Aprovisionamiento de usuarios en empresas

Por Ian Glazer, Lori Robinson, and Mat Hamlin

Tabla de contenido

Resumen

El aprovisionamiento de usuarios es la forma por la cual se crean y mantienen las cuentas de usuario en un sistema (por ej., bases de datos, aplicaciones SaaS, sistemas operativos, etc.). Cuando decimos que un sistema de aprovisionamiento de usuarios mantiene una cuenta de usuario nos referimos a que hace todo, desde cambios en atributos de la cuenta de usuario, cambios en los derechos o privilegios asociados a la cuenta de usuario, bloqueo y desbloqueo de una cuenta de usuario e incluso la eliminación de una cuenta de usuario. El aprovisionamiento de usuario es fundamentalmente un asunto de "admin-tiempo": una cuenta de usuario se crea (o modifica) en base a una acción administrativa, a diferencia de una acción de usuario que ocurre en el momento de uso de un recurso. Este artículo se centra en los usos y componentes de un sistema de aprovisionamiento de usuarios y se enfoca principalmente en las situaciones en las que las cuentas de usuario se mantienen en repositorios centrales, dentro de configuraciones típicas de empresa y de la fuerza laboral.

Introducción

La creación y mantenimiento de cuentas de usuario son los cimientos de cualquier sistema IAM. Generalmente, este proceso es llamado aprovisionamiento de usuarios y se usa para establecer los derechos de un usuario para acceder a recursos protegidos (aplicaciones, documentos o bases de datos) de una organización. Los procesos de aprovisionamiento no solo crean cuentas de usuario y asignan derechos, sino que también mantienen esos derechos de la cuenta de usuario mediante la detección de eventos significativos en el ciclo de vida, como cambios en las responsabilidades laborales y/o en la aplicación de políticas. El aprovisionamiento de usuarios suele usarse para garantizar que las personas indicadas tienen acceso a los sistemas indicados oportunamente y con los derechos apropiados para sus responsabilidades.

Terminología

- **Fuente acreditada:** Es el sistema de registro (SOR, por sus siglas en inglés) de datos de identidad. Una organización puede tener más de una fuente acreditada de datos en su entorno.
- **Catálogo de recursos para la administración de derechos:** Es una base de datos de los derechos y los metadatos asociados. El catálogo incluye una lista de datos de derechos tomados de sistemas de negocios, aplicaciones y plataformas, así como descripciones técnicas y de negocio, de los derechos y de sus usos.
- **Administración del ciclo de vida de identidades:** Es un proceso que detecta cambios en los sistemas de registro acreditados y que actualiza los registros de identidades basándose en políticas.

- **Repositorio de identidades:** Un repositorio de identidades es un directorio o base de datos que puede ser referenciado por sistemas y servicios externos (como servicios de autenticación o autorización).
- **Conciliación:** Es el proceso de identificar y procesar los cambios en los usuarios y en los accesos del usuario hechos directamente en los sistemas objetivo.
- **Aprovisionamiento de usuarios**: Los medios por los cuales se crean, mantienen y desactivan/eliminan las cuentas de usuarios en un sistema de acuerdo con las políticas definidas.

¿Qué es el aprovisionamiento de usuarios?

El aprovisionamiento de usuarios es el acto de establecer los derechos que tiene un usuario para acceder a los recursos que necesita. Las tecnologías de aprovisionamiento de usuario se implementan en múltiples industrias como el sector de la salud, educación, finanzas, gobierno, comercio, manufactura, tecnología, etc.

Las tecnologías de aprovisionamiento de usuarios dan soporte a las siguientes funcionalidades:

Administración del ciclo de vida de identidades: Una identidad y sus atributos asociados son base de las decisiones de autenticación y autorización que se toman en un entorno. Por eso es fundamental que se mantenga un registro de identidad. Los sistemas de aprovisionamiento detectan los cambios en los sistemas de registro acreditados (como una base de datos o repositorio de recursos humanos) y actualizan los registros de identidad en consecuencia.

Aprovisionamiento de cuentas de usuario: Como su nombre lo indica, la función principal de un sistema de aprovisionamiento de usuarios es el aprovisionamiento (y desaprovisionamiento) de cuentas de usuario. Las tecnologías de aprovisionamiento de usuarios automatizan la creación, el mantenimiento y la desactivación/eliminación de cuentas de usuario en un sistema determinado, de acuerdo con las políticas definidas.

Administración de autoservicio y delegada: Los sistemas de aprovisionamiento proveen interfaces que permiten que los usuarios soliciten el acceso a sistemas, administren contraseñas y actualicen su información. Los administradores delegados pueden realizar tareas similares en nombre de otros, como el alta o baja de usuarios, cambios en las contraseñas, actualizaciones del perfil y asignación de derechos.

Flujo de trabajo: Los sistemas de aprovisionamiento usan herramientas de flujo de trabajo que permiten la automatización de los procesos de aprovisionamiento y de los flujos de trabajo de aprobación. Al usar flujos de trabajo de aprobación, las partes interesadas pueden validar y aprobar los cambios propuestos antes de que sean aplicados

en los sistemas correspondientes. Si bien muchas de las decisiones de otorgación de acceso están automatizadas mediante políticas, otras requieren la intervención de un humano.

Auditoría y reporte: Los sistemas de aprovisionamiento registran todas las transacciones de administración en el ciclo de vida de la identidad, políticas de acceso y aprovisionamiento de usuarios, y proveen mecanismos de reporte para extraer los datos registrados.

Una nota sobre gobernanza: Los sistemas de aprovisionamiento de usuarios suelen tener capacidades de gobernanza de la identidad como la evaluación de accesos y certificaciones, el análisis de riesgo y la analítica de identidades. La combinación de soluciones de aprovisionamiento de usuarios y de gobernanza de la identidad pueden ser referidas como Gobernanza y Administración de Identidades (IGA, por sus siglas en inglés). Este documento se enfoca exclusivamente en la funcionalidad de aprovisionamiento de usuario y no incluye información sobre gobernanza de identidades. Este documento tampoco abarca la administración de contraseñas la cual puede estar comprendida en las soluciones de aprovisionamiento.

Impulsores de negocio para el aprovisionamiento de usuarios automáticos

Existen tres impulsores de negocio principales que justifican la implementación de sistemas de aprovisionamiento de usuarios automáticos:

- **Eficacia operacional**: El costo administrativo asociado a la creación y mantenimiento manual de cuentas de usuario es significativo para las organizaciones medianas a grandes. Sin un proceso automático, pueden pasar semanas antes que un usuario tenga acceso a los recursos que necesita para realizar sus tareas laborales o de otra índole. Los sistemas de aprovisionamiento de usuarios automatizan los procesos de administración de cuentas, reduciendo los costos administrativos y aumentando el tiempo de productividad, resultando en una eficacia operacional.
- **Seguridad:** El aprovisionamiento de cuentas de usuario puede llevar a brechas de seguridad como cuentas de usuario con excesos de privilegios o cuentas huérfanas (cuentas activas asignadas a empleados inactivos). Los sistemas de aprovisionamiento de cuentas automáticos mejoran la seguridad al garantizar que el aprovisionamiento de las cuentas de usuario y sus derechos estén de acuerdo con la política, y que el desaprovisionamiento sea oportuno.
- **Cumplimiento**: Varias leyes y regulaciones requieren que las organizaciones demuestren tener control sobre los sistemas, recursos y datos críticos. Los sistemas de aprovisionamiento de usuarios hacen cumplir el control de acceso basado en políticas y permiten que las organizaciones demuestren la eficacia de estos controles con capacidades de reporte y atestación.

Arquitectura lógica del aprovisionamiento de usuarios

Los sistemas de aprovisionamiento de usuarios usan políticas, flujos de trabajo y conectores para sincronizar la información de identidad de un sistema acreditado con un almacén de identidad, y para proveer cuentas de usuario a las aplicaciones objetivo.

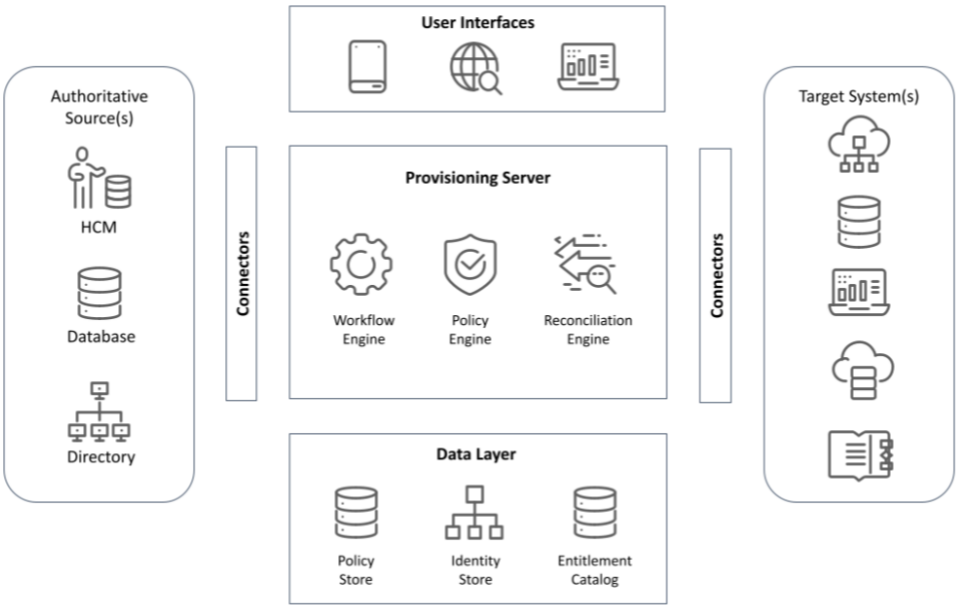

Figura 1: Ilustra los componentes de arquitectura estándar de un ecosistema de aprovisionamiento de usuarios.

Fuente(s) acreditada(s): Es el sistema de registro (SOR, por sus siglas en inglés) de información de identidad. El sistema acreditado comunica los cambios en el sistema de aprovisionamiento. Puede haber más de un sistema acreditado en el entorno. Por ejemplo, en los casos de uso de la fuerza laboral, la Gestión del Capital Humano (HCM, por sus siglas en inglés) / sistema de Recursos Humanos (RRHH) pueden ser la fuente acreditada para la información de empleados, pero la información de contratistas puede estar almacenada en un sistema adquisiciones/contratos.

Sistema(s) objetivo: Los sistemas objetivo se suscriben a los cambios en los registros de identidad y están al final del proceso de aprovisionamiento. Los sistemas de aprovisionamiento crean y gestionan las cuentas de usuario y sus derechos asociados dentro del entorno del sistema objetivo.

Conectores: Son la capa de integración entre el sistema de aprovisionamiento y los sistemas objetivo-acreditados. Existen varios tipos de conectores: personalizados

(conectores específicos de aplicaciones que se comunican con aplicaciones específicas API), genéricos (por ej., LDAP, JDBC, de datos delimitados), o basados en estándares. Para más información sobre la conectividad basada en estándares, vea la sección de estándares de este artículo.

Servidor de aprovisionamiento: La capa *middleware* responsable de la sincronización de datos, mapeo y transformación; la aplicación de la lógica de negocio y políticas de acceso; y la orquestación de los flujos de procesos de aprovisionamiento. El servidor de aprovisionamiento está conformado por los siguientes componentes funcionales:

- **Reglas de correlación de cuenta:** correlaciona o une cuentas de usuario discrepantes (en sistemas objetivo o acreditados) en un único registro de identidad y garantiza que no se creen identidades duplicadas para una misma persona o entidad.
- **Reglas de mapeo de datos:** mapea y transforma datos de la fuente de contexto a la fuente objetivo.
- **Reglas de creación de cuenta:** establece los estándares para crear un registro de identidad como convenciones de nomenclatura, atributos requeridos, políticas de contraseña, políticas de localización, etc.
- **Políticas de acceso**: determina los derechos de acceso que deben ser asignados a un usuario. Para más información sobre los diferentes tipos de políticas de acceso, vea la sección de Políticas.
- **Motor de flujo de trabajo:** orquesta el aprovisionamiento basado en lógica de procesos de negocio y habilita los flujos de trabajo de solicitud, aprobación y evaluación de accesos.
- **Motor de conciliación:** encuentra las cuentas de usuario creadas directamente en los sistemas objetivo (eludiendo los procesos de aprovisionamiento estándares), se asegura de que la cuenta de usuario cumpla con las políticas de acceso y correlaciona la cuenta de usuario con el registro de identidad del individuo.

Repositorio de identidad: Los registros de identidad se almacenan en un repositorio de identidad. El repositorio de identidad es un directorio o base de datos que puede ser referenciado por sistemas y servicios externos (como servicios de autenticación o autorización). El registro de identidad incluye los atributos asociados a la identidad, así como un registro de todas las cuentas de usuario asociadas a la identidad.

Catálogo de derechos: Es una base de datos de derechos y sus metadatos asociados. El catálogo comprende una lista de datos de derechos tomados de sistemas, aplicaciones y plataformas de negocio. Los datos de derechos pueden enriquecerse con metadatos como un puntaje de riesgos y descripciones amigables de los derechos que pueden ser desplegadas a los usuarios durante una solicitud de acceso, evaluaciones de acceso y certificaciones.

Almacén de configuración de sistema y auditoría: Un repositorio dedicado a almacenar información como configuraciones de sistema e información sobre mapeo de identidad, políticas, definición de roles y flujos de trabajo. Este repositorio también puede servir de almacén de registros de auditoría.

Interfaces de usuario: Los sistemas de aprovisionamiento de usuario incluyen interfaces administrativas, de usuario final y de administración delegada. Las interfaces administrativas se usan para configurar el sistema. Las interfaces de usuario final y de administración delegada se usan para las solicitudes de acceso, flujos de trabajo de aprobación, reporte, actualizaciones de perfiles, etc. Los sistemas de aprovisionamiento suelen incluir interfaces web que pueden ser accedidas desde una pc o dispositivo móvil. Si bien no es lo común, algunos vendedores de aprovisionamiento cuentan con una aplicación móvil para los flujos de trabajo de autoservicio y aprobación.

Al ser altamente conectables e interactivos, los sistemas de aprovisionamiento de usuarios deben ser abiertos y extensibles. El proveedor de aprovisionamiento debe proveer APIs abiertas, flujos de trabajo sin código y conectores genéricos que habiliten la flexibilidad del sistema.

Flujo de proceso del aprovisionamiento de usuarios

Las tecnologías de aprovisionamiento de usuarios permiten que las organizaciones administren eficazmente miles de identidades al capturar eventos en los ciclos de vida y garantizando que las cuentas de usuario y sus privilegios asociados estén actualizados y sean correctos. Estos procesos reducen los gastos administrativos y mejoran la seguridad. Dicho esto, el aprovisionamiento automático de cuentas de usuario es un proceso complejo y multifacético que comprende tres fases claras:

- **Evento desencadenante**: Un evento de negocio o cambio en una identidad que desencadena una acción de aprovisionamiento.
- **Administración de políticas**: Es la aplicación de las políticas de acceso que unen la identidad a cuentas de usuario y a derechos específicos.
- **Aprovisionamiento de cuentas de usuario**: La creación, mantenimiento, desactivación o eliminación de cuentas de usuario en aplicaciones objetivo.

Evento desencadenante

El acto de aprovisionamiento se inicia con un evento. Este evento puede ser:

- La creación de nuevo empleado en un sistema de RRHH.
- La modificación de una entrada en un *Active Directory* por el traslado de una persona de una unidad de negocio a otra.
- La creación de un *ticket* en un Servicio de Gestión TI (ITSM, por sus siglas en inglés) o en un sistema de ticket de un Servicio de Ayuda.

- Una persona interactuando directamente con el sistema de aprovisionamiento para solicitar un cambio en una cuenta de usuario.

Existen tres eventos principales:
- Incorporaciones
- Traslados
- Bajas

Las incorporaciones, traslados y bajas (JML, por sus siglas en inglés) son la molienda del molino del aprovisionamiento. La gestión de los procesos JML se convierte en parte de las tareas de un sistema de identidad. Este trabajo incluye conectar el sistema de aprovisionamiento de usuarios con las fuentes desencadenantes, y luego el desarrollo de las políticas que deberán ser evaluadas en cada tipo de evento de cada sistema objetivo.

Incorporación

La manera más sencilla de pensar un evento de incorporación es, por ejemplo, cuando se incorpora un nuevo empleado a una empresa. Esta persona necesitará que sus beneficios y nómina estén configurados en sus cuentas de usuario en los sistemas TI. En su sentido más puro, los eventos de incorporación existen para crear una nueva identidad de red y las nuevas cuentas de usuario de red en los sistemas TI.[1]

Traslado

Cuando una persona cambia de rol dentro de una empresa, probablemente va a necesitar tener acceso a nuevos sistemas de negocio y que se eliminen sus antiguos accesos. Este es el objetivo del evento de traslado. Un traslado puede pensarse como un cambio en la relación entre una organización y una persona. Estos cambios pueden incluir la unidad de negocio a la cual responden, ascensos o cambios en el apellido.[2]

Baja

El mejor ejemplo de un evento de baja es cuando una persona se jubila de su trabajo. En este caso, las cuentas de usuario de la persona deben ser eliminadas o al menos bloqueadas para prevenir su uso en sistemas objetivo. El procedimiento es el mismo: un evento de baja desencadena que el sistema de aprovisionamiento de usuarios elimine el acceso.

Las tecnologías de aprovisionamiento de usuarios ofrecen varios mecanismos de captura de eventos JML, como:

---

[1] Encuentre más información sobre Incorporaciones, Traslados y Bajas en el artículo de Cameron, A. & Grewe, O. (2022) “Un Pantallazo sobre el Ciclo de Vida de la Identidad Digital (v2)”, *Cuerpo de Conocimiento de IDPro* 1(7). doi: https://doi.org/10.55621/idpro.31

[2] Un cambio en el nombre o lugar de residencia puede tener el mismo impacto que un cambio en el rol, función laboral o estructura de subordinación.

- **Aprovisionamiento automático:** El sistema de aprovisionamiento "escucha" los eventos de sistemas de registro como los de Recursos Humanos, ITSM, o un directorio.
- **Procesamiento por lotes:** El sistema de aprovisionamiento ejecuta un proceso programado que regularmente sondea una fuente acreditada sobre cambios y genera un archivo con los resultados.
- **Solicitud de autoservicio:** Las soluciones de aprovisionamiento de usuario actuales incluyen un portal de solicitud de acceso para el usuario final, donde los usuarios finales o administradores pueden solicitar el acceso a los sistemas y a los derechos específicos necesarios para llevar a cabo sus responsabilidades de negocio. El usuario o administrador delegado actualiza el perfil de usuario o realiza una solicitud de cambio de acceso a través de la interfaz de autoservicio.
- **Manual/*Ticket*:** En ocasiones, una organización puede usar un sistema de tickets u otro proceso manual para notificar al equipo de identidad la necesidad de realizar un cambio en el registro de identidad. En este caso, el administrador de identidades actualizará el registro de identidad directamente para desencadenar las consiguientes actividades de aprovisionamiento y aplicación de políticas.
- **Evento de conciliación:** La conciliación es el proceso de identificar y procesar cambios en los usuarios y accesos de usuario hechos directamente en los sistemas objetivo. El hecho que una organización configure una solución de aprovisionamiento de usuarios para una administración de acceso de usuario centralizada no evita que puedan realizarse cambios directamente en el sistema objetivo. Por lo tanto, para garantizar una consistencia en el acceso de usuarios y en los atributos de usuario en toda la organización, el sistema de aprovisionamiento de usuario ***conciliará*** periódicamente qué sabe sobre los usuarios y sobre sus accesos a un sistema objetivo específico. Esta conciliación se lleva a cabo al recolectar y comparar todos los datos de usuario en el sistema objetivo (conciliación total) o procesando cambios conocidos en el acceso de usuario basándose en un registro de cambios o cualquier otro tipo de registro basado en el tiempo. Cuando se identifican cambios o variaciones en un proceso de conciliación, se desencadenan eventos y se procesan basándose en políticas definidas. El resultado de la conciliación puede ser una sincronización de cambios entre el sistema objetivo y otros sistemas, o deshacer cualquier cambio aplicado localmente que haya ocurrido por fuera de la solución de aprovisionamiento de usuarios.

Administración de políticas

En el pasado, las organizaciones administraban los accesos de usuario a los sistemas objetivo de forma *ad hoc*. Ante la complejidad de los entornos empresariales actuales esto ya no es viable. Es necesario contar con reglas documentadas que determinen quién debe tener acceso a qué sistemas objetivo; más aún, deben controlar qué tipo de derechos y privilegios tienen las personas en dichos sistemas objetivo. Este es el rol de las políticas en un sistema de aprovisionamiento de usuarios. En lugar de dejar que un administrador

determine a qué grupos debe pertenecer una cuenta de usuario, una política describe a qué grupos una persona pertenece de forma obligatoria, opcional o incluso a cuáles tiene prohibido pertenecer.

Se puede pensar en las políticas como una forma de unir grupos de personas con grupos de sistemas objetivo con grupos de accesos relacionados (derechos, privilegios, etc.). De esta manera, siempre hay dos componentes en el aprovisionamiento de usuarios: quién y qué. El "quién" de la política describe los criterios que definen a qué personas aplicará la política. Por ejemplo, el "quién" de la política incluye todos los empleados de tiempo completo, contratistas y personal de finanzas. El "qué" de la política describe las cuentas de usuario y los derechos y privilegios asociados que una persona puede tener. El "qué" puede ser de granularidad gruesa, por ejemplo, la creación de una cuenta de usuario en todos los sistemas objetivo, o muy fina, como cuando se crean un derecho y dos privilegios específicos en un sistema objetivo.

Los diferentes tipos de políticas usan diferentes combinaciones de quién y qué para ayudar a los profesionales de la identidad a gobernar el acceso. Si bien existe una inmensa variedad de tipos de políticas, para los fines de este artículo nos enfocaremos en cuatro tipos de políticas:

- Inherentes
- Basada en roles
- Reparto de tareas
- Aprobación de flujos de trabajo

Es importante destacar que un proceso de aprovisionamiento de usuarios no tendrá una única política para un solo sistema objetivo o para un solo evento. Las políticas se combinan y aplican a múltiples sistemas objetivo y eventos desencadenantes.

Inherente

Existen sistemas y derechos específicos que cubren una amplia parte de las necesidades de una organización; este tipo de acceso se considera inherente. Algunos ejemplos son:

- Todos los empleados de tiempo completo necesitan un correo electrónico, calendario/cronograma, colaboración y un uso compartido de archivos.
- Todas las personas del departamento financiero necesitan tener un acceso mínimo al sistema de reporte financiero.
- Los pasantes necesitan tener acceso al canal colaborativo "Equipo de Pasantes *Excellence*".

Las políticas inherentes definen los accesos fundamentales para que determinado tipo de personas tengan una relación con la organización. Este tipo de acceso no requiere una examinación, evaluación o aprobación adicional; simplemente por ser una persona que cumple con los criterios de la política (como ser miembro del departamento financiero),

esa persona puede tener y tendrá cuentas de usuario en determinados sistemas con niveles de acceso específicos (administrados por los derechos y privilegios asociados a sus cuentas de usuario). En la mayoría de los casos, las políticas inherentes otorgan accesos de granularidad gruesa a los sistemas objetivo; es decir que pueden darle una cuenta en un sistema de correo electrónico a una persona sin darle acceso a grupos específicos de distribución. Por lo general, las políticas inherentes se aplican como parte de un evento de incorporación y suele ocurrir al asignar uno o más roles de negocio. Los eventos inherentes también pueden ocurrir como parte de un evento de traslado, concretamente cuando una persona se traslada de una función de negocio a otra. Por ejemplo, cuando una persona se incorpora a la división de Contabilidad dentro de una organización, recibe accesos inherentes como un correo electrónico, acceso al *suite* de productividad y accesos básicos a los sistemas de contabilidad fundamentales. Cuando esa persona se traslada a la división de Estrategia Corporativa, pierde el acceso a los sistemas de contabilidad, recibe acceso a los sistemas de previsión presupuestaria y conserva el acceso a las herramientas de correo electrónico y productividad.

Basada en roles

Dado que una organización puede tener muchas funciones de negocio y por lo tanto muchas responsabilidades de negocio diferentes, así como decenas de miles de derechos individuales en sus sistemas, es imposible administrar los accesos a nivel individual. Intentar hacerlo conducirá rápidamente a tener que administrar decenas de millones de combinaciones de personas y privilegios. Los sistemas de aprovisionamiento de usuarios ponen un poco de orden en este caos al traducir los roles que agrupan personas y derechos en componentes de política más manejables.

En la administración de identidades, se hace mucho énfasis en los roles.[3] Los roles vienen en una variedad de colores y formas; este artículo se enfoca en los roles de negocio y los roles técnicos. Un rol de negocio es una forma de agrupar las personas que comparten las mismas responsabilidades de negocio. Por ejemplo, una organización de banca minorista puede tener un rol de negocio llamado “Cajero” y usarlo para describir el acceso apropiado para las personas que trabajan de cajero. Un rol técnico es una forma de agrupar los derechos y privilegios requeridos en uno o más sistemas objetivo para realizar una tarea. Por ejemplo, ese mismo banco minorista puede tener un rol técnico llamado “Consulta y Actualización de Saldos” que otorga a las cuentas de usuario de sus sistemas la capacidad de consultar y actualizar los saldos de las cajas de ahorro.

Al usar los roles de negocio y técnicos para gobernar el acceso de personas, los derechos y privilegios en los sistemas objetivo, una política basada en roles en un sistema de

---

[3] Encuentre más información en el artículo de McKee, M. K., (2021) “Control de Acceso basado en Políticas”, *Cuerpo de Conocimiento de IDPro* 1(4). doi: https://doi.org/10.55621/idpro.61 y Koot, A., (2020) “Introducción al Control de Acceso (v3)”, *Cuerpo de Conocimiento de IDPro* 1(6). doi: https://doi.org/10.55621/idpro.42.

aprovisionamiento de usuarios gobierna el acceso de un grupo más acotado que las políticas inherentes. Por ejemplo, un sistema de aprovisionamiento de usuarios puede tener una política inherente que otorga el acceso al correo electrónico a todos los empleados de tiempo completo. Una política adicional basada en roles podría otorgar el acceso a listas de *mailing* específicas y al drive compartido a todos los "Cajeros".

Segregación de funciones

A raíz de los escándalos de Contabilidad de WorldCom y Enron, la Ley Sarbanes-Oxley tuvo un impacto profundo en las prácticas de negocio.[4] Como parte de las actividades de cumplimiento de las políticas, las organizaciones acudían a sus políticas de aprovisionamiento de usuarios no solo para otorgar accesos sino también para prevenir "combinaciones tóxicas" de accesos. Una combinación tóxica de acceso ocurre cuando una persona tiene privilegios que podrían habilitar una forma de fraude, como la capacidad de crear un nuevo vendedor y emitir pagos a ese vendedor. Esta combinación de accesos podría permitir que un actor malicioso cree empresas ficticias dentro del sistema financiero y luego desvíe fondos a esas empresas. Otra forma de evitar combinaciones tóxicas de políticas es evitar que cualquiera que no sea el administrador de sistema pueda tener derechos de *system admin* o privilegios elevados.

Si los roles son una forma de describir lo que debe tener una persona, las políticas de segregación de funciones (SoD, por sus siglas en inglés) son una forma de describir lo que no debe tener. Por lo general, estas políticas se ponen en marcha cuando se desencadena un evento de aprovisionamiento para evitar que se introduzcan combinaciones tóxicas en los sistemas objetivo y para que se eliminen y remedien aquellas existentes.

Aprobación de flujos de trabajo

La aprobación de flujos de trabajo es un componente esencial del conjunto de herramientas de la gestión de políticas. Aún en las organizaciones que cuentan con un sistema de aprovisionamiento maduro, solo el 70-80% del aprovisionamiento de accesos se realiza usando reglas de inherencia, basadas en roles o SoD. ¿Cómo se aprovisiona entonces el 20-30% de los accesos restantes? La respuesta es: a través de los flujos de trabajo de autoservicio de solicitud y aprobación de accesos.

Las aprobaciones de flujos de trabajo se usan cuando un humano tiene que tomar una decisión de política. Si una regla o rol no están disponibles, el sistema de aprovisionamiento aplica un proceso de flujo de trabajo que rutea la solicitud de acceso hacia quién esté designado para aprobarla. Por ejemplo, un empleado podría hacer una solicitud de acceso autogestionada que esté ruteada hacia un gerente de línea para su

---

[4] Corporate Finance Institute, "Principales escándalos contables: un resumen de los principales escándalos del pasado," n.d., https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/ (consultado el 17 de mayo de 2022).

aprobación. El proceso de aprobación de flujo de trabajo agrega una capa de control y documenta la decisión de política de acceso.

Aprovisionamiento de cuentas de usuario

Una vez que se desencadena un evento de aprovisionamiento y se evalúa la política para determinar qué atributos, derechos y privilegios de cuenta de usuario deben ser establecidos o modificados, esa información debe trasladarse al sistema objetivo para que se haga efectivo el cambio en la cuenta de usuario almacenada localmente allí. El cómo se realizan las modificaciones necesarias en el sistema objetivo constituye el acto mismo del aprovisionamiento. Fundamentalmente, el aprovisionamiento puede tomar dos formas:

- Automático
- Manual

Automático

El aprovisionamiento automático de cuentas de usuario es el proceso de crear y mantener una cuenta de usuario en el sistema objetivo usando un procesamiento automático. Para automatizar el proceso de aprovisionamiento de cuenta de usuarios, el sistema objetivo debe proveer una API de administración de usuarios u otro tipo de solución de aprovisionamiento de usuarios que cree, administre y desactive/elimine cuentas de usuario sistemáticamente.

El aprovisionamiento automático de cuentas de usuario en sistemas objetivo es el propósito máximo de las tecnologías de aprovisionamiento de usuarios, pero tiene sus desafíos. Cada sistema objetivo es una isla y el sistema de aprovisionamiento de usuarios debe estar conectado con varios sistemas objetivo lo cual puede tornarse pesado.

Manual

El aprovisionamiento manual requiere la intervención humana para la aplicación de un cambio en la cuenta de usuario en el sistema objetivo. Esta intervención suele ser el envío de los detalles de un evento de aprovisionamiento de usuario a un equipo o persona que toma esa información y manualmente la ingresa en el sistema objetivo a través de las interfaces de administración de usuarios únicos en el sistema objetivo. Dicha información puede ser enviada por correo electrónico o en un ticket de tareas.

El aprovisionamiento manual introduce humanos en un paso fundamental del aprovisionamiento de usuarios, generando dos riesgos concretos. El primero es que la persona que opera manualmente el sistema objetivo para crear o modificar cuentas de usuario es, por la definición misma de su trabajo, un usuario con privilegios elevados. El segundo es que el aprovisionamiento manual introduce el riesgo del error humano. La persona podría leer o tipear mal un atributo, derecho o privilegio configurando erróneamente la cuenta de usuario en el sistema objetivo. Si bien el resultado de esto

puede ser una molestia menor, como un nombre de un usuario mal deletreado, también podría conducir a la asignación incorrecta de privilegios o incluso a una combinación tóxica de derechos.

Frente a los riesgos mencionados, es válido cuestionar el uso del aprovisionamiento manual. Sin embargo, el aprovisionamiento manual es necesario porque no todos los sistemas objetivo tienen las API para que los conectores de aprovisionamiento puedan conectarse. Un ejemplo de esto son esos sistemas de contabilidad general desarrollados localmente que se ejecutan en sistemas operativos extremadamente viejos. Otro ejemplo son las situaciones en las que el sistema objetivo es gestionado por un proveedor de servicios y el equipo de identidad no tiene acceso directo a ese proveedor de servicios. En ese caso, una modificación en una cuenta de usuario debe ser enviada por correo electrónico o mediante un ticket al proveedor de servicios desencadenando la ejecución del cambio.

El aprovisionamiento manual es preferible en los casos en los que no vale la pena hacer el esfuerzo de implementar un sistema automático. Pensemos en una aplicación que tiene muy pocos usuarios, derechos o cambios requeridos. Un equipo de identidad puede decidir que no vale la pena implementar (o quizás incluso desarrollar) un conector de aprovisionamiento automático y por lo tanto preferir aceptar el riesgo del error humano que conlleva el aprovisionamiento manual. La mejor práctica indica que se debe usar el aprovisionamiento automático en sistemas de gran volumen (muchos usuarios), gran velocidad (cambios frecuentes en las cuentas de usuarios) y valor elevado (cruciales, material financiero, etc.). En cambio, automatizar cada uno de los sistemas en la empresa no es una buena práctica ya que los altos costos de mantenimiento de los conectores no lo valen.

El rol de los estándares

La industria de la identidad reconoció que la proliferación de las API de administración de usuarios propietarias conduciría a una falta de aprovisionamiento automático dificultando que las organizaciones puedan mitigar los riesgos inherentes al aprovisionamiento manual de usuarios. Empezando por el Lenguaje de Marcado de Servicios de Directorio (DSML, por sus siglas en inglés) en 1999, seguido del Lenguaje de Marcado de Aprovisionamiento de Servicios (SPML, por sus siglas en inglés)[5] en 2003, y finalmente con la llegada del Sistema de administración de identidades entre dominios (SCIM)[6] en 2011, la industria desarrolló varios estándares. La última versión de SCIM, la versión 2, tuvo una adopción significativa y,

[5] En un afán por la transparencia, queremos notar que uno de los autores de este artículo contribuyó en el desarrollo del estándar SPML v2 y se disculpa por los errores que no sabía que estaba cometiendo en ese momento.

[6] En un afán por la transparencia, queremos notar que uno de los autores de este artículo contribuyó en el desarrollo del estándar SCIM v2 y está orgulloso de su trabajo.

en la segunda mitad del año 2021, la comunidad de estándares dió señales de estar interesada en realizar mejoras mayores. El hecho de que haya habido al menos tres estándares diferentes con múltiples versiones cada uno es la viva prueba de lo desafiante que es desarrollar estándares viables y de lo cambiante que es el mundo del desarrollo de aplicaciones.

Para que un estándar de aprovisionamiento de usuarios sea considerado exitoso debe ser adoptado tanto por los proveedores de sistemas de aprovisionamiento de usuarios como por los vendedores de aplicaciones. Este desafío de "se necesitan dos" ha impedido una adopción masiva, especialmente en la era de software local. La era de la computación en la nube y SaaS se vió marcada por un incremento en el número de proveedores de servicios y de proveedores de tecnología de aprovisionamiento de usuarios dispuestos a usar SCIM v2. Si la organización TI del lector de este artículo está desarrollando aplicaciones personalizadas, vale la pena investigar la implementación de SCIM v2 en esas aplicaciones para facilitar el aprovisionamiento automático de usuarios, especialmente en el caso de aplicaciones de gran volumen, gran velocidad y valor elevado.

¿Por qué es desafiante el aprovisionamiento de usuarios?

Los sistemas de aprovisionamiento de usuarios han estado en el mercado por más de veinte años. En ese tiempo se han ganado la reputación de ser complicados y costosos de implementar y para muchas organizaciones los beneficios de tal inversión no son evidentes. ¿A qué se debe esto?

El aprovisionamiento de usuarios se parece de muchas maneras a las tecnologías de integración de datos. Al igual que las tecnologías de integración de datos, los sistemas de aprovisionamiento de usuarios agrupan y sincronizan datos con muchos y variados sistemas y servicios de entorno. Cada conexión nueva agrega un nivel de complejidad. El proceso de incorporar una sola aplicación en un entorno de aprovisionamiento requiere un entendimiento de las API de administración de usuarios de la aplicación y de su constructo de autorización, la implementación de un conector, la configuración de políticas de acceso y la implementación de políticas y procedimientos de administración de usuarios (por ej., reglas que impiden la creación o administración de usuarios directamente dentro de la aplicación). Incorporar una aplicación puede ser complejo; imagina la complejidad que implica tener cientos o miles de aplicaciones en tu entorno.

Otro aspecto que puede ser problemático es la calidad de los datos generados por la fuente acreditada (SOR). Idealmente, solo hay una SOR acreditada pero no siempre es el caso. Cuando la información proviene de múltiples fuentes acreditadas, pueden ocurrir colisiones de datos. Además, los administradores y usuarios de la SOR pueden no entender los efectos posteriores que pueden tener los datos insuficientes y de baja calidad. Por ejemplo, pueden dejar campos incompletos, ingresar datos inexactos o retrasar los eventos desencadenantes. Todo esto tiene consecuencias en la capacidad del sistema de

aprovisionamiento para actualizar los registros de identidad y los derechos de acceso de forma correcta. Gestionar los procesos de calidad de los datos puede ser agotador para los profesionales de la identidad.

Otro desafío común es la definición de políticas. Los profesionales de la identidad son responsables de desarrollar políticas de acceso (reglas/roles) pero no toman las decisiones de acceso. Las decisiones de acceso las toma la línea de negocio que trabaja juntamente con los departamentos de auditoría, legal, gobernanza, gestión de riesgo y cumplimiento (GRC, por sus siglas en inglés), etc. La recopilación de toda esta información necesaria para desarrollar las políticas de aprovisionamiento y definir roles, es una tarea grande.

Por último, pero no por eso menos importante, el mantenimiento de un catálogo de derechos puede ser una tarea difícil. Una sola organización puede tener cientos de miles e incluso millones de derechos. No se debe subestimar la tarea de recopilar los derechos y sus metadatos.

Si bien las ventajas del aprovisionamiento automático de cuentas de usuario son evidentes, su implementación puede ser desafiante. Los profesionales de la identidad deben tener el apoyo ejecutivo de la organización y definir expectativas apropiadas, crear un proceso estructurado para la incorporación de aplicaciones (por ej., recursos dedicados, formulario de ingreso/evaluaciones, automatización, etc.), y establecer indicadores clave de performance que muestren el progreso continuo.

La próxima generación, un abordaje híbrido al aprovisionamiento

Si bien las tecnologías de aprovisionamiento de usuarios existen desde hace bastante tiempo, fueron desarrolladas en una época en la que los entornos TI eran mucho más contenidos. Los sistemas objetivo y los sistemas de registro estaban alojados localmente y los usuarios eran principalmente empleados que accedían a recursos en las instalaciones de la organización.

Tecnologías como las soluciones en la nube, los dispositivos móviles y el trabajo remoto entre otros, cambiaron la dinámica del aprovisionamiento de usuarios. Ahora los sistemas acreditados y los sistemas objetivo están alojados en la nube (y localmente), y hay usuarios externos accediendo a recursos internos.

En los modelos de seguridad tradicionales, el aprovisionamiento es una función “admin-tiempo” (los usuarios son pre-aprovisionados en los sistemas por un administrador). Esto contrasta con las tecnologías de autenticación y autorización que son funciones de tiempo de ejecución que ocurren en el momento que el usuario está iniciando sesión en el

sistema. Las tecnologías de seguridad como SIEM, DLP y la detección de amenazas entran en juego una vez que el usuario ya inició sesión.

Los modelos de seguridad modernos que incluyen el acceso remoto, la computación en la nube y los principios de seguridad de confianza cero, requieren un nuevo abordaje al aprovisionamiento de usuarios: un abordaje "Justo a Tiempo" (JIT, por sus siglas en inglés) de mínimo privilegio. Este abordaje moderno al aprovisionamiento significa que en lugar de pre-aprovisionar usuarios con una función admin-tiempo, los usuarios son aprovisionados en el tiempo de ejecución y se les otorgan los mínimos privilegios necesarios para la realización de una tarea. Por ende, las organizaciones están implementando un abordaje híbrido al aprovisionamiento que comprende una mezcla de conectores tradicionales basados en API, conectores basados en SAML/OIDC y conectores basados en SCIM.

Una arquitectura de aprovisionamiento híbrida permite que las organizaciones puedan pre-aprovisionar un conjunto de aplicaciones (generalmente aplicaciones locales) y usen conectores basados en OIDC, SAML y SCIM para habilitar un aprovisionamiento JIT (principalmente usado en casos de uso de productos en la nube y SaaS).

Biografías de los autores

Ian Glazer: COO, Gestión de Producto, Salesforce

Ian Glazer es vicepresidente ejecutivo de gestión de productos de identidad en Salesforce. Sus responsabilidades incluyen la dirección de los equipos de gestión de productos, estrategia de producto y estándares de identidad. Previo a esto, se desempeñó como vicepresidente de investigación y gestor de agenda de los equipos de estrategias de identidad y privacidad en Gartner, donde supervisó la totalidad de las investigaciones del equipo. Es cofundador de IDPro, la organización profesional para la administración de identidades digitales, y trabaja para aportar más servicios y valor al grupo de miembros de IDPro, recaudar fondos para la organización y fomentar que los profesionales de la

administración de identidades colaboren los unos con los otros. A lo largo de su carrera en la industria de la identidad, ha sido coautor de una patente sobre aprovisionamiento federado de usuarios, coautor y colaborador de especificaciones sobre el aprovisionamiento de usuarios y es un destacado bloguero, orador y fotógrafo aficionado.

Lori Robinson

Lori Robinson es vicepresidenta de la gestión de productos de identidad corporativa en Salesforce donde dirige un equipo responsable del programa de administración de identidades corporativas. Antes de formar parte de Salesforce, fue vicepresidenta de producto y estrategia de Mercado en SailPoint. También se desempeñó como vicepresidenta administrativa y analista en Gartner donde se hacía cargo de la administración y gobernanza de identidades, la administración de accesos privilegiados y de los mercados de consumidores de la IAM. Lori es una reconocida referente de la industria, oradora y autora. Le apasiona generar oportunidades para las mujeres en las TICs y condujo varios grupos de usuarias, mesas redondas y eventos destinados a las mujeres de la industria de la identidad.

Mat Hamlin: V.P., Gestión de Producto, Platform Identity, Salesforce

Mat Hamlin es el Vicepresidente de Gestión de Producto para Platform Identity en Salesforce. Sus responsabilidades incluyen la dirección del equipo de gestión de producto, estrategia de producto e innovación de los Servicios de Identidad en la plataforma central de Salesforce. Antes de formar parte de Salesforce, se desempeñó en múltiples roles de gestión de producto en SailPoint, Oracle y Sun Microsystems; enfocándose en el Aprovisionamiento de Usuarios, la Gobernanza de Accesos y la Administración de Roles Corporativos.