

Proyecto: Seguridad en Azure - MFA, Access Policies, Identity Protection.

Introducción

Este proyecto se centra en la implementación de medidas de seguridad avanzadas en Azure, específicamente en la protección de identidades mediante la configuración de MFA (Multi-Factor Authentication), políticas de acceso, y protección de identidades con Microsoft Entra Identity Protection. El objetivo es asegurar los accesos y mejorar la seguridad en el entorno de Azure AD.

Requisitos

Para completar este laboratorio se requiere una suscripción de Azure activa y acceso a las funcionalidades de Azure AD Premium. El usuario debe contar con permisos de administrador global o similar para configurar estas políticas de seguridad.

Herramientas utilizadas en el proyecto:

- **Azure Active Directory (Azure AD):** Para la gestión de identidades, grupos y roles.
- **Azure Multi-Factor Authentication (MFA):** Para proteger el acceso de los usuarios mediante la autenticación multifactor.
- **Azure AD Conditional Access:** Para crear políticas que requieren MFA u otros controles de acceso.
- **Microsoft Entra Identity Protection:** Para detectar y gestionar riesgos de inicio de sesión y proteger las identidades.
- **Azure Security Center:** Para monitorear eventos de seguridad, configurar alertas y gestionar la seguridad de los recursos en Azure.
- **Azure Portal:** Para administrar y configurar los recursos dentro de la plataforma de Azure.

Pasos del Proyecto

Paso 1: Crear usuarios y grupos en Azure AD

Inicia sesión en Azure Portal y accede a Microsoft Entra ID. Luego, crea un usuario y asigna un grupo con roles específicos que necesitarás para probar las políticas de seguridad.

Microsoft Azure | Actualización | Buscar recursos, servicios y documentos (G+)

Inicio > Directorio predeterminado | Usuarios >

Usuarios

Directorio predeterminado

+ Nuevo usuario | Editar (versión preliminar) | Eliminar | Descargar usuarios | Operaciones masivas | Actualizar | Administrar vista | MFA por usuario

Todos los usuarios | Azure Active Directory ahora es Microsoft Entra ID

Registros de auditoría | Registros de inicio de sesión | Diagnosticar y solucionar problemas | Usuarios eliminados | Restablecimiento de contraseña | Configuración del usuario | Resultados de la operación masiva | Nueva solicitud de soporte técnico

2 usuarios encontrados

<input type="checkbox"/>	Nombre para mostrar ↑↓	Nombre principal de usu... ↑↓	Tipo de usuario	Sincronización l...	Identities	Nombre de la empresa	Tipo de creación
<input type="checkbox"/>	user2	user2@alexisgghotmail.o...	Miembro	No	alexisgghotmail.onmicrosoft.com		
<input type="checkbox"/>	user1	user1@alexisgghotmail.o...	Miembro	No	alexisgghotmail.onmicrosoft.com		

Microsoft Azure | Actualización | Buscar recursos, servicios y documentos (G+)

Inicio > Directorio predeterminado | Grupos > Grupos | Todos los grupos > Empleados

Empleados | Miembros

Grupo

+ Agregar miembros | Operaciones masivas | Actualizar | Administrar vista | Quitar | ¿Tiene algún comentario?

Miembros directos | Todos los miembros

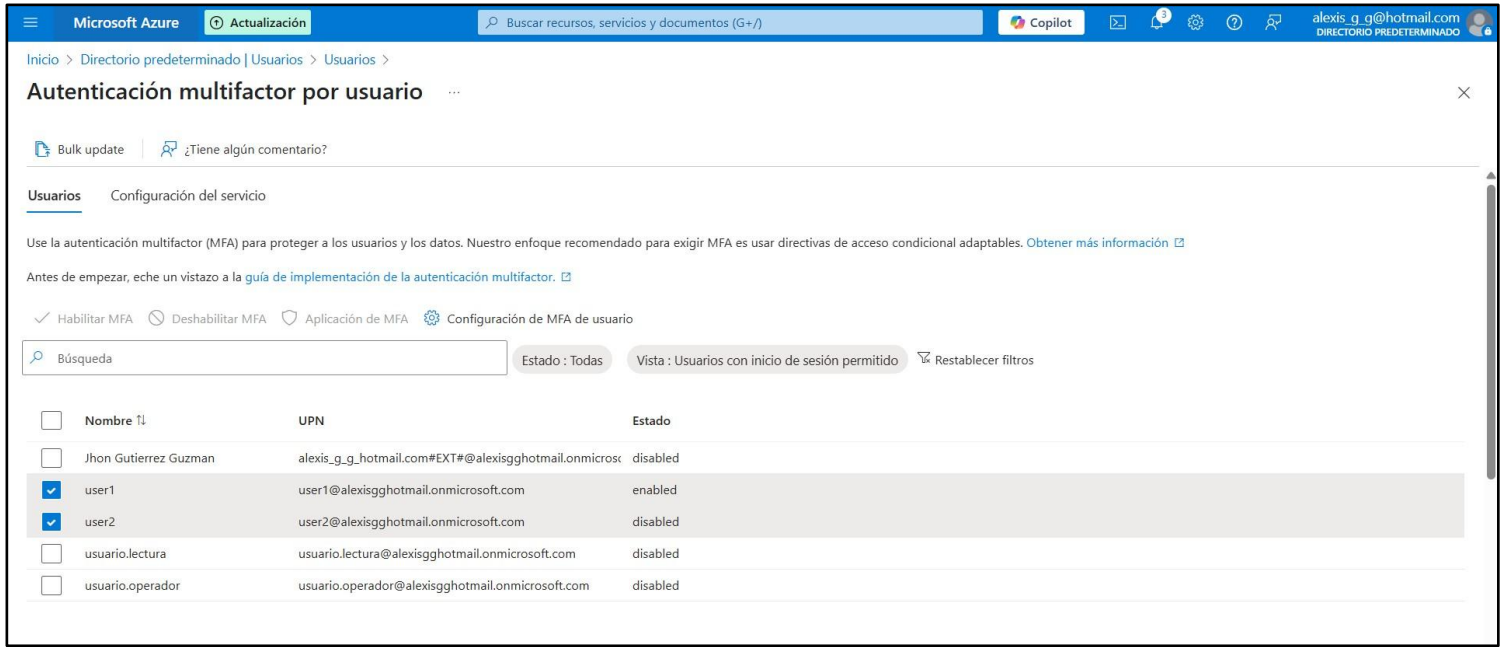
Búsqueda | Agregar filtro

2 miembros del grupo encontrados

<input type="checkbox"/>	Nombre ↑	Tipo	Correo electrónico	Tipo de usuario	Id. de objeto
<input type="checkbox"/>	user1	Usuario		Miembro	f28182f3-37fc-4ca8-9439-dcf
<input type="checkbox"/>	user2	Usuario		Miembro	44ded0da-9521-4a22-91fd-9

Paso 2: Activar MFA (Autenticación Multifactor)

Accede a la configuración de MFA en Microsoft Entra ID. Activa la opción de MFA para los usuarios y aplica políticas para que la autenticación multifactor sea obligatoria en todos los inicios de sesión.



Microsoft Azure Actualización Buscar recursos, servicios y documentos (G+/) Copilot alexis.g.g@hotmail.com DIRECTORIO PREDETERMINADO

Inicio > Directorio predeterminado | Usuarios > Usuarios >

Autenticación multifactor por usuario

Bulk update ¿Tiene algún comentario?

Usuarios Configuración del servicio

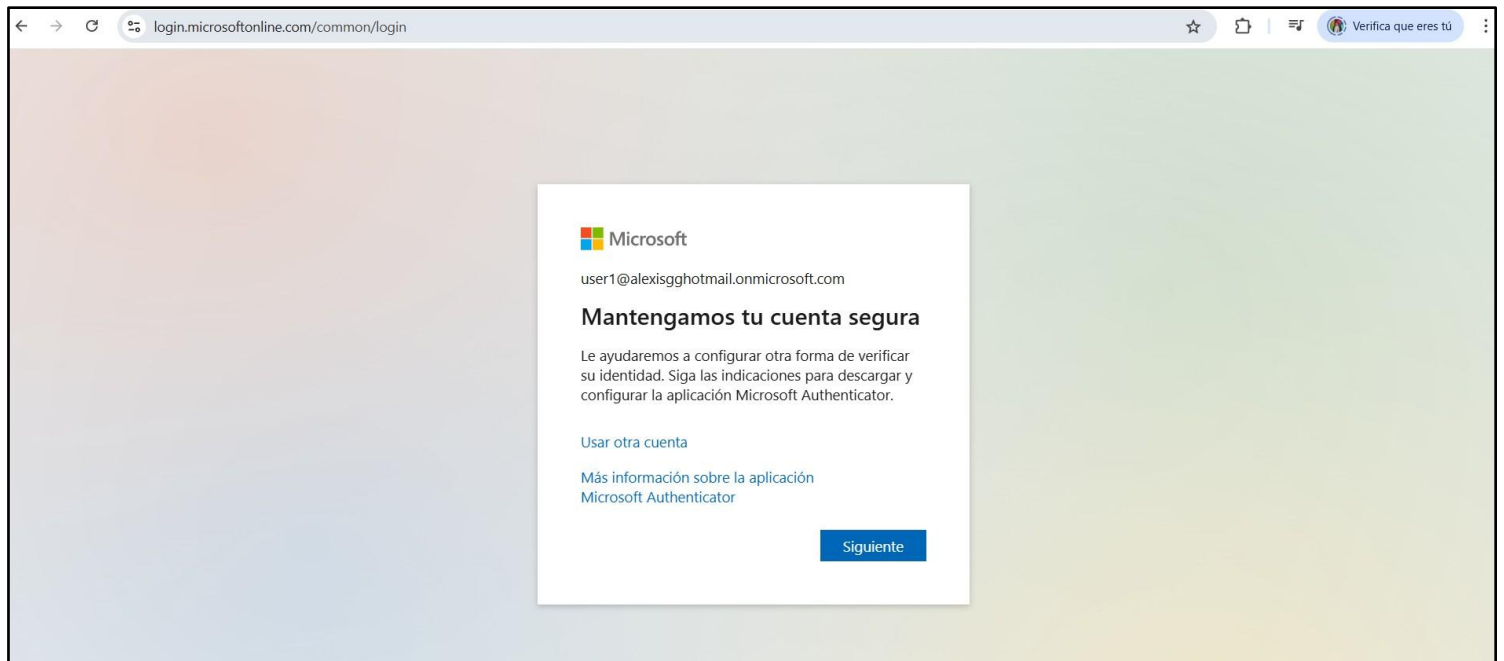
Use la autenticación multifactor (MFA) para proteger a los usuarios y los datos. Nuestro enfoque recomendado para exigir MFA es usar directivas de acceso condicional adaptables. [Obtener más información](#)

Antes de empezar, eche un vistazo a la [guía de implementación de la autenticación multifactor](#).

✓ Habilitar MFA ○ Deshabilitar MFA ○ Aplicación de MFA ⚙ Configuración de MFA de usuario

Búsqueda Estado : Todas Vista : Usuarios con inicio de sesión permitido Restablecer filtros

<input type="checkbox"/>	Nombre ↕	UPN	Estado
<input type="checkbox"/>	Jhon Gutierrez Guzman	alexis_g_g@hotmail.com#EXT#@alexisgghotmail.onmicroso	disabled
<input checked="" type="checkbox"/>	user1	user1@alexisgghotmail.onmicrosoft.com	enabled
<input checked="" type="checkbox"/>	user2	user2@alexisgghotmail.onmicrosoft.com	disabled
<input type="checkbox"/>	usuario.lectura	usuario.lectura@alexisgghotmail.onmicrosoft.com	disabled
<input type="checkbox"/>	usuario.operador	usuario.operador@alexisgghotmail.onmicrosoft.com	disabled



login.microsoftonline.com/common/login Verifica que eres tú

Microsoft

user1@alexisgghotmail.onmicrosoft.com

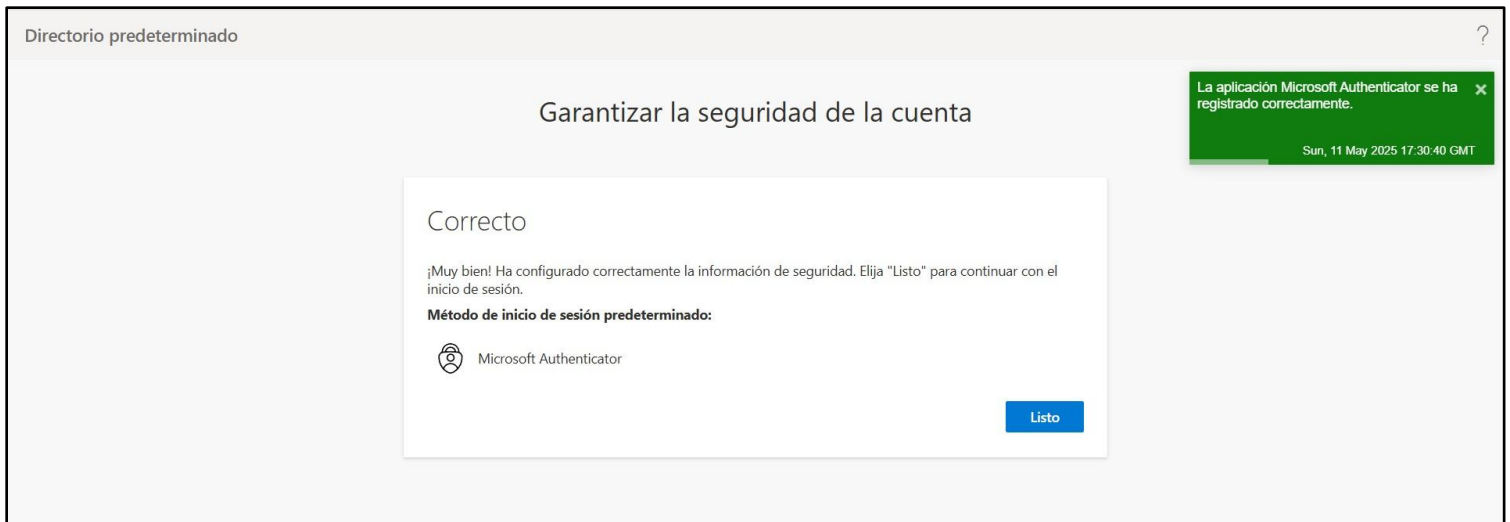
Mantengamos tu cuenta segura

Le ayudaremos a configurar otra forma de verificar su identidad. Siga las indicaciones para descargar y configurar la aplicación Microsoft Authenticator.

[Usar otra cuenta](#)

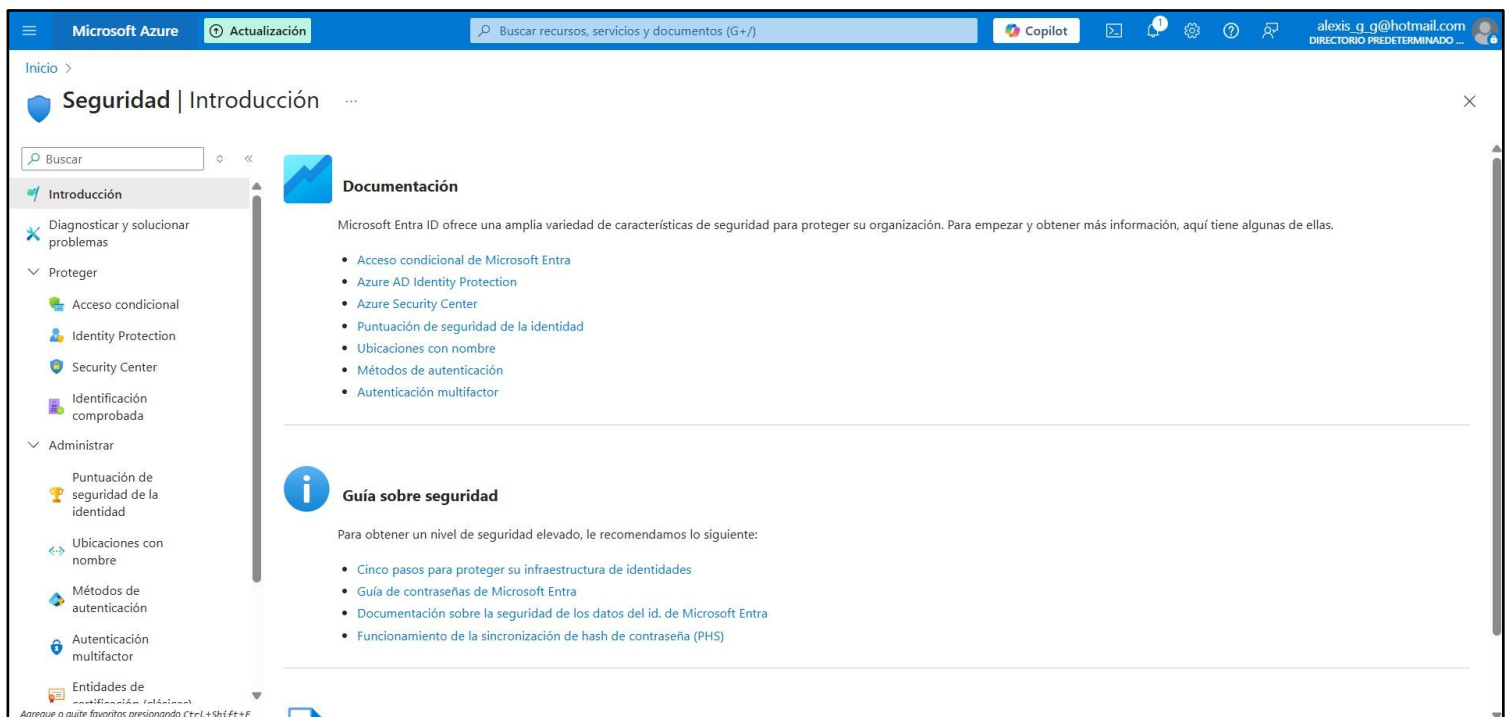
[Más información sobre la aplicación Microsoft Authenticator](#)

[Siguiente](#)



Paso 3: Configurar políticas de acceso condicional

Configura políticas de acceso condicional para requerir MFA o aplicar otras condiciones de seguridad, como la ubicación geográfica o el dispositivo usado para el inicio de sesión.



Microsoft Azure

Buscar recursos, servicios y documentos (G+/)

Copilot

JhonGutierrez@Inmerso...

Todos los servicios >

Directivas

+ Nueva directiva

+ Nueva directiva de plantilla

↑ Cargar archivo de directiva

👤 Qué pasa si

🔄 Actualizar

📄 Características en vista previa (GB)

💬 ¿Tiene algún comentario?

Microsoft Entra las directivas de acceso condicional se usan para aplicar controles de acceso para mantener la seguridad de su organización. [Obtener más información](#)

Todas las directivas

Directivas administradas por Microsoft

6

0

Total

de 6

Búsqueda

Agregar filtro

Se han encontrado 6 de 6 directivas.

Nombre de directiva	Estado	Fecha de creación	Fecha de modificación
Bloquear acceso desde ubicaciones arriesgadas	Activado	11/5/2025, 12:26:50	11/5/2025, 12:27:20
Bloquear todos los inicios de sesión heredados que no admitan MFA	Activado	11/5/2025, 12:14:01	
Requerir MFA cuando se detecten inicios de sesión de riesgo	Activado	11/5/2025, 12:14:03	
Requerir MFA para administradores	Activado	11/5/2025, 12:13:52	
Requerir MFA y un cambio de contraseña cuando se detecte usuarios de alto...	Activado	11/5/2025, 12:14:01	
Requerir la MFA para usuarios externos e invitados	Activado	11/5/2025, 12:13:57	

Microsoft Azure

Buscar recursos, servicios y documentos (G+/)

Copilot

JhonGutierrez@Inmerso...

Todos los servicios > Acceso condicional | Información general >

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](#)

Controle el acceso en función de a quién se aplicará la directiva, como usuarios y grupos, identidades de carga de trabajo, roles de directorio o invitados externos. [Más información](#)

Nombre *

Bloquear acceso desde ubicaciones arries...

Tareas

Usuarios

Usuarios específicos incluidos

Recursos de destino

No se ha seleccionado ningún recurso de destino

Red

NUEVO

Sin configurar

Condiciones

0 condiciones seleccionadas

Habilitar directiva

Solo informe

Activado

Desactivado

Crear

Incluir

Excluir

☐ Ninguno

☐ Todos los usuarios

☒ Seleccionar usuarios y grupos

☐ Usuarios invitados o externos

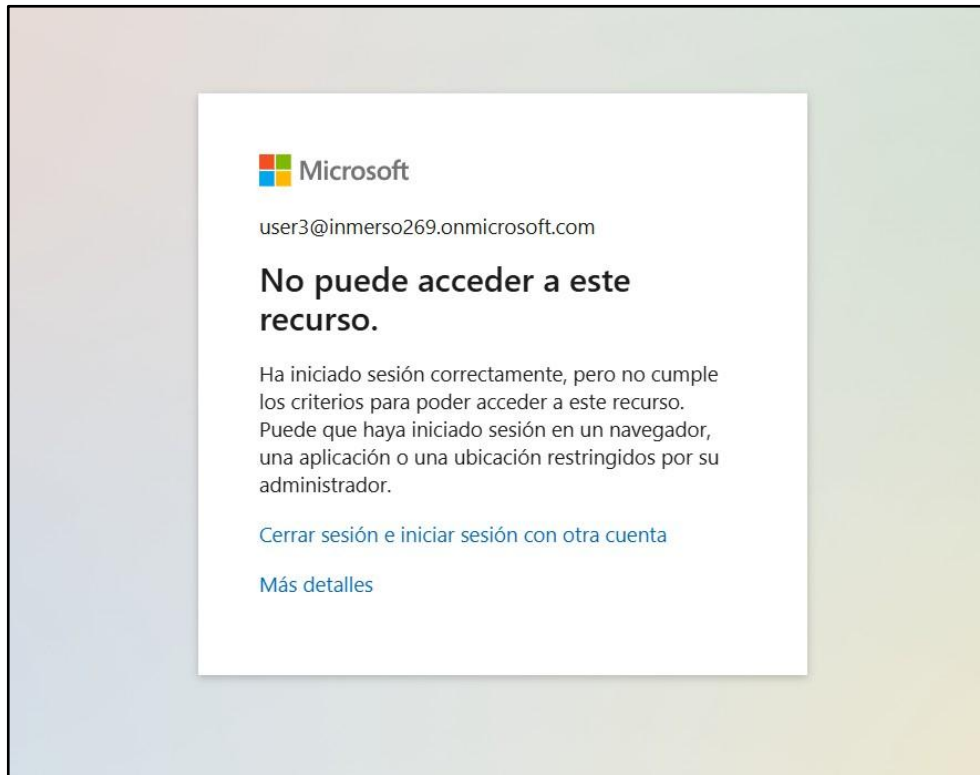
☐ Roles del directorio

☒ Usuarios y grupos

Seleccionar

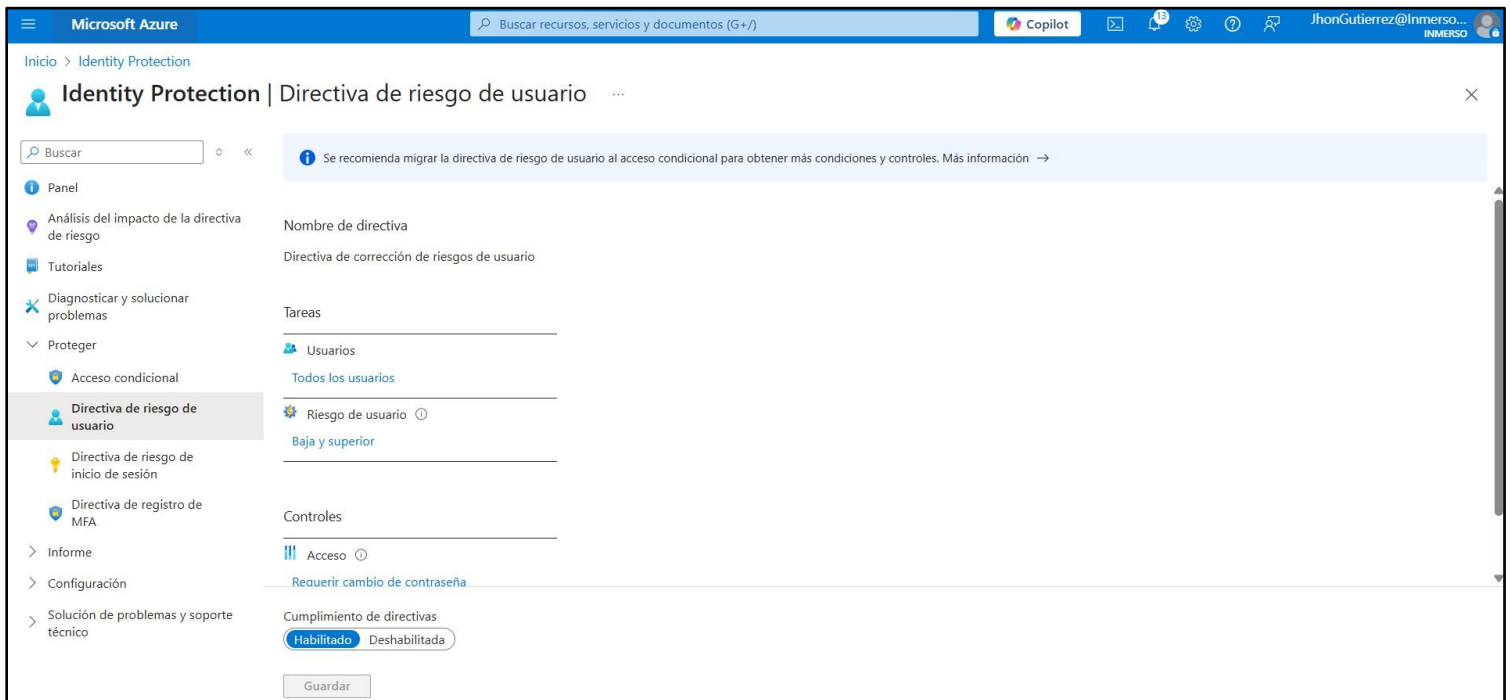
1 usuario

US user3



Paso 4: Usar Microsoft Entra Identity Protection

Configura políticas de protección de identidad con Microsoft Entra Identity Protection. Esto incluye la creación de políticas para detectar riesgos de inicio de sesión y riesgos de usuarios, activando acciones como el bloqueo de acceso o la aplicación de MFA.



Resultados y Aprendizajes

Durante este proyecto, se implementaron medidas avanzadas de seguridad en Azure con los siguientes resultados:

- **MFA (Autenticación Multifactor):**

Se configuró MFA para asegurar el acceso de los usuarios, protegiendo las cuentas contra accesos no autorizados.

- **Políticas de Acceso Condicional:**

Se crearon políticas que exigen MFA o cumplen con otras condiciones como la ubicación o el dispositivo, restringiendo el acceso a los recursos según criterios específicos.

- **Microsoft Entra Identity Protection:**

Se utilizó para detectar riesgos de inicio de sesión y se aplicaron medidas automáticas, como la activación de MFA o el bloqueo de accesos, ante comportamientos sospechosos.

- **Monitoreo y Ajustes de Seguridad:**

A través de Azure Security Center, se monitorearon eventos de seguridad y se ajustaron las políticas en tiempo real para mejorar la protección de los recursos.

Aprendizajes clave:

- La **MFA** es esencial para proteger cuentas y recursos.
- Las **políticas de acceso condicional** mejoran el control de acceso, garantizando solo usuarios legítimos.
- **Microsoft Entra** ayuda a detectar y mitigar riesgos de acceso mediante medidas automáticas.
- El **monitoreo constante** y la capacidad de ajustar las políticas de seguridad en tiempo real son fundamentales para mantener un entorno seguro.

Ing. Jhon Alexis Gutierrez Guzman

Lima, Peru 2025.