

Contenido

Laboratorio: Protección contra Malware y Amenazas Avanzadas de Microsoft 365.	2
Laboratorio: Política de Vínculos seguros de Office 365.	5

Laboratorio: Protección contra Malware y Amenazas Avanzadas de Microsoft 365.

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 Defender for Office 365 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 el 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

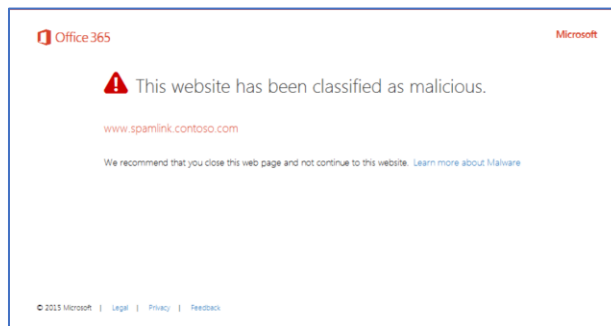
+ información: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/how-policies-and-protections-are-combined?view=o365-worldwide>

Laboratorio: Política de Vínculos seguros de Office 365.

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

Las **directivas** de **ATP Vínculos seguros comprueban todas las URLs** usadas generalmente en ataques de **phishing** para conseguir información sensible del usuario, que se **encuentren en cualquier parte de los emails entrantes** y **archivos adjuntos** en **busca de enlaces maliciosos** en el **instante** en que el usuario hace **clic en ellos**, aparte de por supuesto de analizar el resto de los links **contra su lista de URLs bloqueadas**.

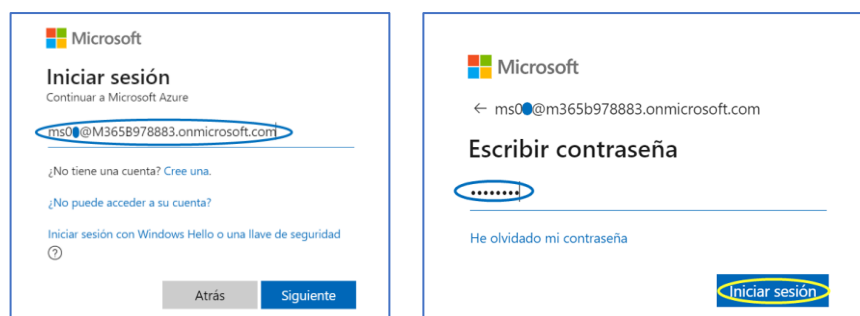
Sí la URL a la que el usuario está intentando acceder es maliciosa, se mostrará esta pantalla en su navegador:



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:

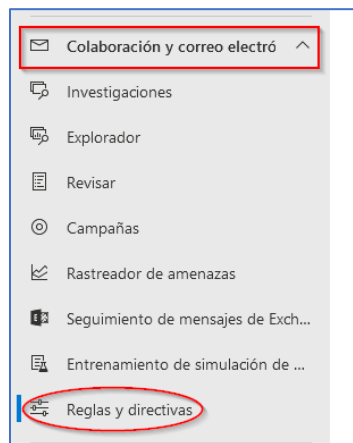
1. **Logarnos** en el **Centro de seguridad de Microsoft 365**, en: <https://security.office.com/> como **admin**.
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó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



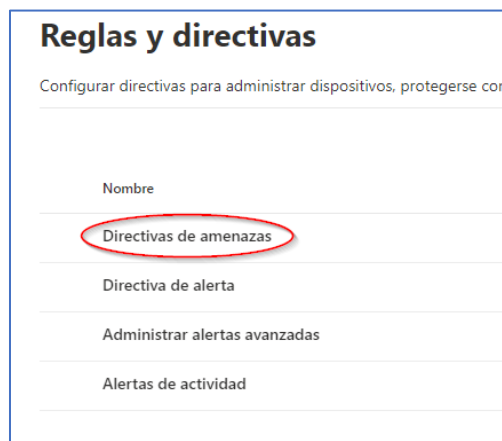
2. Aparecerá la **Dashboard del Portal de Seguridad de Microsoft 365**.



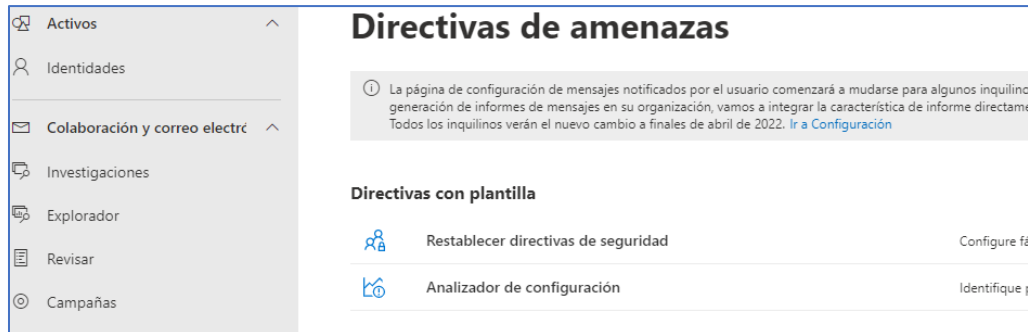
3. **Clic en el menú vertical de la parte izquierda de la pantalla en la entrada Reglas y Directivas dentro de la sección vertical Colaboración y correo electrónico.**



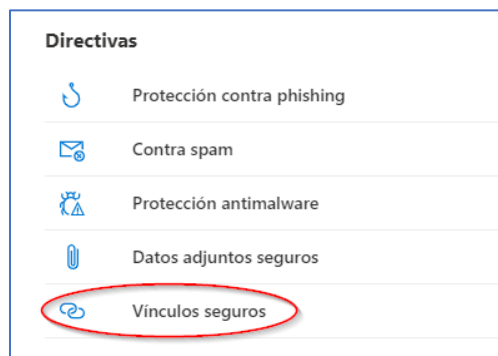
4. **Clic en Directivas de amenazas.**



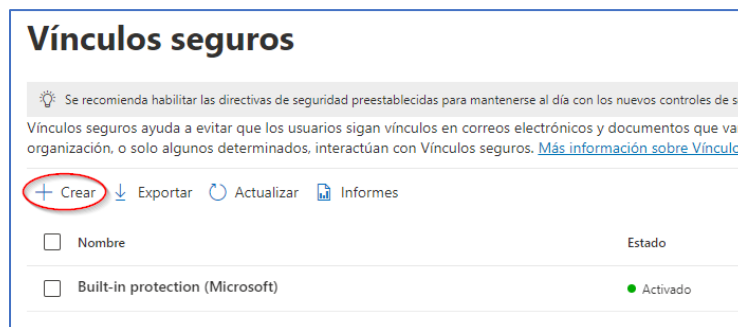
5. En la siguiente ventana, aparecerán las opciones que tenemos disponibles para implementar las directivas de protección. Microsoft pone a nuestra disposición diferentes **plantillas ya creadas**, basadas en **vectores de ataque actuales** que podremos *implementar en pocos clic*.



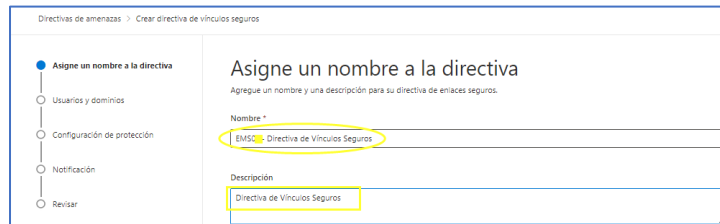
6. **Nosotros en lugar de utilizar las plantillas, nos crearemos desde cero una directiva de: Vínculos seguros.** Para ello, clic en el enlace **Vínculos seguros** en la sección *Directivas*.



7. **Clic en el botón “+ crear”.**



8. Nos aparecerá una **nueva ventana** donde en la **primera sección: Aplique un nombre a la directiva:**
- Nombre:** EMS0x - Directiva de Vínculos Seguros *(la "x" es el usuario que hemos proporcionado al comienzo del curso).*
 - Descripción:** Directiva de Vínculos Seguros.



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



9. A Sección **Usuarios y dominios**. En esta sección configuraremos **a quien** se le **aplicará** dentro de nuestra tenant **esta política**, pudiendo discriminar 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.**



10. Sección **Configuración de protección de direcciones URL y clics**. En esta sección **configuraremos las opciones de análisis y protección** contra malware que se encuentre alojado en las URLs que recibamos o que trabajemos con ellas vía documentación en Teams.

Apartado: Seleccione las acciones a realizar para las direcciones URL desconocidas potencialmente malintencionadas en los mensajes.

Clic en la caja de selección Activado...

Configuración de protección de direcciones URL y clics

Establezca la dirección URL de sus vínculos seguros y haga clic en configuración de protección para esta directiva.
[Más información.](#)

Correo electrónico

☒ Activado: Vínculos seguros comprueba una lista de vínculos malintencionados conocidos cuando los usuarios hacen clic en vínculos en el correo electrónico. Las direcciones URL se reescriben de forma predeterminada.

- ☒ Aplicar vínculos seguros a los mensajes de correo electrónico enviados dentro de la organización
- ☒ Aplicar un análisis de URL en tiempo real para vínculos sospechosos y vínculos que apuntan a archivos
- ☒ Espere a que el análisis de URL se complete antes de entregar el mensaje.
- ☒ No vuelva a escribir las direcciones URL; realice las comprobaciones solo a través de la API de vínculos seguros.

El siguiente apartado **nos permitirá NO reescribir URLs**, *muy útil para web bancarias, financieras, etc. NO especificaremos ninguna*, por regla general, *aquí iremos añadiendo posteriormente URLs cuándo nuestros usuarios, normalmente financieros, etc, nos las vayan especificando.*

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

[Administrar 0 dirección URL](#)

Apartado: Teams. *Activaremos el seguimiento y la protección asociada para URLs potencialmente malintencionadas o desconocidas en Microsoft Teams.*

Clic en la caja de selección Activado.

Teams

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

Apartado: Aplicaciones de Office 365. *Activaremos el seguimiento y la protección asociada para URLs potencialmente malintencionadas o desconocidas en Microsoft Office (tanto online, Office Web Apps como el paquete de Office instalado en cada dispositivo).*

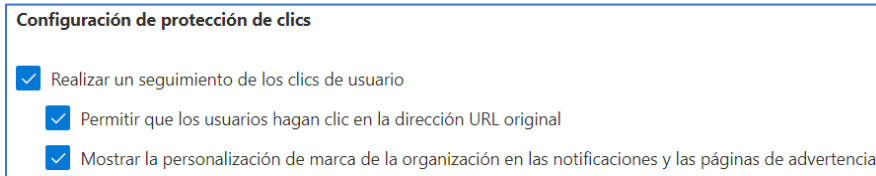
Clic en la caja de selección Activado.

Aplicaciones de Office 365

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

Apartado: Configuración de protección de clics. *Activaremos el seguimiento y la protección asociada para las URLs en las hagan clics nuestros usuarios, permitiendo o no que acceden a la URL original y si no permitimos el acceso que les aparezca la “página de advertencia” en logo de su empresa.*

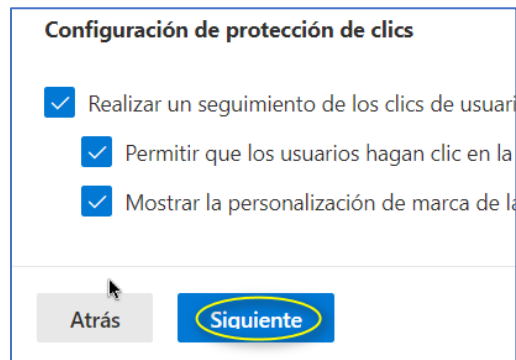
Clic en la todas las opciones.



Configuración de protección de clics

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

Clic en el botón: Siguiente para avanzar a la siguiente sección de este asistente.



Configuración de protección de clics

- ☒ Realizar un seguimiento de los clics de usuario
- ☒ Permitir que los usuarios hagan clic en la
- ☒ Mostrar la personalización de marca de la

Atrás Siguiente

11. Sección **Notificación**: Podemos seleccionar el **texto**, incluso utilizando Microsoft Translator para usuarios que no tengan seleccionado el idioma en que los estamos escribiendo como base de sus Sistema Operativo, que se mostrará a los usuarios advirtiéndoles del peligro de esa URL.

Dentro del campo de escritura, “Copiar y pegar” este texto:

La URL a la estás intentando acceder es maliciosa. Por favor, no hacer clic en ningún enlace que lleve a ella.

Clic en la caja de selección tal y como aparece en la siguiente imagen.

12. Sección **Revisar**: *Revisamos la configuración que hemos creado y clic en el botón: Enviar.*

13. Nos **aparecerán una o varias ventanas informativas**, por favor revisarlas, para **terminar** la creación de esta directiva. **Clic en el botón: Listo.**

