

# **Módulo SC-900T00-A 2: Descripción de las funcionalidades de las soluciones de administración de identidades y acceso de Microsoft**



# Programa del módulo



Explorar los servicios y tipos de identidad de Azure Active Directory (Microsoft Entra)



Explorar las funcionalidades de autenticación de Azure Active Directory



Explorar las funcionalidades de administración de acceso de Azure Active Directory



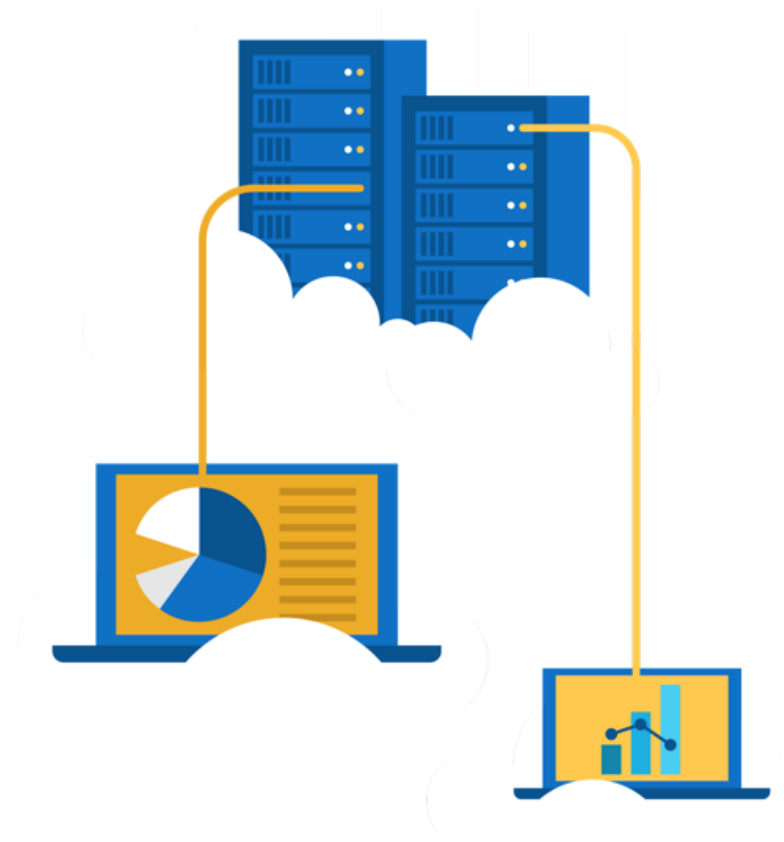
Describir las funcionalidades de gobernanza de la protección de identidades de Azure Active Directory

# Lecturas



# Lecturas

1. Diijase a SC-900: Microsoft Security, Compliance, and Identity Fundamentals
2. Realice la lectura de la ruta de aprendizaje: [Microsoft Security, Compliance, and Identity Fundamentals: descripción de los conceptos de seguridad, cumplimiento e identidad](#)



# Lección 1: Explorar los servicios y tipos de identidad en Azure Active Directory



# Lección 1: Introducción

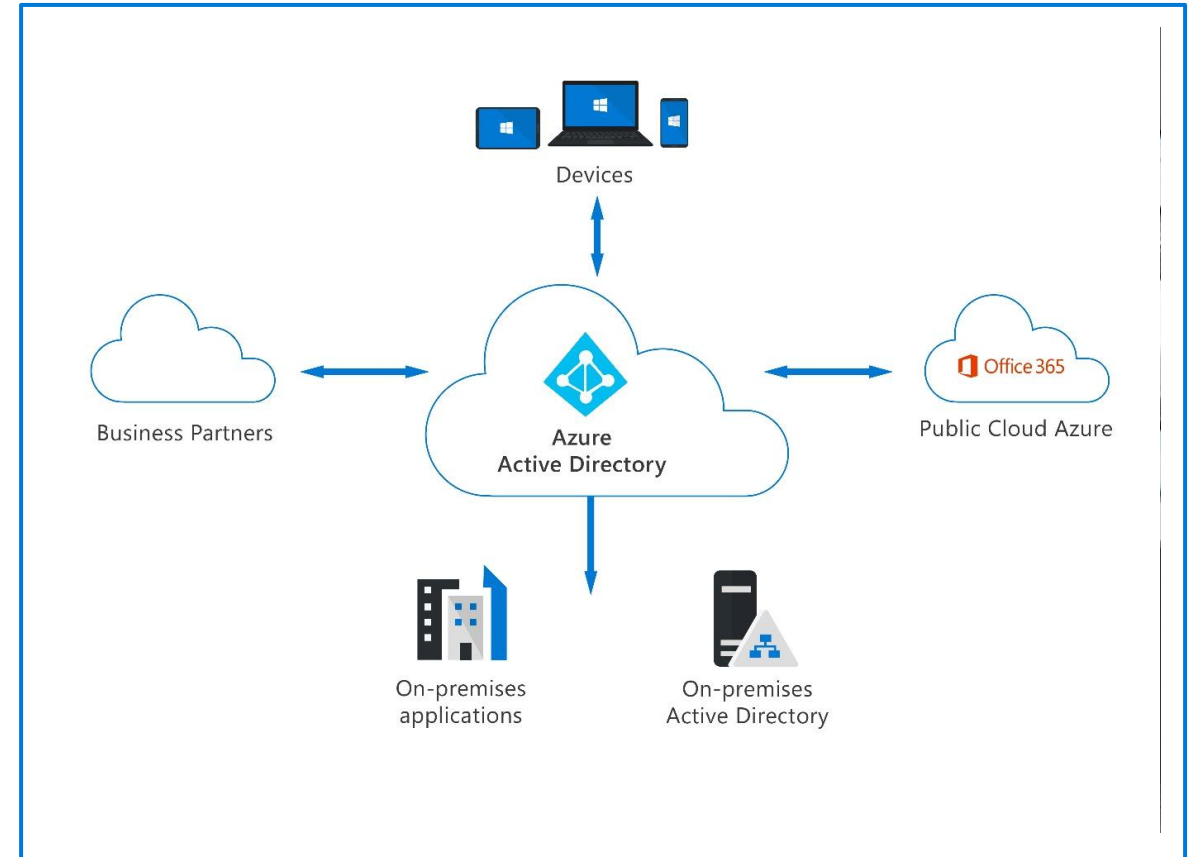
**Después de completar este módulo, podrá hacer lo siguiente:**

- Describir Microsoft Entra (Azure AD)
- Describir los tipos de identidad compatibles con Azure AD

# Azure Active Directory

Azure AD es un servicio de **administración de acceso y de identidades** basado en la nube de Microsoft. Entre las funcionalidades de Azure AD se incluyen las siguientes:

- Las organizaciones pueden permitir que sus empleados, invitados y otras personas inicien sesión y accedan a los recursos que necesitan.
- Dar un único sistema de identidad para sus aplicaciones en la nube y locales.
- Proteger las identidades y credenciales de los usuarios y cumplir con los requisitos de gobernanza de acceso de una organización.
- Cada suscripción de Microsoft 365, Office 365, Azure y Dynamics 365 Online utiliza automáticamente un inquilino de Azure AD.



# Tipos de identidades de Azure AD

Azure AD administra distintos tipos de identidades: usuarios, entidades de servicio, identidades administradas y dispositivos.



**Usuario:** de manera general, un usuario es una representación de la identidad de una persona que se administra mediante Azure AD. Los empleados e invitados se representan como usuarios en Azure AD.

---



**Dispositivo:** un componente de hardware, como dispositivo móvil, portátil, servidor o impresora. Las identidades de dispositivo se pueden configurar de diferentes maneras en Azure AD para determinar ciertas propiedades, como quién es el propietario del dispositivo.

---



**Entidad de servicio:** se puede considerar como una identidad para una aplicación. Una entidad de servicio se crea en todos los inquilinos en los que se usa la aplicación y define quién puede acceder a la aplicación, a qué recursos tiene acceso la aplicación y mucho más.

---



**Identidad administrada :** una identidad administrada proporciona una identidad que las aplicaciones pueden usar al conectarse a los recursos que admiten la autenticación de Azure AD. No es necesario que los desarrolladores administren las credenciales.



# Demostración

## Azure Active Directory user settings



# Identidades externas en Azure AD

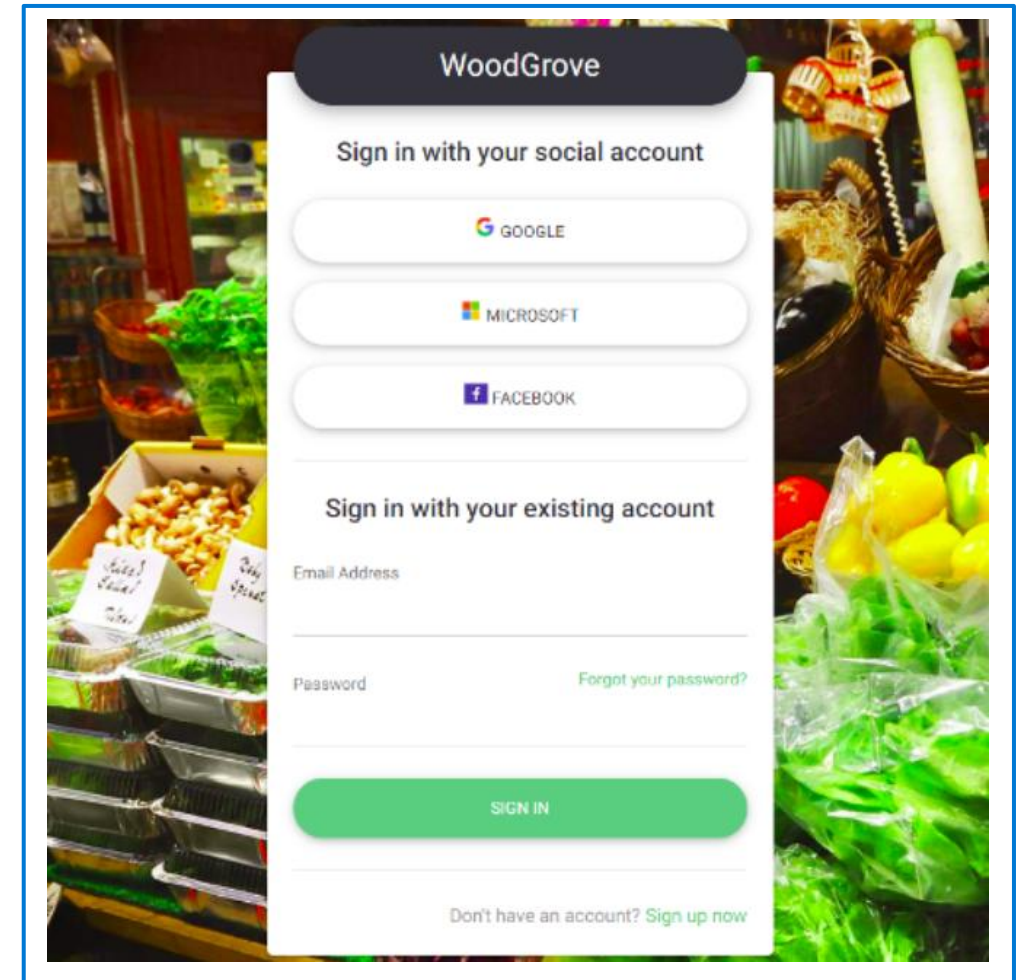
Existen dos identidades externas en Azure AD

## Colaboración B2B

La colaboración B2B le permite compartir sus aplicaciones y recursos con usuarios externos

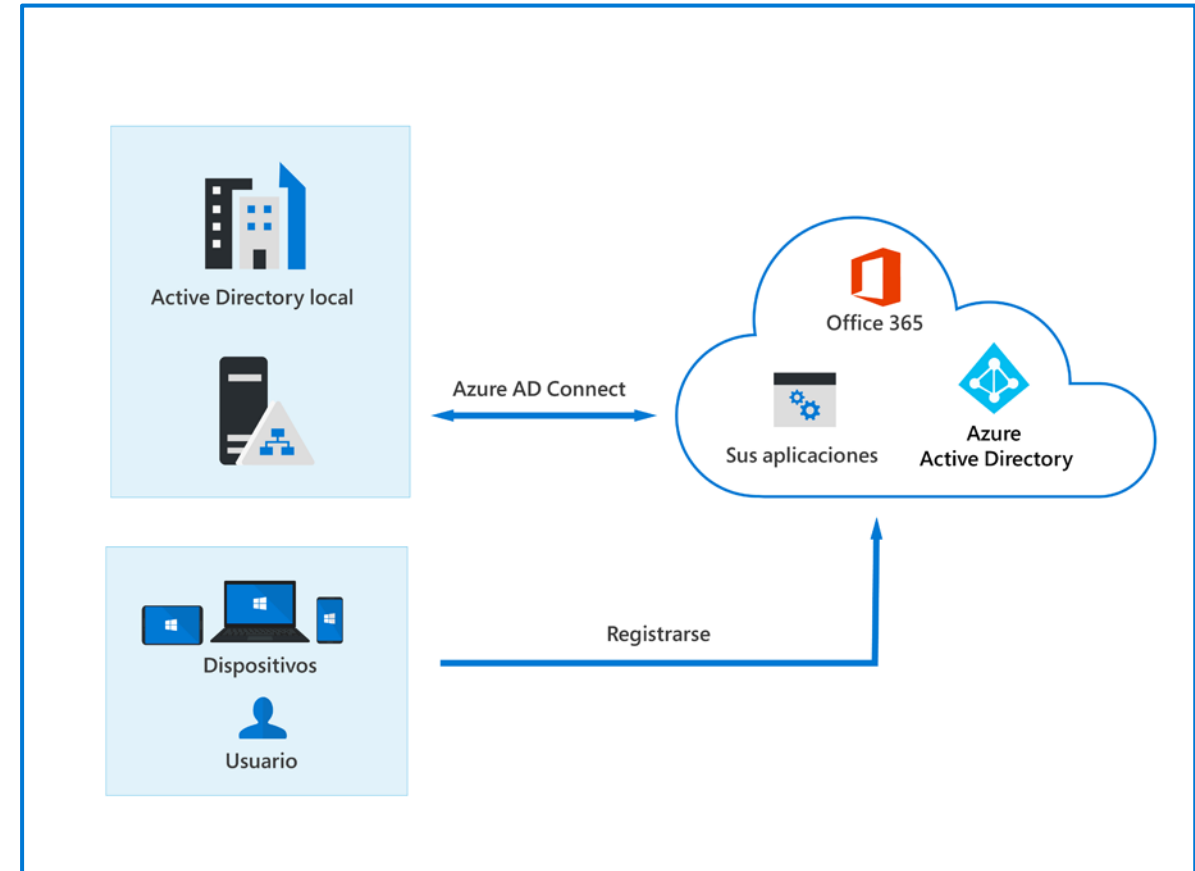
## Administración de acceso de B2C

B2C es una solución de administración de identidades para aplicaciones orientadas al consumidor y al cliente

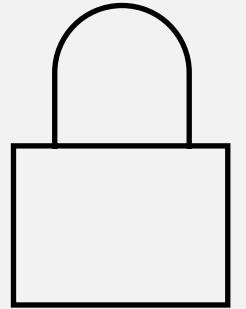


# El concepto de identidades híbridas

- Una **identidad híbrida** es una identidad de usuario común para la autenticación y la autorización en todos los recursos, independientemente de la ubicación (local y en la nube).
- Con **Azure AD Connect**, las actualizaciones de AD DS local se sincronizan con Azure AD
- Métodos de autenticación de identidad híbrida:
  - Sincronización de hash de contraseñas
  - Autenticación transferida
  - Autenticación federada



# Lección 2: Explorar las funcionalidades de autenticación de Azure Active Directory



# Lección 2: Introducción

**Después de completar este módulo, podrá hacer lo siguiente:**

- Describir los métodos de autenticación de Azure AD
- Descripción de la autenticación multifactor en Azure AD
- Describir las funcionalidades de administración y protección de contraseñas de Azure AD.

# Métodos de autenticación de Azure AD

Contraseñas (autenticación principal)

Autenticación basada en teléfono









- SMS (autenticación principal y secundaria)
- Voz (autenticación secundaria)

Estándar OATH para la forma en que se generan los códigos en contraseñas de un solo uso (autenticación secundaria)

- Tokens SW
- Tokens HW

Sin contraseña (autenticación principal y secundaria)

- Biometría (Windows Hello)
- Microsoft Authenticator
- FIDO2

Bien: Contraseña	Mal: Contraseña y...	Mejor: Contraseña y...	Lo mejor: Inicio de sesión sin contraseña
123456 qwerty password iloveyou Password1	 sms  Voz	 Microsoft Authenticator  Tokens de software OTP  Tokens de hardware OTP	 Microsoft Hello  Microsoft Authenticator  Clave de seguridad FIDO2

# Autenticación multifactor (MFA) en Azure AD

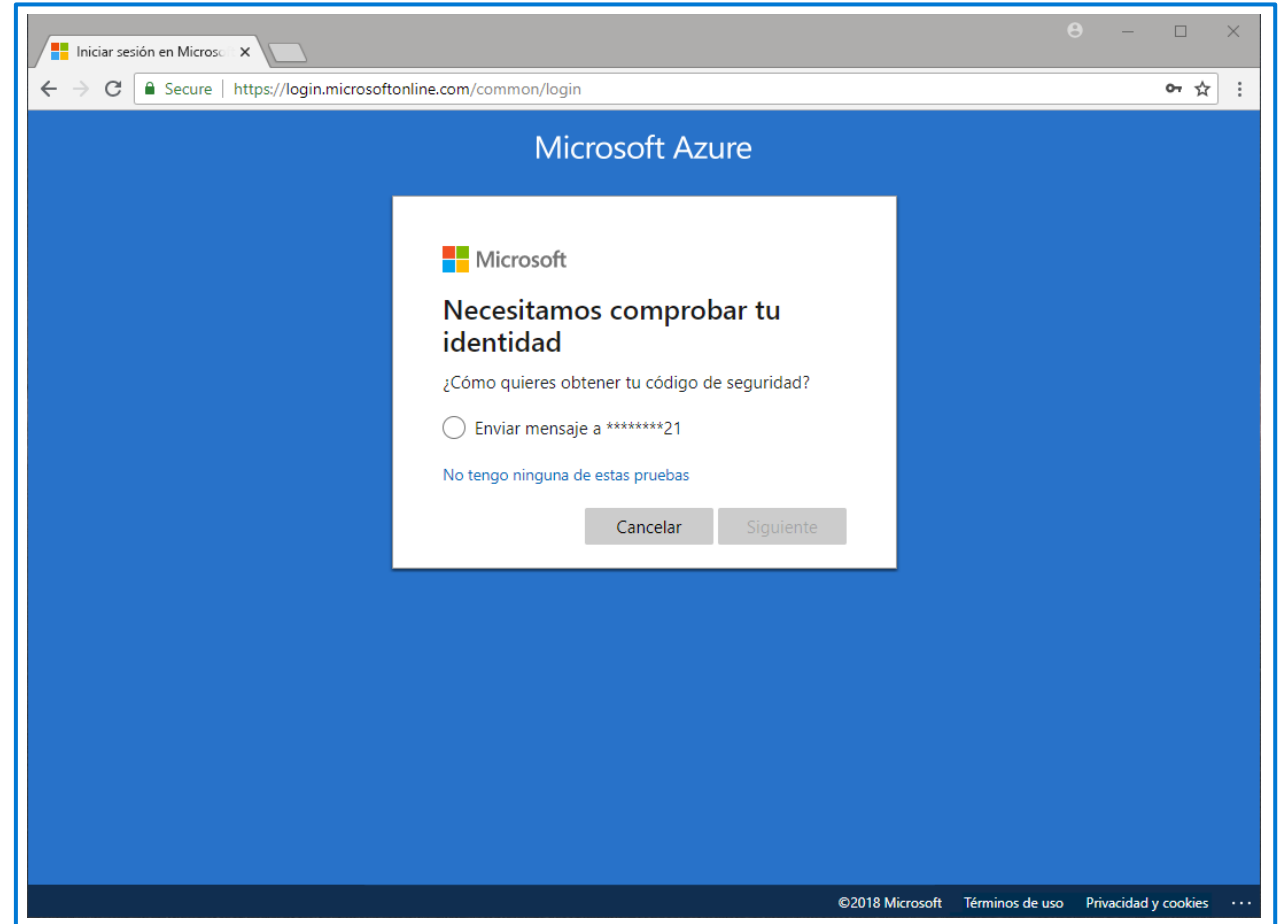
## Autenticación multifactor (MFA) y valores de seguridad predeterminados

### La MFA requiere más de una forma de comprobación:

- Algo que sabe
- Algo que se tiene
- Algo que es

### Valores de seguridad predeterminados:

- Un conjunto de mecanismos básicos de seguridad de la identidad recomendados por Microsoft.
- Una gran opción para las organizaciones que quieren aumentar su posición de seguridad pero no saben por dónde empezar, o para las organizaciones que utilizan las licencias gratuitas de Azure AD.



# Autoservicio de restablecimiento de contraseña (SSPR) en Azure AD

## Beneficios del autoservicio de restablecimiento de contraseña:

- Los administradores pueden cambiar la configuración para adaptarse a los nuevos requisitos de seguridad.
- Ahorra dinero a la organización, ya que reduce el número de llamadas y solicitudes al personal del departamento de soporte técnico.
- Aumenta la productividad, pues permite que el usuario vuelva a trabajar más rápido.

## El autoservicio de restablecimiento de contraseña funciona en los siguientes escenarios:

- Cambio de contraseña
- Restablecimiento de contraseña
- Desbloqueo de cuenta

## Método de autenticación del SSPR:

- Notificación en aplicación móvil
- Código de aplicación móvil
- email
- Teléfono móvil
- Teléfono del trabajo
- Preguntas de seguridad



# Funcionalidades de protección y administración de contraseñas en Azure AD



Lista global de contraseñas prohibidas

---



Listas personalizadas de contraseñas prohibidas

---



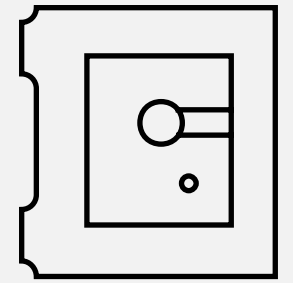
Protección contra la difusión de contraseñas

---



Seguridad híbrida

# Lección 3: Explorar las funcionalidades de administración de acceso de Azure Active Directory



# Lección 3: Introducción

**Después de completar esta unidad, podrá:**

- Describir el acceso condicional y sus ventajas.
- Describir los roles de Azure AD y el control de acceso basado en roles (RBAC)

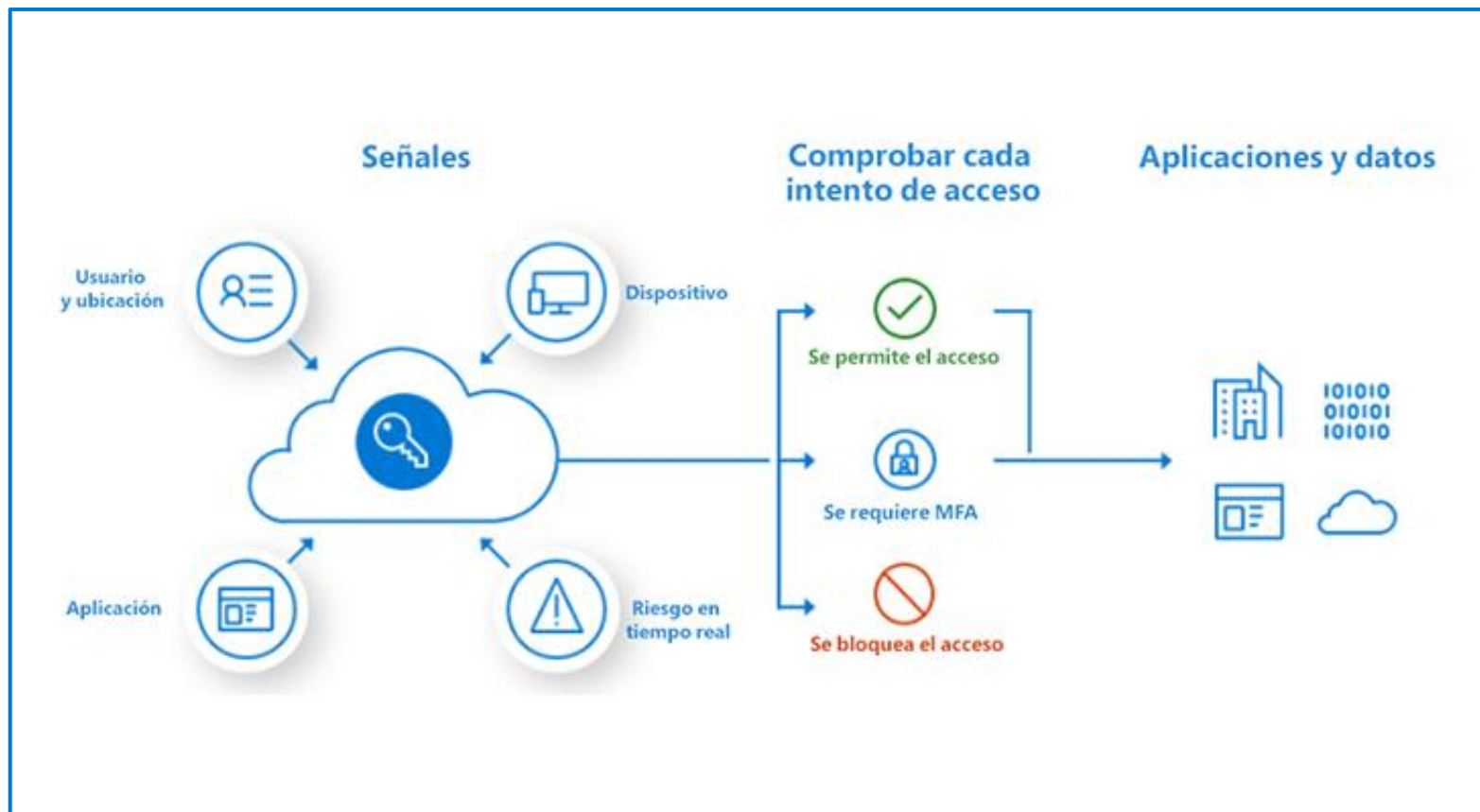
# Acceso condicional

## Señales de acceso condicional:

- Pertenencia a un usuario o grupo
- Información de la ubicación con nombre
- Dispositivo
- Application
- Detección de riesgos de inicio de sesión en tiempo real
- Aplicaciones o acciones en la nube
- Riesgo de usuario

## Controles de acceso:

- Bloquear acceso
- Conceder acceso
- Requerir el cumplimiento de una o varias condiciones antes de conceder el acceso
- Controlar el acceso de los usuarios en función de los controles de sesión para permitir experiencias limitadas dentro de aplicaciones específicas en la nube



# Roles de Azure AD y control de acceso basado en roles (RBAC)

Los roles de Azure AD controlan los permisos para administrar los recursos de Azure AD.



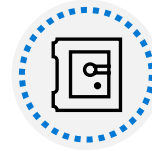
Roles integrados

---



Roles personalizados

---



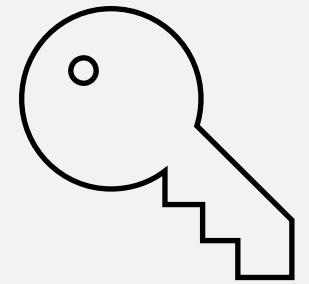
Categorías de roles de Azure AD: Específicos de Azure AD, específicos de un servicio, entre servicios

---



Solo se debe conceder el acceso que los usuarios necesitan

# Lección 4: Describir las funcionalidades de protección y gobernanza de identidades de Azure Active Directory



# Lección 4: Introducción

**Después de completar este módulo, podrá hacer lo siguiente:**

- Describir las funcionalidades de gobernanza de identidades de Azure AD.
- Describir las ventajas de Privileged Identity Management (PIM).
- Describir las funcionalidades de Azure AD Identity Protection.

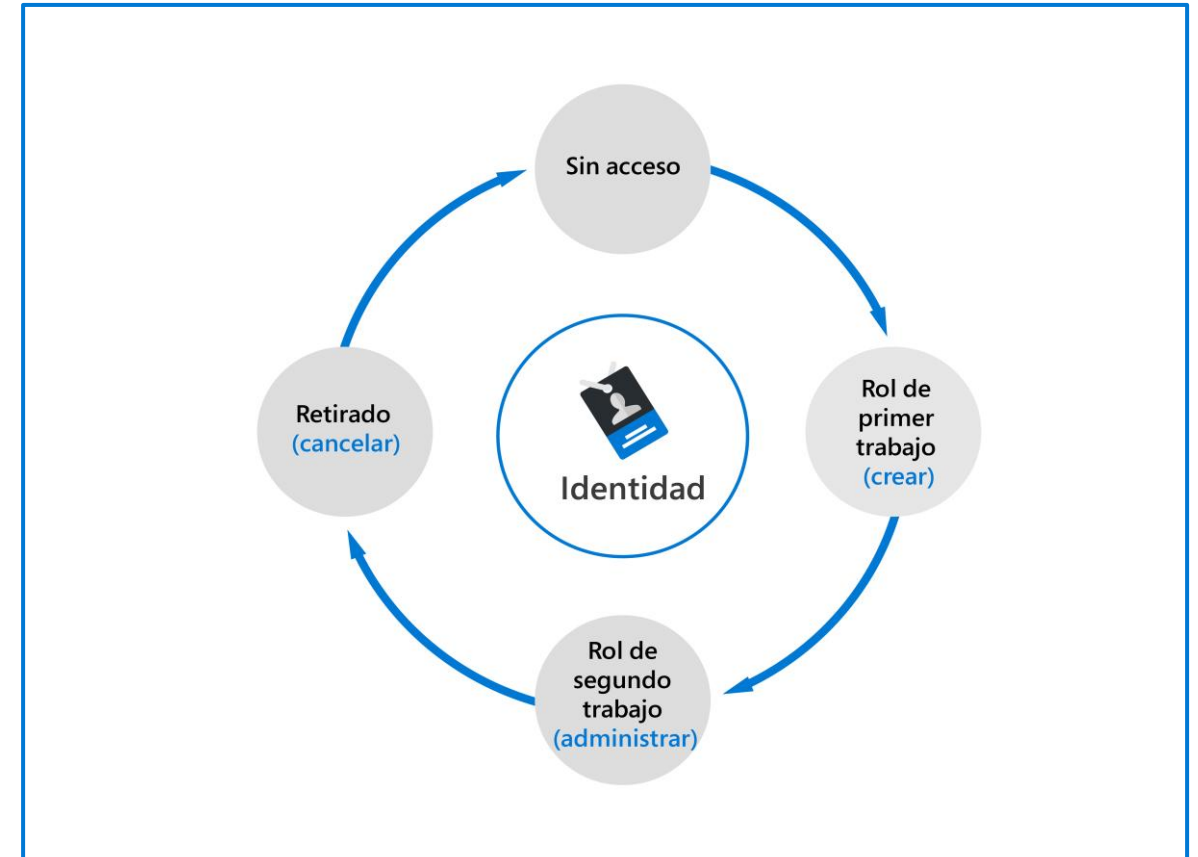
# Gobernanza de identidades en Azure AD

## Las tareas de Azure AD Identity Governance

- Administrar el ciclo de vida de las identidades.
- Administrar el ciclo de vida de los accesos.
- Proteger el acceso con privilegios para la administración.

## Ciclo de vida de las identidades

- Unirse: se crea una nueva identidad digital.
- Trasladar: actualizar autorizaciones de acceso.
- Abandonar: puede que haya que eliminar el acceso.





# Administración de derechos y revisiones de acceso

## Administración de derechos

- Se trata de una característica de gobernanza de identidades que permite a las organizaciones administrar el ciclo de vida de identidad y acceso a escala.
- Automatiza los flujos de trabajo de las solicitudes de acceso, las asignaciones de acceso, las revisiones y la expiración.

## Revisiones de acceso

- Permite a las organizaciones administrar de forma eficiente las pertenencias a grupos, el acceso a las aplicaciones empresariales y las asignaciones de roles.
- Garantiza que solo las personas adecuadas tengan acceso a los recursos.
- Se utiliza para revisar y administrar el acceso tanto de los usuarios como de los invitados.

## Términos de uso

- Permiten que se presente información a los usuarios, antes de que accedan a los datos o a una aplicación.
- Garantizan que los usuarios lean las declinaciones de responsabilidades pertinentes o los requisitos legales o de cumplimiento.

*Contoso*

### Revise el acceso de los usuarios a la aplicación Finance Web en FrickelsoftNET

Sarah Hoelzel, su organización ha pedido que apruebe o rechace el acceso continuado para uno o más usuarios a la aplicación **Finance Web** en la revisión de acceso de **FinanceWeb**. El período de revisión finalizará el **5 de septiembre de 2020**.

Hola, equipo de FinanceWeb: revisen la lista de usuarios que tienen acceso a su aplicación FinanceWeb. Necesitamos su ayuda para eliminar los accesos indeseados de usuarios que ya no trabajan con la aplicación. Más información:

<https://finweb.contoso.com/access/reviews>

**Iniciar revisión >**

Obtenga información sobre cómo [ejecutar una revisión de acceso](#) mediante las revisiones de acceso de Azure Active Directory.

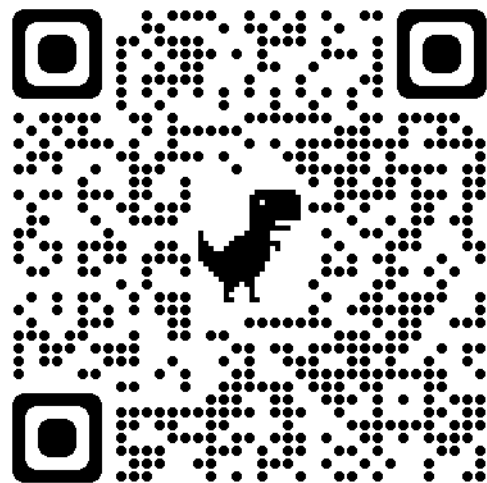
[Declaración de privacidad](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitado por



# ¿Para qué es útil Azure Active Directory (Administration de Derechos y revisions de acceso)?



# Privileged Identity Management (PIM)

PIM le permite administrar, controlar y supervisar el acceso a recursos importantes de la organización.



Just-in-Time, ya que proporciona acceso con privilegios solo cuando sea necesario, no antes.

---



Sujeto a plazos mediante la asignación de fechas iniciales y finales que indican cuándo un usuario puede acceder a los recursos.

---



Basado en la aprobación, ya que requiere de una aprobación específica para activar los privilegios.

---



Visible, ya que envía notificaciones cuando se activan los roles con privilegios.

---



Se puede auditar, ya que permite descargar un historial de acceso completo.

# Azure Active Directory Identity Protection

Permite a las organizaciones realizar tres tareas clave:

- Automatizar la detección y corrección de riesgos basados en la identidad.
- Investigar los riesgos de usar los datos en el portal.
- Exportar los datos de detección de riesgos a utilidades de terceros para su posterior análisis.

Puede clasificar y calcular el riesgo:

- Clasificar el riesgo en tres niveles: bajo, medio y alto.
- Calcular el riesgo de inicio de sesión y el riesgo de identidad del usuario.

Da a las organizaciones tres informes:

- Usuarios de riesgo
- Inicios de sesión no seguros
- Detecciones de riesgo

# Resumen del módulo

En este módulo, ha aprendido a:

- Ha aprendido sobre Azure AD y los servicios y tipos de identidad compatibles con Azure AD
- Ha explorado las funcionalidades de autenticación de Azure AD y MFA
- Ha explorado las funcionalidades de administración de acceso de Azure AD con acceso condicional y RBAC de Azure AD
- Ha descrito las funcionalidades de protección y gobernanza de identidades de Azure AD, incluido PIM, la administración de derechos y revisiones de acceso.
- Ha aprendido las funcionalidades de Azure AD Identity Protection.

