

## Contenido

---

Laboratorio: Directivas de Acceso condicional.....	2
--	---

## Laboratorio: Directivas de Acceso condicional.

**Objetivo:** Habilitar la Autenticación MFA del usuario **jose-MS0x** (la "x" es el usuario que los instructores os hemos proporcionado al comienzo del curso) cuando se encuentre fuera de la oficina a través de las **Directivas de Acceso condicional**.

El **acceso condicional** es una característica de Azure Active Directory que nos **permite aplicar controles** (con acciones que tendrá que realizar el usuario) **cuando quiera acceder a un recurso de nuestro Azure Active Directory** (su buzón de correo, una App que estemos publicando o cualquier otro recurso o acceso a todos los recursos) para mantener la organización segura y no interferir con el resto de los usuarios que no estén en su situación.

En este laboratorio, vamos a **crear una política de Acceso Condicional** en la que vamos a **requerir que el usuario jose-EMS0x cuando esté trabajando fuera de nuestra red corporativa** se le solicite el **MFA para acceder a los servicios de Office 365**. **NO** se le **pedirá** al resto de usuario ni a este **mismo usuario siempre** que esté conectándose *desde la oficina de la empresa*.

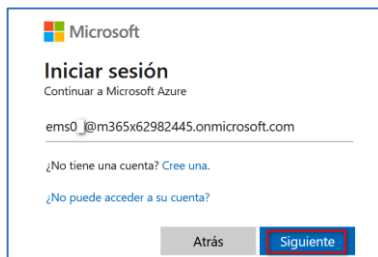
**Prerrequisitos:** Tener una tenant de Microsoft propia o de prueba con los planes o servicios correspondientes, Business Premium, Planes Empresa o Servicios "sueños" (Exchange Online P1/P2, SharePoint Online P1/P2, Teams, etc).

### Pasos a realizar:

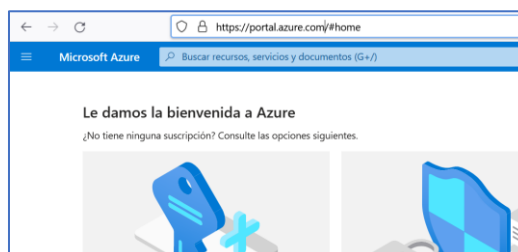
1. Logarnos al Portal Azure, en este enlace- <https://portal.azure.com/> como admin.

**Usuario:** [EMS0x@m365\\*\\*\\*\\*\\*.onmicrosoft.com](mailto:EMS0x@m365*****.onmicrosoft.com) (la "x" es el usuario que os hemos dado al comienzo del curso).

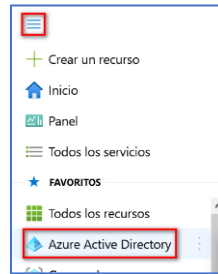
**Contraseña:** HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



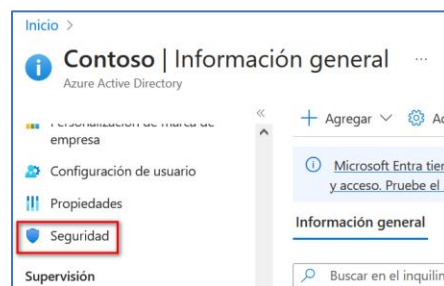
2. Aparecerá la **Dashboard de Microsoft Azure AD**.



3. Clic en  Microsoft Azure en la **parte izquierda de la pantalla** para ver el **menú del portal de Azure**

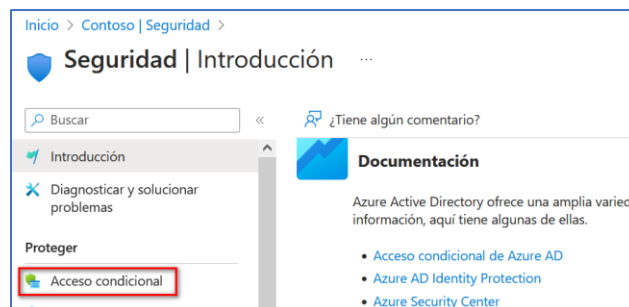


4. **Clic en Azure Active Directory.** En la nueva pantalla dentro de la sección **Administrar.** Clic en la opción **Seguridad:**

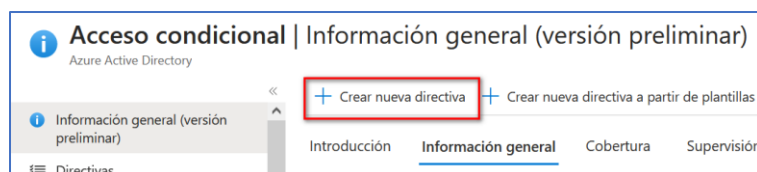


5. **Clic en Acceso condicional** en la *sección Proteger.*

**El acceso condicional nos da la posibilidad de obligar a los usuarios a cumplir los requisitos de acceso** cuando se produzcan **determinadas condiciones** y **ellos** tendrán que realizar **las acciones** que los admins **les obliguemos** para **poder acceder.** *Por ejemplo:* Cuando un usuario está fuera de la red de la empresa, le **exigiremos** el **MFA.**

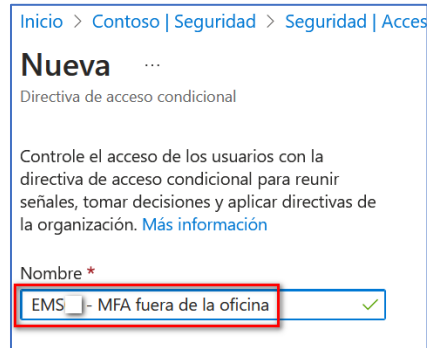


6. **Nos aparecerá la ventana de configuración del Acceso condicional.** Clic en **+ nueva directiva** en la **barra horizontal,** para comenzar a crearnos la **directiva:**

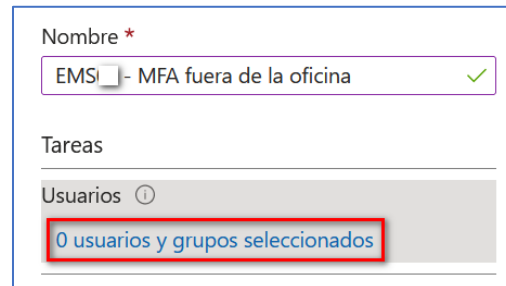


7. Aparecerá la ventana de configuración de la directiva.

Escribimos el nombre de la directiva: EMS0x - MFA fuera de la oficina *(la "x" es el usuario que los instructores os hemos proporcionado al comienzo del curso)*.



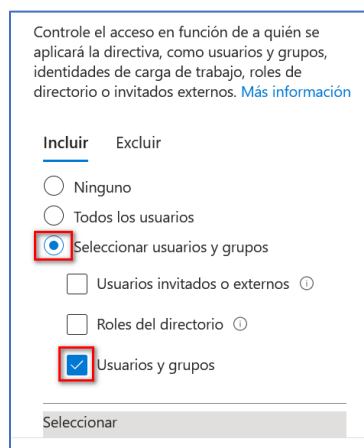
8. Clic dentro de la sección Tareas en la entrada 0 usuarios y grupos seleccionados.



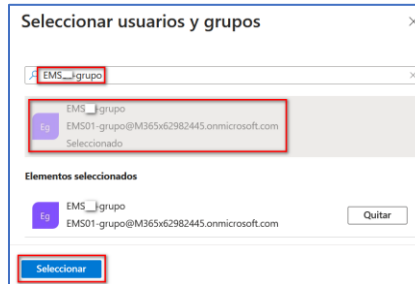
9. En la nueva Blade a la derecha de la pantalla. En la sección: Incluir.

Clic en radio button: Seleccionar usuarios y grupos.

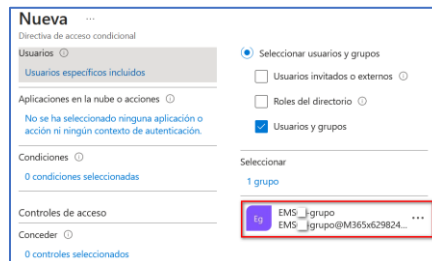
Clic en el cuadro: Usuarios y grupos.



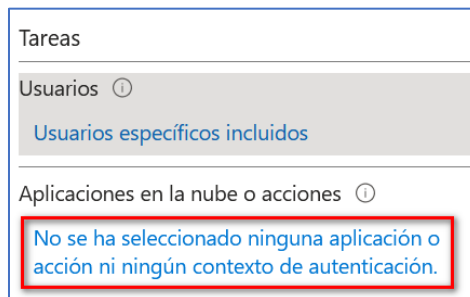
10. Aparecerá otra **Blade** a la derecha de la pantalla, en el campo de búsqueda escribimos el nombre de nuestro grupo: **EMS0x-grupo** (la "x" es el usuario que los instructores os hemos proporcionado al comienzo del curso). Clic en el nombre del grupo. Clic en el botón inferior de la pantalla **Seleccionar**.



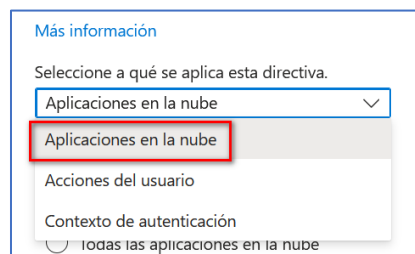
11. Nos aparecerá el grupo de usuarios como seleccionado.



12. Clic dentro de la sección: **Aplicaciones en la nube o acciones**. En el link: **No se ha seleccionado ninguna aplicación o acción ni ningún contexto de autenticación**.



13. Clic en el desplegable: **Seleccione a qué se aplica esta directiva**. Clic: **Seleccionar aplicaciones en la nube**.



14. En la *sección: Incluir*, clic en el **radio button: Seleccionar aplicaciones**.

**Clic en el link dentro la sección Seleccionar: Ninguno**

Incluir Excluir

☐ Ninguno

☐ Todas las aplicaciones en la nube

☒ Seleccionar aplicaciones

Editar filtro (versión preliminar)

[Ninguno](#)

Seleccionar

[Ninguno](#)

15. Aparecerá una *nueva Blade a la derecha de la pantalla*. En el **campo de búsqueda** escribir: **office**.

**Clic en la caja de selección a la izquierda de Office 365 para seleccionarlo.**

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

Seleccionar

Aplicaciones en la nube

office

☒ Office 365

☐ Office 365 Exchange On...

☐ Office 365 SharePoint O...

Elementos seleccionados

☒ Office 365

Quitar

Seleccionar

16. **Clic dentro de la sección: Condiciones**, en el **enlace: 0 condiciones seleccionadas**.

Inicio > Contoso | Seguridad > Seguridad | Acc

**Nueva** ...

Directiva de acceso condicional

Tareas

Usuarios <sup>?</sup>

[Usuarios específicos incluidos](#)

Aplicaciones en la nube o acciones <sup>?</sup>

[1 aplicación incluida](#)

Condiciones <sup>?</sup>

[0 condiciones seleccionadas](#)

17. En la *Blade* (ventana) de la izquierda: **Riesgo de usuario**. Clic en el *enlace*: **Sin configurar**.

18. En la blade que saldrá en la parte izquierda de la pantalla. En el deslizable de la sección: *Configurar*, poner el **desplegable** en **Sí**.

**Clic en la caja de selección** del establecer en: **Alta**.

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

19. En la *sección inferior de esta misma ventana*. Dentro de la *opción*: **Nivel de riesgo de inicio de sesión**.

**Clic en el enlace Sin configurar.**

20. En la *Blade* que saldrá en la parte izquierda de la pantalla. En el **deslizable** de la *sección Configurar*, poner el **desplegable** en **Sí**.

**Clic** en la caja de selección en el lado izquierdo de la pantalla en las **opciones: Alta y Mediana**.

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

**Riesgo de inicio de sesión**

Controle el acceso de los usuarios para responder a niveles de riesgo específicos de inicio de sesión. [Más información](#)

Configurar ☐ **Sí** ☐ No

El nivel de riesgo de inicio de sesión se genera en función de todas las detecciones de riesgo en tiempo real.

Seleccionar el nivel de riesgo de inicio de sesión al que se aplicará la directiva

☒ Alta  
☒ Mediana  
☐ Baja  
☐ Sin riesgo

**Listo**

21. En la *siguiente sección de esta misma blade*: En la parte: **Plataformas de dispositivo**. **Clic** en el *enlace: Sin configurar*. Seleccionamos desde a que plataforma se aplicará la directiva.

**Nueva** ...  
Directiva de acceso condicional

Controle el acceso de los usuarios con la directiva de acceso condicional para reunir señales, tomar decisiones y aplicar directivas de la organización. [Más información](#)

Nombre \*  
EMSOx - MFA fuera de la oficina ✓

Tareas  
Usuarios ☐  
[Usuarios específicos incluidos](#)

Aplicaciones en la nube o acciones ☐  
[1 aplicación incluida](#)

Controle el acceso de los usuarios en función de las señales de las condiciones como el riesgo, la plataforma del dispositivo, la ubicación, las aplicaciones cliente o el estado del dispositivo. [Más información](#)

Riesgo de usuario ☐  
[1 incluido](#)

Riesgo de inicio de sesión ☐  
[2 incluido](#)

Plataformas de dispositivo ☐  
**Sin configurar**

22. En la Blade que saldrá en la parte izquierda de la pantalla. En el **deslizable** de la *sección Configurar*, poner el **desplegable** en **“Sí”**. **Clic** en la *caja de selección* en el lado izquierdo de la pantalla en la *opción: Cualquier dispositivo* dentro de la *sección Incluir*.

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

**Plataformas de dispositivo**

Aplicar directiva a las plataformas de dispositivo seleccionadas. [Más información](#)

Configurar ☐ **Sí** ☐ No

Incluir Excluir

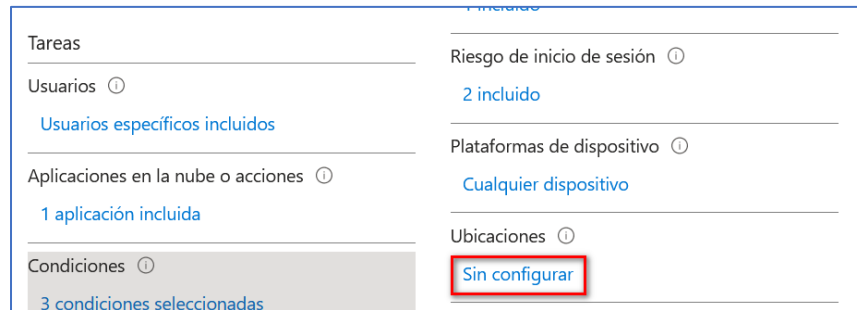
☒ **Cualquier dispositivo**  
☐ Seleccionar plataformas de dispositivo

☐ Android  
☐ iOS  
☐ Windows Phone  
☐ Windows  
☐ macOS

**Listo**

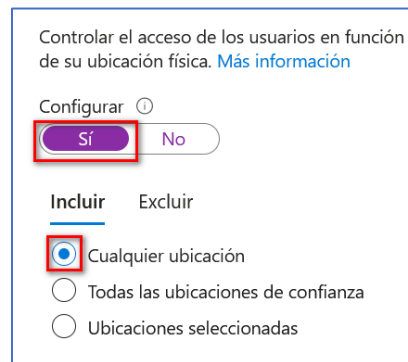


23. En la siguiente sección de la *ventana del medio de la pantalla*: **Ubicaciones**. Clic en el enlace: **Sin configurar**.



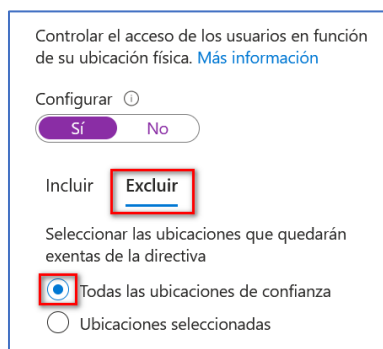
The screenshot shows the 'Ubicaciones' (Locations) section in the Microsoft 365 Identity Management console. The section is titled 'Ubicaciones' and has a sub-header 'Sin configurar'. Below this, there are two columns of settings. The left column includes 'Tareas' (Tasks), 'Usuarios' (Users) with a link 'Usuarios específicos incluidos', 'Aplicaciones en la nube o acciones' (Cloud apps or actions) with a link '1 aplicación incluida', and 'Condiciones' (Conditions) with a link '3 condiciones seleccionadas'. The right column includes 'Riesgo de inicio de sesión' (Sign-in risk) with a link '2 incluido', 'Plataformas de dispositivo' (Device platforms) with a link 'Cualquier dispositivo', and 'Ubicaciones' (Locations) with a link 'Sin configurar'.

24. clic en el deslizable: **Sí** Clic dentro de la *sección*: **Incluir en: Cualquier ubicación**.



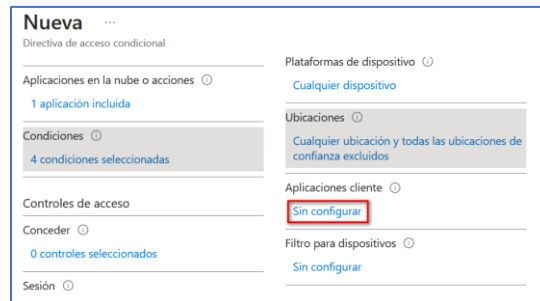
The screenshot shows the 'Ubicaciones' configuration window. The title is 'Controlar el acceso de los usuarios en función de su ubicación física. Más información'. Below the title is a 'Configurar' section with a 'Sí' (Yes) toggle highlighted by a red box. Below the toggle are two tabs: 'Incluir' (selected) and 'Excluir' (Excluded). Under the 'Incluir' tab, there are three radio buttons: 'Cualquier ubicación' (Any location) highlighted by a red box, 'Todas las ubicaciones de confianza' (All trusted locations), and 'Ubicaciones seleccionadas' (Selected locations).

25. Clic en la *sección*: **Excluir de esta misma ventana**. Clic en la *caja de selección* **Todas las ubicaciones de confianza**.



The screenshot shows the 'Ubicaciones' configuration window. The title is 'Controlar el acceso de los usuarios en función de su ubicación física. Más información'. Below the title is a 'Configurar' section with a 'Sí' (Yes) toggle. Below the toggle are two tabs: 'Incluir' (Included) and 'Excluir' (Excluded) highlighted by a red box. Under the 'Excluir' tab, there are two radio buttons: 'Todas las ubicaciones de confianza' (All trusted locations) highlighted by a red box, and 'Ubicaciones seleccionadas' (Selected locations).

26. Dentro de la *sección: Aplicaciones cliente*. Clic en el *enlace: Sin configurar*. Aquí seleccionaremos con que **Software** permitimos que **el usuario pueda acceder** a la suite de Office 365



**Nueva** ...

Directiva de acceso condicional

Aplicaciones en la nube o acciones ⓘ

1 aplicación incluida

Condiciones ⓘ

4 condiciones seleccionadas

Plataformas de dispositivo ⓘ

Cualquier dispositivo

Ubicaciones ⓘ

Cualquier ubicación y todas las ubicaciones de confianza excluidas

Aplicaciones cliente ⓘ

**Sin configurar**

Controles de acceso

Conceder ⓘ

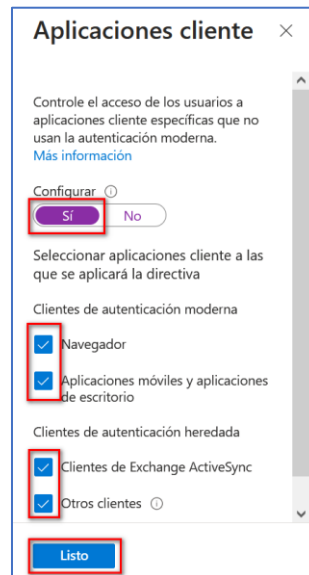
0 controles seleccionados

Filtro para dispositivos ⓘ

Sin configurar

Sesión ⓘ

27. Clic en el *deslizable: Sí* de la *sección Configurar*.  
**Clic: Navegador, App móviles y apps de escritorio, Otros clientes.**  
**Clic en el botón Listo**



**Aplicaciones cliente** ×

Controle el acceso de los usuarios a aplicaciones cliente específicas que no usan la autenticación moderna.  
[Más información](#)

Configurar ⓘ

**Sí** No

Seleccionar aplicaciones cliente a las que se aplicará la directiva

Clientes de autenticación moderna

☒ Navegador

☒ Aplicaciones móviles y aplicaciones de escritorio

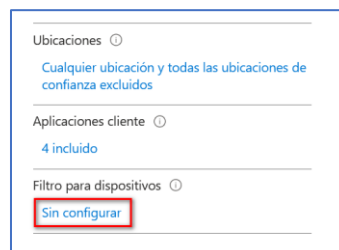
Clientes de autenticación heredada

☒ Clientes de Exchange ActiveSync

☒ Otros clientes ⓘ

**Listo**

28. Dentro de la *sección: Filtro para dispositivos*. Podríamos configurar el modelo, fabricante, si está o no unido a Azure Active Directory, etc de los dispositivos desde dónde nuestros usuarios iniciarán sesión. Revisar las opciones, **PERO** dejarlo: **Sin configurar (para evitar desconfiguraciones)**.



Ubicaciones ⓘ

Cualquier ubicación y todas las ubicaciones de confianza excluidas

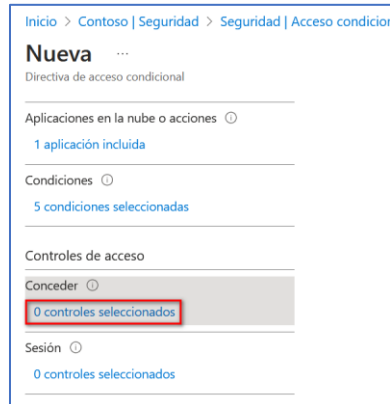
Aplicaciones cliente ⓘ

4 incluido

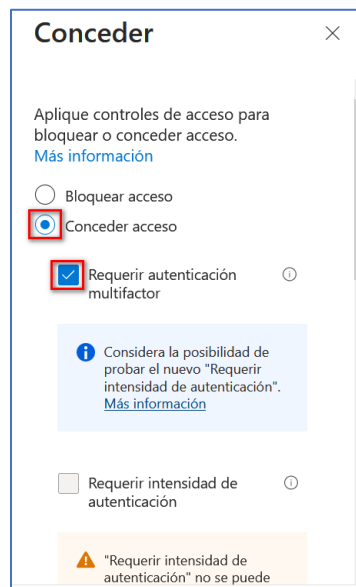
Filtro para dispositivos ⓘ

**Sin configurar**

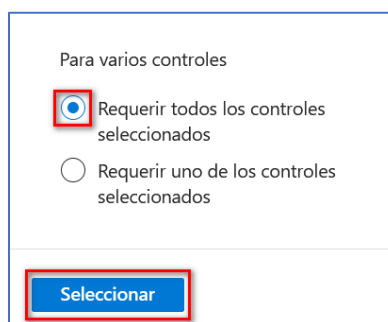
29. Ahora **pasamos** a la **sección: Controles de acceso** de la **ventana principal** a la **derecha de la pantalla**.  
Dentro de la **sección: Conceder**. **Clic** en el **enlace: “0 controles seleccionados”**.



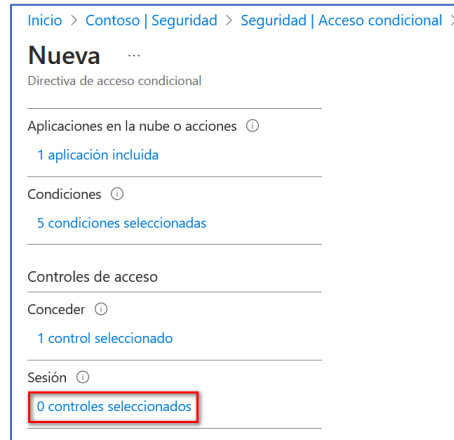
30. Nos aparecerá una **nueva ventana de configuración** en la parte derecha del navegador.  
**Clic** en **Conceder acceso** y **clic** en la opción: **Requerir autenticación multifactor**.



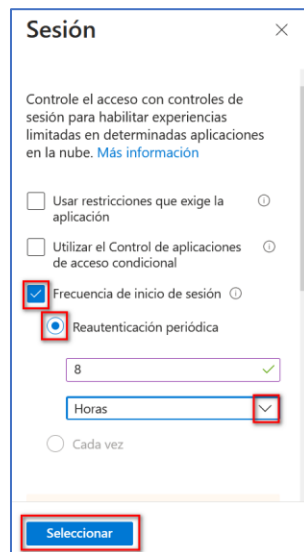
31. En la sección **Para varios controles: Requerir todos los controles seleccionados**.  
**Clic** en el botón inferior: **Seleccionar**.



32. Ahora pasamos a la *sección: Sesión* de la *ventana principal* a la *derecha de la pantalla*.  
Dentro de la *sección: Sesión*. Clic en el *enlace: "0 controles seccionados"*.



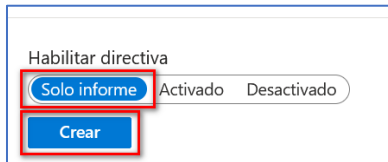
33. Nos aparecerá una **nueva ventana de configuración** en la parte derecha del navegador.  
**Clic en Frecuencia de inicio de sesión** y clic en la opción: **Reautenticación periódica**. En el *desplegable inferior* seleccionar: **horas** y en el *cuadro de texto superior* escribir: **8 horas**.  
**Clic en el botón inferior: Seleccionar**.



34. Por último. Clic en el **deslizable Solo Informe**, para tener un tiempo en el cual **NO** se **aplique** esta directiva y **poder comprobar los posibles “falsos positivos”** que pudieran ocurrir.

Pasado ese tiempo de comprobación. Clic en el botón **Activado** para realizar su activación

Clic en el botón: **Guardar**.



35. Podremos ver la **Directivas de Acceso condicional** que nos acabamos de crear.

