**Introducción**

La transición de las cargas de trabajo a la nube conlleva algo más que mover servidores, sitios web y datos. Las empresas deben pensar en cómo proteger sus recursos e identificar los usuarios autorizados.

En este módulo, su empresa planea Microsoft Entra ID y características como la unión a Microsoft Entra y el autoservicio de restablecimiento de contraseña. Debe comprender cómo elegir la edición de Microsoft Entra que funcione mejor para su organización y explorar cómo implementar las características necesarias.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Definir los conceptos de Microsoft Entra, incluidas las identidades, las cuentas y los inquilinos.
* Describir las características de Microsoft Entra para admitir diferentes configuraciones.
* Comprender las diferencias entre Microsoft Entra ID y Active Directory Domain Services (AD DS).
* Elegir entre las ediciones admitidas de Microsoft Entra ID.
* Implementar la característica de unión a Microsoft Entra.
* Usar la característica de autoservicio de restablecimiento de contraseña de Microsoft Entra.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/certifications/exams/az-104). Los conceptos del módulo tratan los siguientes aspectos:

Administración de identidades y gobernanza en Azure (15-20 %)

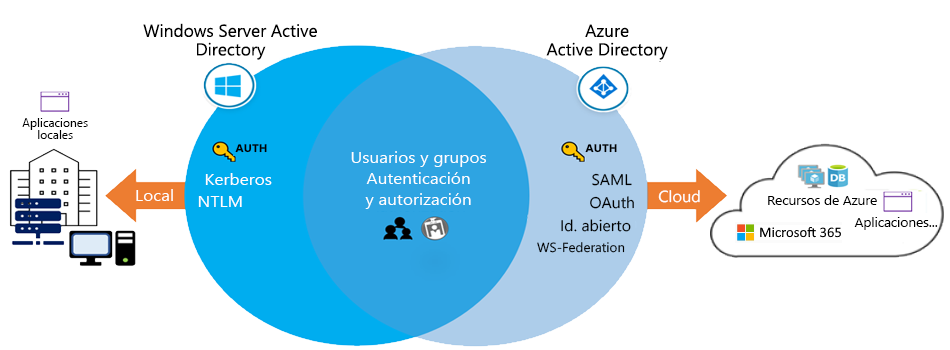
* Administrar objetos de Microsoft Entra
  + Configurar el autoservicio de restablecimiento de contraseña
  + Configurar la unión a Microsoft Entra

**Descripción de las ventajas y características de Microsoft Entra ID**

[Microsoft Entra ID](https://learn.microsoft.com/es-es/azure/active-directory/) es el servicio de directorio multiinquilino basado en la nube y de administración de identidades de Microsoft. Microsoft Entra ID ayuda con el acceso de los usuarios a recursos y aplicaciones, por ejemplo:

* Recursos y aplicaciones internos ubicados en la red corporativa.
* Recursos externos como Microsoft 365, Azure Portal y aplicaciones SaaS.
* Aplicaciones en la nube desarrolladas para la organización.

En el diagrama siguiente se muestra un ejemplo de implementación de Microsoft Entra ID. En este escenario, Windows Server AD usa la [autenticación Kerberos](https://learn.microsoft.com/es-es/windows-server/security/kerberos/kerberos-authentication-overview) y [NTLM](https://learn.microsoft.com/es-es/windows-server/security/kerberos/ntlm-overview) en las aplicaciones locales.



**Aspectos que se deben conocer sobre las características de Microsoft Entra**

Vamos a examinar algunas de las características destacadas de Microsoft Entra ID.

| **Característica de Azure AD** | **Descripción** |
| --- | --- |
| **Acceso mediante inicio de sesión único (SSO)** | Microsoft Entra ID proporciona inicio de sesión único (SSO) seguro en aplicaciones web en la nube y en aplicaciones locales. Los usuarios pueden iniciar sesión con el mismo conjunto de credenciales para acceder a todas sus aplicaciones. |
| **Compatibilidad con dispositivos omnipresente** | Microsoft Entra ID funciona con dispositivos iOS, macOS, Android y Windows, y ofrece una experiencia común en todos los dispositivos. Los usuarios pueden iniciar aplicaciones desde un panel de acceso personalizado basado en web, una aplicación móvil, Microsoft 365 o portales de empresa personalizados con sus credenciales de trabajo existentes. |
| **Acceso remoto seguro** | Microsoft Entra ID permite el acceso remoto seguro a aplicaciones web locales. El acceso seguro puede incluir la autenticación multifactor (MFA), las directivas de acceso condicional y la administración de acceso basada en grupos. Los usuarios pueden acceder a aplicaciones web locales desde cualquier lugar, incluido desde el mismo portal. |
| **Extensibilidad a la nube** | Microsoft Entra ID puede extenderse a la nube para ayudarle a administrar un conjunto coherente de usuarios, grupos, contraseñas y dispositivos en todos los entornos. |
| **Protección de datos confidenciales** | Microsoft Entra ID ofrece funcionalidades únicas de protección de identidades para proteger los datos confidenciales y las aplicaciones. Los administradores pueden supervisar si hay actividad de inicio de sesión sospechosa y posibles vulnerabilidades en una vista consolidada de usuarios y recursos en el directorio. |
| **Soporte mediante autoservicio** | Microsoft Entra ID le permite delegar tareas en empleados de la empresa que, de otro modo, podrían realizar administradores con mayores privilegios de acceso. Proporcionar acceso a aplicaciones de autoservicio y administración de contraseñas mediante pasos de comprobación puede reducir las llamadas al departamento de soporte técnico y mejorar la seguridad. |

**Aspectos que se deben tener en cuenta al usar características de Microsoft Entra**

Microsoft Entra ID ofrece muchas características y ventajas. Tenga en cuenta qué características se pueden usar para admitir mejor los escenarios corporativos.

* **Considere la posibilidad de habilitar el acceso con inicio de sesión único**. Habilite el acceso SSO para que los usuarios se conecten a la nube o usen las aplicaciones locales. El inicio de sesión único de Microsoft Entra es compatible con Microsoft 365 y miles de aplicaciones SaaS, como Salesforce, Workday, DocuSign, ServiceNow y Box.
* **Tenga en cuenta la experiencia de usuario y la compatibilidad con dispositivos**. Cree una experiencia de usuario coherente que funcione para todos los dispositivos y puntos de acceso de directorio. Puede diseñar portales de empresa personalizados y acceso personalizado basado en web para los empleados que les permita conectarse con sus credenciales de trabajo existentes.
* **Tenga en cuenta las ventajas del acceso remoto seguro**. Proteja las aplicaciones web locales mediante la implementación del acceso remoto seguro con MFA y directivas de acceso.
* **Tenga en cuenta las ventajas de la extensibilidad a la nube**. Conecte Active Directory y otros directorios locales de la nube a Microsoft Entra en unos pocos pasos. Puede facilitar a los administradores la administración de los mismos usuarios, grupos, contraseñas y dispositivos en todos los entornos admitidos.
* **Considere la posibilidad de usar la protección avanzada para los datos confidenciales**. Mejore la seguridad de los datos confidenciales y de las aplicaciones mediante las características de protección integradas de Microsoft Entra ID. Los administradores pueden utilizar los informes de seguridad avanzados, las notificaciones, las recomendaciones de corrección y las directivas basadas en riesgos.
* **Tenga en cuenta las opciones de autoservicio de costo reducido**. Aproveche las ventajas de las características de autoservicio de Microsoft Entra para ayudar a reducir los costos de su organización. Delegue determinadas tareas, como el restablecimiento de contraseñas o la creación y administración de grupos, a los usuarios que no son administradores.

En la siguiente unidad, exploraremos los conceptos de Microsoft Entra que hacen posible estas características.

**Descripción de los conceptos de Microsoft Entra**

Para implementar Microsoft Entra ID en la configuración corporativa, debe comprender los componentes clave del servicio. En la tabla siguiente se describen los principales componentes y conceptos de Microsoft Entra ID y se explica cómo funcionan conjuntamente para admitir las características de servicio.

| **Concepto de Azure AD** | **Descripción** |
| --- | --- |
| **Identidad** | Una *identidad* es un objeto que se puede autenticar. La identidad puede ser un usuario con un nombre de usuario y una contraseña. Las identidades también pueden ser aplicaciones u otros servidores que requieren autenticación mediante certificados o claves secretas. Microsoft Entra ID es el producto subyacente que proporciona el servicio de identidad. |
| **Cuenta** | Una *cuenta* es una identidad que tiene datos asociados. Para tener una cuenta, primero debe tener una identidad válida. No puede tener una cuenta sin una identidad. |
| **Cuenta de Microsoft Entra** | Una *cuenta de Azure AD* es una identidad que se crea mediante Microsoft Entra ID u otro servicio en la nube de Microsoft, como Microsoft 365. Las identidades se almacenan en Microsoft Entra ID y pueden acceder a ellas las suscripciones de servicio en la nube de su organización. La cuenta de Microsoft Entra también se denomina *cuenta profesional o educativa*. |
| **Inquilino (directorio) de Azure** | Un *inquilino* de Azure es una instancia única, dedicada y de confianza de Microsoft Entra ID. Cada inquilino (también denominado *directorio*) representa una sola organización. Cuando su organización se registra a una suscripción de servicio en la nube de Microsoft, automáticamente se crea un nuevo inquilino. Dado que cada inquilino es una instancia dedicada y de confianza de Microsoft Entra ID, puede crear varios inquilinos o instancias. |
| **Suscripción de Azure** | Una suscripción de Azure se usa para pagar los servicios en la nube de Azure. Cada suscripción se une a un único inquilino. Puede tener varias suscripciones. |

**Sugerencia**

Si es cliente de Microsoft 365, Azure o Dynamics CRM Online, es posible que ya esté usando Microsoft Entra ID. Cada inquilino de Microsoft 365, Azure y Dynamics CRM ya es un inquilino de Microsoft Entra. Puede empezar a usar el inquilino para administrar el acceso a miles de otras aplicaciones en la nube que se integran con Microsoft Entra ID.

**Comparación de Active Directory Domain Services y Microsoft Entra ID**

Active Directory Domain Services (AD DS) es la implementación tradicional de Active Directory basado en Windows Server en un servidor físico o virtual. Active Directory Domain Services (AD DS) también incluye Servicios de certificados de Active Directory (AD CS), Active Directory Lightweight Directory Services (AD LDS), Servicios de federación de Active Directory (AD FS) y Active Directory Rights Management Services (AD RMS).

**Importante**

Si bien puede implementar y administrar AD DS en Azure Virtual Machines, se recomienda usar Microsoft Entra ID, a menos que su configuración tenga como destino cargas de trabajo de IaaS que dependan específicamente de AD DS.

**Aspectos que se deben tener en cuenta al usar Microsoft Entra en lugar de AD DS**

Microsoft Entra ID es similar a AD DS, pero hay diferencias importantes. Es importante comprender que el uso de Microsoft Entra ID para la configuración es diferente de implementar un controlador de dominio de Active Directory en una máquina virtual de Azure y, a continuación, agregarlo al dominio local.

A medida que planee la estrategia de identidad, tenga en cuenta las siguientes características que distinguen Microsoft Entra ID de AD DS.

* **Solución de identidad**: AD DS es principalmente un servicio de directorio, mientras que Microsoft Entra ID es una solución de identidad completa. Microsoft Entra ID está diseñado para aplicaciones basadas en Internet que usan comunicaciones HTTP y HTTPS. Las características y capacidades de Microsoft Entra ID admiten la administración segura de identidades de destino.
* **Protocolos de comunicación**: Dado que Microsoft Entra ID se basa en HTTP y HTTPS, no usa la autenticación Kerberos. Microsoft Entra ID implementa los protocolos HTTP y HTTPS, como SAML, WS-Federation y OpenID Connect para la autenticación, así como OAuth para la autorización.
* **Servicios de federación**: Microsoft Entra ID incluye servicios de federación y muchos servicios de terceros como Facebook.
* **Estructura plana**: Los usuarios y grupos de Microsoft Entra se crean en una estructura plana. No hay unidades organizativas (UO) ni objetos de directiva de grupo (GPO).
* **Servicio administrado**: Microsoft Entra ID es un servicio administrado. Solo se administran los usuarios, los grupos y las directivas. Si implementa AD DS con máquinas virtuales mediante Azure, administra muchas otras tareas, como la implementación, la configuración, las máquinas virtuales, la aplicación de revisiones y otros procesos de back-end.

**Selección de las ediciones de Microsoft Entra**

Microsoft Entra ID incluye cuatro ediciones: **Gratis**, **Aplicaciones de Microsoft 365**, **Premium P1**y **Premium P2**. La edición Free se incluye con una suscripción de Azure. Las ediciones Premium están disponibles mediante un Contrato Enterprise de Microsoft, el programa Licencia por volumen abierto y el programa Proveedores de soluciones en la nube. Los suscriptores de Azure y Microsoft 365 también pueden comprar Microsoft Entra ID P1 y P2 en línea.

**Aspectos que se deben conocer sobre las ediciones de Microsoft Entra**

Tenga en cuenta las siguientes características que distinguen las distintas ediciones de Microsoft Entra ID. Después de revisar las características y descripciones, piense en qué edición funciona mejor para su organización. Un X indica que se admite la característica.

| **Característica** | **Gratuito** | **Aplicaciones de Microsoft 365** | **Premium P1** | **Premium P2** |
| --- | --- | --- | --- | --- |
| **Objetos de directorio** | 500.000 | Sin límite | Sin límite | Sin límite |
| **Single Sign-on** (Inicio de sesión único) | Sin límite | Sin límite | Sin límite | Sin límite |
| **Administración de identidades y acceso principales** | X | X | X | X |
| **Colaboración de negocio a negocio** | X | X | X | X |
| **Administración de identidades y acceso para Aplicaciones de Microsoft 365** |  | X | X | X |
| **Características de la edición Premium** |  |  | X | X |
| **Identidades híbridas** |  |  | X | X |
| **Administración avanzada de acceso a grupos** |  |  | X | X |
| **Acceso condicional** |  |  | X | X |
| **Identity Protection** |  |  |  | X |
| **Identity Governance** |  |  |  | X |

**Microsoft Entra ID Free**

La edición Gratis proporciona administración de usuarios y grupos, sincronización de directorios locales e informes básicos. El acceso con inicio de sesión único se admite en Azure, Microsoft 365 y muchas aplicaciones SaaS populares.

**Microsoft Entra Aplicaciones de Microsoft 365**

Esta edición se incluye con Microsoft 365. Además de las características de la edición Gratis, esta edición proporciona administración de identidades y acceso para aplicaciones de Microsoft 365. La compatibilidad adicional incluye personalización de marca, MFA, administración de acceso a grupos y autoservicio de restablecimiento de contraseña para los usuarios en la nube.

**Microsoft Entra ID P1**

Además de las características de la edición Gratis, la edición Premium P1 permite a los usuarios de entornos híbridos acceder a recursos locales y en la nube. Esta edición admite la administración avanzada, como los grupos dinámicos, la administración de grupos de autoservicio y capacidades de escritura diferida en la nube. La edición P1 también incluye Microsoft Identity Manager, un conjunto de administración de identidades y acceso local. Las características adicionales de la edición P1 permiten el autoservicio de restablecimiento de contraseña para los usuarios locales.

**Microsoft Entra ID P2**

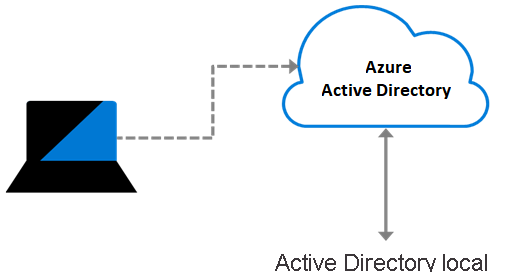
Además de incluir las características de las ediciones Gratis y P1, la edición Premium P2 ofrece Microsoft Entra ID Protection para facilitar el acceso condicional basado en riesgos a las aplicaciones y a los datos críticos de la empresa. Privileged Identity Management se incluye para descubrir, restringir y supervisar a los administradores y su acceso a los recursos, y proporcionar acceso Just-in-Time cuando sea necesario.

**Sugerencia**

La [**página de precios de Microsoft Entra**](https://azure.microsoft.com/pricing/details/active-directory) contiene información detallada sobre lo que se incluye en cada edición.

**Implementación de la unión a Microsoft Entra**

Microsoft Entra ID habilita el inicio de sesión único (SSO) en dispositivos, aplicaciones y servicios desde cualquier ubicación. Para admitir el SSO, los administradores de TI deben asegurarse de que los recursos corporativos están protegidos y de que los dispositivos cumplen los estándares de seguridad y cumplimiento.



La característica de unión a Microsoft Entra funciona con SSO para proporcionar acceso a aplicaciones y recursos de la organización, así como simplificar las implementaciones de dispositivos de trabajo Windows.

**Aspectos que se deben saber sobre la característica de unión a Microsoft Entra**

Veamos algunas de las ventajas de usar dispositivos unidos:

| **Prestación** | **Descripción** |
| --- | --- |
| **Inicio de sesión único (SSO)** | Los dispositivos unidos ofrecen acceso SSO a sus servicios y aplicaciones SaaS administrados por Azure. Los usuarios no tendrán solicitudes de autenticación adicionales cuando accedan a los recursos de trabajo. La función SSO está disponible incluso cuando no están conectados a la red de dominios. |
| **Enterprise State Roaming** | A partir de Windows 10, los usuarios pueden sincronizar de forma segura su configuración de usuario y los datos de configuración de la aplicación con dispositivos unidos. La itinerancia de estado empresarial reduce el tiempo para configurar un nuevo dispositivo. |
| **Windows Hello** | Proporcione a los usuarios un acceso seguro y cómodo a los recursos de trabajo desde dispositivos unidos. |
| **Restricción de acceso** | Restrinja el acceso de los usuarios a las aplicaciones para que solo se produzca desde dispositivos unidos que cumplan las directivas de cumplimiento. |
| **Acceso sin problemas a los recursos locales** | Los dispositivos unidos tienen acceso ininterrumpido a los recursos locales cuando el dispositivo tiene línea de visión al controlador de dominio local. |

**Aspectos que se deben tener en cuenta al usar dispositivos unidos**

Su organización está interesada en usar dispositivos unidos en su estrategia de administración. A medida que planee cómo implementar la característica, revise estos puntos de configuración:

* **Tenga en cuenta las opciones de conexión**. Conecte el dispositivo a Microsoft Entra ID de una de estas dos maneras:
  + **Registre** el dispositivo en Microsoft Entra ID para que pueda administrar la identidad del dispositivo. El registro de dispositivos de Microsoft Entra proporciona una identidad al dispositivo que se utiliza para autenticarlo cuando el usuario inicia sesión en Microsoft Entra. Puede utilizar esta identidad para habilitar o deshabilitar el dispositivo.
  + **Únase** al dispositivo, que es una extensión del registro de un dispositivo. La unión ofrece las ventajas del registro, y también cambia el estado local del dispositivo. El cambio del estado local permite a los usuarios iniciar sesión en un dispositivo mediante una cuenta profesional o educativa en lugar de con una cuenta personal.
* **Considere la posibilidad de combinar el registro con otras soluciones**. Combine el registro con una solución de administración de dispositivos móviles (MDM), como Microsoft Intune para proporcionar otros atributos de dispositivo en Microsoft Entra ID. Puede crear reglas de acceso condicional que obliguen a que el acceso desde dispositivos cumpla con los estándares de seguridad y cumplimiento de la organización.
* **Tenga en cuenta otros escenarios de implementación**. Aunque la unión a AD está pensada para organizaciones que tengan una infraestructura de Windows Server Active Directory local, se puede usar en otros escenarios, como sucursales.

**Implementar el autoservicio de restablecimiento de contraseña de Microsoft Entra**

Muchas de las llamadas al departamento de soporte técnico son solicitudes a fin de restablecer contraseñas para los usuarios. La característica de **autoservicio de restablecimiento de contraseña** (SSPR) de Microsoft Entra le permite dar a los usuarios la posibilidad de omitir el departamento de soporte técnico y restablecer sus propias contraseñas.

**Aspectos que se deben conocer sobre la característica SSPR de Microsoft Entra**

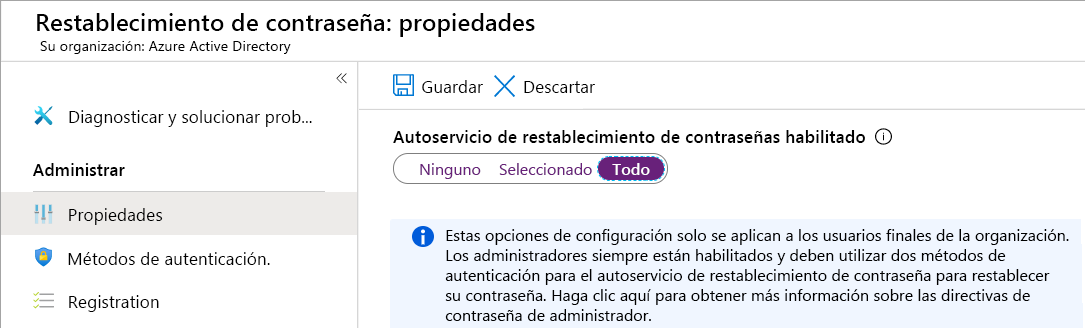
Examine las siguientes características y requisitos de la característica SSPR:

* SSPR requiere una cuenta de Microsoft Entra con privilegios de administrador global para administrar las opciones de SSPR. Esta cuenta siempre puede restablecer sus propias contraseñas, independientemente de las opciones configuradas.
* SSPR usa un grupo de seguridad para limitar los usuarios que tienen privilegios de SSPR.
* Todas las cuentas de usuario de la organización deben tener una licencia válida para usar SSPR.

**Aspectos que se deben tener en cuenta al usar SSPR**

Su organización quiere implementar la compatibilidad con SSPR en su solución de administración. A medida que planee la configuración, revise los siguientes puntos:

* **Piense en quién puede restablecer sus contraseñas**. Decida qué usuarios de la organización deben tener la posibilidad de usar la característica. En Azure Portal, hay tres opciones para la característica SSPR: **Ninguno**, **Seleccionados** y **Todos**.



La opción **Seleccionados** es útil para crear grupos concretos que tengan SSPR habilitado. Puede crear grupos para pruebas o pruebas de concepto antes de aplicar la característica a un grupo más grande. Cuando esté listo para implementar SSPR en todas las cuentas de usuario del inquilino de Microsoft Entra, puede cambiar la configuración.

* **Tenga en cuenta los métodos de autenticación**. Determine cuántos métodos de autenticación se requieren para restablecer una contraseña y seleccione las opciones de autenticación para los usuarios.
  + El sistema debe requerir al menos un método de autenticación para restablecer una contraseña.
  + Un plan de SSPR seguro ofrece varios métodos de autenticación para el usuario. Las opciones incluyen notificaciones por correo electrónico, mensajes de texto o códigos de seguridad enviados al teléfono móvil o de la oficina del usuario. También puede ofrecer al usuario un conjunto de preguntas de seguridad.
  + Puede requerir que las preguntas de seguridad se registren para los usuarios del inquilino de Microsoft Entra.
  + Puede configurar las preguntas de seguridad correctamente respondidas que considere necesarias para obtener un restablecimiento de contraseña correcto.
* **Considere la posibilidad de combinar métodos para mejorar la seguridad**. Las preguntas de seguridad pueden ser menos seguras que otros métodos de autenticación. Es posible que algunos usuarios conozcan las respuestas de las preguntas de un usuario determinado o que las preguntas sean fáciles de resolver. Si admite preguntas de seguridad, combine esta opción con otros métodos de autenticación.

**Prueba de conocimientos**

Supongamos que su empresa busca una solución de identidad sólida. Su trabajo es decidir si la opción óptima es Microsoft Entra ID o Active Directory Domain Services (AD DS). Si elige Microsoft Entra ID, debe seleccionar la edición que mejor satisfaga las necesidades de su organización y determinar qué características se van a implementar.

A continuación se indican algunos requisitos para el diseño:

* **Los usuarios deben poder iniciar sesión en dispositivos, aplicaciones y servicios desde cualquier lugar**.
* **El equipo de TI quiere que los usuarios administren sus propias contraseñas y realicen tareas relacionadas**.
* **El departamento legal solicita protección para los datos confidenciales para cumplir los estándares de cumplimiento de gobernanza**.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las preguntas siguientes. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Qué opción describe correctamente Microsoft Entra ID?**

Microsoft Entra ID se puede consultar mediante LDAP.

Microsoft Entra ID es principalmente una solución de identidad.

Microsoft Entra ID usa unidades organizativas (UO) y objetos de directiva de grupo (GPO).

**2. ¿Qué término define una instancia dedicada y de confianza de Microsoft Entra ID?**

Inquilino de Azure

Identidad

Cuenta de Microsoft Entra

**3. Sus usuarios quieren tener la posibilidad de iniciar sesión en dispositivos, aplicaciones y servicios desde cualquier lugar. Los usuarios quieren iniciar sesión mediante una cuenta profesional o educativa en lugar de con una cuenta personal. ¿Qué debe hacer primero?**

Habilitar el dispositivo en Microsoft Entra ID.

Unir el dispositivo a Microsoft Entra ID.

Registrar el dispositivo con Microsoft Entra ID.

1. B
2. A
3. B

Final del formulario

**Resumen y recursos**

Los administradores de Azure deben estar familiarizados con Microsoft Entra ID y sus conceptos.

En este módulo, ha obtenido información sobre las características de Microsoft Entra y ha explorado los escenarios de implementación. Ha revisado los componentes principales de Microsoft Entra ID, incluidos los inquilinos, las identidades y las cuentas, y ha aprendido cómo están relacionados. Ha comparado Active Directory Domain Services con Microsoft Entra ID y ha descubierto cómo las diferentes ediciones de Microsoft Entra admiten características. Ha explorado las ventajas de las características de unión a Microsoft Entra y autoservicio de restablecimiento de contraseña (SSPR) y ha pensado en cómo implementarlas para su organización.

**Más información con la documentación de Azure**

* Obtenga más información sobre [Microsoft Entra ID](https://learn.microsoft.com/es-es/azure/active-directory/).
* Unir dispositivos mediante la [identidad del dispositivo de Microsoft Entra](https://learn.microsoft.com/es-es/azure/active-directory/devices/).
* Configure [Autoservicio de restablecimiento de contraseña de Microsoft Entra](https://learn.microsoft.com/es-es/azure/active-directory/authentication/concept-sspr-howitworks).

**Más información con el aprendizaje autodirigido**

* Administre la identidad del dispositivo con [Unión a Microsoft Entra y Enterprise State Roaming](https://learn.microsoft.com/es-es/training/modules/manage-device-identity-ad-join/).
* Implemente y administre una [identidad híbrida](https://learn.microsoft.com/es-es/training/modules/implement-manage-hybrid-identity/).

**Más información con ejercicios prácticos opcionales**

* Permitir que los usuarios restablezcan su contraseña con el [Autoservicio de restablecimiento de contraseña (espacio aislado) de Microsoft Entra](https://learn.microsoft.com/es-es/training/modules/allow-users-reset-their-password/).