Contenido

Laboratorio: Microsoft 365 Defender, Protección contra phishing.

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, Protección contra phishing 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 decorreo electrónico	Categoría en función del etiquetado el msg	¿Dónde se administra?
1	**Malware**	CAT: MALW	Configurar directivas antimalware en EOP
2	**Phishing**	CAT: PHSH	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 decorreo electrónico	Categoría en función del etiquetado el msg	¿Dónde se administra?
8,5*	**Suplantación 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 Protección contra phishing.

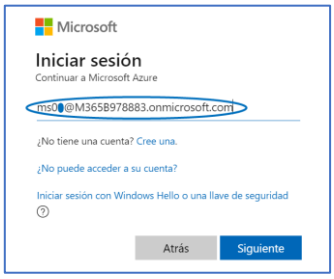
Objetivo: Entender y desplegar **directivas** de **protección contra suplantaciones** tanto de **dominios** como de **usuarios**. Los atacantes se harán pasar por nuestra organización, suplantando el dominio completo o suplantando la identidad de un usuario real o imaginario con el que intentarán realizar transacciones tanto con usuarios internos como externos para conseguir información, dinero, etc.

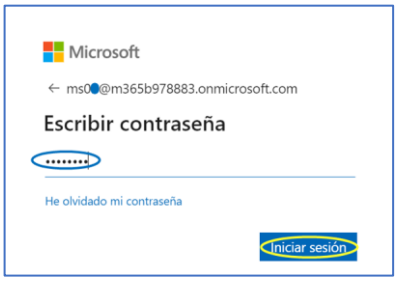
Podemos **configurar tanto** la **Directiva predeterminada** de **ATP Protección contra phishing**, como **una directiva nueva a un usuario o grupo de usuarios** para **detectar** y **prevenir** mejor los **ataques** de **suplantación de identidad/s** y **suplantación/es electrónica/s**.

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

Pasos a realizar:

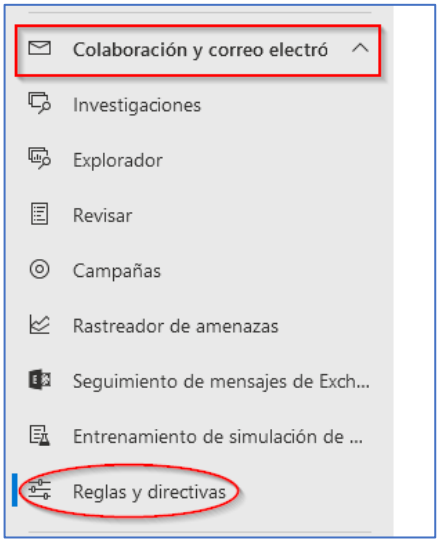
1. **Logarnos** en el **Centro de seguridad de Microsoft 365**, en: https://security.office.com/ como **admin**.
   Usuario: EMS0x@m365********.onmicrosoft.com *(la "**x**" es el usuario que os hemos dado al comienzo del curso)*.
   Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el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



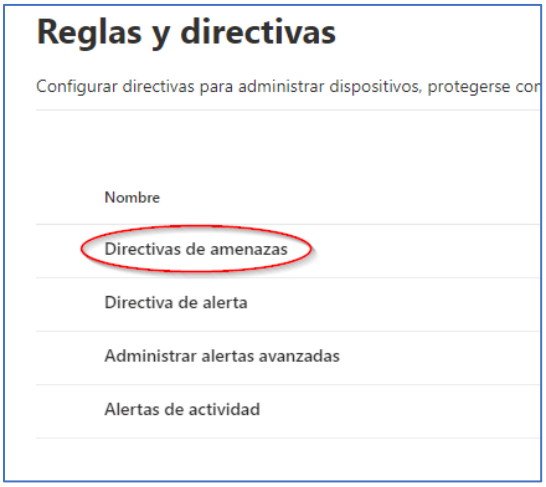


2. Aparecerá la **Dashboard** del **Portal de Seguridad de Microsoft 365**.

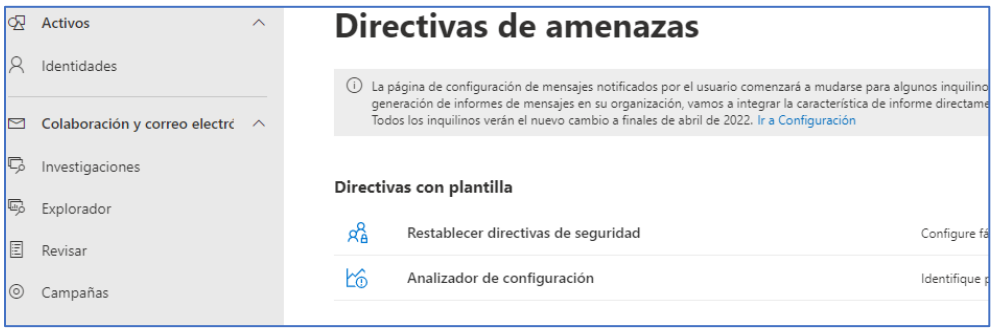
3. **Clic** en el **menú vertical de la parte izquierda de la pantalla** en la entrada **Reglas y Directivas** *dentro de la sección vertical* **Colaboración y correo electrónico**.



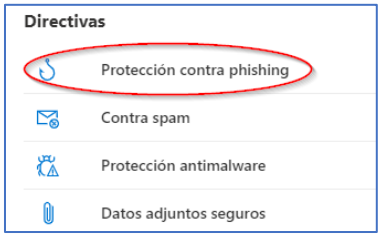
4. **Clic** en **Directivas de amenazas.**



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 clics*.

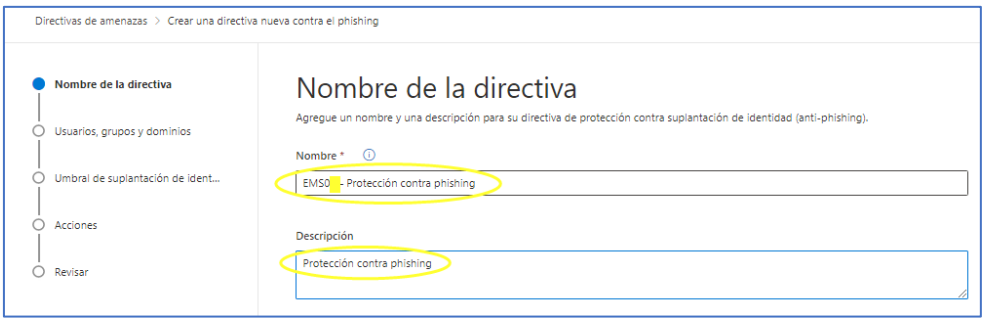


6. **Nosotros** en **lugar de utilizar** las **plantillas**, nos **crearemos** una directiva de este tipo desde **cero**. **Clic** en el **enlace Protección contra phishing** en la sección *Directivas*.

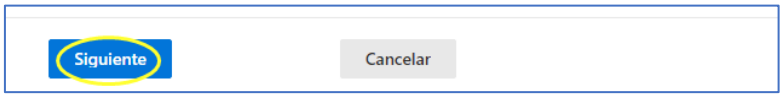


7. Aquí encontraremos las directivas que creemos para **analizar** y **protegernos** del **vector de ataque** que suponen los engaños fraudulentos que podemos recibir. **Clic** en el **botón "+ crear"**.

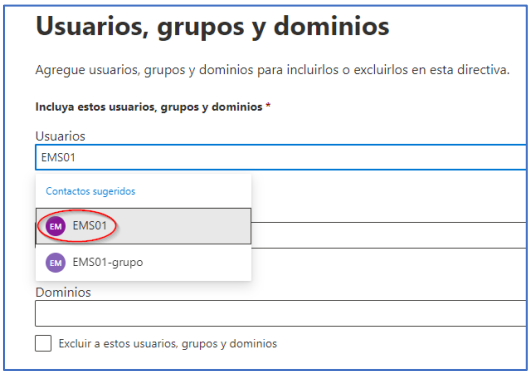
8. Aparecerá una **nueva ventana** donde podremos configurar la **nueva directiva** de **protección** de **Datos Adjuntos Seguros**.
   a. **Nombre**: **EMS0x – Protección contra phishing** *(la "**x**" es el usuario que los instructores os hemos proporcionado al comienzo del curso)*.
   b. **Descripción**: **Protección contra phishing.**



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

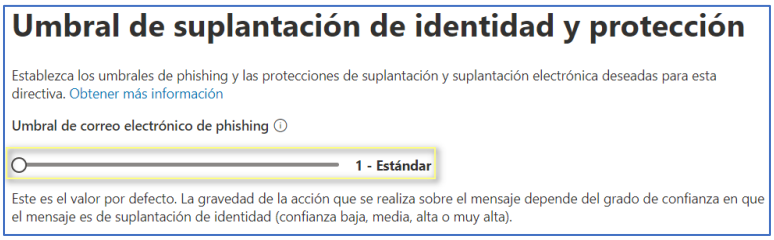


9. Sección **Usuarios y dominios.** En esta sección configuraremos **a quien** se le **aplicará** dentro de nuestra tenant **esta política**, pudiendo discriminar entre **usuario/s**, **Grupos de Microsoft 365** o **Dominios.**
   *¡¡¡POR FAVOR!!!. Seleccionar **nuestro usuario**, lo habitual sería crear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

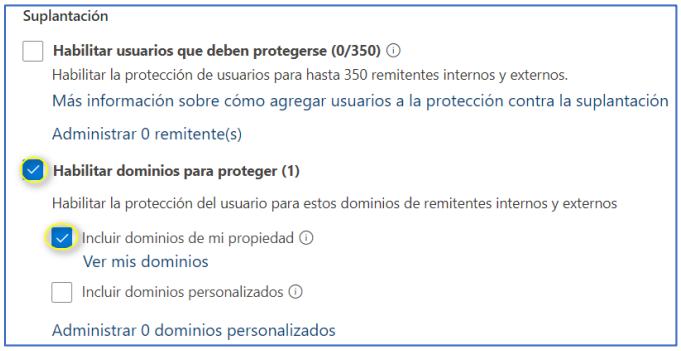


   Clic en el **botón: Siguiente**.

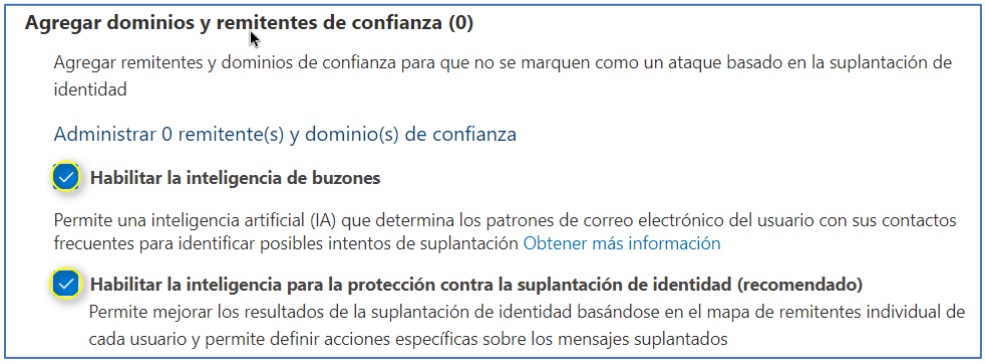
10. Sección **Umbral de suplantación de identidad y protección: Siempre estará habilitado**, la inteligencia de **Microsoft protegerá basándose en umbrales** que **definamos**.
    Dejará en 1- Estándar.
    ***NOTA**: Sí queréis podéis dedicar unos instantes a revisar que involucra cada uno de los umbrales del deslizable.*



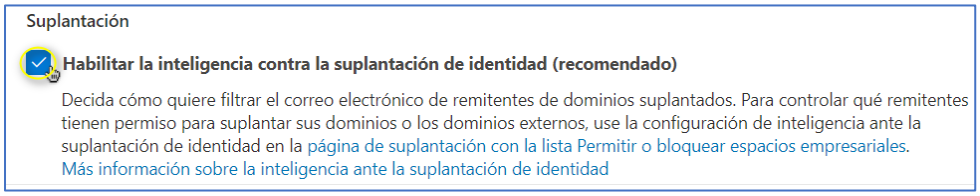
11. **Clic** en la *caja de selección*: **Habilitar dominios para proteger**.
    Clic en la *caja de selección*: **Incluir dominios de mi propiedad**. Para **proteger** los **dominios** que tenemos **dados de alta y verificados** en el *portal de administración de Microsoft 365 (incluyendo el dominio *.onmicrosoft.com)*.



12. **Clic** en las **2 opciones** dentro de la *sección*: **Agregar dominios y remitentes de confianza**.



13. **Clic** en la *caja de selección*: **Habilitar la inteligencia contra la suplantación de identidad (recomendado)**.



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

15. Dentro de la *sección*: **Acciones en mensajes**. Configurar las **siguientes opciones**. Básicamente todos los *mensajes detectados* los pondremos en **cuarentena**, de esta forma, podremos gestionar la cuarenta para *forensia* y por sí algún *usuario* nos pide algún email que haya sido detectado como *falso positivo* **EXCEPTO** *la opción: Si se detecta que el mensaje es falso* que los remitiremos a la gestión de nuestros propios usuarios:
    a. *Si el mensaje se detecta como un usuario suplantado*: **No** lo **podremos configurar** ya que no estamos protegiendo usuarios "*sueltos*" sino que estamos **protegiendo todos los dominios** que tenemos dados de alta y verificados en nuestra tenant.

       Aparecerá un **nuevo desplegable** donde seleccionaremos la *directiva de cuarenta*: **AdminOnlyAccessPolicy**.

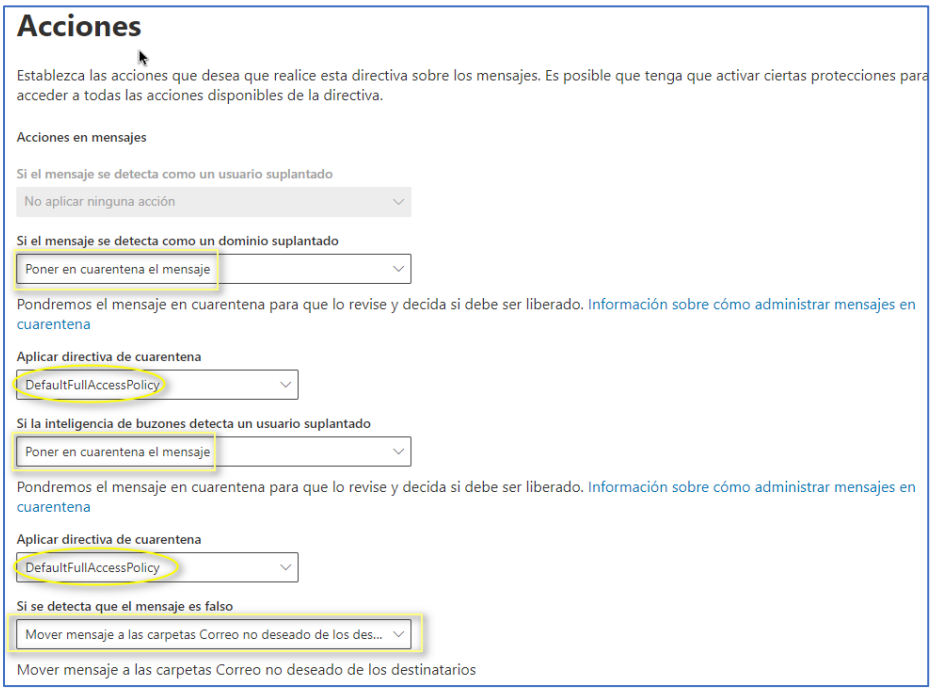
    b. *Si el mensaje se detecta como un dominio suplantado*. **Poner en cuarentena el mensaje**.

       Aparecerá un **nuevo desplegable** donde seleccionaremos la *directiva de cuarenta*: **AdminOnlyAccessPolicy**.

c. *Si la inteligencia de buzones detecta un usuario suplantado*. **Poner en cuarentena el mensaje**.

Aparecerá un **nuevo desplegable** donde seleccionaremos la *directiva de cuarenta*: **AdminOnlyAccessPolicy**.

d. *Si se detecta que el mensaje es falso*.**Mover mensaje a las carpetas Correo no deseado de los destinatarios**.
Con esta **acción**, **marcamos** los **emails como no deseados** y permitimos que sean los propios **usuarios quienes** realicen las **acciones** que **consideren oportunas**. Seleccionaremos esta opción, tal y como aparece en la imagen.



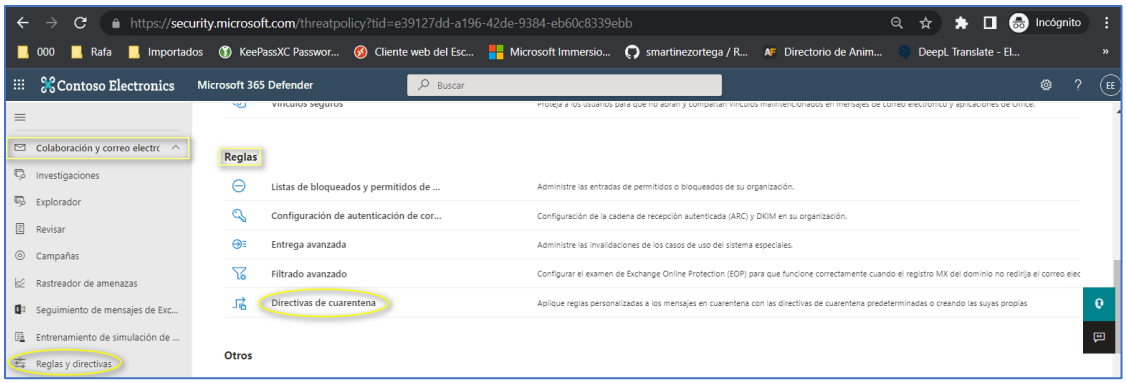
***NOTA**: Cuándo seleccionamos la opción: **Poner en cuarentena el mensaje,**. La que haremos, será* enviar los emails a la zona de cuarentena *(la tenemos disponible tanto para emails como para archivos). Para poder trabajar con ellos, **eliminarlos, enviados**, **liberarlos**, etc…*

***NOTA**: ¿Dónde encontrar información sobre la cuarentena?*
En este link: https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide

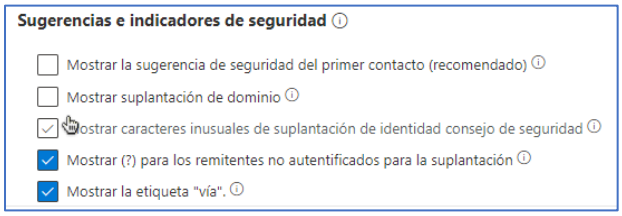
***NOTA**: ¿Dónde podemos ver los mensajes que van a la cuarentena?*
En este link: https://security.microsoft.com/quarantine *o lo gestionarla vía comandos de PowerShell.*

***NOTA**: ¿Dónde configurar las directivas de acceso a la consola de gestión de la cuarentena?*
En este link: *https://security.microsoft.com/*

***NOTA**: Podremos configurar las **directivas de cuarenta**, en la consola de seguridad, Dentro de la sección: Colaboración y correo electrónico > Reglas y directivas. Dentro de la sección: **Reglas**, Directivas de cuarentena.*

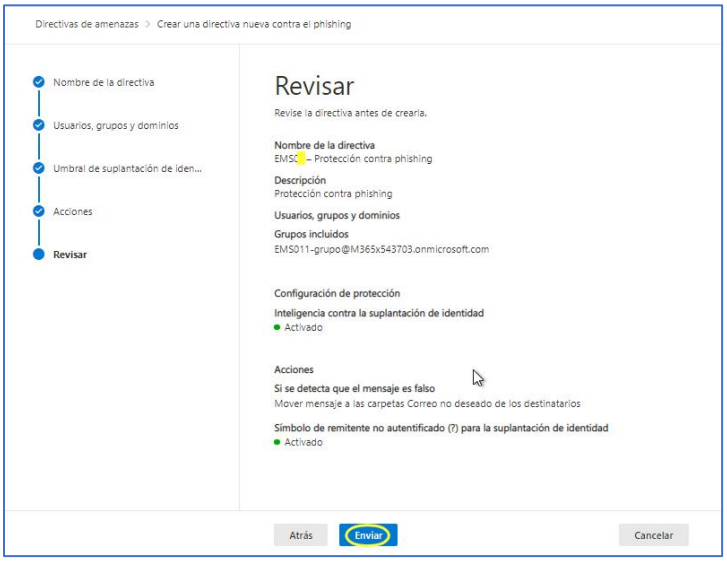


16. En esta *subsección*, configuraremos los **mensajes de advertencia** que se muestran a los *destinatarios* al *abrir mensajes* de *correo electrónico sospechosos*.
    Dejaremos las opciones por defecto.

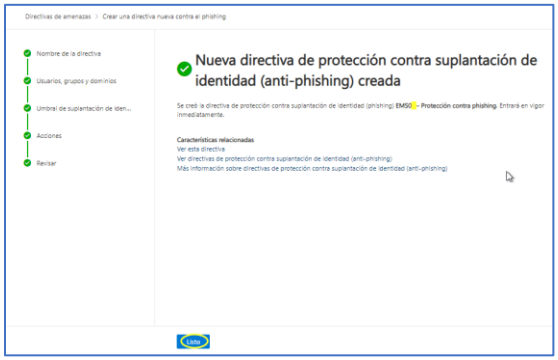


17. **Clic** en el **botón** inferior de la pantalla**: Siguiente.**

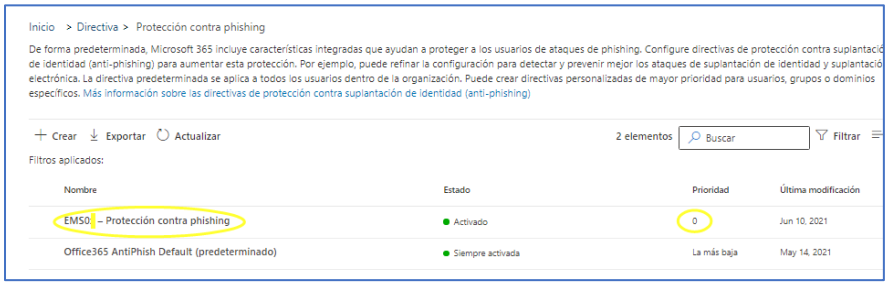
18. Sección: **Revisar**. Nos aparece un **resumen** de lo que hemos seleccionado. **Clic** en el **botón Enviar**.



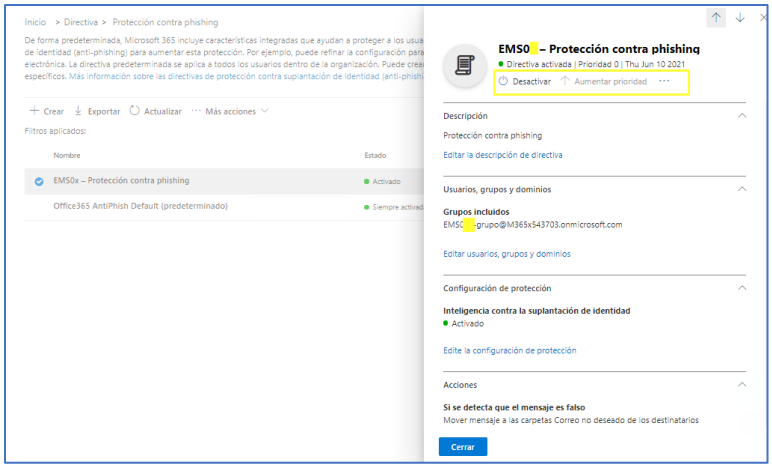
19. Nos aparecerán varias **ventanas informativas sobre** la creación de esta directiva. **Clic** en el **botón Listo**.



20. Nos aparecerá **la nueva directiva** que nos acabamos de crear y podemos comprobar que tiene una **prioridad más alta**, dentro de la lista de directivas, superior a la directiva por defecto que nos aplica Microsoft



21. *Por defecto*, la **directiva estará activada**. Sí queremos *desactivarla* o *editarla*, **clic** en **su nombre** para que aparezcan estas opciones.



NOTA: *Más información en este enlace*: https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-atp-anti-phishing-policies