**Describir la gobernanza de identidades en Azure AD**

Azure AD Identity Governance ofrece a las organizaciones la posibilidad de realizar las siguientes tareas:

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

Estas acciones se pueden completar para empleados, socios comerciales y proveedores en varios servicios y aplicaciones, tanto locales como en la nube.

Están diseñadas para ayudar a las organizaciones a abordar las siguientes cuatro preguntas clave:

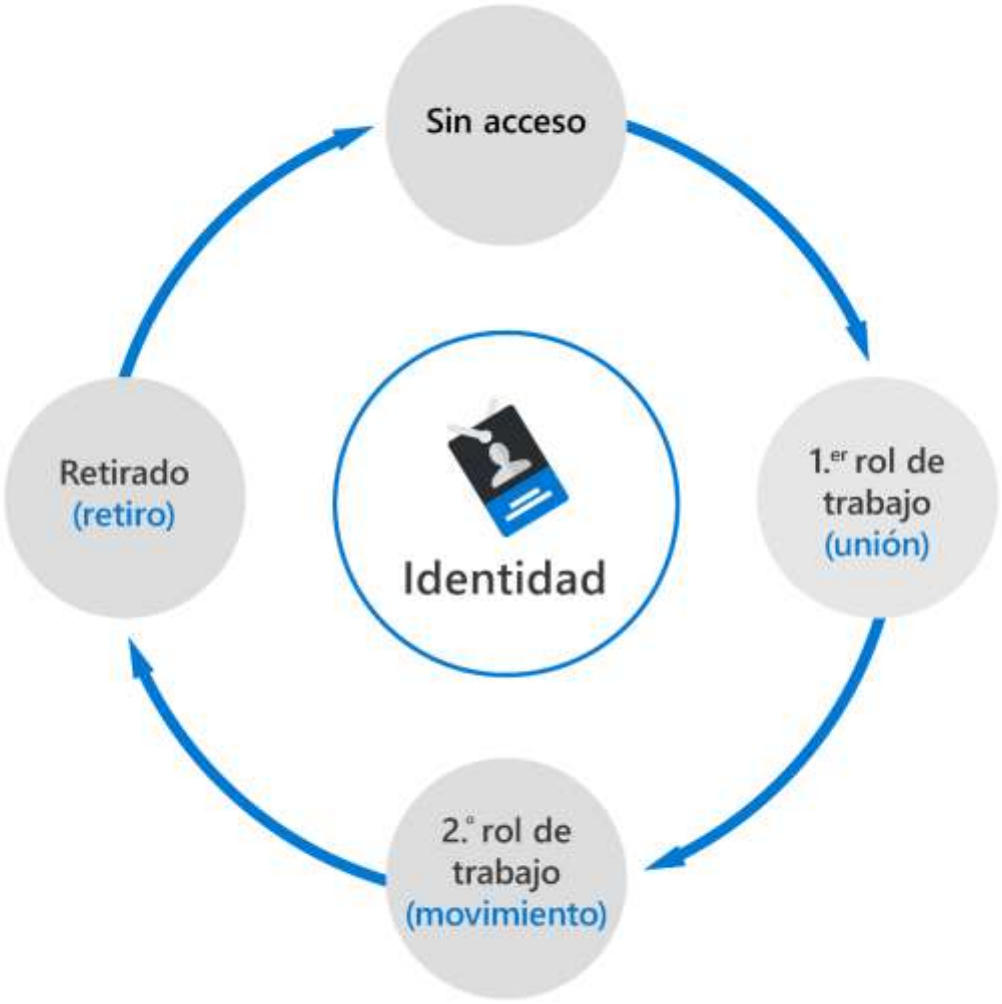
- ¿Qué usuarios deben tener acceso a qué recursos?
- ¿Qué hacen esos usuarios con el acceso concedido?
- ¿La organización cuenta con controles eficaces para administrar el acceso?
- ¿Los auditores pueden comprobar qué controles funcionan?

**Ciclo de vida de las identidades**

La administración del ciclo de vida de las identidades de los usuarios es el alma de la gobernanza de identidades.

Al planear la administración del ciclo de vida de la identidad para los empleados, por ejemplo, muchas organizaciones modelan el proceso de "unirse, trasladar y abandonar". Cuando una persona se une por primera vez a una organización, se crea una nueva identidad digital si aún no hay ninguna disponible. Cuando una persona se mueve entre límites organizativos, es posible que se deban agregar o eliminar autorizaciones de acceso adicionales a su identidad digital. Cuando una persona se va, es posible que sea necesario eliminar el acceso, y la identidad puede ya no ser necesaria, salvo con fines de auditoría.

En el diagrama siguiente se muestra una versión simplificada del ciclo de vida de la identidad.




Para muchas organizaciones, este ciclo de vida de la identidad para los empleados está ligado a la representación del usuario en un sistema de recursos humanos (RR. HH.), como Workday o SuccessFactors. El sistema de RR. HH. está autorizado para proporcionar la lista actual de empleados y algunas de sus propiedades, como el nombre o departamento.

Azure AD Premium ofrece integración con los sistemas de recursos humanos basados en la nube. Cuando se agrega un nuevo empleado a un sistema de recursos humanos, Azure AD puede crear la cuenta de usuario correspondiente. De manera similar, si las propiedades como, por ejemplo, el departamento o estado laboral, cambian en el sistema de RR. HH., la sincronización de esas actualizaciones con Azure AD garantiza la coherencia.

Azure AD Premium incluye también Microsoft Identity Manager, que permite importar registros desde los sistemas de recursos humanos locales, como SAP HCM, Oracle eBusiness y Oracle PeopleSoft. Para obtener más información, consulte la documentación de

Microsoft Identity Manager que se muestra en la sección Más información de la unidad de resumen y recursos.

En general, la administración del ciclo de vida de una identidad consiste en actualizar el acceso que necesitan los usuarios, ya sea a través de la integración con un sistema de recursos humanos, o a través de aplicaciones de aprovisionamiento de usuarios.

**Ciclo de vida de los accesos**

El ciclo de vida de acceso es el proceso para administrar el acceso todo el tiempo que el usuario permanece en la organización. Los usuarios requieren distintos niveles de acceso desde el momento en el que se unen a una organización hasta que la abandonan. En varias fases intermedias, necesitarán derechos de acceso a distintos recursos en función de su rol y sus responsabilidades.

Las organizaciones pueden automatizar el proceso del ciclo de vida de los accesos con determinadas tecnologías, como los grupos dinámicos. Los grupos dinámicos permiten a los administradores crear reglas basadas en atributos para determinar la pertenencia a grupos. Cuando cambia cualquier atributo de un usuario o dispositivo, el sistema evalúa todas las reglas de grupos dinámicos de un directorio para ver si la modificación desencadenaría la adición o retirada de usuarios en un grupo. Si un usuario o dispositivo cumple una regla de un grupo, se agrega a este como miembro. Si ya no cumple la regla, se quita del grupo.

**Ciclo de vida de los accesos con privilegios**

La supervisión del acceso con privilegios es una parte fundamental de la gobernanza de identidades. Cuando se asignan derechos administrativos a los empleados, proveedores y contratistas, debe haber un proceso de gobernanza debido a la posibilidad de un uso incorrecto.

Azure AD Privileged Identity Management (PIM) ofrece controles adicionales que están adaptados para proteger los derechos de acceso. PIM le ayuda a minimizar el número de personas que tienen acceso a los recursos a través de Azure AD, Azure y otras servicios en línea de Microsoft. PIM proporciona un conjunto completo de controles de gobernanza para ayudar a proteger los recursos de la empresa. PIM es una característica de Azure AD Premium P2.

**Descripción de qué son la administración de derechos y las revisiones de acceso**

La administración de derechos es una característica de gobernanza de identidades que permite a las organizaciones administrar el ciclo de vida de las identidades y el acceso a escala. La administración de derechos automatiza los flujos de trabajo de las solicitudes de acceso, las asignaciones de acceso, las revisiones y la expiración.

El vídeo siguiente es una introducción a la administración de derechos y examina cómo se usan los paquetes de acceso para los recursos.

Como se describe en el vídeo, las organizaciones empresariales suelen enfrentar desafíos al administrar el acceso de los empleados a recursos, por ejemplo:

- Es posible que los usuarios no sepan qué acceso deben tener e, incluso si lo saben, pueden tener dificultades para encontrar los usuarios adecuados que lo aprueben.

- Una vez que los usuarios buscan y reciben acceso a un recurso, puede que conserven el acceso por más tiempo del necesario para los fines empresariales.
- Administración del acceso para usuarios externos.

La administración de derechos incluye las siguientes funcionalidades para solucionar estos desafíos:

- Delegue la creación de paquetes de acceso a usuarios que no son administradores. Estos paquetes de acceso contienen recursos que los usuarios pueden solicitar. A continuación, los administradores de paquetes de acceso delegados definen las directivas, que incluyen reglas como qué usuarios pueden solicitar acceso, quién lo debe aprobar y cuándo expira.
- Administración de usuarios externos. Cuando un usuario que todavía no está en su directorio solicita acceso y este se aprueba, se le invita automáticamente al directorio y se le asigna acceso. Cuando expira su acceso, si no tiene otras asignaciones de paquete de acceso, su cuenta de B2B en el directorio se puede quitar automáticamente.

La administración de derechos es una característica de Azure AD Premium P2 que usa paquetes de acceso para administrar el acceso a los recursos.

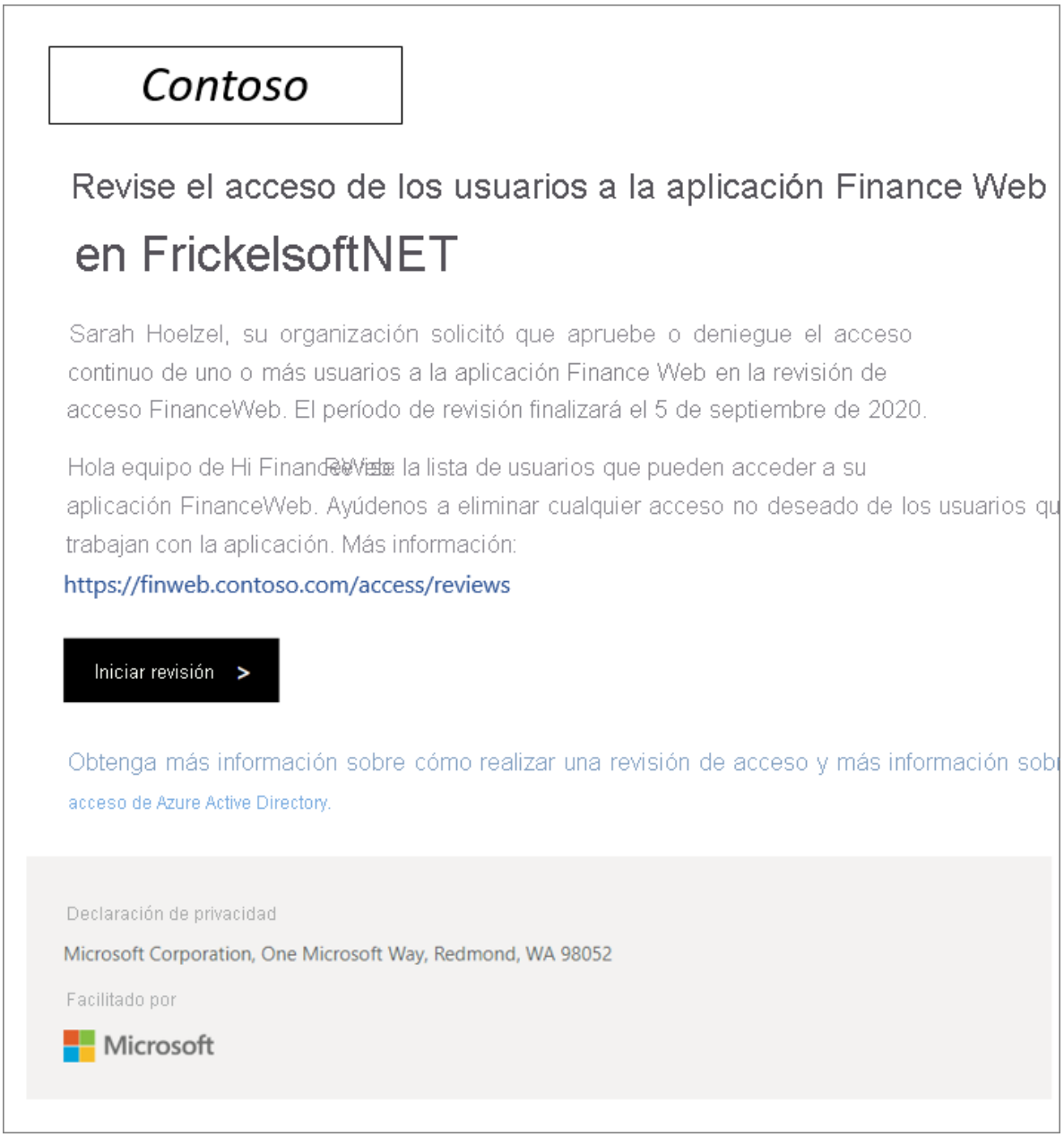
**Revisiones de acceso de Azure AD**

Las revisiones de acceso de Azure Active Directory (AD) permiten a las organizaciones administrar de forma eficiente la pertenencia a grupos, el acceso a las aplicaciones empresariales y la asignación de roles. Las revisiones de acceso periódicas garantizan que solo las personas adecuadas tienen acceso a los recursos. Los derechos de acceso excesivos suponen un riesgo de seguridad conocido. Sin embargo, cuando las personas se transfieren de un equipo a otro, o cuando asumen o ceden responsabilidades, los derechos de acceso pueden ser difíciles de controlar.

Las revisiones de acceso son útiles cuando:

- Demasiados usuarios tienen roles con privilegios, como el administrador global.
- No es posible la automatización; por ejemplo, cuando los datos de recursos humanos no están en Azure AD.
- Quiere controlar el acceso a datos críticos para la empresa.
- Las directivas de gobernanza requieren revisiones periódicas de los permisos de acceso.

Las revisiones de acceso se pueden crear a través de las revisiones de acceso de Azure AD o de Azure AD Privileged Identity Management (PIM). Las revisiones de acceso se pueden usar para revisar y administrar el acceso tanto para usuarios como para invitados. Cuando se crea una revisión de acceso, se puede configurar para que cada usuario revise su propio acceso, o para que uno o varios usuarios revisen el acceso de todos. Del mismo modo, se puede solicitar a todos los invitados que revisen su propio acceso, o que lo examinen uno o varios usuarios.




Los administradores que crean revisiones de acceso pueden realizar un seguimiento del progreso a medida que los revisores completen el proceso. Los derechos de acceso no se cambian hasta que finaliza la revisión. Sin embargo, puede detener una revisión antes de que llegue a su final programado.

Una vez completada la revisión, se puede establecer para que los cambios se apliquen de forma manual o automática para quitar el acceso de una asignación de aplicación o pertenencia a un grupo, excepto para grupos dinámicos o grupos que se originen del entorno local. En esos casos, los cambios se deben aplicar directamente al grupo.

Las revisiones de acceso son una característica de Azure AD Premium P2.

**Condiciones de uso de Azure AD**

Los términos de uso de Azure AD permiten que se presente información a los usuarios antes de que tengan acceso a los datos o a una aplicación. Los términos de uso garantizan que los usuarios lean las declinaciones de responsabilidad pertinentes para conocer los requisitos legales o de cumplimiento.

Entre los casos de uso de ejemplo en los que es posible que los empleados o invitados deban aceptar condiciones de uso se incluyen los siguientes:

- Antes de acceder a datos confidenciales o a una aplicación.
- De forma periódica, a fin de recordarles las regulaciones.
- En función de los atributos del usuario, como los términos aplicables a roles concretos.
- Presentación de los términos a todos los usuarios de su organización.

Los términos de uso se presentan en formato PDF, con contenido que crea el usuario, como un documento de contrato existente. Los términos de uso también se pueden presentar a los usuarios en dispositivos móviles.

Las directivas de acceso condicional se usan para solicitar que se muestren los términos de uso y garantizar que el usuario ha aceptado esos términos antes de acceder a una aplicación. A continuación, los administradores pueden ver quién ha aceptado las condiciones de uso y quién las ha rechazado.

**Descripción de las funcionalidades de Privileged Identity Management**

Privileged Identity Management (PIM) es un servicio de Azure Active Directory (Azure AD) que permite administrar, controlar y supervisar el acceso a recursos importantes de la organización. Esto incluye a los recursos de Azure AD, Azure y los de otros servicios en línea de Microsoft, como Microsoft 365 o Microsoft Intune. PIM mitiga los riesgos de los permisos de acceso excesivos, innecesarios o mal utilizados. Requiere una justificación para saber por qué los usuarios quieren los permisos y aplica la autenticación multifactor para activar cualquier rol.

PIM tiene las siguientes características:

- 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.

Privileged Identity Management es una característica de Azure AD Premium P2.

**¿Por qué se utiliza PIM?**

PIM reduce la posibilidad de que un actor malintencionado obtenga acceso, pues reduce al mínimo el número de personas que tienen acceso a información o recursos seguros. Al limitar el tiempo a los usuarios autorizados, se reduce el riesgo de que un usuario autorizado afecte involuntariamente recursos confidenciales. PIM también permite supervisar lo que hacen los usuarios con sus privilegios de administrador.

En este vídeo, aprenderá qué es PIM y por qué podría usarlo:

https://www.microsoft.com/es-mx/videoplayer/embed/RE4ILbu?postJsllMsg=true&autoCaptions=es-mx

En el vídeo se mostró cómo PIM reduce el riesgo de los privilegios elevados para las organizaciones. También se explicaron las ventajas específicas del uso de las características de PIM y cuándo las usaría una organización.

**Descripción de Azure AD Identity Protection**

Identity Protection es una herramienta que 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.

Microsoft analiza 6,5 billones de señales al día para identificar posibles amenazas. Estas señales provienen de los aprendizajes que Microsoft ha adquirido de su puesto en organizaciones con Azure AD, el espacio de consumidor con cuentas de Microsoft y juegos con Xbox.

Las señales que generan estos servicios se cargan en Identity Protection. A continuación, las herramientas como el acceso condicional pueden usar estas señales para tomar decisiones sobre el acceso. Las señales también se cargan en las herramientas de administración de eventos e información de seguridad (SIEM), como Microsoft Sentinel, para investigación adicional.

Identity Protection clasifica el riesgo en tres niveles: bajo, medio y alto. También puede calcular el riesgo de inicios de sesión y el riesgo de identidades del usuario.

Un riesgo de inicio de sesión representa la probabilidad de que el propietario de la identidad no haya autorizado una solicitud de autenticación determinada. El riesgo de inicio de sesión se puede calcular en tiempo real o sin conexión, usando orígenes de inteligencia sobre amenazas internos y externos de Microsoft. A continuación, se enumeran algunos de los riesgos de inicio de sesión que Identity Protection de Azure AD puede identificar:

- Dirección IP anónima. Este tipo de detección de riesgo indica un inicio de sesión desde una dirección IP anónima, por ejemplo, el explorador Tor o redes VPN anónimas.
- Viajes atípicos. Este tipo de detección de riesgos identifica dos inicios de sesión procedentes de ubicaciones geográficamente distantes, donde al menos una de las

ubicaciones puede también ser inusual para el usuario, según su comportamiento anterior.

- Dirección IP vinculada a malware. Este tipo de detección de riesgos indica inicios de sesión desde direcciones IP infectadas con malware, que se sabe que se comunican activamente con un servidor bot.
- Propiedades de inicio de sesión desconocidas. Este tipo de detección de riesgo tiene en cuenta el historial de inicio de sesión anterior para determinar inicios de sesión anómalos. El sistema almacena información sobre las ubicaciones anteriores que ha utilizado un usuario y considera que estas ubicaciones "conocidas". La detección de riesgos se desencadena cuando el inicio de sesión se produce desde una ubicación que no está en la lista de ubicaciones conocidas.
- Difusión de contraseña. Esta detección de riesgo se desencadena cuando se realiza un ataque de difusión de contraseñas.
- Inteligencia sobre amenazas de Azure AD. Este tipo de detección de riesgo indica una actividad de inicio de sesión poco común para el usuario en cuestión o que es coherente con patrones de ataque conocidos basados en orígenes de inteligencia sobre amenazas internas y externas de Microsoft.

Un riesgo de usuario representa la probabilidad de que una identidad o cuenta determinada esté en peligro. Los riesgos se calculan sin conexión, usando orígenes de inteligencia sobre amenazas internos y externos de Microsoft. A continuación, se enumeran algunos de los riesgos de usuario que Identity Protection de Azure AD puede identificar:

- Filtración de credenciales. Este tipo de detección de riesgo indica que se han filtrado las credenciales válidas del usuario. Cuando los cibercriminales llegan a poner en peligro las contraseñas válidas de usuarios legítimos, es frecuente que las compartan. Normalmente lo hacen publicándolas en la Web oscura, los sitios de pegado, o bien mediante el intercambio o la venta de esas credenciales en el mercado negro. Cuando el servicio de credenciales filtradas de Microsoft adquiere las credenciales de usuario de la Web oscura, los sitios de pegado u otros orígenes, se comparan con las credenciales válidas actuales de los usuarios de Azure AD para encontrar coincidencias válidas.
- Inteligencia sobre amenazas de Azure AD. Este tipo de detección de riesgo indica una actividad de usuario poco común para el usuario en cuestión o coherente con patrones de ataque conocidos basados en orígenes de inteligencia sobre amenazas internas y externas de Microsoft.

Identity Protection solo genera detecciones de riesgos cuando se usan las credenciales correctas en la solicitud de autenticación. Si un usuario usa credenciales incorrectas, no se marcará con Identity Protection, ya que no hay un riesgo de que las credenciales se pongan en peligro a menos que un infiltrado use las credenciales correctas. Luego, las detecciones de riesgos pueden desencadenar acciones como solicitar que los usuarios proporcionen autenticación multifactor, restablezcan su contraseña o bloqueen el acceso hasta que un administrador tome medidas.

Identity Protection proporciona a las organizaciones tres informes que pueden usar para investigar los riesgos de identidad en su entorno. Estos informes son sobre los **usuarios de riesgo**, los **inicios de sesión de riesgo** y las **detecciones de riesgo**. La investigación de eventos es clave para comprender e identificar los puntos débiles de la estrategia de seguridad.

Después de completar una investigación, los administradores deberán tomar medidas para corregir el riesgo o desbloquear usuarios. Las organizaciones también pueden habilitar la corrección automática mediante las directivas de riesgo. Microsoft recomienda terminar los eventos pronto, ya que el tiempo es importante cuando se trabaja con riesgos.

Identity Protection es una característica de Azure AD Premium P2.