

## Contenido

---

Laboratorio: Microsoft 365 Defender, Contra spam y Protección antimalware.....	2
Laboratorio: Directiva Contra spam y Protección antimalware. ....	5

## Laboratorio: Microsoft 365 Defender, Contra spam y Protección antimalware.

**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, Contra spam y Protección antimalware** 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	<a href="#">Configurar directivas antimalware en EOP</a>
2	Phishing	CAT: PSHH	<a href="#">Configuración de directivas contra correo no deseado en EOP</a>
3	Correo no deseado de alta confianza	CAT: HSPM	<a href="#">Configuración de directivas contra correo no deseado en EOP</a>
4	Suplantación de identidad (phishing)	CAT: SUPLANTACIÓN DE IDENTIDAD	<a href="#">Configurar inteligencia de identidades en EOP</a>
5	Correo no deseado (SPAM)	CAT: SPM	<a href="#">Configuración de directivas contra correo no deseado en EOP</a>
6	Masivo (SPAM)	CAT: BULK	<a href="#">Configuración de directivas contra correo no deseado en EOP</a>
0,7*	Suplantación dominio (usuarios protegidos)	DIMP	<a href="#">Configurar directivas contra phishing de ATP</a>

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

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

## Laboratorio: Directiva Contra spam y Protección antimalware.

**Objetivo:** Entender y desplegar **directivas** de **protección** antimalware, antispyware, etc. Exchange Online Protection (EOP) pone en cuarentena y analiza en tiempo real tráfico de correo electrónico y datos adjuntos que entran y salen del sistema en busca de virus y otro malware.

Características de la protección:


- **Defensa basada en capas:** Varios motores de detección antimalware usados en EOP ayudan a protegerse contra las amenazas conocidas y desconocidas. Dichos motores incluyen una potente detección heurística contra ataques de día cero.
- **Respuesta de amenaza en tiempo real:** Durante algunos brotes, el equipo antimalware puede tener suficiente información sobre un virus u otra forma de malware para escribir reglas de directiva sofisticadas que detecten la amenaza incluso antes de que una definición esté disponible en cualquiera de los motores que usa el servicio. 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 equipo antimalware de Microsoft se apoya en terceros que desarrollan motores antimalware, con lo que recibirá y querrá integrar definiciones y revisiones de malware antes de que se lancen al público. Permitiendo desarrollar soluciones propietarias. Las definiciones de todos los motores de terceros se actualizan cada hora.

Las directivas de protección, como estamos viendo, también amplían esta protección con el resto de las directivas de protección que nos estamos creando en este laboratorio.

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

### Pasos para realizar:

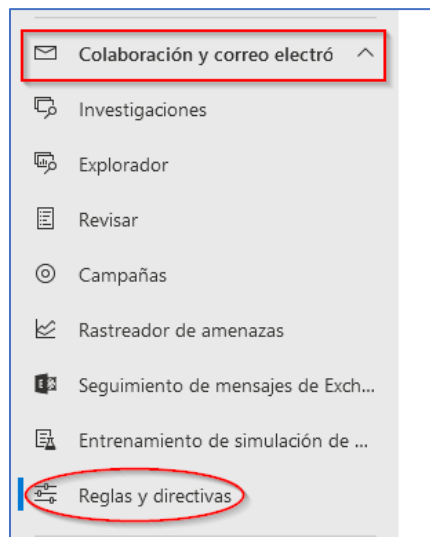
1. **Logarnos en el Centro de seguridad de Microsoft 365**, en: <https://security.office.com/> como **admin**.  
**Usuario:** [EMS0x@m365\\*\\*\\*\\*\\*.onmicrosoft.com](mailto:EMS0x@m365*****.onmicrosoft.com) (la “x” es el usuario que os hemos dado al comienzo del curso).  
**Contraseña:** HolaMundo01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



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



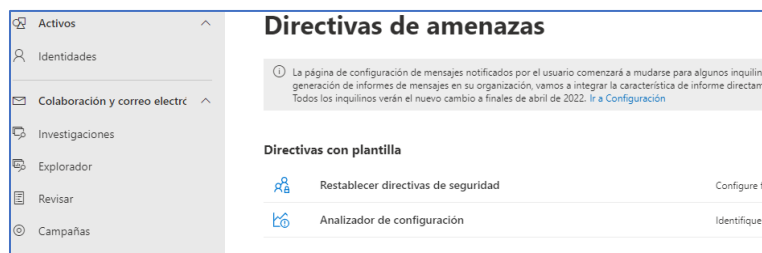
3. **Clic en el menú vertical de la parte izquierda de la pantalla en la entrada Reglas y Directivas dentro de la sección vertical Colaboración y correo electrónico.**



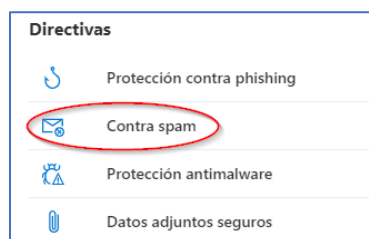
4. **Clic en Directivas de amenazas.**



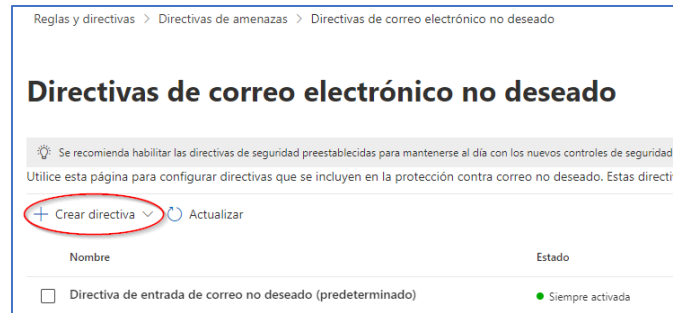
5. En la siguiente ventana, aparecerán las opciones que tenemos disponibles para implementar las directivas de protección. Microsoft pone a nuestra disposición diferentes **plantillas ya creadas**, basadas en **vectores de ataque actuales** que podremos *implementar en pocos clic*.



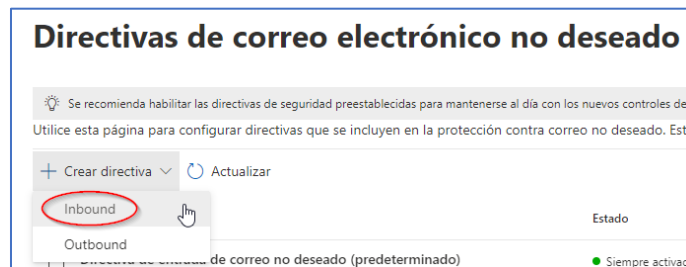
6. **Nosotros en lugar de utilizar las plantillas**, nos **crearemos** una directiva de este tipo desde **cero**. **Clic** en el **enlace Contra spam** en la sección *Directivas*.



7. Aquí encontraremos las directivas que creemos para analizar y protegernos del vector de ataque que suponen los ficheros adjuntos. **Clic** en el **botón "+ Crear directiva"**.



Seleccionaremos la **dirección de entrada o salida** desde el **punto de vista de nuestra tenant**.  
Clic en la *opción*: **Inbound** para proteger a los usuarios de nuestra tenant de M365.



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

a. **Nombre:** EMS0x – Protección Spam Entrada *(la "x" es el usuario que los instructores os hemos proporcionado al comienzo del curso)*.

b. **Descripción:** Protección antispam para nuestros usuarios.

Protección antispam para nuestros usuarios

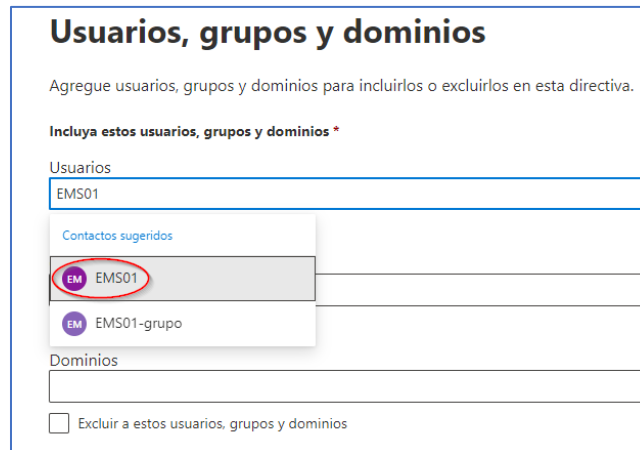
en el **botón** inferior de la pantalla: **Siguiente**.

c. 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.



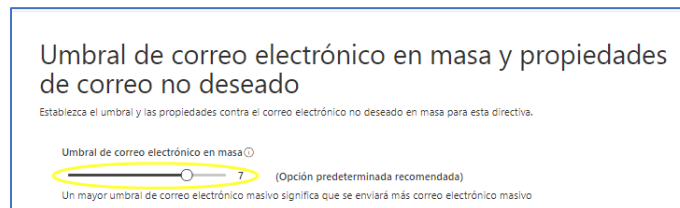
**NOTA:** podemos excluir usuarios dentro de los grupos que estemos seleccionando.



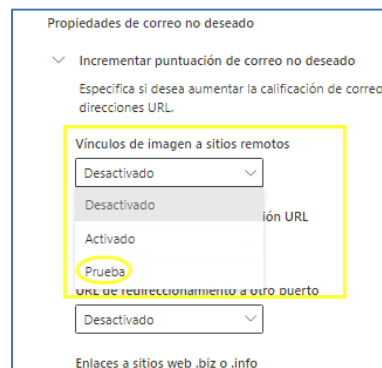
Clic en el botón inferior de la pantalla: **Siguiente**.



9. En la sección: **Umbral de correo electrónico en masa y propiedades de correo no deseado**. Podremos influir en las opciones que incrementan la opción predeterminada recomendada por Microsoft, por defecto, marcada en “7”.



**¡¡¡POR FAVOR!!!** Revisar las opciones que tenemos disponibles, pero **NO** activar ninguna (sí quieres marcar alguna entre las tres opciones disponibles: Desactivado, Activado y Prueba, selecciona la última de ellas para no impactar en el flujo de información que reciben nuestros usuarios y una vez probaba podremos activarla o no en función de los falsos positivos o negativos que recibamos).



**Dejar SIN Activar TODAS las opciones.**

Propiedades de correo no deseado

✓ Incrementar puntuación de correo no deseado  
Especifica si desea aumentar la calificación de correo no deseado para los mensajes que incluyan estos tipos de vínculos o de direcciones URL.

Vínculos de imagen a sitios remotos  
Desactivado

Dirección IP numérica en dirección URL  
Desactivado

URL de redireccionamiento a otro puerto  
Desactivado

Enlaces a sitios web .biz o .info  
Desactivado

✓ Marcar como correo no deseado  
Especifica si desea marcar los mensajes que incluyan estas propiedades como correo no deseado.

Mensajes vacíos  
Desactivado

Etiquetas insertadas en HTML

*Sí seleccionamos el modo prueba. Podremos configurar que acción tomar sí se produce alguna coincidencia. RECOMENDADO, sí lo habéis marcado.*

Modo de prueba

Configure las opciones de modo Prueba para cuando se produce una coincidencia para una opción avanzada habilitada para pruebas.

☐ Ninguno

☐ Agregar texto de encabezado X predeterminado

☒ Enviar mensaje CCO

correobulk@miempresa.es

**SI HABÉIS HECHO CASO a lo dicho en puntos anteriores NO tenéis que seleccionar nada. Tal y como aparece en la siguiente pantalla:**

Modo de prueba

Configure las opciones de modo Prueba para cuando se produce una coincidencia para una opción avanzada habilitada para pruebas.

☒ Ninguno

☐ Agregar texto de encabezado X predeterminado

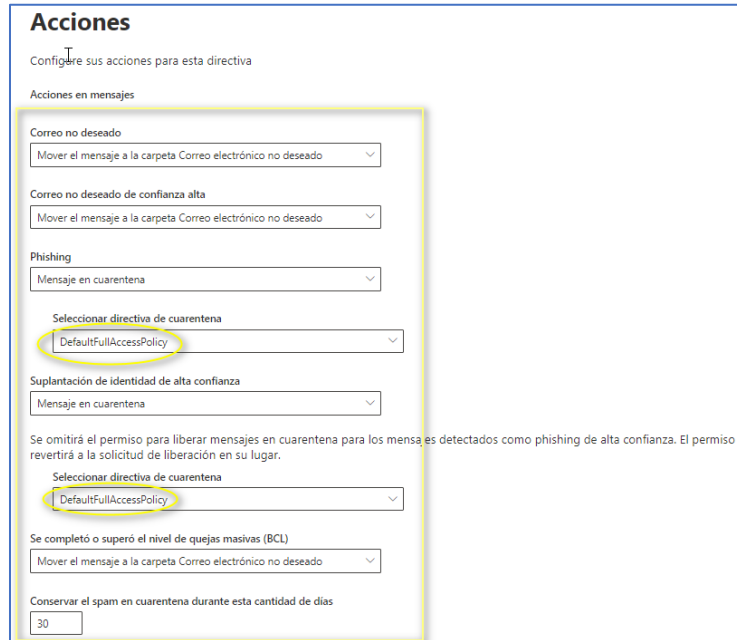
☐ Enviar mensaje CCO

correobulk@miempresa.es

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

Atrás **Siguiente** Cancelar

10. Sección: **Acciones**. **Seleccionaremos las acciones a realizar** que se realizarán sobre los emails que reciban los usuarios de nuestra tenant, dependiendo de cómo la Inteligencia Artificial de Microsoft que nos entrega este servicio, los marque.



**Podemos seleccionar las acciones a realizar en los mensajes en función del marcado que Microsoft hacer por nosotros:**

- a. Correo no deseado: Mover el mensaje a la carpeta de correo no deseado**
- b. Correo no deseado de confianza alta: Mover el mensaje a la carpeta de correo no deseado**
- c. Phishing: Mensaje en cuarentena**
- d. Suplantación de identidad de alta confianza: Mensaje en cuarentena**
- e. En masa: Mover el mensaje a la carpeta de correo no deseado**

## Acciones

Configure sus acciones para esta directiva

### Acciones en mensajes

#### Correo no deseado

Mover el mensaje a la carpeta Correo electrónico no deseado

#### Correo no deseado de confianza alta

Mover el mensaje a la carpeta Correo electrónico no deseado

#### Phishing

Mensaje en cuarentena

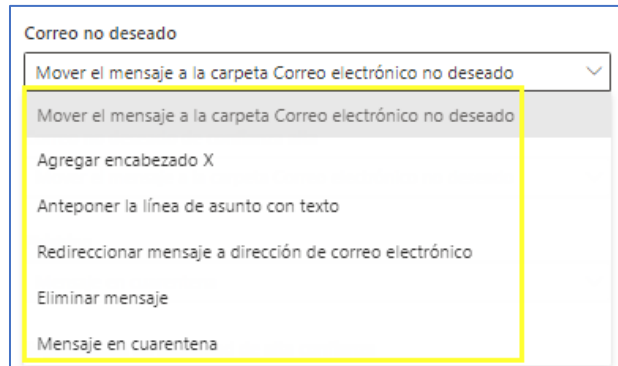
#### Suplantación de identidad de alta confianza

Mensaje en cuarentena

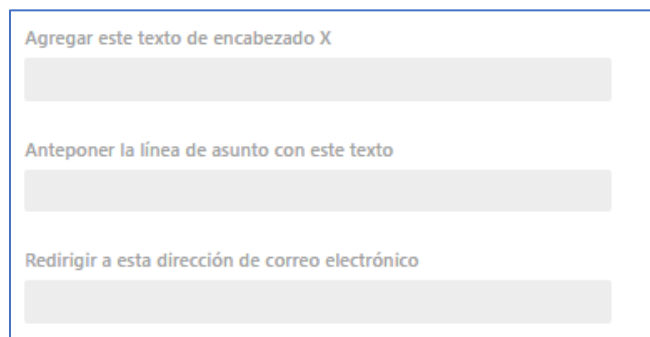
#### En masa

Mover el mensaje a la carpeta Correo electrónico no deseado

¿Qué estamos seleccionando con cada una de las acciones marcadas en el pantallazo anterior?:



1. **Mover el mensaje a la carpeta de correo no deseado.** El email se entrega al buzón en la carpeta de correo no deseado. Esto sucederá si la regla de correo no deseado está habilitada en el buzón (predeterminada).
2. **Agregar encabezado X.** Agregaremos un encabezado que nosotros podemos definir en el apartado: que configuraremos más abajo en esta ventana del asistente de configuración.



3. **Anteponer la línea de asunto con texto.** Lo mismo que el punto anterior. Lo configuraremos en el mismo "pantallazo".
4. **Redireccionar mensaje a dirección de correo electrónico:** envía el mensaje a los destinatarios especificados en lugar de a los destinatarios deseados. Lo mismo que en los dos puntos anteriores. Lo configuraremos en el mismo "pantallazo".
5. **Eliminar mensaje:** Elimina silenciosa y completa del email **antes de su entrega** al destinatario legítimo dentro de nuestra empresa (cuerpo y ficheros adjuntos).
6. **Mensaje en cuarentena.** No se entregará el correo a su destinatario, en lugar de eso, se enviará a cuarenta. Para poder trabajar con ellos, una vez estén en nuestra zona de cuarentean (*enviados, liberarlos, etc...*)

Tendremos que logarnos como **admin en la URL de gestión** de la **cuarenta de nuestra tenant** que **Microsoft** pone a nuestra disposición: <https://security.microsoft.com/quarantine> o lo gestionarla vía comandos de PowerShell.

**NOTA:** Para + información al respecto, clic en la siguiente URL: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide>

**Acciones que podemos tomar en dependiendo de cada uno de los filtros de correo no deseado y explicación que es cada una de las opciones: “alta confianza”, “correo masivo”, etc:**

	Correo no deseado	Correo no Deseado de alta confianza	Correo de phishing (Suplantación de identidad)	Correo de phishing de alta confianza	Correo masivo
<b>Mover el mensaje a la carpeta de Correo no deseado</b> , una vez entregado	Sí	Sí	Sí	Sí	Sí
<b>Agrega un encabezado X</b> (se define posteriormente) y se entrega el msg	Sí. Va a la carpeta correo no deseado	Sí. Va a la carpeta correo no deseado	Sí	No	Sí
<b>Anteponer la línea de asunto con texto.</b> Agrega texto al principio del asunto del msg. Se entrega en la carpeta correo no deseado	Sí	Sí	Sí	No	Sí
<b>Redireccionar mensaje a dirección de correo electrónico</b> (se define posteriormente).	Sí	Sí	Sí	Sí	Sí
<b>Eliminar mensaje.</b> Se elimina completamente (incluyendo adjuntos)	Sí	Sí	Sí	No	Sí
<b>Mensaje en cuarentena</b>	Sí	Sí	Sí	Sí	Sí
<b>Ninguna acción</b>	No	No	No	No	Sí

**NOTA:** ¿Qué son los umbrales de correo masivo para Microsoft?.

Los **servicios de filtrado de Exchange Online Protection (EOP)** asignan y modifican la **cabecera de los emails entrantes** añadiendo una serie de valores numéricos correspondientes al marcado de la detección o no de las diferentes capas de tecnología que se aplican. Este es el valor **BCL (Bulk Complaint Level)**. Cuánto **más alto** sea el **valor numérico “BCL”** con el que ha sido marcado un mensaje, más probabilidad tiene de ser SPAM Microsoft usa tanto tecnología propietaria como la de terceros para identificar el correo masivo y determinar y marcar con un valor numérico BCL adecuado a cada email que pasa por sus filtros de protección).

**Ejemplo de cabecera de correo electrónico modificada** donde podemos ver los **diferentes marcadores numéricos** en cada email procesado por **Exchange Online Protection**:

- **SCL** = The Spam Confidence Level.
- **PCL** = The Phishing Confidence Level.
- **BCL** = The Bulk Complaint Level. (1 - 9).

#### Message source

```
X-MS-Exchange-Organization-Network-Message-Id: 37152c12-e862-4229-be51-08d5593681fb
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-Microsoft-Exchange-Diagnostics:
1;CO1NAM03FT035;1:5kDTNuarNk913y2CRVFuaEHbgGeqOWlc/HDeXAeb5d/gIPBx/JBn7/NbFBXh0RnMQsvvCa6cusmNMF36bsbtxfb8Gy
obxj3T/b0E3dvfthRf5XgR2eJbDLfxxk8DqSP
X-Forefront-Antispam-Report: EFV:NLj;SFV:NSPM;SFS:
(98901004);DIR:INB;SPF:SCL:1;SRVR:CO1NAM03HT234;H:smtpi.msn.com;FPR:;SPF:None;LANG:;
X-MS-Exchange-Organization-AuthSource: CO1NAM03FT035.eop-NAM03.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: 37152c12-e862-4229-be51-08d5593681fb
X-Microsoft-Antispam: BCL:0;PCL:0;RULEID:(5000109)(4604075)(4605076)(610169)(640170)(650170)(8291510171);SRVR:CO1NAM03HT234;
X-Microsoft-Exchange-Diagnostics:
1;CO1NAM03HT234;3:hky8M5HOUaAegENPrMfN7UNclpyVq8HdZBhwQNmt0MNPkF0Oy5dW7rTGJW4f+1Ea6mhXJDHRPV27vblAoxPg
maWHkpiQ83m0V64PYZe+XbNQ662haa5LkXTSr6OWd9j+YfV9qANGs3rBUf8exlPc74u1n05EGmaxm+5Al8Ya3x4aG4UcDZhhDY8OYCMp
PCsmRy4p9iyR9ifaGhufwtPZgm5PmEr3bWtizT8k66ZVINj8dx1OzxMq5CCtNv0nN8Tqsp2YJ5xQqsBM+hjGMHwH+5IOj4MJQusbis9IU5LH
```

**NOTA:** El listado de encabezados con los que EOP marca cada email los podemos encontrar en esta URL: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/anti-spam-message-headers?view=o365-worldwide#PCL>

**NOTA:** Un valor: "6" corresponde a correo no deseado. Más información: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/bulk-complaint-level-values?view=o365-worldwide> )

**NOTA:** Más información: <https://docs.microsoft.com/es-es/microsoft-365/enterprise/microsoft-365-malware-and-ransomware-protection?view=o365-worldwide>

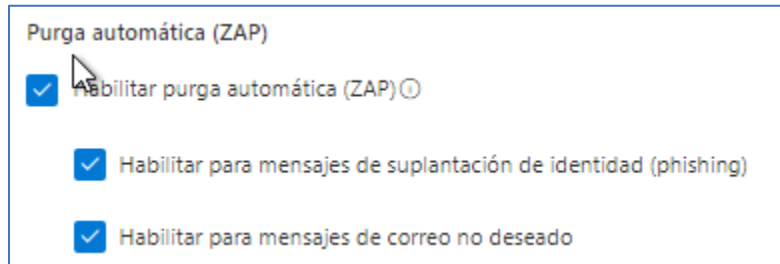
- Sugerencias de seguridad:** Avisaremos a los usuarios con una franja horizontal en los emails sospechosos que pueden estar abriendo un email que forma parte de una campaña de SPAM.

#### Sugerencias de seguridad

☒ Habilitar sugerencias de seguridad para el spam ⓘ

- Purga automática (ZAP).** Tecnología propietaria de Microsoft. La utiliza para dar una **protección completa** y la encontramos en **varias casuísticas** (Habilitar para mensajes de suplantación de identidad (phishing **y/o** Habilitar para mensajes de correo no deseado)).

Gracias a ella, podremos **ejecutar acciones**, como la eliminación o purga de correo no deseado o correo con phishing, una vez que **ya ha sido entregado el mensaje al usuario, actuando** sobre su buzón de **Exchange Online**.



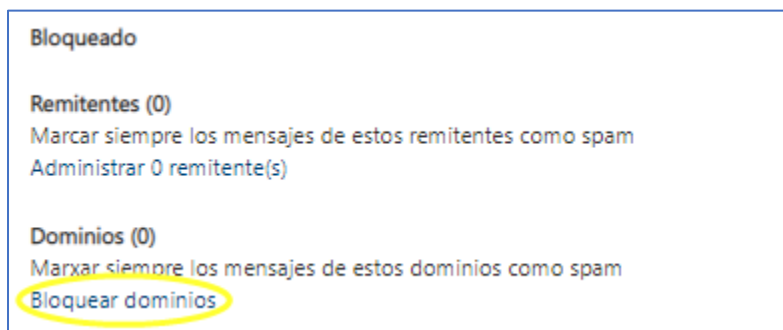
**NOTA:** Más información sobre esta característica la podéis encontrar en este URL: <https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide>

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



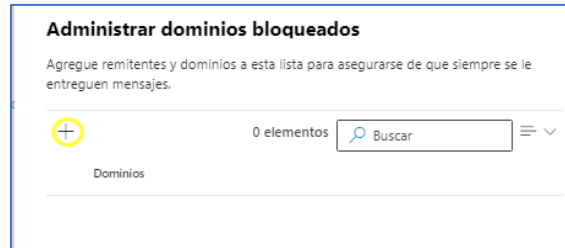
9. Sección: **Lista de bloqueados y admitidos**. Microsoft nos permite que personalizemos las Listas de remitentes y/o Dominios Permitidos o Bloqueados para nuestros usuarios.
- a. **Permitido**. Nos podemos crear una **lista blanca** con los **remitentes** o **dominios** de los que siempre **queremos aceptar sus emails saltándonos los filtros de correo electrónico no deseado**.
  - b. **Bloqueado**. Nos podemos crear una **lista negra** con los **remitentes** o **dominios** de los que **NO queremos recibir emails**

En nuestro caso, bloquearemos el dominio de todohacker.com. Para ello, clic en el enlace **Bloquear dominios** dentro de la última sección de la pantalla **Dominios**.





En la **nueva Blade** de la parte derecha que aparecerá en la ventana. **Clic en el icono, “+”**:



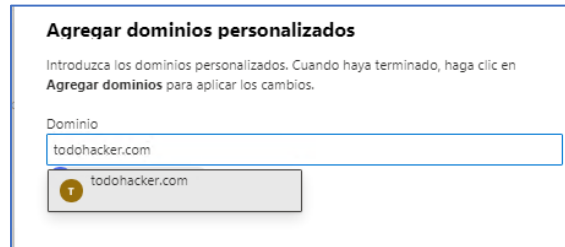
**Administrar dominios bloqueados**

Agregue remitentes y dominios a esta lista para asegurarse de que siempre se le entreguen mensajes.

+ 0 elementos

Dominios

En el campo de escritura **Dominio** escribimos **todohacker.com\_**



**Agregar dominios personalizados**

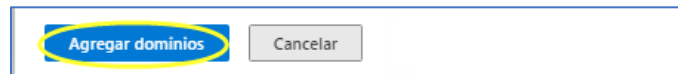
Introduzca los dominios personalizados. Cuando haya terminado, haga clic en **Agregar dominios** para aplicar los cambios.

Dominio

todohacker.com

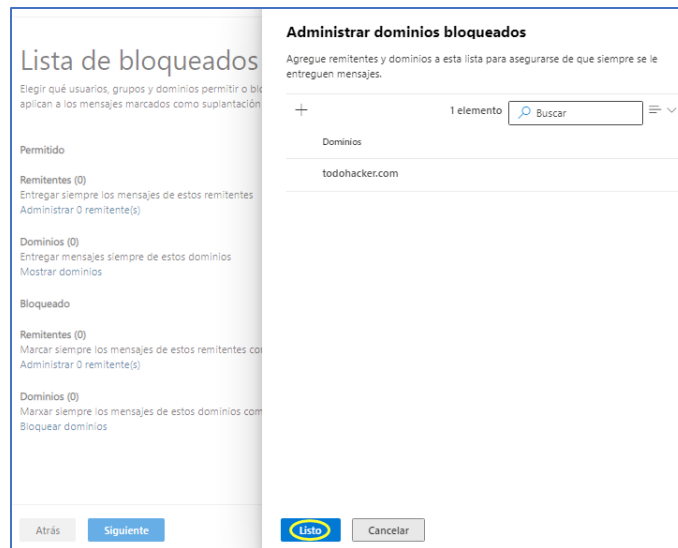
todohacker.com

**Clic en el botón inferior de la Blade: Agregar dominios.**



Agregar dominios Cancelar

**Clic en el botón inferior de la Blade: Listo.**



**Lista de bloqueados**

Elegir qué usuarios, grupos y dominios permitir o bloquear aplican a los mensajes marcados como suplantación.

Permitido

Remitentes (0)  
Entregar siempre los mensajes de estos remitentes.  
Administrar 0 remitente(s)

Dominios (0)  
Entregar mensajes siempre de estos dominios.  
Mostrar dominios

Bloqueado

Remitentes (0)  
Marcar siempre los mensajes de estos remitentes como suplantación.  
Administrar 0 remitente(s)

Dominios (0)  
Marcar siempre los mensajes de estos dominios como suplantación.  
Bloquear dominios

Atrás Siguiente Listo Cancelar

**Administrar dominios bloqueados**

Agregue remitentes y dominios a esta lista para asegurarse de que siempre se le entreguen mensajes.

+ 1 elemento

Dominios

todohacker.com

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



Atrás Siguiente Cancelar

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

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

**Revisar**

**Nombre de la directiva**  
EMSO - Protección antimalware

**Descripción**  
Directiva de Protección antimalware

**Usuarios, grupos y dominios**  
**Grupos incluidos**  
EMSO-grupo@M365x543703.onmicrosoft.com

**Umbral y propiedades del spam**  
**Acción de correo no deseado en masa**  
● Activado

**Umbral de correo electrónico en masa**  
7

**URL a sitios web .biz o .info**  
Desactivado

**Vínculos de imagen a sitios remotos**  
Desactivado

**Dirección IP numérica en dirección URL**  
Desactivado

**URL de redireccionamiento a otro puerto**  
Desactivado

**Mensajes vacíos**  
Desactivado

Atrás **Crear**

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

Reglas y directivas > Directivas de amenazas > Create anti-spam inbound policy

**Revisar**

Enviando...

**Nombre de la directiva**  
EMSOx - Protección antimalware

**Descripción**  
Directiva de Protección antimalware

**Usuarios, grupos y dominios**  
**Grupos incluidos**  
EMSO11-grupo@M365x543703.onmicrosoft.com

**Umbral y propiedades del spam**  
**Acción de correo no deseado en masa**  
● Activado

**Umbral de correo electrónico en masa**  
7

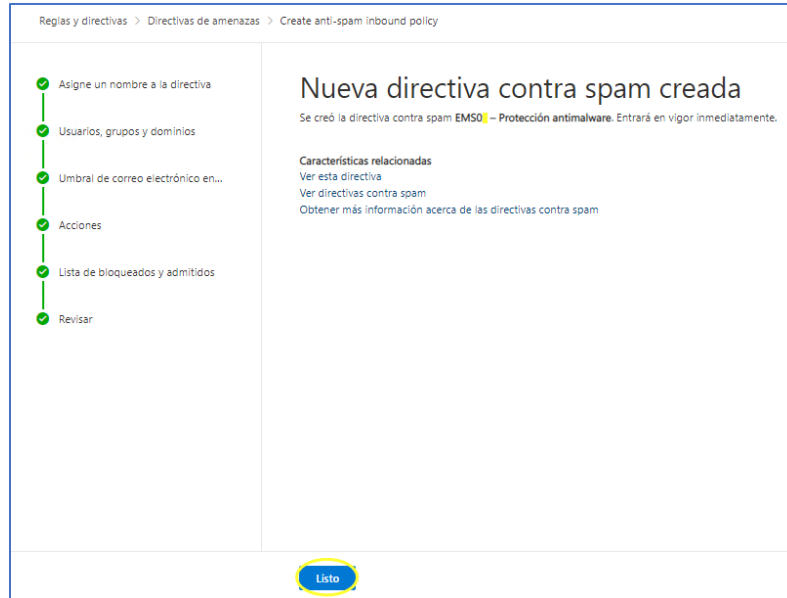
**URL a sitios web .biz o .info**  
Desactivado

**Vínculos de imagen a sitios remotos**  
Desactivado

**Dirección IP numérica en dirección URL**  
Desactivado

**URL de redireccionamiento a otro puerto**  
Desactivado

Atrás **Crear**



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

12. 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

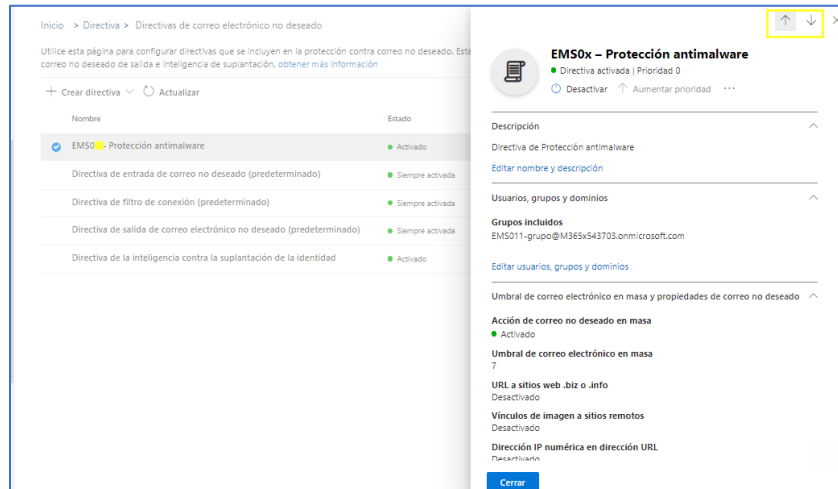
## Directivas de correo electrónico no deseado

💡 Se recomienda habilitar las directivas de seguridad preestablecidas para mantenerse al día con los nuevos controles de seguridad y la configuración. Utilice esta página para configurar directivas que se incluyen en la protección contra correo no deseado. Estas directivas incluyen:

+ Crear directiva ▼ Actualizar

Nombre	Estado
<input type="checkbox"/> EMS0x - Protección Spam Entrada	● Activado
<input type="checkbox"/> Directiva de entrada de correo no deseado (predeterminado)	● Siempre activada

13. Podemos **Desactivar, editar y eliminar** (para eliminar una directiva primero tendrás que desactivarla para poder borrarla) dentro de la **lista de directivas**, haciendo **clik** en el **nombre** de una de ellas en la opción superior.



Por favor, revisar pro vuestra cuenta las opciones que tenemos disponibles para las directivas antimalware. Son muy pocos pasos a seguir, por ese motivo, **NO** hemos creído necesario incluir todos ellos en este laboratorio.

### Configuración de protección

Establecer la configuración para esta directiva antimalware

**Configuración de protección**

☒ Habilitar el filtro de datos adjuntos comunes ⓘ  
.ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com y 43 otros tipos de archivos  
[Seleccionar tipos de archivo](#)

**Cuando se encuentran estos tipos de archivo**

☒ Rechazar el mensaje con un informe de no entrega (NDR) ⓘ  
☐ Poner en cuarentena el mensaje

☒ Habilitar la purga automática contra malware (recomendado) ⓘ

**Directiva de cuarentena**

AdminOnlyAccessPolicy

Se omitirá el permiso para liberar mensajes en cuarentena para los mensajes con malware detectado y, en su lugar, revertiremos a la solicitud de liberación.

**Notificación**

**Notificaciones del administrador**

☐ Notificar a un administrador sobre mensajes no entregados de remitentes internos  
☐ Notificar a un administrador sobre mensajes no entregados de remitentes externos

**Personalizar notificaciones**

☐ Usar texto de notificación personalizado ⓘ

Atrás **Siguiente**