

## Contenido

---

Laboratorio: Protección y Seguridad en Microsoft 365: Secure Score.....	2
---	---

Laboratorio: Protección y Seguridad en Microsoft 365: Secure Score.

**Objetivo:** Microsoft 365 tiene múltiples características de seguridad que pueden ser configuradas para securizar nuestras empresas. Pero, **es complicado conocer todas estas medidas de seguridad plasmadas en directiva que se aplican a nuestra empresa**, en que **orden abordarlas** o cómo **nos pueden afectar** en el día a día. Para ello, **Microsoft nos facilita dos servicios: Trust Center y Secure Score.**

**Secure Score**, analiza las **medidas de seguridad** que **tenemos ahora mismo implementadas**, a nivel de tenant (*TODOS los servicios que estamos consumiendo, Microsoft 365, Azure, Dynamics 365, etc*), **asignándonos una puntuación**. Lo que nos permite **ver en qué punto estamos** (*cual es nuestro nivel actual de seguridad*), en cuanto a **postura de seguridad** se refiere y nos **propone una serie de recomendaciones** a seguir en función de nuestra empresa (*sector económico, uso de la plataforma, etc*) para **mejorar los PKIs de cumplimiento de seguridad**.

La **puntuación** se basa en el **sistema relativo**, teniendo en cuenta las **características que la empresa ha habilitado** en su tenant, **las que están disponibles en el servicio** y los **riesgos** que podrían presentarse. Si realizamos las acciones sugeridas por el portal, la **puntuación se recalculará cada 24 ó 48 horas**.

**Secure Score** es un **servicio vivo** (*las recomendaciones son revisadas y actualizadas continuamente por Microsoft*) con una lista con más de 1 docena de configuraciones de seguridad y está disponible para las empresa que tengan una **suscripción de Office/Microsoft 365 Business Premium o Enterprise**. Los **usuarios** que **gestionen** este **consola** deben tener en rol de **administradores globales**.

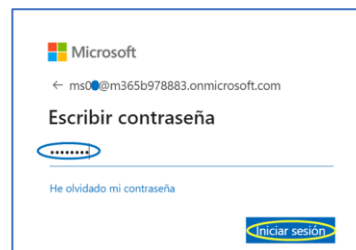
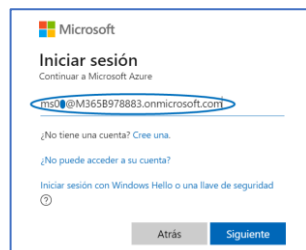
#### + Información:

<https://docs.microsoft.com/es-es/microsoft-365/security/mtp/microsoft-secure-score?view=o365-worldwide>

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

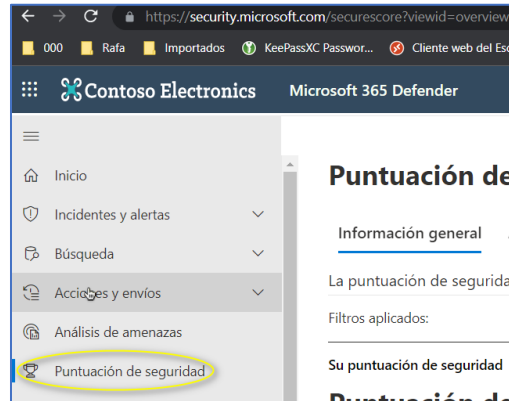
#### Pasos a realizar:

1. **Logarnos** en el portal de **Microsoft 365 Defender** en: <https://security.microsoft.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**.

**Clic en la opción: Puntuación de seguridad**, dentro del *menú vertical de la izquierda de la pantalla*:



3. La primera sección **Información general**. En la parte superior derecha de la ventana, tenemos la información sobre cuando se calculó las puntuaciones que nos está presentando Secure Score.

**Puntuación de seguridad de Microsoft**

Último cálculo de la puntuación: 09/03 ; 2:00 AM

Información general Acciones de mejora Historial Métricas y tendencias

La puntuación de seguridad de Microsoft es una representación de la posición de seguridad de su organización, y una oportunidad de mejorarla.

Filtros aplicados: ⌵ Filtrar

Su puntuación de seguridad Incluir

**Puntuación de seguridad:**  
17.24 %

10/58 puntos obtenidos

100%  
50%  
0%

07/03 07/07 07/11 07/15 07/19 07/23 07/27 08/01 08/05 08/09 08/13 08/17 08/21 08/25 08/29 09/02

Puntos de desglose por: Categoría

Categoría	Puntos obtenidos	Oportunidad
Identidad	No hay datos que mostrar	
Datos	No hay datos que mostrar	
Dispositivo	No hay datos que mostrar	
Aplicaciones	No hay datos que mostrar	
Infraestructura	No hay datos que mostrar	

■ Puntos obtenidos ■ Oportunidad

**Acciones para revisar**

En regresión	Dirección de destino	Planeado	Riesgo aceptado	Agregado recientemente	Actualizaciones recientes
0	9	0	0	0	0

**Acciones de mejora principales**

Acción de mejora	Impacto de...	Estado	Categoría
Requerir MFA para roles administrativos	+17.24 %	<input type="radio"/> Dirección de destirrididad	
Asegúrese de que todos los usuarios puedan completar la autenti...	+15.52 %	<input type="radio"/> Dirección de destirrididad	
Habilitar la directiva para bloquear la autenticación heredada	+13.79 %	<input type="radio"/> Dirección de destirrididad	
Activar la directiva de riesgo de inicio de sesión	+12.07 %	<input type="radio"/> Dirección de destirrididad	
Activar la directiva de riesgo de usuario	+12.07 %	<input type="radio"/> Dirección de destirrididad	
No permitir que los usuarios concedan acceso a aplicaciones no a...	+6.9 %	<input type="radio"/> Dirección de destirrididad	
Habilitar el autoservicio de restablecimiento de contraseña	+1.72 %	<input type="radio"/> Dirección de destirrididad	
Activar la característica Caja de seguridad del cliente	+1.72 %	<input type="radio"/> Dirección de destirrididad	

[Ver todo](#)

**Comparación**

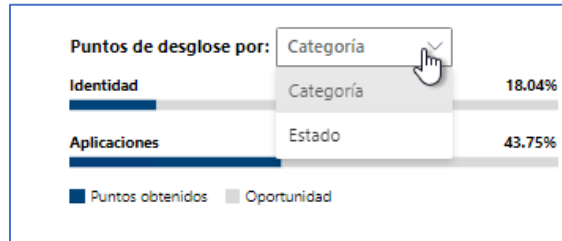
Métrica	Valor
Su puntuación	17.23999999999995%
Organizaciones como la suya	22.150000000000006%
Comparación personalizada	Aún no se ha creado

[Administrar comparaciones](#)

**Recursos**

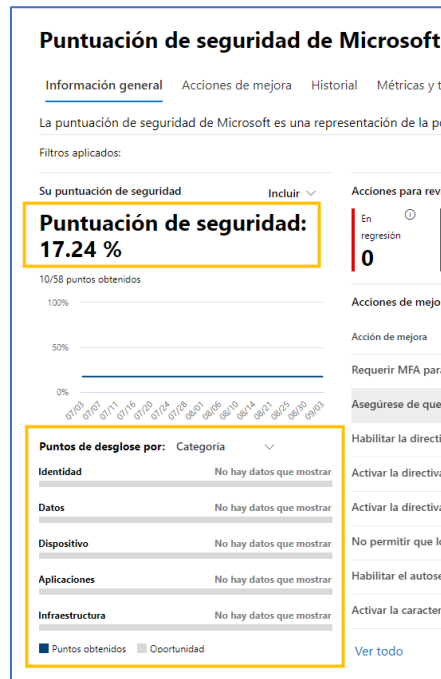
- [Obtener información acerca de las capacidades de puntuación de seguridad](#)  
Obtenga información sobre las acciones de mejora y cómo mejorar su puntuación.
- [Actualizaciones de la experiencia de partners](#)  
Obtenga información sobre la incompatibilidad temporal con la Puntuación de seguridad de identidad y la API de Graph.

- a. En la *parte media/izquierda* de la ventana, está la información sobre nuestra **puntuación de seguridad actual** y el **listado de categorías de que evalúa Secure Score**: En el **cuadro Puntos de desglose por: ...** En el **desplegable** podremos **seleccionar** entre **Categoría** y **Estado**.

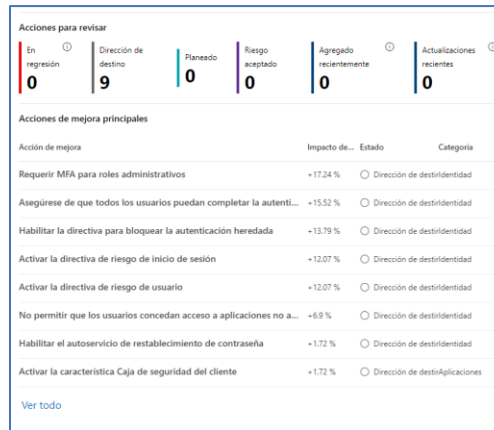


### Categorías:

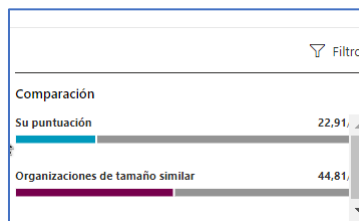
- i. Identidad.
- ii. Datos.
- iii. Dispositivos.
- iv. Aplicaciones.



- b. En el *centro de la ventana*, tenemos disponible un **menú interactivo**, si hacemos **clic** en cada una de las sugerencias (*especificadas por filas*) accedemos a la **hoja de ruta planificada** que nos recomienda Microsoft para realizarlas y nos llevará a la **Segunda sección: Acciones de mejora**.



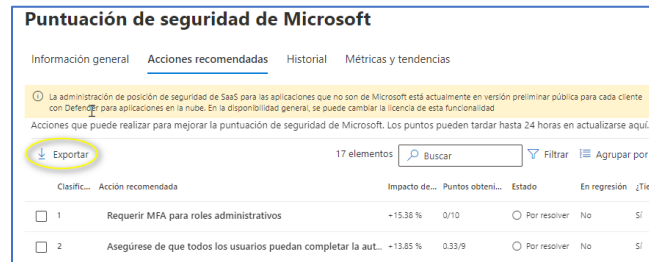
- c. En la parte izquierda, tenemos la **Comparación** de nuestra postura de seguridad actual con las medidas de seguridad implementadas por otras empresas (*en sus tenants*).



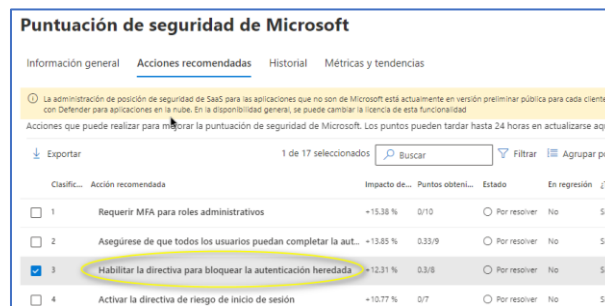
4. **Segunda pestaña: Acciones recomendadas.** Nos aparecerá la lista de acciones que podemos realizar en este momento para mejorar nuestra puntuación de seguridad. Esta lista esta “viva”, es decir, Microsoft la irá actualizando, dependiendo de nuestras acciones y de los diferentes patrones y/o vectores de ataque que vayan identificando sus servicios de seguridad embebidos en la plataforma de M365.

<

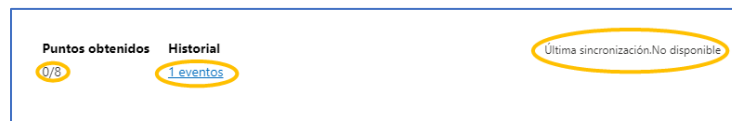
- d. Podremos: **Exportar, Buscar, Filtrar o Agrupar por**, según nuestras necesidades en la barra horizontal.



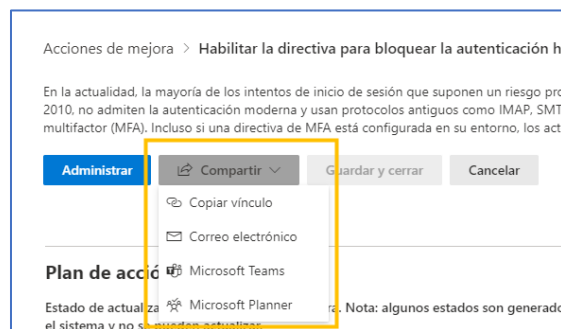
- e. Clic en la fila: **Habilitar la directiva para bloquear la autenticación heredada.**



- i. Nos aparecerá una nueva ventana. Nada más entrar en ella, seremos conscientes de los **puntos que ya hemos obtenido, de su historial** (el número de eventos relacionados con esta recomendación) y **cuándo fue la última vez que Microsoft actualizo** la información de seguridad que aparece en pantalla.



- ii. **Clic en el botón Compartir.** Así podemos tomar el control sobre esta recomendación en concreto. Pudiendo **seleccionar y delegar** en un equipo de trabajo o un administrador esta **acción de mejora** en particular.



iii. En la *parte izquierda* de la ventana tenemos la *sección vertical*: **Plan de acción**. Dónde definiremos

1. **Estado de esta acción recomendada**. Clic en el **círculo de selección: Planeado**
2. Podremos tanto añadir **Notas**: Escribir: Ya está asignado al equipo de administradores de esta tenant.
3. Asignaremos **Etiquetas**: Admins.

iv. En la *parte media* de la ventana tenemos la *sección vertical*: **De un vistazo**. Veremos **información** sobre la acción, como su **categoría**, **sobre que proteger** (si hacemos clic en los enlaces aparecerá otra Blade con más información), el **producto** o **servicio** de **Microsoft 365** relacionado y el **Impacto que puede producir en los usuarios** (para tomar las acciones que consideremos oportunas, como informarles vía correo electrónico, etc).

- v. En la *parte derecha* de la ventana tenemos la *sección vertical: Implementación*. Nos guiará a través del proceso de despliegue **de esta acción**. Haciendo **clic en cada uno de los enlaces** podríamos comenzar a trabajar sobre esta acción correctora para subir nuestra puntuación de seguridad en Secure Score.

### Implementación

**Requisitos previos**

- ✓ Dispone de Azure Active Directory Premium P1.

**Siguientes pasos**

Implementación estándar: si la organización no tiene requisitos de seguridad complejos, puede habilitar los valores predeterminados de seguridad para bloquear la autenticación heredada y requerir el registro y habilitación de MFA para todos los usuarios. [Más información sobre cómo activar los valores predeterminados de seguridad.](#)

Implementación personalizada: en el [Portal de acceso condicional de Azure AD](#)

1. Seleccione + **Nueva directiva**.
2. Asigne un nombre a la directiva. Microsoft recomienda que las organizaciones creen una norma relevante para los nombres de las directivas.
3. En Asignaciones, seleccione **Usuarios y grupos**. En Incluir, seleccione **Todos los usuarios**. En Excluir, seleccione **Usuarios y grupos** y elija las cuentas que deben mantener la capacidad de usar la autenticación heredada.
4. En Condiciones > Aplicaciones cliente, establezca Configurar en **Sí**. Active solo las casillas **Aplicaciones móviles y clientes de escritorio** y **Otros clientes**. Luego, seleccione **Listo**.
5. En Controles de acceso > Conceder, seleccione **Bloquear acceso**.
6. Confirme la configuración y establezca Habilitar directiva en **Activada**.
7. Seleccione **Crear** para crear y habilitar la directiva.

Nota: no se puntúan las directivas de acceso condicional clásico. Use los pasos recomendados para recibir crédito.

**Estado de la implementación**

24 de 25 usuarios no tienen bloqueada la autenticación heredada.


**Más información**

[Bloquear la autenticación heredada en Azure AD con acceso condicional](#)

[Bloquear autenticación heredada](#)

[¿Qué son los valores predeterminados de seguridad?](#)


- vi. **Clic en el botón superior Guardar y cerrar.**


**Seguridad de Microsoft 365**

Acciones de mejora > **Habilitar la directiva para bloquear la autenticación heredada**

En la actualidad, la mayoría de los intentos de inicio de sesión que suponen un riesgo provienen de la autenticación no admiten la autenticación moderna y usan protocolos antiguos como IMAP, SMTP y POP3. La autenticación heredada. Incluso si una directiva de MFA está configurada en su entorno, los actores maliciosos pueden eludir estas medidas.

Administrar

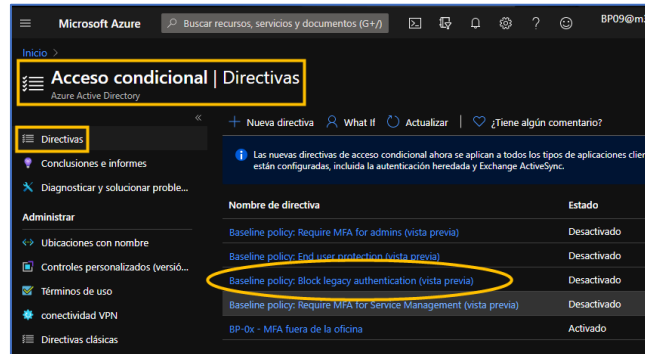
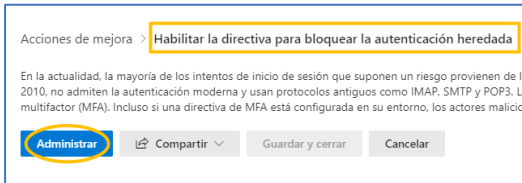

 Compartir ▼

**Guardar y cerrar**

Cancelar



- vii. También podemos hacer clic en el botón **Administrar**. El cual, nos llevará automáticamente a la **directiva** sobre la cual está **basada** esta **acción de mejora**. Desde este punto, podemos seguir la guía recomendada por Microsoft en el anterior punto de esta laboratorio, el “v”.



### Baseline policy: Block legacy authentication (vista previa)

Directivas

Nombre

Baseline policy: Block legacy authentication...

Esta directiva se ha dejado de usar y ya no se está aplicando. Si quiere habilitar una funcionalidad similar, se recomienda habilitar los valores predeterminados de seguridad o configurar las directivas de acceso condicional equivalentes.

NOTA: Los valores predeterminados de seguridad no se admiten en inquilinos de Azure AD B2C.

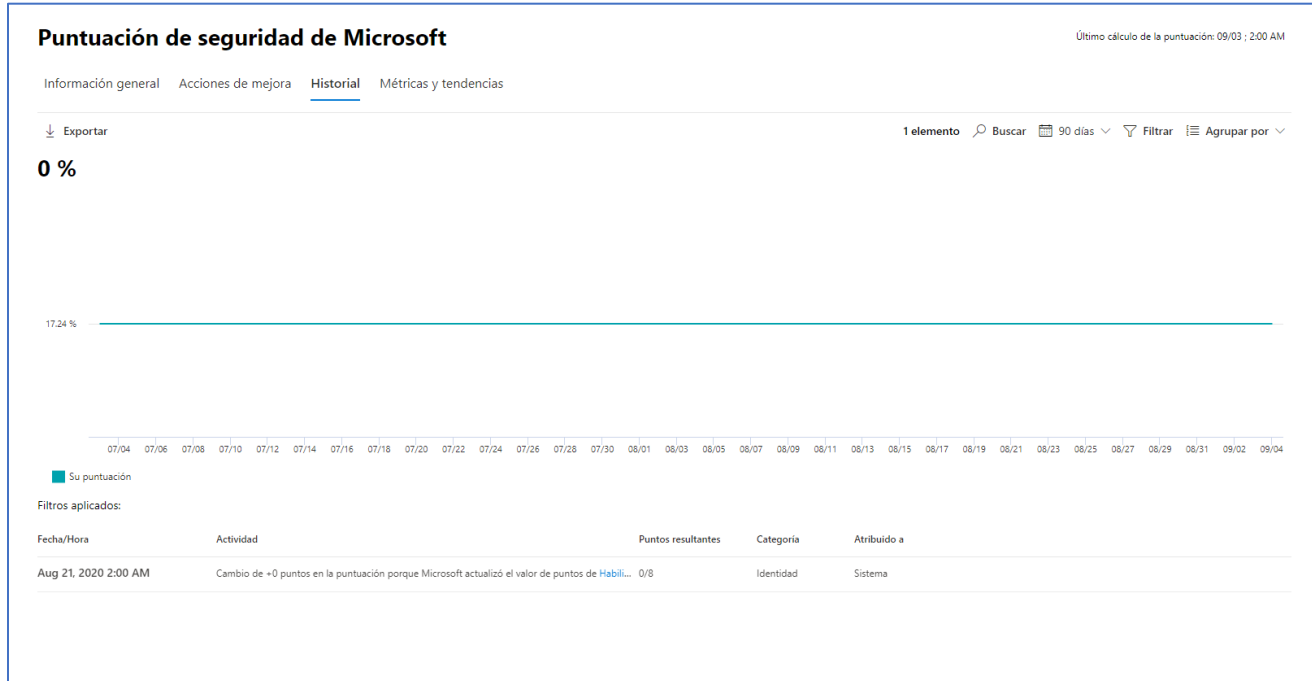
Esta directiva bloquea todos los inicios de sesión que usan protocolos de autenticación heredados que no admiten la autenticación multifactor (como IMAP, POP o SMTP). La directiva no bloquea Exchange ActiveSync.

- Office 2013 (sin claves del registro)
- Office 2010
- Cliente de Thunderbird
- Skype Empresarial heredado
- Cliente de correo Android nativo

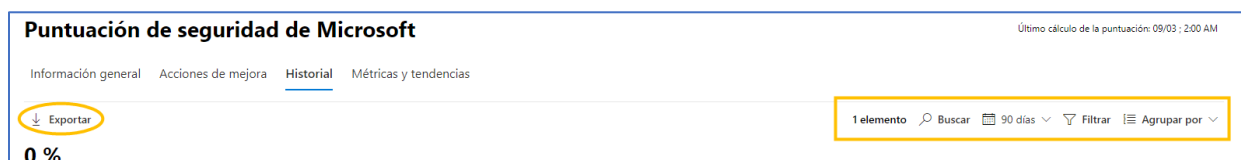
Más información

**⚠** Esta directiva ha quedado obsoleta. Ya no se aplica y no se puede habilitar. Haga clic aquí para ver una guía donde se indica paso a paso cómo configurar la directiva equivalente usando el acceso condicional.

5. **Tercera sección: Historial.** Sí acabamos de abrir esta tenant para nuestros clientes, como es este el caso, *en esta sección todavía no encontraremos información en el tiempo de las acciones que hemos desarrollado en la tenant.* El gráfico que aparece en pantalla corresponde al **historial de los últimos 30, 60 y 90 días**, mostrando la **puntuación obtenida** en estos rangos de tiempo.



- f. Podremos al igual que en la sección anterior: **Exportar, Buscar, Filtrar o Agrupar por**, según nuestras necesidades en la barra horizontal.



- g. En la parte inferior de la pantalla, podremos encontrar la información sobre las acciones que acabamos de realizar en la sección de configuración anterior.

Filtros aplicados:

Fecha/Hora	Actividad	Puntos resultantes	Categoría	Atribuido a
Sep 4, 2020 2:05 PM	BP09 marcó <b>Habilitar la directiva para bloquear la autenticación heredada</b> como planeado	0/8	Identidad	BP09
Aug 21, 2020 2:00 AM	Cambio de +0 puntos en la puntuación porque Microsoft actualizó el valor de puntos de Habili...	0/8	Identidad	Sistema

6. **Cuarta sección: Métricas y tendencias.** Tendremos un **resumen actualizado** con **toda la información** relativa a nuestra **postura de seguridad** (*comparación, tendencia aceptación de riesgo, cambios de puntuación, etc*).

