Introducción a la identidad: Parte 1: tiempo de administración (v2)

Por Ian Glazer, editado por Espen Bago

Para comentar este artículo, visite nuestro repositorio de GitHub y reporte un problema.

Tabla de contenidos

Resumen

Este artículo presenta los conceptos de identidad digital y gestión de identidad y acceso (IAM). También analiza los grupos de interés a los que los profesionales de la identidad brindan servicio, compara y contrasta los casos de uso de identidad de empresa a empleado (B2E, por sus siglas en inglés) y de empresa a consumidor (B2C, por sus siglas en inglés), y considera las tecnologías IAM desde la perspectiva de las tecnologías administrativas o de tiempo de administración. A modo de comparación, se mencionan las tecnologías IAM y los casos de uso que se centran en interacciones activas en vivo o en tiempo de ejecución.

Introducción: cómo abordar la identidad y la IAM

La identidad digital es un gran tema; afecta todos los aspectos de los sistemas y servicios técnicos de una empresa. Este artículo no ofrecerá una taxonomía de identidad. En cambio, es de la idea de que cada individuo y organización probablemente abordará la identidad digital desde una perspectiva y nivel de comprensión diferentes, dadas sus necesidades específicas (aunque perfectamente válidas) para su sistema o servicio de identidad local.

La identidad es un término a menudo debatido. Tanto los profesionales veteranos como los nuevos miembros de la industria luchan con el significado de “identidad”. Este artículo sugiere que no existe una definición única y definitiva de identidad. En cambio, alienta al lector a considerar su propio contexto local y adaptar las definiciones aproximadas aquí para que se ajusten a su organización.

Este artículo adopta un enfoque contextual, muestra algunas formas posibles de dividir el mundo de IAM y ofrece algunos ejemplos de uso en contexto. Se debe tener en cuenta que IAM no se trata solo de tecnología. Se trata de la profesión misma y de nosotros como profesionales.

Terminología

Certificación de acceso: la certificación es la revisión continua de quién tiene qué acceso (es decir, el proceso comercial para verificar que los derechos de acceso sean correctos).

Gestión de derechos: catalogar y gestionar todos los accesos que pueda tener una cuenta. Este es el proceso de negocio para proporcionar acceso.

Análisis e inteligencia de identidad (IdA, por sus siglas en inglés): el análisis de identidad y la inteligencia significan observar los datos de derechos, observar su asignación y tratar de descubrir y definir el riesgo. IdA proporciona un enfoque basado en riesgos para gestionar las identidades y el acceso del sistema, con la intención de centralizar la gobernanza, la visibilidad y la generación de informes para el riesgo basado en el acceso.

Gobernanza y administración de identidades: una disciplina que se centra en la gestión del ciclo de vida de las identidades y el control de acceso desde una perspectiva administrativa.

Prueba de identidad: acumulación de evidencia para respaldar "quién es esta persona". La prueba de identidad es la última parte, pero no menos importante, de esta sección de tiempo de administración. Este es el proceso de recopilar y verificar información sobre una persona con el fin de proporcionar una cuenta o la credencial correspondiente. Por lo general, esto se realiza antes de que se cree una cuenta, se emita la credencial o se otorgue un privilegio especial.

Incorporaciones, traslados y bajas (JML, *joiners, movers and leavers*): El ciclo de vida JML de la identidad de un empleado considera tres etapas en el ciclo de vida: incorporarse a la organización, moverse dentro de la organización y abandonar la organización.

Gestión de cuentas privilegiadas: centrada en un control especial para el acceso riesgoso de alto nivel. La gestión de cuentas privilegiadas (PAM, por sus siglas en inglés) es un mecanismo para controlar esas cuentas especiales.

Gestión de roles: una forma de agrupar reglas de acceso para hacerlas más manejables

Control de acceso basado en roles (RBAC, por sus siglas en inglés): el uso de roles en tiempo de ejecución; una forma de gobernar quién tiene acceso a qué mediante el uso de roles.

Fuentes de "verdad": donde viven datos autorizados sobre las personas.

Aprovisionamiento de usuarios y gestión del ciclo de vida: cómo los registros de los usuarios llegan a donde deben estar, pero solo durante el tiempo necesario.

Grupos de interés - ¿a quién servimos?

Es fácil que los árboles nos impidan ver el bosque en el mundo de IAM, ya que hay muchos pequeños fragmentos, matices, abreviaturas y factores aleatorios. Pensar en el destinatario final para quien se realiza el trabajo de identidad es una manera de mantener el foco en el panorama general.

Hay una variedad de grupos diferentes a los que servimos como profesionales de la identidad, lo que significa que se necesita una variedad de tecnologías diferentes para ayudarlos. Estos grupos pueden incluir al empleado tradicional o grupos más complejos como clientes, empleados no remunerados, contratistas y aquellos que no se encuentran dentro de los límites habituales de una organización.

Ya sea que ese grupo incluya empleados, socios comerciales, ciudadanos o estudiantes, en todo lo que haga como profesional de la identidad, debe tener en cuenta la experiencia del individuo. Tener en mente al individuo otorga más contexto y una visión más amplia. Este enfoque le ayuda a darse cuenta de que "Oye, la razón por la que estoy haciendo este proyecto de aprovisionamiento automatizado es que estamos a punto de contratar a 5000 personas nuevas y queremos que sean productivas desde su primer día de trabajo".

De empresa a empleado (B2E): hacer que los empleados sean productivos

Para los empleados y contratistas, la principal preocupación es la productividad. La empresa quiere que su personal sea productivo desde el primer día y quiere que se les elimine el acceso inmediatamente después de su salida. La misión aquí es conseguir el acceso adecuado a las personas adecuadas en el lugar adecuado y en el momento adecuado. Eso es lo que los profesionales de la identidad están tratando de hacer: darles a las personas el acceso adecuado para que puedan ser productivas.

La mayoría de las veces, el departamento de Recursos Humanos (RRHH) está a cargo de los datos de los empleados y el sistema de RRHH es la fuente de verdad. Los desafíos con esto incluyen:

- Posibles problemas de integridad de los datos.
- La organización puede tener múltiples sistemas de recursos humanos.
- Otros datos que no son de empleados pueden (¡o no!) residir en este sistema de recursos humanos.

Independientemente de los desafíos involucrados, esta suele ser nuestra fuente de verdad porque si alguien aparece en el sistema de recursos humanos, se le pagará, por lo que debemos asegurarnos de que sea productivo; esa es una fuente de verdad muy práctica.

Si hay una cita en la que pensar en relación con la identidad de los empleados, es "¿Quién tiene acceso a qué?" Se trata de garantizar que las personas adecuadas tengan acceso al material adecuado. El ciclo de vida que rige, en este caso, es el conocido como modelo JML.

- Las personas se **incorporan** a una organización.
- Sus roles cambian a medida que avanzan o se **trasladan** dentro de la organización.
- Después de un tiempo, se van y se les da de **baja** en una organización.

El sistema (o sistemas) de recursos humanos actúa como una fuente de verdad para los eventos del ciclo de vida de los empleados y los datos relacionados, como códigos de roles o puestos de trabajo.

Aunque los contratistas tienen necesidades similares de identidad y acceso, es posible que no compartan las mismas fuentes de información. Puede haber casos en los que el sistema de recursos humanos no incluya a la población de contratistas. En muchas empresas, encontrar una fuente única de verdad para un contratista puede ser un verdadero desafío. Algunos usan su sistema de adquisiciones, otros usan sistemas personalizados, algunos usan hojas de cálculo y algunos incluso usan su sistema de aprovisionamiento de cuentas de usuario. Para los trabajadores temporales o estacionales, puede ser más eficiente utilizar un proveedor de identidad de redes sociales para incorporar este tipo de personal a corto plazo, siempre que la organización pueda obtener el nivel de seguridad necesario.

Empresa a empresa (B2B): conexión con socios

El siguiente grupo es el de nuestros socios comerciales. En todas las industrias, necesitamos conectarnos con ellos. Esta conexión realmente consiste en asegurarse de que los miembros de tu cadena de suministro (o valor) puedan interactuar contigo: les están dando aplicaciones para que las utilicen para trabajar contigo, pero ¿de dónde provienen los registros de identidad de estas personas?

Lo ideal es que los socios lleguen con los datos de identidad proporcionados por tu organización. En ese caso, estamos tratando con el sistema de registro del socio comercial, probablemente tu sistema de recursos humanos, y te encuentras a un grado de distancia de él. Esta distancia a menudo significa que has delegado la administración de la gestión del ciclo de vida. Sin embargo, en aplicaciones de alto riesgo, es posible que el propietario de la aplicación desee controlar el acceso en lugar de confiar en el socio comercial.

Desde una perspectiva de IAM, B2B y B2E son muy similares. La diferencia clave es la fuente de verdad. A menudo, la empresa no cuenta con un sistema que rastree específicamente a las personas que son empleados de sus socios comerciales. En cambio, delegan la gestión de esas personas a otros sistemas, ya sea en su propia empresa o en la organización del socio. La mayoría de las veces, los sistemas IAM se convierten de facto en una fuente de verdad para las identidades de los socios individuales.

Empresa a Consumidor (B2C): comprometerse digitalmente

Por último, pero no menos importante, está la Empresa a Consumidor (B2C, por sus siglas en inglés). B2C le dice a la gente todas las cosas maravillosas que tu organización hace o vende. Cuando hablas con las personas de tu empresa que crean el servicio de cara al consumidor, a menudo los oirás describir la forma en que un consumidor interactúa de esta manera: “La persona hará esto y luego hará esto otro. " Y un profesional de la identidad haría preguntas como "¿Cómo llegó esa persona allí?" y la respuesta sería: "Bueno, ella inició sesión". Y de repente, te das cuenta de que las personas que crean el servicio no tienen idea de lo que hacemos nosotros, como profesionales de la identidad. Esta falta de comprensión es una oportunidad increíble para que esa cosa increíble que hace tu organización les llegue a las personas adecuadas. Esa es tu misión.

Pero en este mundo, los ciclos de vida son diferentes. Se trata del individuo, del ciudadano, del consumidor. En muchos sentidos, ellos tienen el control del ciclo de vida, no tú, y debes poder adaptarte a eso.

La misión de la empresa es: "Quiero ofrecer una experiencia increíble". Nadie está en el negocio para simplemente darle a la gente una cuenta y dar por terminado el asunto. En un entorno B2C, no se puede decir: “¡Genial! Puedes iniciar sesión, ya terminé aquí”. No, eso es sólo el comienzo de la relación. Hay un enfoque en la experiencia del cliente y nosotros, como profesionales de la identidad, estamos ayudando a brindar esa experiencia. Somos una vía de acceso fundamental para ello.

Los casos de uso de B2C ilustran que nosotros, como profesionales de la identidad, no estamos solos en nuestras empresas. No podemos hacer nuestro trabajo sin nuestros pares en seguridad y privacidad. Hay tres patas en este taburete para que funcione. Para la privacidad, la identidad proporciona controles operativos, especialmente en el contexto del acceso a los datos. Y para la seguridad, la identidad ofrece un marco valioso. Ponemos el "quién" en las preguntas como "quién diablos está en mi red". Entonces, si estás trabajando en un entorno B2C (o B2B) y no has conocido a tus pares en el equipo de privacidad y seguridad, búscalos. Tienen herramientas valiosas que podrás mejorar y que también pueden ayudarte a ti.

Tecnologías involucradas: tiempo de administración versus tiempo de ejecución

Una vez establecidos los grupos de interés a los que servimos, es hora de analizar algunas de las tecnologías que utilizamos para hacerlo. Un enfoque entre muchas formas válidas de clasificar las diversas tecnologías y términos es dividir el mundo en discusiones administrativas (o de tiempo de administración) y de tiempo de ejecución.

Esencialmente, las tecnologías y disciplinas utilizadas para configurar las cosas están en el lado del tiempo de administración, y las cosas que se utilizan cuando el usuario inicia sesión o pasa por un proceso de olvido de contraseña están en el lado del tiempo de ejecución.

Tecnologías de tiempo de administración

Las tres áreas principales dentro del ámbito del tiempo de administración son:

- Fuentes de "verdad": donde viven datos autorizados sobre las personas.
- Gobernanza y administración de identidades: una disciplina que realmente trata sobre la gestión del ciclo de vida y el control de acceso desde una perspectiva administrativa.

- Inteligencia y análisis de identidad: de particular interés para grandes empresas para ayudar a garantizar que el acceso sea correcto.

Dos áreas adicionales también son de tiempo de administración, pero no siempre caben en el mismo grupo. A algunos analistas de la industria les gusta agregar estas categorías:

- Gestión de cuentas privilegiadas: centrada en un control especial para el acceso riesgoso de alto nivel.
- Prueba de identidad: acumulación de pruebas que respalden "quién es" la persona.

Fuentes de "verdad"

¿Cómo sé quién es alguien? Puede que sea una pregunta demasiado difícil de responder desde una perspectiva tanto metafísica como práctica. En su lugar, podemos formularla así: "¿Cómo puedo encontrar registros autorizados y razonablemente buenos sobre las personas? Necesito enviar su cheque de pago a alguna parte". O "Necesito la dirección de envío de mi socio comercial. ¿Cómo encuentro estos datos? [i]

Para los empleados, la respuesta tiende a ser RRHH. Para los socios, tiende a ser ese administrador delegado a un paso de distancia de su sistema de recursos humanos. Y en el ámbito del consumidor, las cosas se complican más. En zonas de bajo riesgo, la respuesta es el individuo. Son la fuente autorizada de gran parte de la información que se utilizará. Para mayor comodidad, esto puede provenir de un perfil de redes sociales, por ejemplo. Pero en áreas de mayor riesgo, como las financieras o médicas, la respuesta puede incluir fuentes autorizadas como su institución de educación superior o su gobierno local. En un entorno educativo, un sistema de información estudiantil puede servir como fuente de verdad para los estudiantes.

Aquí, la calidad de los datos es un elemento esencial. Dependemos de los datos para hacer cosas como garantizar que las personas tengan el acceso adecuado. Pero los datos de la fuente de verdad no siempre son confiables, por lo que es posible que tengamos que operar bajo el supuesto de que pueden existir problemas de calidad de los datos.

Gobernanza y administración de identidad

Estas son las herramientas que gestionan quién tiene acceso a qué. Son las herramientas que dependen de una fuente de verdad (el quién) para gobernar los derechos (el acceso) en los sistemas de destino (el qué) a través de conectores.

Las herramientas de gobernanza y administración de las identidades (IGA, por sus siglas en inglés) tradicionalmente se centran más en empleados, contratistas o estudiantes. A menudo se puede considerar que estas herramientas son herramientas más tradicionales,

centradas en la empresa, relacionadas con los sistemas de planificación de recursos empresariales (ERP, por sus siglas en inglés).

Esta área es considerablemente más grande que las otras cinco áreas de la esfera del tiempo de administración, y cubriremos las siguientes subsecciones:

- Aprovisionamiento de usuarios y gestión del ciclo de vida: cómo los registros de usuarios llegan a donde deben estar, pero solo durante el tiempo que sea necesario.
- Gestión de derechos: el proceso empresarial para proporcionar acceso.
- Administración de funciones: una forma de agrupar reglas de acceso para hacerlas más manejables.
- Control de acceso basado en roles (RBAC, por sus siglas en inglés): el uso de roles en tiempo de ejecución.
- Certificación de acceso: el proceso empresarial para verificar que los derechos de acceso sean correctos.

Aprovisionamiento de usuarios y gestión del ciclo de vida

El aprovisionamiento de usuarios es el mecanismo que ayuda a crear, mantener y, eventualmente, eliminar cuentas de usuario en los sistemas de destino. Este mecanismo puede "escuchar" eventos de incorporación, traslado o baja de las fuentes de verdad (por ejemplo, un conector al sistema de recursos humanos que "escucha" eventos como la incorporación de un nuevo empleado). Luego, ese evento activa el sistema de aprovisionamiento para evaluar al usuario a través de reglas comerciales para realizar las acciones requeridas, como crear una nueva cuenta de usuario en *Active Directory*. El mecanismo también tiene reglas que describen cuáles son esas acciones desencadenadas, como comenzar a configurar el acceso en función de algunos atributos de los datos de los nuevos empleados. Por lo general, eso significa asignar derechos, lo que puede ser algo que requiera aprobación. Para derechos básicos como el acceso por "derecho de nacimiento", es posible que no necesitemos aprobación. Por ejemplo, todos los empleados deben tener acceso al paquete de productividad y al correo electrónico, ninguno de los cuales requiere aprobación. Si, por otro lado, alguien quiere obtener acceso al *mainframe* como administrador de sistemas, necesitará cierta aprobación. Existen ambos tipos (acceso que requiere aprobación explícita y acceso que no la requiere) en casi todas las organizaciones.

Un error común es intentar automatizar todo. ¡Debes evitar esto! Hay cientos, sino miles, de sistemas y servicios en tu empresa. Intentar automatizar el aprovisionamiento de todo eso solo reducirá tu rendimiento. Entonces, ¿qué debería automatizarse? Los candidatos para la automatización que debes identificar son los sistemas con la mayor población de usuarios o la mayor rotación en esos sistemas. La automatización es esencial para sistemas de gran volumen o alta velocidad. Otros candidatos son sistemas con demasiadas

solicitudes para que las administre su equipo de soporte técnico, o aquellos tan sensibles que deseas bloquear las reglas sobre quién tiene acceso a ellos. En estos casos, tiene sentido automatizarlos.

Los sistemas de acceso desde el primer día son excelentes candidatos para la automatización. En parte porque hasta cierto punto no es controvertido; obtienes un correo electrónico, ingresas al portal del empleado, tal vez obtengas una VPN. La creación de estas cuentas de usuario debe realizarse para todos los empleados nuevos y representa una gran carga administrativa lista para la automatización.

Después del primer día de incorporación y para la gran cantidad de sistemas restantes, proporcionarás acceso adicional manualmente. Esto significa que las personas solicitarán acceso y/o tú crearás la cuenta manualmente (a menudo porque no necesitas hacerlo con mucha frecuencia). Y en algunos casos, el sistema en el que deseas crear una cuenta existe fuera de tu esfera de influencia directa; no tendrás un conector al sistema. Para tales sistemas, la única forma de acceder es abriendo un *ticket* de soporte, y un humano tendrá que acceder directamente al sistema para crear o cambiar la cuenta de usuario. Por lo general, no es necesario automatizarlos.

Por último, los sistemas de aprovisionamiento suelen participar en la configuración de contraseñas. Esta participación significa que los sistemas de aprovisionamiento a menudo necesitan tener reglas para crear contraseñas. Eso plantea todo tipo de desafíos porque diferentes sistemas pueden tener reglas internas y capacidades de contraseña radicalmente diferentes. Por ejemplo, es posible que tengas una regla de contenido de contraseña que exija la inclusión de un carácter especial. Debido a las tendencias del sistema, una persona podría proporcionar una contraseña con un carácter especial que la base de datos Oracle no podría aceptar, pero *Active Directory* sí. Los sistemas de aprovisionamiento de usuarios (o gestión de contraseñas) tienen que afrontar estos problemas potenciales de la forma más elegante posible.

Gestión de derechos

Ahora tenemos una fuente de verdad y los usuarios fluyen hacia un repositorio de datos, y eso activa nuestros sistemas de aprovisionamiento de usuarios y comienza a crear usuarios en nuestras aplicaciones o servicios de destino. Pero no basta sólo con crear una cuenta de usuario; también tenemos que saber qué puede hacer esa cuenta. Este conjunto de acciones es lo que llamamos gestión de derechos. La gestión de derechos puede volverse con rapidez realmente detallada porque pueden llegar a ser muchísimos pequeños privilegios los que rigen lo que un usuario puede hacer en un sistema. No es extraño tener cientos, sino miles, de privilegios individuales en un sistema. Esos privilegios a menudo se agregan en grupos o roles de usuarios, que también pueden llegar a ser bastante numerosos. Es como granos de arena en la playa, por eso intentamos agregarlos. Imagina que tienes tres empleados, un sistema y cuatro privilegios: crear orden de compra (PO, por sus siglas en inglés), actualizar la PO, leer la PO y eliminar la PO. Es posible

conectar a cada persona con el conjunto correcto de privilegios, pero esto se vuelve inmanejable muy rápidamente.

Ahí es donde entran las capas de abstracción: colocamos algo entre el usuario y los privilegios llamado derecho. Decimos: "Esto le permite gestionar órdenes de compra". Y son estas cosas las que reparte el sistema de aprovisionamiento, en lugar de los privilegios detallados en sí, porque hay demasiados privilegios discretos para poder darles seguimiento. Abstraemos los detalles y en su lugar decimos: "Aquí hay una habilidad" o "Aquí hay algo asociado con su responsabilidad laboral". Desafortunadamente, esos privilegios discretos y detallados aún deben existir para permitir el nivel de granularidad que requieren los procesos de negocios de una organización y para proporcionar el nivel de instrucción al sistema que se puede codificar en el entorno.

La gestión de derechos significa catalogar todos los accesos que una persona puede tener, lo que implica una tarea enorme. Por ejemplo, un banco mediano puede tener diez sistemas principales (pero a menudo muchos más), lo que significa que puede tener miles y miles de privilegios, que se suman en aproximadamente mil derechos. Luego hay que descubrir cómo adaptarlo a las necesidades del negocio. La gestión de derechos es este proceso de catalogación.

Lo ideal sería agrupar los privilegios en conjuntos que tengan cierto sentido para las personas y la organización. Por ejemplo, imagina que deseas reunir todos los derechos que necesitaría alguien que trabaja en compras. O que deseas asegurarte de haber reunido los derechos relevantes a los que tiene acceso un socio comercial (en el nivel Oro pero no en el nivel Plata). Este nivel de eficiencia es en lo que tú y tus colegas de identidad están trabajando para que el acceso a los recursos empresariales sea manejable.

También tiende a ser un trabajo obligatorio si alguna vez vas a realizar un análisis de segregación de funciones[ii], por ejemplo, para el cumplimiento de Sarbanes-Oxley (SOX)[iii] o los requisitos de cumplimiento del Reglamento General de Protección de Datos (RGPD)[iv]. donde tenemos que identificar combinaciones de accesos que en conjunto son peligrosos. Por ejemplo, las personas que pueden autorizar pagos a socios no deberían poder crear un socio fraudulento y pagarles.

Gestión de roles

Pero incluso cuando hayamos reducido estos derechos a un nivel en el que sean entidades manejables en sí mismas, utilizarlos de manera efectiva será un gran desafío. La respuesta a ese desafío para muchas organizaciones, aunque no para todas, es intentar hacer algo llamado gestión de roles. Es posible que hayas oído hablar de esto como el control de acceso basado en roles (RBAC, por sus siglas en inglés). La esencia de esto es la siguiente: en algunas organizaciones, las funciones laborales son muy regulares. Las funciones

laborales regulares se encuentran con mayor frecuencia en organizaciones jerárquicas. En el otro extremo de la escala, esto funciona bastante mal en organizaciones matriciales; esto se debe a que es difícil identificar, por ejemplo, las tres principales responsabilidades laborales, ya que siempre están cambiando.

La gestión de roles puede resultar útil para decir: "Este tipo de responsabilidades laborales necesita este tipo de acceso, así que lo llamaremos un rol". Además, a veces tienes algo llamado rol técnico, que dice: "Aquí están los bits de bajo nivel que necesitarás para hacer tu trabajo", y se convierte en un paquete útil para asignar a las personas. Imagina los roles como una agrupación a la que podrías brindar acceso de manera común. Solo debes crear roles si vas a aprovisionar o controlar el acceso a un grupo de manera diferente. En el nivel más alto, sólo podrías tener un puñado de roles y deberías revisarlos periódicamente a medida que tu organización evoluciona.

Control de acceso basado en roles

RBAC es solo una forma de gobernar quién tiene acceso a qué mediante el uso de roles. No hay necesidad de pensar demasiado en ello. Funciona muy bien en organizaciones regulares, jerárquicas y homogéneas. No es sorprendente que funcione muy bien para lugares como el Departamento de Defensa de Estados Unidos. No funciona muy bien para una empresa emergente de 150 personas; no lo intentes.

Cuando se piensa demasiado en RBAC, o con el tiempo en general, se puede producir lo que llamamos una “explosión de roles”, en la que se tienen más roles que personas. Algunos veteranos resentidos dicen: “Oh, sí, sobreviví a eso. Me dijeron que era una buena idea. Fue una pésima idea”. Trata de evitar esta situación; rara vez termina bien.

Certificación de acceso

Llegado a este punto, la gente tiene acceso. Son productivos desde el primer día. Son productivos el segundo día. Al tercer día, empiezan a convertirse en una amenaza privilegiada porque tienen demasiado acceso. Y la mejor manera de conseguir cada vez más capacidades en una empresa es simplemente cambiar de trabajo. Pasas de hacer este trabajo a otro, y si tus reglas de negocio no impedían explícitamente la continuación del acceso, la experiencia demuestra que no pierdes tu acceso anterior, simplemente lo mantienes encima de los nuevos accesos.

Otro ejemplo de acumulación de accesos es cuando incorporas a alguien nuevo, con la temida duda de "¿a qué otra persona deberíamos emular tu acceso?". Cualquiera que haya pasado por algún tipo de auditoría de seguridad de TI sabe lo horrible que puede ser una auditoría. Comúnmente, la respuesta a la pregunta de quién modelar un conjunto de nuevos accesos para otorgarle a un nuevo empleado es: su jefe. Es probable que el jefe sea la mayor fuente de violaciones de acceso porque ha acumulado acceso a lo largo de los

años. Por lo tanto, sería la peor persona a la que emular, desde una perspectiva de gestión de riesgos.

La certificación es la revisión continua de quién tiene qué acceso, proceso que se popularizó con la introducción de la Ley Sarbanes Oxley (SOX) en Estados Unidos. Es una gran herramienta para evitar que las personas conserven el acceso que ya no necesitan. Un auditor podría decir que esto debería hacerse trimestralmente, algo que rápidamente resulta muy agotador. Existen mejores métodos como activar revisiones basadas en cambios en los derechos, cambios en el riesgo general del usuario o intentar detectar si alguien se desvía de una norma. En otras palabras, queremos certificar si, en comparación con un conjunto de pares, eres un caso atípico. Queremos descubrir por qué es así. Es una manera poderosa de asegurarse de no tener problemas con el acceso y los derechos que has asignado de forma no automatizada.

Todos los elementos mencionados se suman a una gran cantidad de datos que fluyen. El total de todos los usuarios, multiplicados por todos los sistemas, multiplicados por todos los derechos, multiplicados por todos los roles, multiplicados por todos los privilegios, puede llegar a ser asombroso. ¿Cómo podemos darle sentido a todo esto?

Análisis de identidad

Una de las formas es a través del análisis de identidad (IdA, por sus siglas en inglés) y la inteligencia, que es más que simplemente informar sobre "quién tiene acceso a qué".

El análisis de identidad y la inteligencia significan observar los datos de derechos, observar su asignación y tratar de descubrir y definir cómo se ve el riesgo. ¿Cómo es un usuario normal? Comparado con eso, ¿cómo es un usuario con muchos privilegios? ¿Cómo es el modelo de administrador de sistemas en comparación con el de un desarrollador, alguien que trabaja en finanzas o alguien que trabaja en el campo de ventas de una organización?

El objetivo es encontrar puntos en común de valores atípicos entre las poblaciones de usuarios y comprender cómo se ve el riesgo relacionado con el acceso en la organización. Otros objetivos de IdA incluyen poder agrupar derechos asignados comúnmente como roles candidatos, identificar usuarios con exceso de privilegios y descubrir derechos de acceso indocumentados con altos privilegios asignados a cuentas normales sin privilegios. IdA también puede medir e informar con precisión sobre la postura de riesgo de usuarios, cuentas, derechos, aplicaciones, departamentos y organizaciones.

IdA proporciona un enfoque basado en riesgos para gestionar las identidades y el acceso del sistema, con la intención de centralizar la gobernanza, la visibilidad y la generación de informes para el riesgo basado en el acceso. Utiliza puntuaciones de riesgo dinámicas y análisis avanzados para determinar el nivel de riesgo asociado y derivar indicadores clave para automatizar el aprovisionamiento, desaprovisionamiento, autenticación y gestión de

acceso privilegiado de cuentas. Este enfoque reduce la superficie de ataque a la identidad al identificar (para su reparación) accesos innecesarios, no utilizados y atípicos.

Otra característica de esta función de determinación de riesgos en tiempo de administración es que los indicadores y datos que produce pueden integrarse y utilizarse en sus sistemas de tiempo de ejecución. Por ejemplo, durante el proceso de inicio de sesión: si sabemos que una persona no es particularmente riesgosa, es posible que no sea necesario cuestionarse por factores de autenticación adicionales. Pero si, por otro lado, esa persona tiene muchos privilegios y poder en los sistemas, y tal vez se desvía de la norma en su puesto de trabajo, entonces es posible que deba proporcionar una verificación adicional. Un análisis de determinación de riesgos en tiempo de ejecución como este puede automatizarse parcial o totalmente, dependiendo de la calidad de los datos del indicador y la madurez de la organización que los utiliza.

Gestión de cuentas privilegiadas

Algunas de las cuentas de usuario existentes son especiales. Sus cuentas de administrador de sistemas, sus cuentas raíz, etc. Estas cuentas no están necesariamente vinculadas a personas. Pero son cuentas de usuarios súper privilegiados. Es posible que tengamos todo un equipo de personas que deban actuar como administradores raíz. La gestión de cuentas privilegiadas (PAM, por sus siglas en inglés) es un mecanismo para controlar esas cuentas especiales. Básicamente, puedes registrarlos y retirarlos según sea necesario: "Oye, necesito entrar y aplicar un parche de día cero, así que debo actuar como administrador raíz para esto", y el sistema otorgará el acceso relevante para esa finalidad, previa validación de quién es el usuario. También puede grabar la pantalla, de modo que a medida que el usuario realiza sus acciones, se registra lo que sucede. Un caso de uso para esto podría ser cuando tenemos un proveedor de servicios externo que viene y realiza el mantenimiento de equipos especializados, donde necesitamos tener un registro de auditoría de las acciones que tomaron. Este registro sería como la función de registro en la gestión de cuentas privilegiadas. Otra función importante es codificar la contraseña de estas cuentas especiales, de modo que nadie conserve la contraseña de la cuenta raíz o de administrador del sistema una vez finalizado el trabajo, como el trabajo de parche en el ejemplo anterior.

Prueba de identidad

La prueba de identidad es la última parte, pero no menos importante, de esta sección de tiempo de administración. Este es el proceso de recopilar y verificar información sobre una persona con el fin de proporcionar una cuenta o la credencial correspondiente. Por lo general, esto se realiza antes de que se cree una cuenta, se emita la credencial o se otorgue un privilegio especial. También tiende a ser un proceso más largo la primera vez que nos encontramos con un individuo en particular, a diferencia de la prueba secundaria requerida para propósitos de recuperación de cuenta.

El proceso se encuentra a menudo en industrias reguladas, como la bancaria, con requisitos para conocer a su cliente (KYC, por sus siglas en inglés) y combatir el lavado de dinero. Estos requieren que los documentos gubernamentales se presenten de alguna manera, se demuestre que son precisos y válidos y luego se asocien con el individuo. Este es el proceso de revisión.

Dependiendo de la cuenta o credencial que se emita, existen diferentes formas de realizar pruebas, muchas de ellas vinculadas a la identidad emitida por el gobierno. Otras, en cambio, se basan en lo que llamamos autoafirmación.

En un entorno empresarial, B2E, en relación con los empleados, la verificación es un proceso muy común, que implica verificaciones de antecedentes y mostrar documentación (por ejemplo, tu pasaporte o una licencia de conducir) para conseguir tu trabajo. Queremos hacer esto para los empleados porque es así como conseguirán un nuevo trabajo. Pero para un entorno B2B, la situación es muy diferente. ¿Cómo incorporamos a un nuevo socio comercial? Además de asegurarnos de quién es esa persona, es posible que necesitemos pruebas de que esta es la organización con la que queremos trabajar y que esta persona es alguien con quien queremos trabajar dentro de esa organización. Estos diferentes criterios crean un tipo de proceso de revisión muy diferente.

¿Qué pasa con la prueba de identidad en casos de uso B2C? ¿Cómo se puede conocer y confiar en un nuevo cliente y lo que afirma sobre sí mismo? Aquí la cuestión es cuánto debemos preocuparnos por eso. Existe un equilibrio en el mundo B2C entre velocidad y veracidad. Para algunas organizaciones y aplicaciones, la prioridad será la velocidad: lograr que las personas se registren rápidamente y accedan a la aplicación lo más rápido posible. El recorrido del usuario está optimizado para esto. Tendrán un acceso muy limitado y el umbral para el registro de usuarios es muy bajo.

Para otros, la prioridad es la veracidad, ya sea por la experiencia de marca, por el negocio en el que se encuentran, por lo que quieren ofrecer en términos de valor o en relación con la posibilidad de fraude. En este caso, la empresa quiere datos más verificables sobre la persona. La empresa determina que es importante tener un mayor nivel de seguridad de que el nuevo cliente es realmente la persona que dice ser.

Conclusión

La identidad digital, como indicamos al principio, es un gran tema. Hemos abordado los grupos a los que sirve IAM, las tecnologías involucradas, la gobernanza, el análisis, las cuentas privilegiadas y la prueba de identidad. Cada uno de esos temas puede completar un capítulo completo por sí solo (y con suerte así será, en futuras versiones del Cuerpo de Conocimientos de IDPro).

El artículo ofreció al profesional de IAM la oportunidad de comprender algunas de las principales consideraciones que afectarán a sus sistemas y servicios; los lectores deben considerar su propio contexto local y adaptar las definiciones aproximadas que se ofrecen aquí para que se ajusten a su propia organización. Un artículo futuro profundizará en el concepto de tecnologías de tiempo de ejecución.

Biografía de los autores

Ian Glazer

Ian Glazer es vicepresidente de gestión de productos de identidad en Salesforce. Sus responsabilidades incluyen liderar el equipo de gestión de productos, la estrategia de productos y el trabajo de estándares de identidad. Antes de eso, fue vicepresidente de investigación y gerente de agenda en el equipo de estrategias de identidad y privacidad de Gartner, donde supervisó el equipo de investigación. Es el fundador y presidente de IDPro, la organización profesional para la gestión de la identidad digital. También fue miembro fundador del Consejo de Administración y la junta directiva del Grupo Directivo del Ecosistema de Identidad de EE. UU. (IDESG, por sus siglas en inglés). Durante sus más de diez años en la industria de la identidad, fue coautor de una patente sobre aprovisionamiento de usuarios federados, fue coautor de la especificación *Service Provisioning Markup Language* (SPML) versión 2, contribuyó al sistema para la gestión de identidades entre dominios (SCIM, por sus siglas en inglés) especificación de la versión 2, y es un destacado bloguero, orador y fotógrafo de sus calcetines.

Espen Bago


Espen Bago se dio cuenta en 2002 de que, como administrador de sistemas, ya había estado trabajando en identidad durante un tiempo y decidió a partir de ahí explorar a fondo de qué se trataba todo esto de la identidad. Ha sido asesor de identidad independiente y coordinador de grandes empresas durante los últimos años, pero en 2021 se convirtió en director de identidad de la administración de trabajo y bienestar de Noruega. Como tal, su objetivo es garantizar que las identidades (y las personas reales que éstas representan) no sean olvidadas cuando los gobiernos inevitablemente se vuelvan totalmente digitales. También es miembro fundador de IDPro y miembro del Comité del Cuerpo de Conocimiento de IDPro y del Comité de Certificación de IDPro.

Registro de cambios

Fecha	Cambio
30-06-2021	Actualizaciones editoriales; adición de una sección de terminología; actualizar a la sección B2E

---

[i] Una organización no siempre necesita saber "quién" es una persona en ningún nivel de especificidad. Solo necesitan saber cosas como "¿es la misma persona cada vez?" o "¿esta cuenta está autorizada para realizar esta acción?".

[ii] AICPA, “Segregación de funciones”, consultado el 11 de enero de 2020, https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html

[iii] Estados Unidos. 2002. Ley Sarbanes-Oxley de 2002, [Washington, D.C.]: [EE.UU. GPO], https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

[iv] *Reglamento General de Protección de Datos de la UE (RGPD): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO 2016 L 119/1*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.