**Manual de configuraciones defender for 365**

**1.- Directiva de cuarentena “Para licenciamiento A3 y a5”.**

Nos vamos al portal de defender for 365 (security) en: <https://security.microsoft.com/>, el menú izquierdo vamos a seleccionar la opción de **colaboración y correo electrónico** en **reglas y directivas** daremos clic en **directivas de amenazas:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En directivas de amenazas nos deslizamos hacia abajo y buscamos la opción que dice **Reglas** y damos clic en **directivas de cuarentena**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerá una ventana donde vienen por default 3 directivas y en la opción de **+Agregar directiva personalizada** podemos crear más directivas de cuarentena:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez que le demos clic nos saldrá una ventana donde vamos a empezar a configurar nuestra directiva personalizada, agregaremos un nombre a la directiva y le damos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

En acceso a mensajes de destinatario seleccionaremos la opción Acceso limitado y daremos clic en siguiente:Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana en notificación de cuarentena vamos a habilitar la casilla y daremos clic en siguiente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nos aparecerá el resumen de la configuración, damos clic en enviar:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Y en la siguiente ventana damos clic en listo:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Hasta ver que la directiva se encuentra en la lista inicial:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**2.- Lista de bloqueados y permitidos “Para licenciamiento A3 y a5”.**

Nos vamos al portal de administración en: <https://admin.microsoft.com/> , en el menu de la parte izquiera nos vamos a la opcion de **centros de administración** y seleccionamos **seguridad:**

Diagrama

Descripción generada automáticamente con confianza media

Nos aparecerá una ventana nueva del centro de administración de defender for 365 ó podemos ingresar directamente desde: <https://security.microsoft.com/> , en el menú izquierdo vamos a seleccionar la opción de **colaboración y correo electrónico** en **reglas y directivas** daremos clic en **directivas de amenazas:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ya en directivas de amenazas nos deslizamos hacia abajo y buscamos la opción que dice **Regla**s y damos clic en **lista de bloqueados y permitidos**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerá una ventana donde vemos una lista donde estarán los bloqueados y permitidos, podemos bloquear desde **dominios y direcciones, remitentes suplantados, direcciones URL y archivos.**

Por ejemplo, desde la opción **+bloquear** daremos clic:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerá una ventana donde vamos a anotar los dominios o páginas que se vallan a bloquear, después viene una opción donde vamos a seleccionar los días que estará bloqueada la página o si no expira:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez seleccionadas las opciones deseadas daremos clic en el botón azul que dice agregar: Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerán las opciones en la lista: Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**3.- Liberar mensajes de cuarentena “Para licenciamiento A3 y a5”**

Para ver la lista de los mensajes que se han mandado a cuarentena en el portal de defender for 365 (Security) nos vamos al menú de la izquierda en **colaboración y correo electrónico** en la opción de **revisar,** después damos clic en la opción que dice **cuarentena**:

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Veremos la lista de los correos que se han mandado directamente a cuarentena:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Para liberar algún correo que sea un falso positivo y después de revisarlo, vamos a dar clic en el correo y nos abrirá una ventana, nos vamos a ir a los tres puntos que están en la parte superior derecha y seleccionamos liberar correo electrónico:

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nota: desde esta ventana podemos ver las demás opciones antes de liberar el correo como la vista previa entre otras opciones de administración.

Nos mandara otra ventana donde veremos a quien queremos liberar el correo y podemos habilitar dos opciones de notificación, damos clic en liberar mensaje:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerá el mensaje de que el correo se ha enviado a las bandejas de entrada, damos clic en listo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora en la lista de los correos en cuarentena el correo tendrá una nueva leyenda de que se ha liberado el correo: Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**4.- Simulación de ataque “Configurar esta directiva si tenemos la licencia A5”.**

Nos vamos al portal de defender for 365 (security) en: <https://security.microsoft.com/>, el menú izquierdo vamos a seleccionar la opción de **colaboración y correo electrónico** en **entrenamiento de simulación de ataque:**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Vamos a seleccionar la opción que dice simulaciones y daremos clic en iniciar una simulación:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Seleccionamos una de las opciones de tipos de simulación, por ejemplo, cosecha de credenciales y le damos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

En la siguiente ventana nombraremos la simulación y agregaremos una breve descripción para reconocer la directiva y su función (es opcional):

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez que tengamos el nombre de la simulación vamos a buscar de todas las plantillas la de nombre: “Microsoft 365 suscription expired” la seleccionamos y le damos clic en siguiente:

**Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente**

En la siguiente ventana vamos a seleccionar los usuarios o grupos que se les valla a enviar el correo de la simulación, seleccionamos incluir solo usuarios y grupos específicos, y damos clic en **+agregar usuarios**:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Nos abrirá una nueva ventana para seleccionar los usuarios o grupos para la simulación, en la barra de búsqueda agregaremos los nombres de los usuarios o grupos y daremos clic en agregar usuario:

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

Una vez que seleccionemos los usuarios o grupos se vera la lista de los usuarios, daremos clic en siguiente:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Después nos aparecerá una ventana donde tenemos los usuarios o grupos que se quieran excluir en la simulación en caso de haber seleccionado todos los usuarios en la institución, en caso de no excluir solo seleccionar el botón siguiente:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Nos mandará la siguiente ventana en donde podremos asignar un pequeño curso para los usuarios en caso de caer en la simulación y personalizar el tiempo que estará el curso en su correo, seleccionamos asignar entrenamiento para mí y le damos clic en el botón siguiente:

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente con confianza media**

En la siguiente ventana dejaremos la opción usar paginas de aterrizaje de la biblioteca, pero igual podemos personalizar la página:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

En la lista de las plantillas seleccionamos la primera y en el idioma “español”, damos clic en siguiente:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Bajamos a las opciones de notificación y seleccionamos las preferencias de entrega, cambiamos el idioma a español y después damos clic en el botón de siguiente:

**Interfaz de usuario gráfica

Descripción generada automáticamente**

En la siguiente ventana seleccionaremos iniciar simulación tan pronto como haya terminado, en la opción de días que estará disponible la simulación lo dejaremos en 7dias y seleccionaremos la opción de permitir la entrega en la zona horaria teniendo conocimiento de la región, después daremos clic en siguiente:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Veremos al final los puntos que se configuraron y daremos clic en el botón de enviar:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Esperamos unos minutos y nos mandara la siguiente ventana donde menciona que ya se envió la simulación que realizamos, damos clic en listo:

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Al final veremos en la lista principal la simulación creada: **Interfaz de usuario gráfica, Texto

Descripción generada automáticamente**

**5.- Vínculos seguros “solo configurar esta directiva si tenemos la licencia A3”**

Para la directiva de vínculos seguros nos vamos a el portal de security en el siguiente link: <https://security.microsoft.com/,en> el menu izquierdo buscamos la opcion de **reglas y directivas** y le damos clic,despues seleccionamos la opcion de **directivas de amenazas**:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Buscamos la lista de **directivas** y seleccionamos la opción de **vínculos seguros:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana veremos la lista de las directivas que Microsoft tiene predeterminadas y para crear una nueva vamos a darle clic en **+crear**:Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana nombraremos la directiva y daremos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana vamos a seleccionar los usuarios y/o grupos a los que se aplicara la directiva y damos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana vamos a seleccionar las tres primeras casillas y daremos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Carta, Correo electrónico

Descripción generada automáticamente

Nos aparecerá una ventana para las notificaciones donde dejaremos la opción de utilizar el texto de notificación predeterminado y daremos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Después veremos las configuraciones que se realizaron y daremos clic en enviar para habilitar la directiva:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana daremos clic en listo:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez creada la directiva se reflejará en la lista:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**6.- Vínculos seguros “configurar esta directiva si tenemos la licencia A5”**

Para la directiva de vínculos seguros nos vamos a el portal de security en el siguiente link: <https://security.microsoft.com/,en> el menu izquierdo buscamos la opcion de **reglas y directivas** y le damos clic,despues seleccionamos la opcion de **directivas de amenazas**:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Buscamos la lista de **directivas** y seleccionamos la opción de **vínculos seguros:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana veremos la lista de las directivas que Microsoft tiene predeterminadas y para crear una nueva vamos a darle clic en **+crear**:Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana nombraremos la directiva y daremos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana vamos a seleccionar los usuarios y/o grupos a los que se aplicará la directiva y damos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana vamos a seleccionar las tres primeras casillas:

Interfaz de usuario gráfica, Texto, Aplicación, Carta, Correo electrónico

Descripción generada automáticamente

Nos desplazamos hacia abajo y habilitaremos las opciones de teams y aplicaciones de office 365 y daremos clic en siguiente:Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

v

v

Nos aparecerá una ventana para las notificaciones donde dejaremos la opción de utilizar el texto de notificación predeterminado y daremos clic en siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

v

Después veremos las configuraciones que se realizaron y daremos clic en enviar para habilitar la directiva:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la siguiente ventana daremos clic en listo:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez creada la directiva se reflejará en la lista:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**7.- Phishing “Para licencia A3 y A5”.**

Nos vamos al portal de administración en: <https://admin.microsoft.com/> , en el menu de la parte izquiera nos vamos a la opcion de **centros de administración** y seleccionamos **seguridad:**

Diagrama

Descripción generada automáticamente con confianza media

Nos aparecerá una ventana nueva del centro de administración de defender for 365 ó podemos ingresar directamente desde: <https://security.microsoft.com/> , en el menú izquierdo vamos a seleccionar la opción de **colaboración y correo electrónico** en **reglas y directivas** daremos clic en **directivas de amenazas:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ya en directivas de amenazas nos deslizamos hacia abajo y buscamos la sección **DIRECTIVAS** y damos clic en **Protección contra phishing**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nos aparecerá una ventana donde vemos una lista de políticas. Todos los Tenant de Microsoft 365 tienen una política por default, aquí es donde podemos ir agregando nuevas políticas o personalizar las existentes**.**

Vamos a generar una nueva política, desde la opción **+crear** daremos clic:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos aparecerá una ventana, ingresamos un nombre y descripción para nuestra política:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Al finalizar damos clic en siguiente.

Dependiendo de la administración del directorio activo se puede agregar los usuarios o grupos de Microsoft365, por ahora se habilita por dominio ingresando el nombre en el campo correspondiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Al finalizar damos clic en siguiente.

Dependiendo de nuestro licenciamiento, son las opciones a configurar. El umbral de protección (Disponible sólo en A5) nos permite aumentar el nivel de restriciones en la herramienta comenzando de 1. Para nuestro caso, establecemos un nivel de umbral 2 y en los próximas semanas o meses se debe de monitorear si es necesario disminuir o aumentar dependiendo de nuestro tipo de usuario:

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Nos desplazamos a la parte inferior y marcamos los checkbox de inteligencia de buzones, inteligencia para la protección de identidad y/o suplantación de identidad, dependiendo los que aparezcan según nuestro licenciamiento:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Al finalizar, damos clic en siguiente.

Ahora, vamos a configurar las listas disponibles dependiendo de nuestro licenciamiento. Para el caso de **Si la inteligencia de buzones detecta un usuario suplantado** colocamos poner el mensaje en cuarentena y en **Aplicar directiva de cuarentena** colocamos **adminOnlyAccessPolicy**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos desplazamos hacia abajo y establecemos nuevamente **Mandar a cuarentena y AdminOnlyAccessPolicy** para las dos opciones siguientes:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Debemos marcar todos los checkbox disponibles de la parte inferior y damos clic en siguiente.

Nos mostrará un resumen de todas las configuraciones realizadas, si está todo bien, damos clic en enviar.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nos aparecerá el mensaje de confirmación en unos minutos y damos clic en listo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora, nos aparecerá en la lista principal nuestra directiva creada.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Si necesitamos revisar la configuración o eliminar la directiva, podemos dar clic en el nombre. Aparecerá un panel a la derecha con la configuración actual y opciones para volver a editar cada sección de los pasos anteriores, según lo necesitemos.

**8.- Directivas de Malware “Para licencia A5 yA3”**

Nuevamente en el menú de directivas de amenazas nos deslizamos hacia abajo y buscamos la opción que dice **Directivas** y damos clic en **Protección AntiMalware**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Dentro de esta opción seleccionaremos **Crear** en la parte superior izquierda.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteEstaremos dando los primeros pasos para configurar nuestra directiva de Anti-Malware donde nos pedirá un nombre para la directiva, en esta sección ingresaremos cualquier palabra que deseemos, en la parte inferior también podemos ingresar una breve descripción sobre el fin de esta misma.

Una vez ingresados estos caracteres damos en **Siguiente** en la parte inferior izquierda.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En este paso agregaremos aquellos usuarios, grupos o dominios que vamos a asignarle esta directiva, para este caso agregaremos los dominios de nuestro tenant en este caso demostrativo el dominio donde se encuentran todos los usuarios del tenant es único, en dado caso de contar con múltiples dominios agregarlos todos.

Una vez agregados los dominios vamos a darle en **Siguiente** en la parte izquierda inferior.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En esta parte de la configuración seleccionaremos la opción **Poner en cuarentena el Mensaje** y también habilitaremos el recuadro de **Habilitar la purga automática contra Malware,** cuando seleccionemos estas dos opciones damos scroll hacia abajo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En la parte de notificación habilitaremos la casilla **Notificar a un administrador sobre mensajes no entregados de remitentes externos** e ingresamos en la parte del recuadro blanco el correo (usuario dentro de la organización) del personal de TI o de soporte técnico.

Una vez configurado todo como se muestra en pantalla vamos a darle clic en la opción de **Siguiente**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

En esta última ventana veremos el **Resumen** de lo que acabamos de configurar, una vez que determinemos que todo es correcto, seleccionaremos la opción de **Enviar** en la parte inferior izquierda. Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nos confirmara la plataforma de la creacion exitosa de la directiva.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Podemos confirmar la creación de la directiva y sus configuraciones en la pantalla principal

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y dando clic sobre esta misma nos aparecerá del lado derecho su descripción

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente