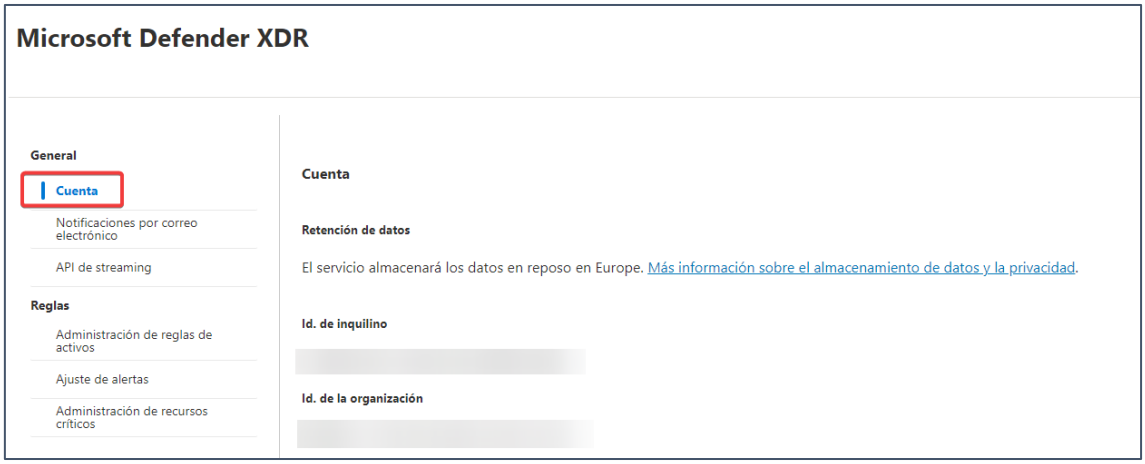
2.2.1 PROTECCIÓN DE LA INFORMACIÓN

Microsoft Defender XDR opera bajo Microsoft Azure y se ubica en los centros de datos de la Unión Europea, el Reino Unido y los Estados Unidos. Los datos de cliente recopilados por el servicio se almacenan en reposo en (a) la ubicación geográfica del Tenant identificada durante el aprovisionamiento o, (b) si Microsoft Defender XDR usa otro servicio en línea de Microsoft para procesar dichos datos, la geolocalización definida por las reglas de almacenamiento de datos de ese otro servicio en línea.

Accediendo al portal de M365XDR en la opción [Configuración| Microsoft Defender XDR]:



En la sección “Cuenta” puede consultarse donde se almacenan los datos:



La información almacenada para Microsoft Defender XDR cumple las siguientes características:

- **No se puede cambiar la ubicación** donde se almacenan los datos. Esto proporciona una forma cómoda de minimizar el riesgo de cumplimiento seleccionando activamente las ubicaciones geográficas donde residirán los datos.
- De forma predeterminada, los datos **se conservan durante 180 días**; sin embargo, se puede ampliarse puede especificar la directiva de retención de datos para los datos.
- **Microsoft aísla los datos** mediante la autenticación de acceso y la segregación lógica basada en el identificador del cliente. Cada cliente solo puede acceder a los datos recopilados de su propia organización y a los datos genéricos que Proporciona Microsoft.
- **Los desarrolladores y administradores de Microsoft** tienen, por diseño, privilegios suficientes para llevar a cabo sus tareas asignadas para operar y desarrollar el servicio. Microsoft implementa combinaciones de controles preventivos, de detective y reactivos. Además, Microsoft lleva a cabo comprobaciones en segundo plano de cierto personal de operaciones y limita el acceso a aplicaciones, sistemas e infraestructura de red en proporción al nivel de verificación en segundo plano. El personal de operaciones sigue un proceso formal cuando se les exige tener acceso a la cuenta de un cliente o a la información relacionada en el rendimiento de sus funciones.

La información relativa de Microsoft Defender para Office 365 depende del tipo de licenciamiento:

Características	Periodo de retención
Microsoft Defender for 365 Plan 1	
Detalles de metadatos de alerta (alertas de Defender para Office 365)	90 días.
Detalles de metadatos de entidad (Email)	30 días.
Detalles de alertas de actividad (registros de auditoría)	7 días.
Página de la entidad de correo electrónico	30 días.
Cuarentena	30 días (configurable; 30 días es el máximo).
Informes	90 días para los datos agregados. 30 días para obtener información detallada.
Envíos	30 días.
Detecciones de Real-Time	30 días.

Características	Periodo de retención
Microsoft Defender for 365 Plan 2	
Centro de actividades	180 días. Centro de acciones de Office 30 días.
Búsqueda avanzada	30 días.
AIR (investigación y respuesta automatizadas)	60 días para los metadatos de las investigaciones. 30 días para los metadatos de correo electrónico.
datos Entrenamiento de simulación de ataque	18 meses.
Campañas	30 días.
Incidentes	30 días.
Remediación	30 días
Análisis de amenazas	30 días.
Explorador de amenazas	30 días.
Rastreadores de amenazas	30 días.

2.2.2 PROTECCIÓN DE LOS SERVICIOS

2.2.2.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

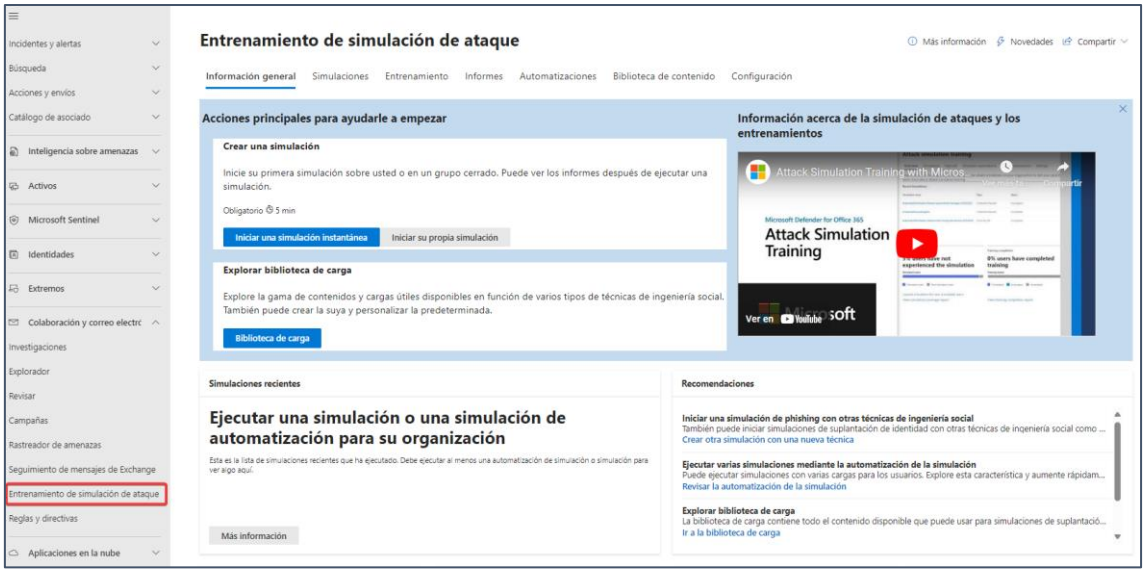
Office 365 ofrece un sistema avanzado de **detección de amenazas** y **sistemas de mitigación** para proteger la infraestructura subyacente de los ataques de *denegación de servicio* (DoS) y prevenir la interrupción de servicio a los clientes.
El sistema de defensa DDoS de Azure está diseñado no solo para resistir ataques desde el exterior, sino también desde otros *Tenants* de Azure. Los mecanismos de limitación de peticiones de Exchange Online y SharePoint Online forman parte de un enfoque de varias capas para defenderse contra ataques DoS.

Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure] para obtener más información sobre el *sistema de defensa DDoS de Azure*.

3. OTRAS CONSIDERACIONES DE SEGURIDAD

3.1 ENTRENAMIENTO DE SIMULACIÓN DE ATAQUE

Es una herramienta muy interesante, desde el punto de vista de la seguridad, al permitir ejecutar escenarios de ataque realistas en la organización y así poder identificar vulnerabilidades.



Están disponibles las simulaciones de los tipos de ataques habituales: cosecha de credenciales, adjunto de malware, vínculos a malware, etc.

- **Recolección de credenciales**: un atacante envía al destinatario un mensaje que contiene una dirección URL. Cuando el destinatario hace clic en la dirección URL, se le traslada a un sitio web que normalmente muestra un cuadro de diálogo que pide al usuario su nombre de usuario y contraseña. Normalmente,

la página de destino tiene un formato que representa un sitio web conocido para generar confianza en el usuario.

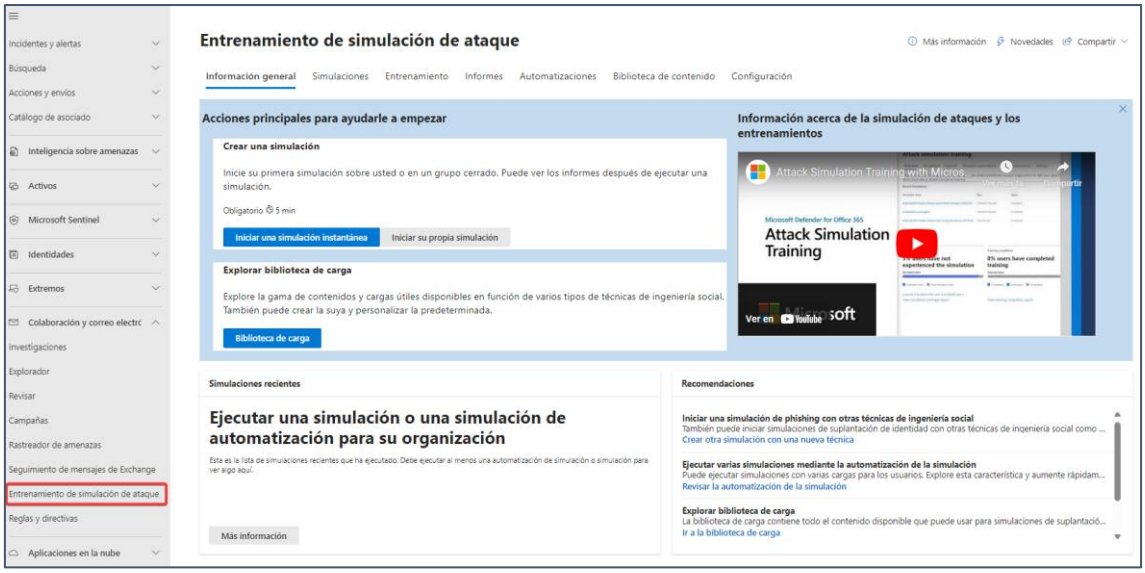
- **Datos adjuntos de malware**: un atacante envía al destinatario un mensaje que contiene datos adjuntos. Cuando el destinatario abre los datos adjuntos, el código arbitrario (por ejemplo, una macro) se ejecuta en el dispositivo del usuario para ayudar al atacante a instalar código adicional o atrincherarse aún más.
- **Vínculo en datos adjuntos**: se trata de un híbrido de una recolección de credenciales. Un atacante envía al destinatario un mensaje que contiene una dirección URL dentro de un archivo adjunto. Cuando el destinatario abre los datos adjuntos y hace clic en la dirección URL, se le traslada a un sitio web que normalmente muestra un cuadro de diálogo que pide al usuario su nombre de usuario y contraseña. Normalmente, la página de destino tiene un formato que representa un sitio web conocido para generar confianza en el usuario.
- **Vínculo a malware**: un atacante envía al destinatario un mensaje que contiene un vínculo a un archivo adjunto en un sitio de uso compartido de archivos conocido (por ejemplo, SharePoint Online o Dropbox). Cuando el destinatario hace clic en la dirección URL, se abren los datos adjuntos y se ejecuta código arbitrario (por ejemplo, una macro) en el dispositivo del usuario para ayudar al atacante a instalar código adicional o reforzarse aún más.
- **Drive-by-url**: un atacante envía al destinatario un mensaje que contiene una dirección URL. Cuando el destinatario hace clic en la dirección URL, se las traslada a un sitio web que intenta ejecutar código en segundo plano. Este código en segundo plano intenta recopilar información sobre el destinatario o implementar código arbitrario en su dispositivo. Normalmente, el sitio web de destino es un sitio web conocido que se ha visto comprometido o un clon de un sitio web conocido. La familiaridad con el sitio web ayuda a convencer al usuario de que el vínculo es seguro para hacer clic. Esta técnica también se conoce como ataque de agujero de agua.
- **Concesión de OAuth**: un atacante crea un Aplicación de Azure malintencionado que busca obtener acceso a los datos. La aplicación envía una solicitud de correo electrónico que contiene una dirección URL. Cuando el destinatario hace clic en la dirección URL, el mecanismo de concesión de consentimiento de la aplicación solicita acceso a los datos (por ejemplo, la Bandeja de entrada del usuario).
- **Guía paso a paso:** guía didáctica que contiene instrucciones para los usuarios (por ejemplo, cómo informar de mensajes de phishing).

3.1.1 CREAR UNA SIMULACIÓN DE ATAQUE

El aprendizaje de simulación de ataques en Microsoft Defender Office 365 permite ejecutar simulaciones de ciberataque benignas en la organización. Estas simulaciones prueban las directivas y prácticas de seguridad, así como capacitan a los empleados para aumentar su concienciación y disminuir su susceptibilidad a los ataques.

En esta sección se explica cómo crear un *ataque de suplantación de identidad* simulado mediante el entrenamiento de simulación de ataques.

1. En el portal Microsoft Defender XDR, seleccionar la opción [Colaboración y correo electrónico| Entrenamiento de simulación de ataque]. https://security.microsoft.com/attacksimulator?viewid=simulations



2. En la pestaña “Simulaciones”, pulsar “Iniciar una Simulación”:

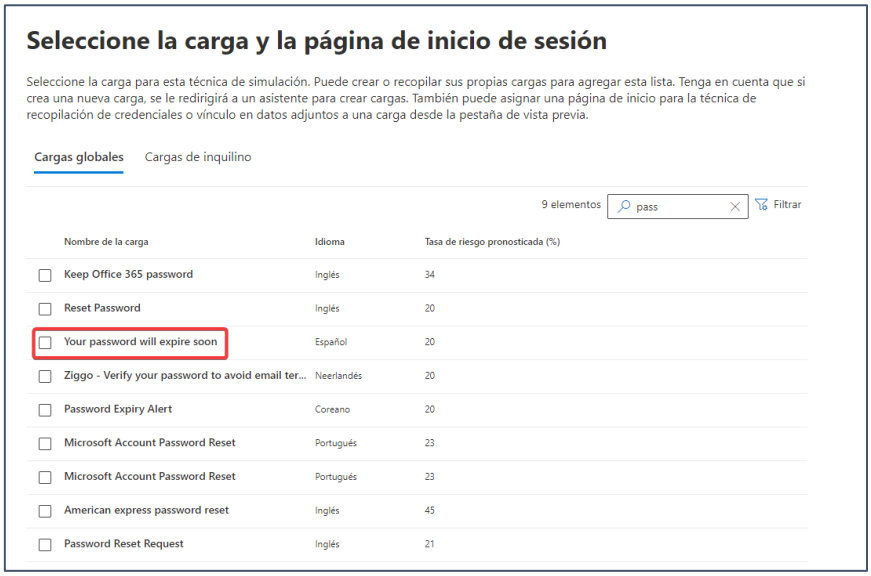
3. Se abrirá el Asistente para creación de simulación.

* Para el ejemplo se seleccionará Cosecha de credenciales (Credential Harvest).

4. Introducir un nombre y una descripción de la simulación:

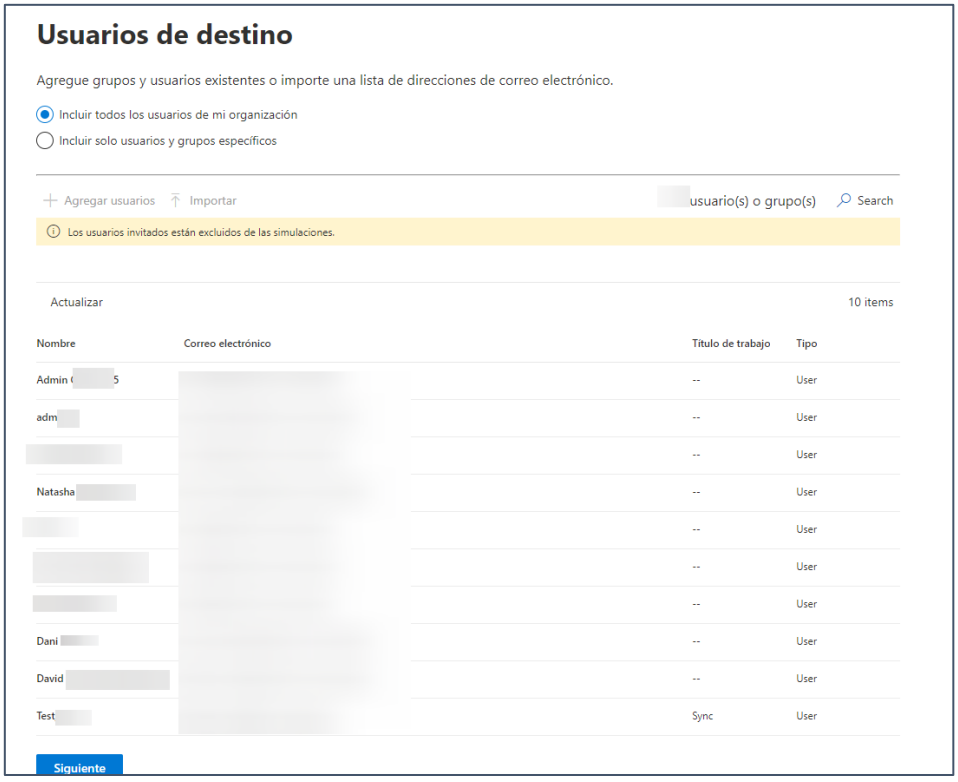
5. Seleccionar la carga (*payload*) para la simulación:

* Puede ordenarse por Idioma para ver las disponibles en español. Para el ejemplo se seleccionará “Your password will expire soon”.

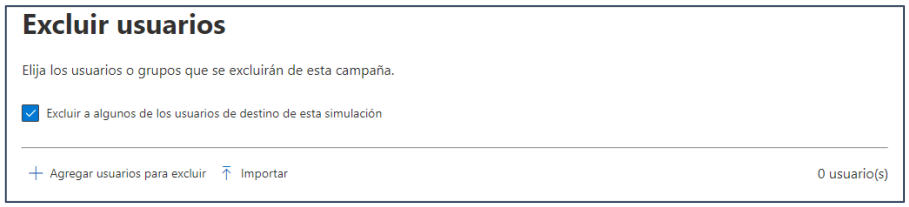


6. Seleccionar los usuarios de destino.

Agregar grupos y usuarios existentes o importar una lista de direcciones de correo electrónico.

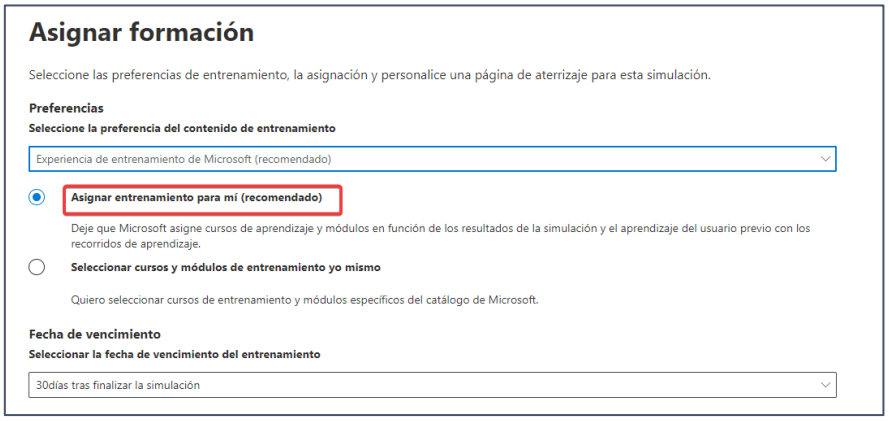


7. Si fuese necesario, se excluyen los usuarios necesarios. Bien importando un csv o excluyendo directamente a través de botón “add users to exclude”

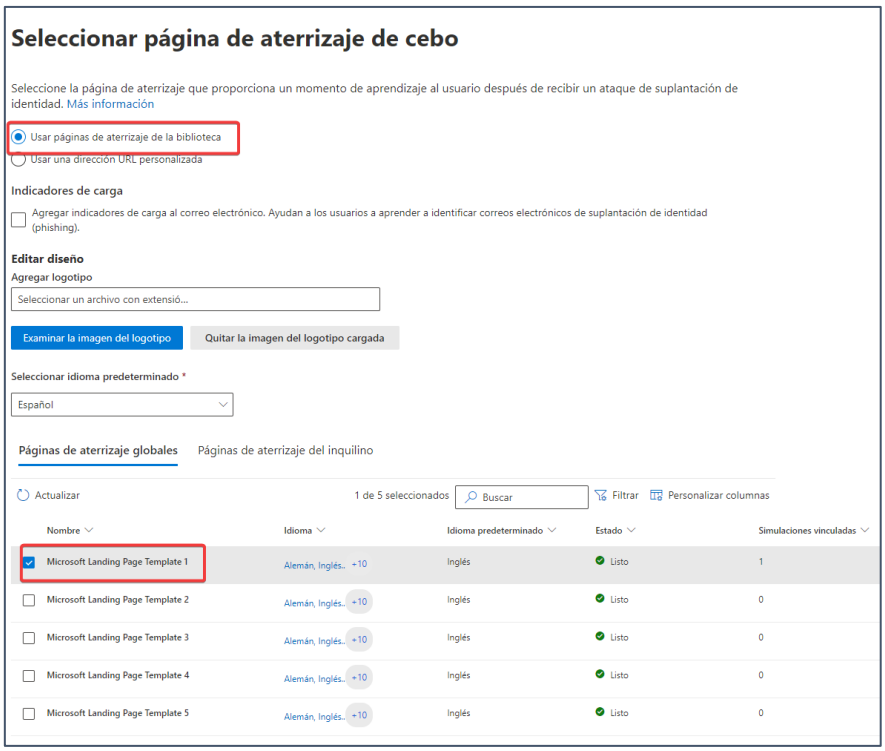


8. Asignar entrenamiento.

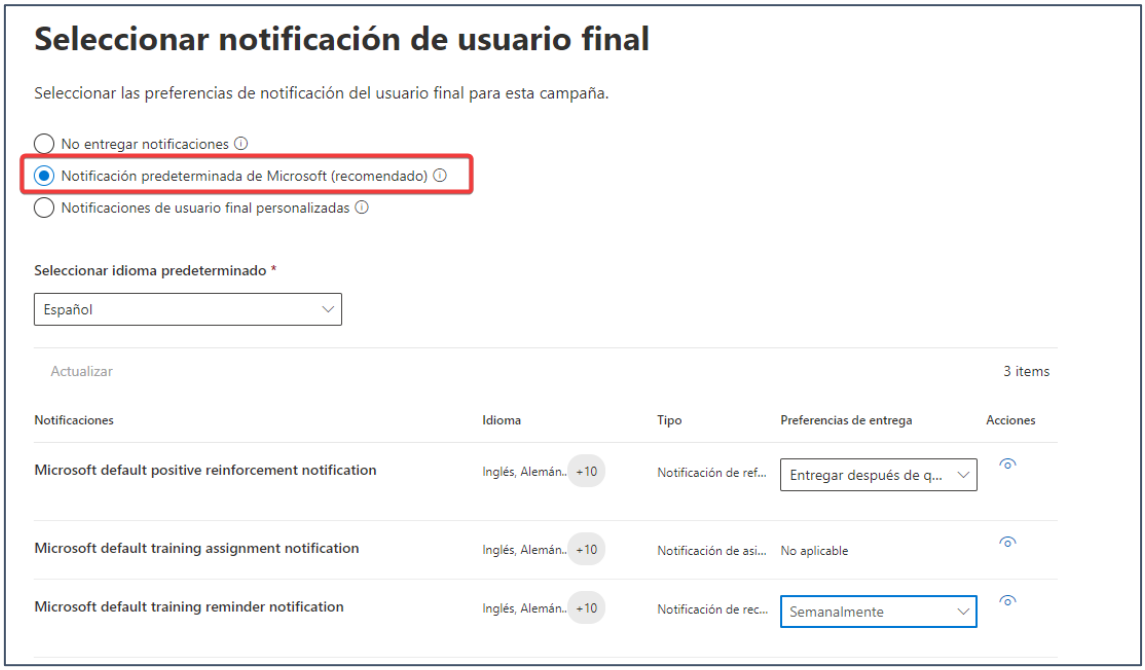
Seleccionar las preferencias de entrenamiento, y la asignación.



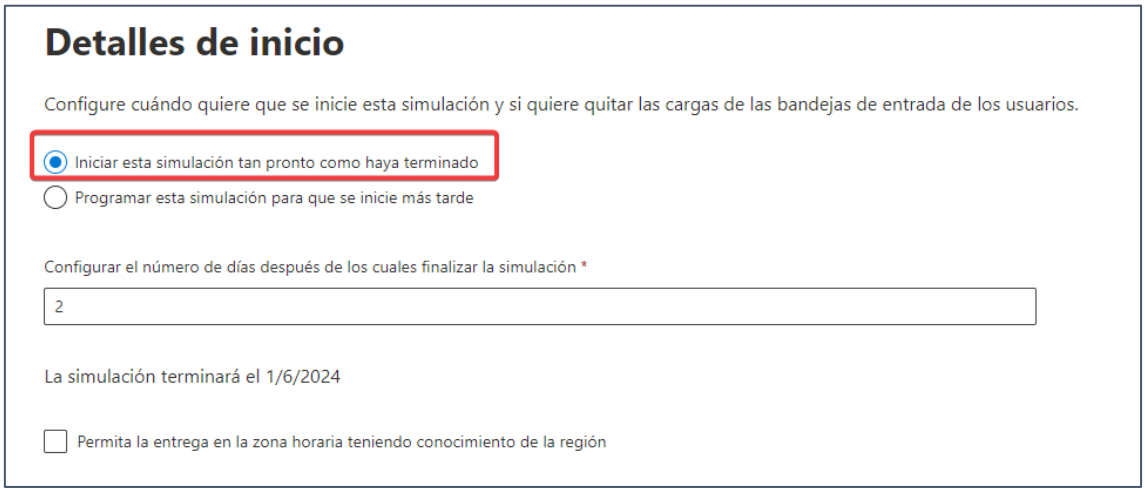
9. Personalizar una página de aterrizaje para esta simulación, a través de las plantillas que proporciona Microsoft o bien con una personalizada.



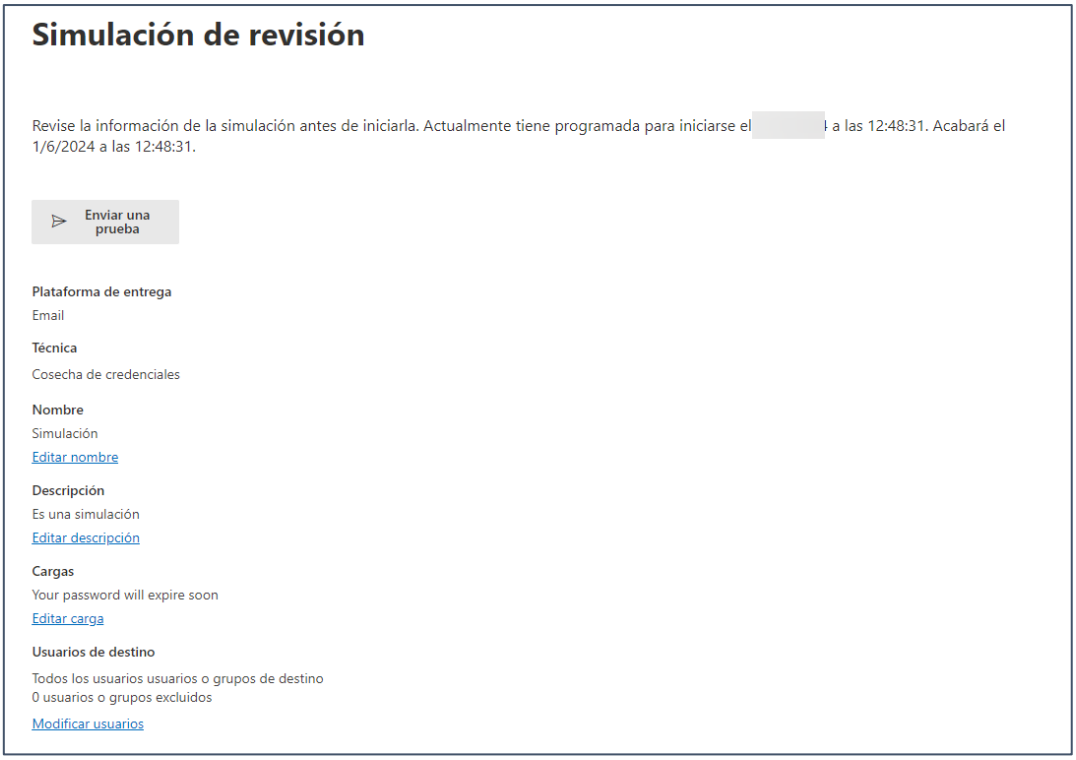
10. Seleccionar la notificación al usuario final. Al igual que en punto anterior es posible personalizar la notificación, así como su idioma.



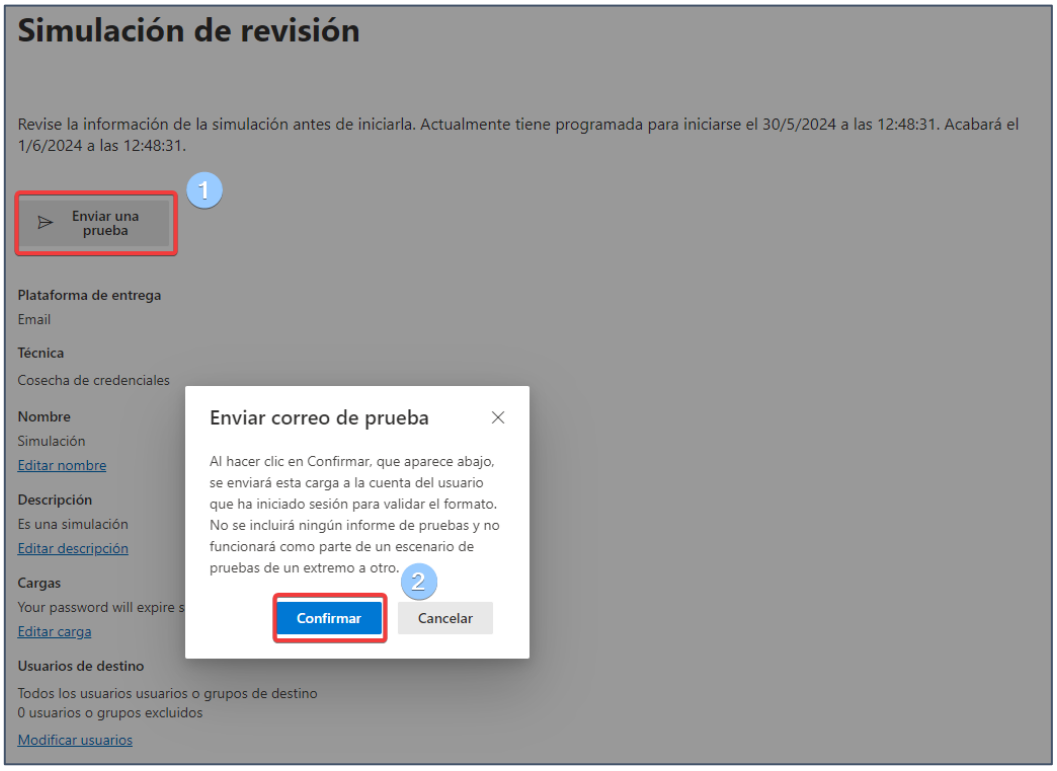
11. Configurar detalles del inicio.



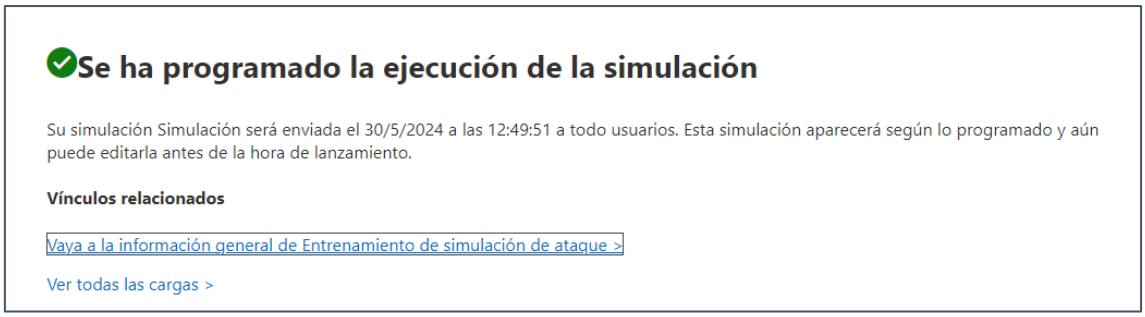
12. Revisar simulación.



Es conveniente enviar una prueba antes de lanzar a todos los usuarios.

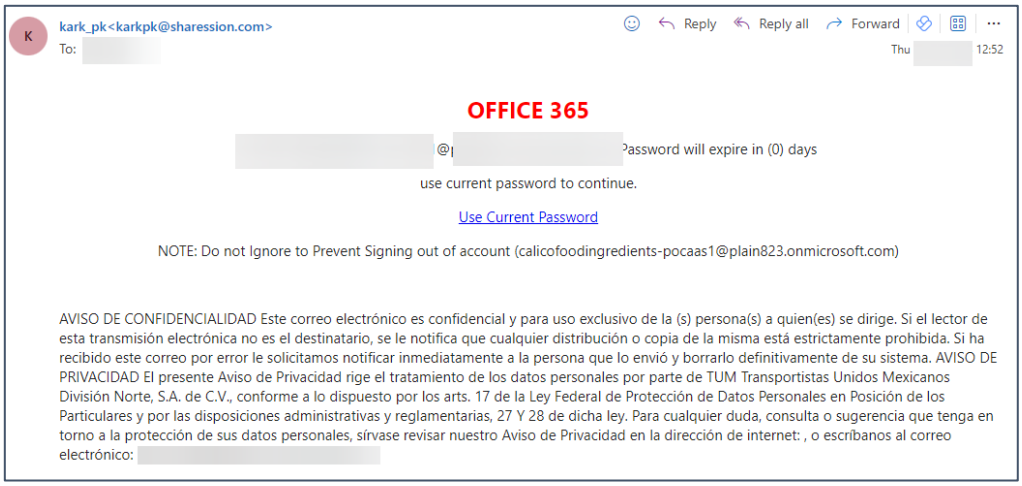


Una vez comprobado, pulsar Enviar. Al finalizar el envío, aparecerá el siguiente mensaje:

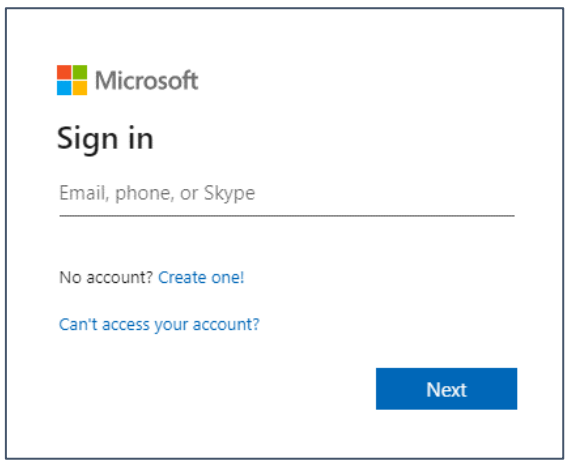


3.1.2 USUARIO AFECTADO POR LA SIMULACIÓN

Al usuario final objeto de la simulación, y poniendo como ejemplo la campaña realizada en el apartado anterior, le llegaría un email del tipo:



Al pulsar en el enlace, se le deriva a una ventana de login para que introduzca sus credenciales. Es una simulación parecida a la que utilizan los atacantes reales:

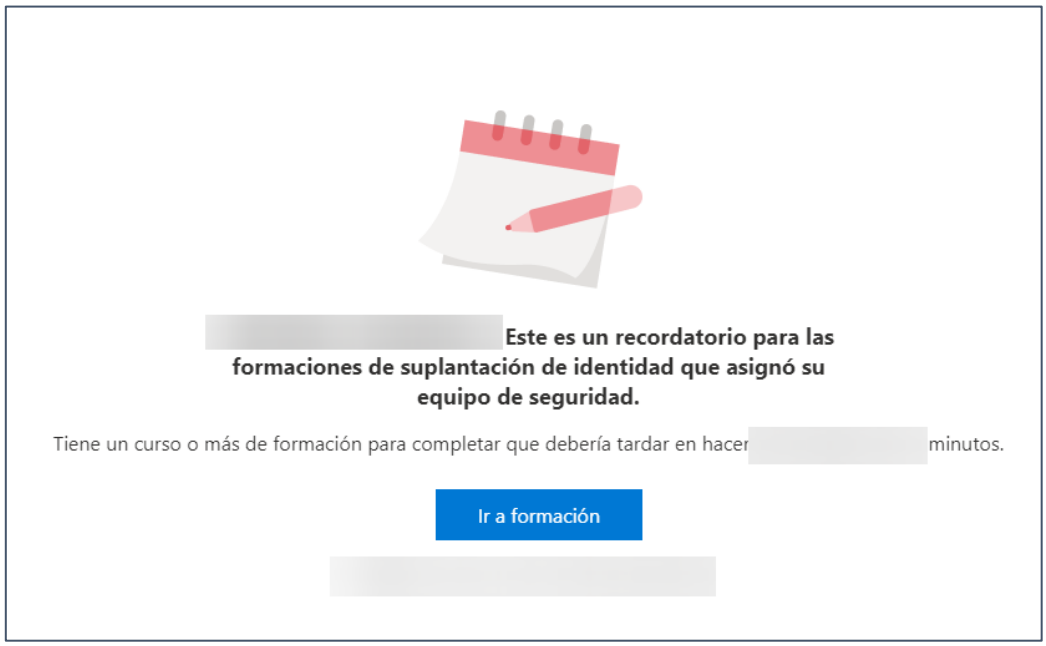


Tras finalizar el proceso, se advierte al usuario de que ha podido ser objeto de una suplantación de identidad:

3.1.3 ENTRENAMIENTO PARA EL USUARIO AFECTADO POR LA SIMULACIÓN

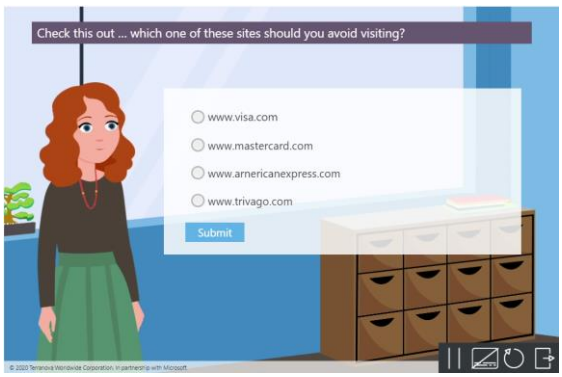
Después de notificar al usuario que ha podido ser un objeto de suplantación de identidad, se envía un correo electrónico para realizar un pequeño workshop de como detectar ataques de suplantación de identidad.

Recibirá el siguiente correo:



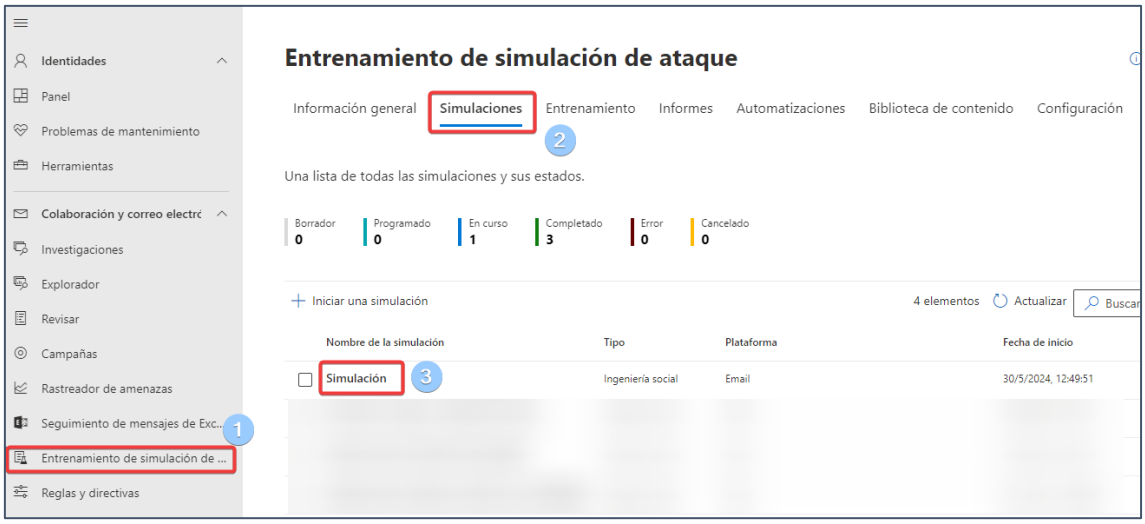
Que dará lugar a un pequeño taller o workshop.

Donde se incluyen varias preguntas.

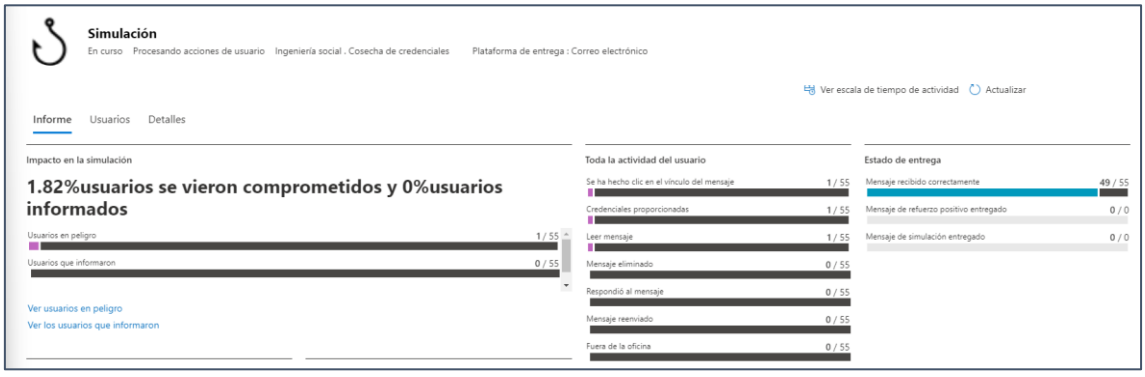


3.1.4 ANÁLISIS DE LA CAMPAÑA

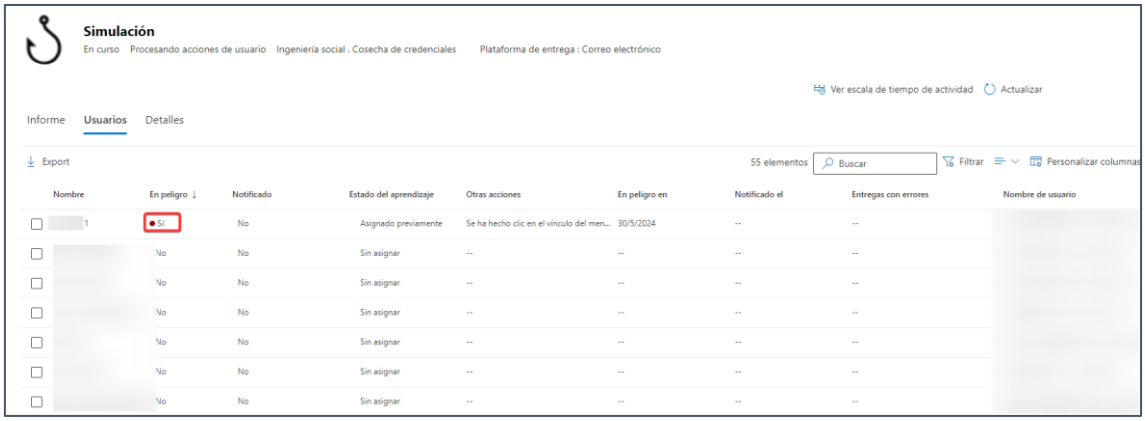
Desde el portal de seguridad, en la opción [Colaboración y correo electrónico| Entrenamiento de simulación de ataque], puede hacerse un seguimiento del resultado de la campaña y analizar los resultados.



Al pulsar en la simulación, se mostrará un resumen del impacto en la organización:



Incluso obtenerse un informe de los usuarios afectados:



4. GLOSARIO Y ABREVIATURAS

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

Término	Definición
AAD	*Azure Active Directory (Directorio Activo de Azure).*
AD DS	*Active Directory Domain Services (Servicios de dominio de Directorio Activo).*
AIP	*Azure Information Protection.*
AIR	*Automated Investigation and Response. Investigación y respuesta automatizada ante incidentes.*
Anti-phishing	*Medida que combate el phishing. El phishing es una técnica muy utilizada por los ciberdelincuentes para engañar a los usuarios y obtener información personal como contraseñas, tarjetas de crédito, cuentas bancarias etc.*
Anti-spam	*Medida que combate el spam. El spam es el correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.*
Anti-spoofing	*Medida que combate el spoofing. El spoofing consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet.*
Entra ID	*Microsoft Entra ID*
Centro de Administración de Microsoft 365	*Portal de Administración de Office 365.* *Accesible desde la url: admin.microsoft.com.*
CSC	*Centro de Seguridad y Cumplimiento de Office 365.*
DDoS	*Distributed Denial of Service (Ataque de Denegación de Servicio Distribuido), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.*
ENS	*Esquema Nacional de Seguridad.*

EOP	*Exchange Online Protection*
Malware	*Malware o "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.*
MFA	*Multifactor Authentication (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una app, sms, etc.*
Microsoft Intune	*Microsoft Intune es un servicio de administración de movilidad empresarial (EMM) basado en nube que ayuda a los empleados a ser productivos mientras mantiene protegidos los datos corporativos. Al igual que otros servicios de Azure, Microsoft Intune está disponible en el portal de Azure. Intune permite:* *-Administrar los dispositivos móviles y los equipos que los empleados usan para tener acceso a datos de la empresa.* *-Administrar las aplicaciones móviles que usa la plantilla.* *-Proteger la información de la empresa al ayudar a controlar la manera en que los empleados tienen acceso a ella y la comparten.* *-Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad de la empresa*
O365	*Office 365.*
Azure PowerShell	*PowerShell (originalmente llamada Windows PowerShell) es una interfaz de consola (CLI) con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts).*
PS	*PowerShell.*
SaaS	*Software as a Service (Software como Servicio). Modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de TIC, y se accede vía internet.*
Spoof intelligence insight	*Protección contra la suplantación de identidad en EOP.*
Tenant	*Un tenant de Office 365 es un espacio reservado en la nube de Microsoft desde el que tendremos acceso a los recursos y servicios que Microsoft ofrece.*

TLS	*TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos.*
ZAP	*ZAP – zero hour auto purge. En Microsoft 365 organizaciones con buzones en Exchange Online, la purga automática de hora cero (ZAP) es una característica de protección de correo electrónico que detecta y neutraliza de forma retroactiva mensajes de phishing, correo no deseado o malware malintencionados que ya se han entregado Exchange Online buzones de correo.*
XDR	*Solución que unifica múltiples productos de seguridad en una sola plataforma para mejorar la detección, investigación y respuesta a amenazas*
Workshop	*Evento educativo y participativo diseñado para que los asistentes aprendan y desarrollen habilidades específicas en un área determinada*
IA	*Es una rama de la informática que se enfoca en la creación de sistemas y tecnologías capaces de realizar tareas que normalmente requieren inteligencia humana*
Defender IT	*Microsoft Defender Threat Intelligence es una solución de ciberseguridad que proporciona información detallada y accionable sobre amenazas para ayudar a las organizaciones a identificar, protegerse y responder a ataques cibernéticos*
Workload	*Dentro de Microsoft Defender XDR son los diferentes tipos de recursos y servicios que pueden ser protegidos por la solución. Esto incluye dispositivos, identidades, aplicaciones, correo electrónico, entornos de nube y aplicaciones SaaS, ofreciendo una protección integral y unificada contra diversas amenazas y vulnerabilidades en toda la infraestructura de TI de una organización.*

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización podrá valorar qué medidas de las propuestas se cumplen.

<table>
<tr><th>Control ENS</th><th colspan="2">Configuracion</th><th>Estado</th></tr>
<tr><td>op</td><td colspan="3">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="3">Control de Acceso</td></tr>
<tr><td rowspan="3">Op.acc.3</td><td colspan="3">Segregación de funciones y tareas</td></tr>
<tr><td rowspan="2">Se ha asignado adecuadamente los roles de administración y la asignación de los usuarios a los grupos de seguridad (en función de los accesos que se quieran permitir).</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
</table>

Op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Se encuentra habilitado el “doble factor de autenticación” y se dispone de una adecuada política de gestión de credenciales.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.acc.6	**Mecanismo de autenticación (usuarios de la organización)**		
	Se ha activado la Ubicación de red para permitir el acceso solo desde determinadas direcciones IP. Y la limitación de acceso a los administradores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.6	**Protección frente a código dañino**		
	Se ha habilitado el filtro de datos adjuntos comunes y añadido los tipos de archivos correspondientes.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.exp.6	**Protección frente a código dañino**		
	Se ha activado la protección ZAP (Zero-hour auto purge).	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.6	**Protección frente a código dañino**		
	Se ha activado las notificaciones de malware a los administradores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.6	**Protección frente a código dañino**		
	Se ha establecido adecuadamente un umbral de correo electrónico de phishing y spam, así como el resto de las acciones descritas en la sección [3.1.2.1 Protección frente a código dañino].	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.mon	**Monitorización del sistema**		
	Se ha activado el registro de auditoría (on) para ver los datos en los informes de protección contra amenazas, de seguridad de correo electrónico y poder explotar la herramienta Explorador	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.vig	**Vigilancia**		
	Se ha revisado la configuración actual, con los planes estrictos o estandar que nos ofrece Microsoft para seguir sus buenas prácticas	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Otras	**Crear simulacion de ataque**		
	Se ha generado al menos una campaña de simulación de ataque para ver el nivel de adopción que existe en la organización frente ataques de phishing.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL