

Contenido

Laboratorio: Microsoft 365 Defender: Archivos adjuntos.....	2
Laboratorio: Política de Archivos adjuntos seguros.	5

Laboratorio: Microsoft 365 Defender: Archivos adjuntos.

Objetivo: Entender las **capacidades** y **características** de **seguridad** que tenemos disponibles tanto en **Azure** como en **Microsoft 365**.

Exchange Online Protection (EOP) nos provee **una protección basada en múltiples capas** para proteger a los usuarios de una gran variedad de amenazas o de ataques (*como phishing, spoofing, spam, el correo electrónico masivo y el malware*).

Microsoft 365 Defender amplía la **protección proporcionada** por **EOP** al **filtrar los ataques dirigidos** que podrían pasar a través de la línea de defensas de **EOP** (*amenazas avanzadas como los ataques de día cero en archivos adjuntos de correo electrónico y documentos de Office, y la protección en "tiempo clic" contra las URL maliciosas, campañas de phishing*).

Cuando se integran juntos, EOP y Microsoft Defender representan la **línea de protección antimalware** en **Microsoft 365** con niveles más eficientes contra amenazas básicos y Ataques Dirigidos avanzados.

Dependiendo del plan (o planes) contratados en la tenant tenemos **diferentes características de seguridad**:

- **Exchange Online Protection (EOP):** Filtrado de emails tanto en Cloud como on-premise.
 - Protección Anti-malware, Protección Anti-phishing, Protección Anti-spam y Purga automática Zero-hour (remediación de la amenaza después de la entrega).
- **Exchange Online:** 2 planes disponibles, el Plan 2 incluye Prevención de fuga de datos (DLP).
 - Informes de Auditorías.
- **Microsoft Defender for Office 365 (antiguo ATP):** Incluido en EMS E5 o adquirido como un Add-on.
 - Monitorizar y remediar ataques avanzados tanto on-premises como Cloud, Protección de Identidades e Indicarnos Anomalías de comportamiento (*Flag behavioral anomalies*).
- **Microsoft 365 ATP:** Incluido en Microsoft E5 o adquirido como un Add-on.
 - Office 365 ATP Plan 1. Protección como enlaces maliciosos en emails y protección para ficheros de Office y en emails (*ATP Safe Attachments policies, ATP Safe Links policies*) y Protección Advanced anti-phishing.
 - Office 365 ATP Plan 2. Todo los servicios incluidos en Office 365 ATP Plan 1, Simulador de Ataques, Investigación y Respuesta ante incidentes de seguridad automatizada, Threat explorer y Threat trackers.

+ **Info:** <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

Podemos definir **varias directivas** para **proteger** a los **usuarios** de **servicios de Microsoft 365** (*Exchange, SharePoint, OneDrive y Microsoft Teams*):

- **Archivos adjuntos seguros.** Protección contra archivos adjuntos maliciosos de día cero. NO está basado en firmas, sí no en características de sandboxing Cloud (*abre el archivo adjunto desconocido en un entorno especial de hipervisor y detonándolo, comprobando su comportamiento real*).
- **Vínculos seguros de Office 365.** Protección en el momento de hacer clic en los links que recibimos por email o en documentos, evitando que vayan a sitios web maliciosos o contra ataques de phishing (*estafas*).

- **anti-phishing protection, Antimalware y SPAM.** Aplica a todos los emails un extenso conjunto de modelos de aprendizaje automático entrenados y algoritmos avanzados para detectar mensajes de phishing, con malware o que pertenezcan a una campaña de correo no deseado o correo masivo (SPAM) y protegerse contra ellos.
- **Cuarentena.** Se pueden enviar a cuarentena los emails que el servicio de Office 365 identifique como spam, (*correo masivo*), correos con phishing, con malware o por coincidencia con una regla de flujo de correo. De forma predeterminada, Office 365 envía los emails con phishing y con malware directamente a la cuarentena. Los usuarios autorizados pueden revisar, eliminar o administrar estos emails enviados a cuarentena.

Exchange Online Protection pone a nuestra disposición **una protección basada en filtros**. Cada email que recibe un usuario **pasará todos y cada uno de estos filtros**, siguiendo un **estricto orden y prioridad de filtrado** para que cuando el email sea **entregado** estemos seguros de que es un **correo legítimo y sin malware**.

Sí el email hace match en **cualquiera** de los **filtros de protección**, se **aplicará la/s directiva/s** que **correspondan**, enviando el email a cuarentena, eliminándolo, entregándolo modificado, etc.

¿Cuál es el **orden** y la **prioridad** que **Exchange Online Protection** aplica para proteger la mensajería del servicio provisto por Exchange Online?:

Prioridad	Protección de correo electrónico	Categoría en función del etiquetado del msg	¿Dónde se administra?
1	Malware	CAT: MALW	Configurar directivas antimalware en EOP
2	Phishing	CAT: PSHH	Configuración de directivas contra correo no deseado en EOP
3	Correo no deseado de alta confianza	CAT: HSPM	Configuración de directivas contra correo no deseado en EOP
4	Suplantación de identidad (phishing)	CAT: SUPLANTACIÓN DE IDENTIDAD	Configurar inteligencia de identidades en EOP
5	Correo no deseado (SPAM)	CAT: SPM	Configuración de directivas contra correo no deseado en EOP
6	Masivo (SPAM)	CAT: BULK	Configuración de directivas contra correo no deseado en EOP
0,7*	Suplantación dominio (usuarios protegidos)	DIMP	Configurar directivas contra phishing de ATP

Prioridad	Protección de correo electrónico	Categoría en función del etiquetado del msg	¿Dónde se administra?
8,5*	Suplantación de usuario (dominios protegidos)	UIMP	Configurar directivas contra phishing de ATP

+ información: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/how-policies-and-protections-are-combined?view=o365-worldwide>

Laboratorio: Política de Archivos adjuntos seguros.

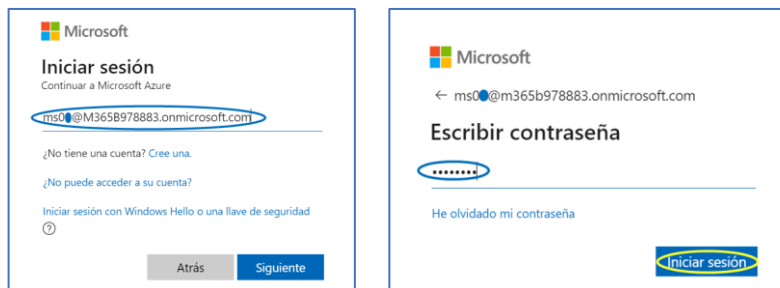
Objetivo: Entender y desplegar una política de protección contra amenazas sobre emails legítimos y ficheros.

Las directivas de **Microsoft 365 Defender: Archivos adjuntos seguros comprueban** en todos los mensajes entrantes, archivos adjuntos en busca de contenido malicioso. Búsqueda basada en firmas de virus/malware (tanto de Microsoft como de terceros). Si no se detecta en el fichero adjunto, malware o este fichero no forma parte de alguna campaña contra nuestra empresa (como pieza de un ataque dirigido), el mensaje se entregará a su destinatario o siguiente MTA de salto hacia su destino final. Los archivos adjuntos se enviarán su detección a en un entorno de sandboxing (entorno virtualizado con diferentes versiones de Apps y SO Windows) donde se le someterá a un análisis de comportamiento para determinar si tiene una carga útil maliciosa que modifica el registro, la configuración del sistema, elevación de permisos, escaneo de puertos, etc.

Prerrequisitos: Tener una tenant de Microsoft propia o de prueba con los planes o servicios correspondientes, Business Premium, Planes Empresa o Servicios “suelos” (Exchange Online P1/P2, SharePoint Online P1/P2, Teams, etc).

Pasos a realizar:

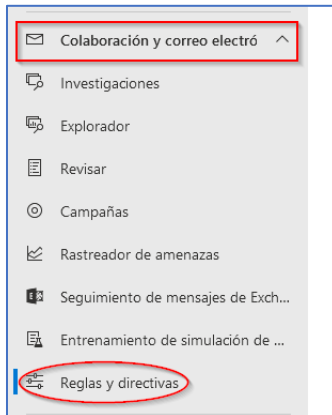
1. **Logarnos** en el **Centro de seguridad de Microsoft 365**, en: <https://security.microsoft.com/> como **admin**.
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



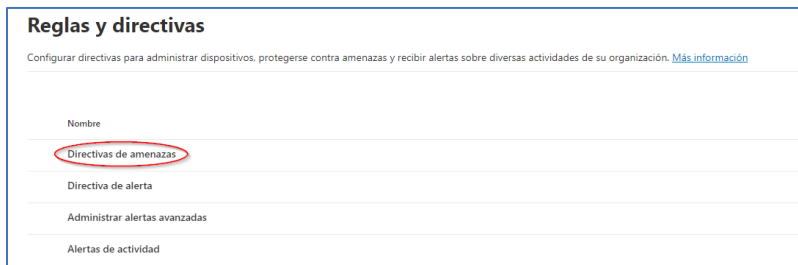
2. Aparecerá la **Dashboard** del **Portal de Seguridad de Microsoft 365**.



3. Clic en el **menú vertical de la parte izquierda de la pantalla** en la entrada **Reglas y Directivas** dentro de la sección vertical **Colaboración y correo electrónico**.



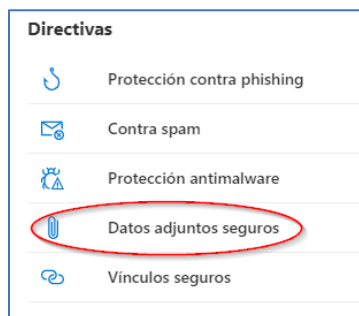
4. En la siguiente ventana, clic en **Directivas de amenazas**.



5. Aparecerán las opciones disponibles de: **Directivas de amenazas**. Microsoft crea diferentes **plantillas**, basadas en **vectores de ataque actuales** que podremos *implementar en pocos clics*.



6. **Nosotros en lugar de utilizar las plantillas, nos crearemos desde cero una directiva de: Archivos adjuntos seguros.** Para ello, clic en el *enlace: Datos adjuntos seguros* en la sección *Directivas*.



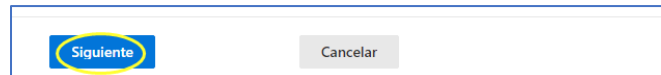
7. Clic en el botón “+ crear”.



8. Aparecerá una **nueva ventana** donde podremos configurar la **nueva directiva de protección de Datos Adjuntos Seguros**.

- Nombre:** EMS0x - Directiva de Datos Adjuntos Seguros *(la “x” es el usuario que los instructores os hemos proporcionado al comienzo del curso).*
- Descripción:** Directiva de Datos Adjuntos Seguros.

Clic en el botón inferior de la pantalla: **Siguiente**.



- Sección **Usuarios y dominios**. En esta sección configuraremos a **quien** se le **aplicará** dentro de nuestra tenant **esta política**, eligiendo entre **usuario/s**, **Grupos de Microsoft 365** o **Dominios**. **¡¡¡POR FAVOR!!!**. Seleccionar **nuestro usuario**, lo habitual sería crear un grupo con los usuarios a los que queramos aplicar esta directiva.
NOTA: podemos excluir usuarios dentro de los grupos que estemos seleccionando.

Clic en el **botón** inferior de la pantalla: **Siguiente**.

- d. Sección **Configuración**: Seleccionamos la respuesta contra el malware, que vamos a realizar cuando se detecte un malware desconocido en adjuntos o ficheros con los que están trabajando nuestros usuarios.

Tenemos varias opciones, en nuestro caso, **clic** en la última opción: **Entrega dinámica**.

¿Qué es Entrega dinámica?:

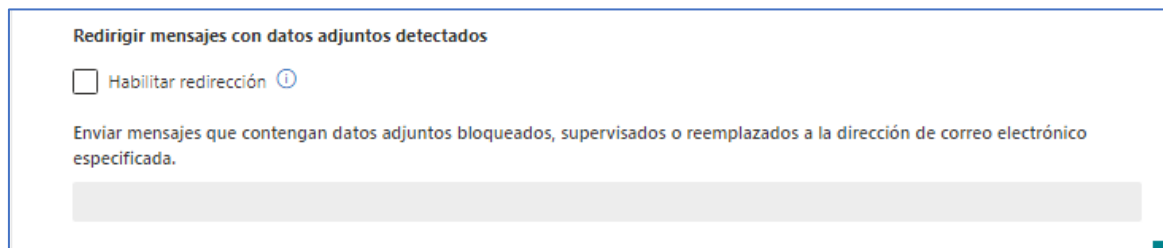
- Esta opción entrega el mensaje automáticamente al buzón del usuario.
- Reemplaza los archivos adjuntos por archivo marcadores de posición hasta que se complete su análisis y si no se detecta ningún malware los vuelve a adjuntar.
- Vista previa, durante el escaneo, de archivos adjuntos para la mayoría de los PDF y archivos de Office.

- iv. Envía los mensajes con malware detectado a la Cuarentena, donde un administrador o analista de seguridad puede revisar, liberar o eliminarlos.

NOTA: En Directiva de cuarentena. No podremos seleccionar nada ya que no tenemos ninguna creada.

- e. Dentro de la sección: **Redirigir mensajes con datos adjuntos al detectarlos**. Nos permitiría trabajar con Exchange Online como lo hacen la mayoría de software de seguridad de terceros del mercado cuando están protegiendo un Microsoft Exchange Server on-premise (*en las instalación de nuestros clientes*), es decir, **crearnos un buzón compartido** (*para no pagar una licencia por él*) y **utilizarlo** como un **buzón de correo tipo: Bulk**, **redirigiendo todos los emails con malware a este buzón**, para posteriormente poder realizar tareas de forensia, sobre esta primera parte de la cadena de ataque que conforma este primer paso, en mundo on-premise, se asigna un buzón bulk ya que, al no ser un servicio SaaS, no se suele incurrir en costes, ya que se asume en el almacenamiento de la MTA (*Microsoft Exchange Server*).

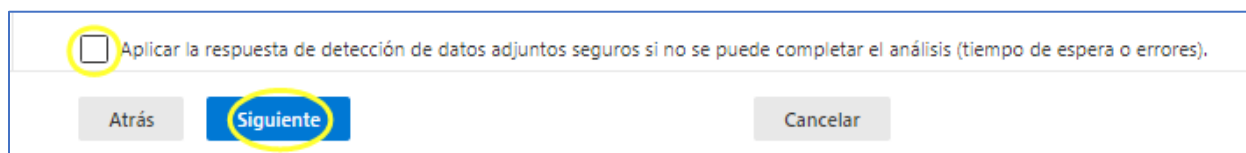
NO seleccionaremos NINGÚN buzón. Recomendado crear un buzón compartido en Exchange administration Center anteriormente para poder seleccionarlo.



+ info: En esta **URL** encontraremos que **conllea seleccionar** cada una de estas opciones:

<https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policies?view=o365-worldwide>

- f. Podemos definir nuestra respuesta base de forma tangencial, pase lo que pase. **NO hacer clic** en la **caja de selección**. Sí hacemos clic tendremos que definir un buzón “bulk” en la opción anterior.



Clic en el botón inferior de la pantalla: Siguiente.

- g. Sección **Revisar**. En esta sección **revisaremos las opciones** que hemos seleccionado y **clíc** en el **botón Enviar**.

- h. Nos **aparecerán una o varias ventanas informativas**, por favor revisarlas, para **terminar** la creación de esta directiva.

Clíc en el botón inferior: **Listo**.

+ info: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policies?view=o365-worldwide#policyoptions>