Introducción al Control de Acceso (v4)

Por André Koot
© 2022 IDPro, André Koot

Por comentarios sobre este artículo, contacte nuestro Repositorio GitHub o reporte un problema

Tabla de contenidos

Resumen

Como su nombre lo indica, la Administración de Identidades y Accesos (IAM, por sus siglas en inglés) se divide en dos funciones: administrar la información de identidad y llevar a cabo el control de acceso. Aunque es polémico decirlo, si no existieran requisitos de control de acceso no habría necesidad de administrar identidades. Y allí es donde deben poner el foco los profesionales de IAM. En esencia, el control de acceso es garantizar que los usuarios estén autenticados para acceder a recursos protegidos. Esto se lleva a cabo administrando los derechos de los usuarios y cumpliendo con los requisitos de aplicaciones confiables de modo que los usuarios solo puedan acceder a los sistemas y a la información a la que tienen derecho a acceder. Este artículo repasa la historia de la administración de accesos, las funcionalidades esperadas hoy en día y las posibles tendencias.

Introducción

Como concepto, el control de acceso tiene una larga historia. Para explorar los desafíos y soluciones actuales, comenzaremos por evaluar un modelo tradicional muy antiguo de clasificación de documentos gubernamentales.

Generalmente, la información contenida en documentos almacenados en archivos no debería ser accesible a todos. Probablemente, la información está clasificada y solo aquellas personas que posean el nivel de autorización necesario puedan acceder a los archivos clasificados. El control de acceso físico es relativamente sencillo y toma la forma de: una carpeta con un sello visible donde se lee “Confidencial” o “Restringido” o “Secreto” [1]

En este ejemplo simple, ya se abordan varios conceptos fundamentales de la seguridad.

En primer lugar, está la información en sí misma. La información puede estar clasificada como “C onfidencial”, pero eso debe ser definido por alguien que tenga el nivel de autoridad indicado, como el propietario de la información, del documento o del archivo/carpeta. Seguidamente, el impacto del nivel de clasificación debe estar claro; el nivel de clasificación es necesario para diferenciar los distintos niveles de acceso y usos de la información. El propietario del documento recibirá una guía sobre los niveles de clasificación aplicables y sobre qué tipo de usuario puede accederlo.

[1] Contribuyentes de Wikipedia, "Información clasificada," *Wikipedia, La Enciclopedia Libre,* https://es.wikipedia.org/wiki/Informaci%C3%B3n_clasificada (consultado el 24 de noviembre de 2022).

En segundo lugar, se encuentra el nivel de autorización de un actor, es decir el usuario de la información. En este caso, el agente de servicio secreto estará identificado y aprobado de forma tal que su acceso a información de diferentes niveles de seguridad es confiable.

En tercer lugar, tanto el nivel de clasificación como el de autorización deberán ser alineados con un mapa de autorización para garantizar que únicamente la persona con el nivel de autorización correcto pueda acceder a la información clasificada. El propietario clasificará el documento y determinará un nivel de seguridad específico por el cual el documento solo podrá ser accedido por un agente que tenga el nivel de confianza predefinido.

En cuarto lugar, antes de entregar el archivo/carpeta al agente de servicio secreto, la persona responsable de almacenar y recuperar la carpeta del archivo (es decir el administrador de la carpeta o controlador de acceso) debe verificar que el agente que está solicitando la carpeta es en efecto el usuario legítimo. Es decir que el controlador de acceso deberá identificar al agente y el agente deberá demostrar su permiso de acceso. Esta verificación puede realizarse mediante la presentación de una placa o identificación de servicio secreto y de una carta firmada que demuestre que el agente tiene permiso para acceder a la carpeta. El administrador de archivo también tendrá que validar que la firma en la carta es la indicada.

Solo una vez que estas responsabilidades hayan sido cumplidas, se entregará la carpeta al agente de servicio secreto. La entrega queda registrada en un registro diario.

El controlador de acceso siempre supervisará el acceso, en este caso implica únicamente verificar el sello en la carpeta. En este ejemplo, el robo de información—por ej., la filtración de información— es literal: la carpeta es retirada del lugar. Una carpeta con el sello "confidencial" no debería andar por ahí sin supervisión.

En este escenario, el control de acceso es bastante sencillo porque se puede ver literalmente las infracciones de acceso. El acceso se otorga entregando físicamente la carpeta a la persona con el nivel de autorización indicado que ha sido validado por su placa o identificación personal, y puede ser preservado aún más si se restringe el acceso a una ubicación o lugar específico.

En este ejemplo encontramos los siguientes temas:

1. La clasificación de la información: es un aspecto de la gestión de riesgos
2. La clasificación de usuarios: es un aspecto de la administración de identidades
3. El mapa de autorización: pertenece a la administración de autorizaciones
4. La autenticación: esta verificación forma parte tanto de la administración de identidades como de la administración de acceso
5. El acceso otorgado: esto es el control de acceso

Con la llegada de las computadoras surgió la necesidad de controlar el acceso a sistemas, documentos y otros recursos protegidos. Para modelar los mecanismos de control de acceso en los inicios de la era de las computadoras, se usaban procesos similares a los de las viejas películas de espías. Se utilizaban conceptos como "propietario de un recurso" y "lector de un recurso". Los programadores desarrollaron mecanismos de control de acceso como el Control de Acceso Discrecional (DAC, por sus siglas en inglés) ("nunca podrás pasar por encima del controlador de acceso", funcionalidad que aún se puede encontrar en el sistema de archivo NTFS de Windows) y el Control de Acceso Obligatorio (MAC, por sus siglas en inglés) ("solo se puede acceder a la información desde una ubicación específica" como una estación de trabajo en un espacio específico).[2,3] El crecimiento rápido de la tecnología de la información resultó en una creciente necesidad de desarrollar y mejorar el control de acceso. El creciente número de usuarios y de sistemas, así como un crecimiento exponencial de la información procesada dejan en evidencia que la metáfora del mundo físico de los papeles no es viable en el mundo digital.

Rápidamente se comprendió que el concepto de niveles de confianza—por ej., administrar individualmente el nivel de autorización de un lector de documento— es difícil de implementar. Esto ocurre porque hay muchos actores en juego y ya no hay un control de seguridad físico que pueda implementarse (ya no puedes ver la luz roja). En cambio, puede haber múltiples copias de una carpeta o archivo en múltiples ubicaciones y un robo ya no significa que la información fue extraída, sino que implica que la información fue copiada sin el consentimiento de su propietario. Lo que era fácil de implementar en el mundo físico no es fácil de implementar en el mundo digital. Dicho esto, es importante mencionar que las lecciones aprendidas en el mundo físico en respecto a la identificación, autenticación, autorización, el control de acceso, inicio de sesión y auditoría, se conservaron.

El acceso a la información, datos, servicios y sistemas, así como el acceso a ubicaciones físicas está regido por políticas de seguridad. Estas políticas de seguridad deben formalizarse y ejecutarse por el propietario del recurso. Eso significa que el propietario administra el riesgo involucrado en el acceso, como el riesgo de abuso de uso de la información, filtración de la información, robo, fraude y otras amenazas a la seguridad. Para estar en control, el propietario debe tener garantías sobre el nivel de seguridad que son capaces de alcanzar los controles de seguridad implementados.

---

[2] Davis, Shannon, "*A Look at Discretionary Access Control*," blog, *TED Systems*, 1 de diciembre de 2020, https://www.tedsystems.com/look-at-discretionary-access-control/ (accessed November 23, 2022).
[3] Rouse, Margaret, "*mandatory access control (MAC)*," TechTarget, diciembre de 2013, https://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC (consultado el 23 de noviembre de 2022).

Más allá de los conceptos vinculados al control de acceso, la propiedad en sí misma es un tema complejo. Al analizar el concepto de propiedad, identificamos varios criterios para definir la propiedad.
Alguien puede ser propietario de una información porque:

- Es el creador de la información
- Es fundador de la instalación o servicio de procesamiento de la información
- Es información sobre sí mismo (por ej., el historial médico de un paciente)

Pueden existir muchos otros criterios para identificar a un propietario, pero esto forma parte de la gobernanza de datos y está por fuera del alcance de este artículo. En el caso de los archivos médicos, el objeto, es decir el paciente, tiene varios derechos inherentes sobre la información lo cual genera que esa persona sea en parte responsable de la decisión de su acceso.

Terminología

- Identificación – Establecer inequívocamente al usuario de un sistema o de una aplicación.
- Autenticación – La demostración de que un usuario o una aplicación son confiables y tienen la autoridad para acceder a un recurso protegido al validar las credenciales del solicitante de acceso (un usuario, un proceso, un sistema o una cosa).
- Autenticación de Múltiples Factores (MFA, por sus siglas en inglés) – Es un método por el cual la identidad de un usuario es validada al nivel de confianza requerido de acuerdo con una política de seguridad para un recurso que es accedido utilizando más de un factor (algo que sabes —como tu contraseña—, algo que tienes —como tu teléfono inteligente—, algo que eres —como tu huella digital—).
- Autorización – El acto de determinar el derecho de un usuario para acceder a una funcionalidad con una aplicación de computadora y el nivel en el cual ese acceso debe ser otorgado. En la mayoría de los casos, una “autoridad” define y provee el acceso, pero en algunos casos el acceso es concedido por derechos inherentes (como en el caso de un paciente accediendo a su propio registro médico).
- Responsabilidad – La obligación de una persona de aceptar el resultado de una acción propia sea positiva o negativa. A menudo, esta persona es también algún tipo de propietario.
- Recurso protegido - Es un sistema, proceso, servicio, objeto de información o incluso una ubicación física que está sujeta al control de acceso en función de cómo esté delimitada por el propietario del recurso y por otras partes interesadas como pueden serlo los propietarios de procesos de negocio o los gestores de riesgos.
- Control de acceso – Controlar quién tiene acceso a un recurso protegido (datos, sistemas, servicios, recursos, ubicaciones). “Quién” puede ser un usuario, un dispositivo o un servicio, entre otros.
- Gobernanza de acceso – La garantía de que todos los accesos han sido otorgados correctamente siguiendo todos los parámetros y criterios establecidos.

- Política de acceso – Definición de las reglas que autorizan o deniegan el acceso a objetos seguros.
- Solicitante de acceso – La persona, proceso, sistema, dispositivo u otro que quiere acceder a un recurso protegido.
- Proveedor de acceso – El componente que otorga acceso a datos, sistemas o servicios después de que los requisitos de la política de acceso (definidos en el Punto de Administración de Políticas) han sido cumplidos por el solicitante de acceso.
- Motor de política - Es un componente de seguridad que valida si un actor tiene permitido acceder a un recurso protegido, siguiendo los requisitos de una política de acceso. Un motor de política puede concebirse como un componente que nace de la combinación de un PDP y un PAP.
- Punto de Aplicación de Políticas (PEP, por sus siglas en inglés) – Es la autoridad que habilitará únicamente a un solicitante de acceso a conectarse al proveedor de acceso si el Punto de Decisión de Políticas lo permite.
- Punto de Decisión de Políticas (PDP, por sus siglas en inglés) – Es el motor de políticas que valida las solicitudes de acceso y los atributos provistos ante la política de acceso (tal y como definido en el Punto de Administración de Políticas).
- Punto de Administración de Políticas (PAP, por sus siglas en inglés) – Es la ubicación donde los diferentes tipos de propietarios definen las políticas de acceso.
- Punto de Información de Políticas – Es la autoridad que consulta a los proveedores confiables (externos) de los atributos que serán usados en la decisión de acceso. Un ejemplo de esto es el servicio credly.com que administra las insignias abiertas (*open badges*) de certificación como CIDPRO™ o *Certified Information Systems Security Professional* (CISSP).

Acrónimos

- ABAC – Control de Acceso Basado en Atributos
- ACL – Listas de Control de Acceso
- AIAC – Control de Acceso basado en Inteligencia Artificial
- CBAC –Control de Acceso Basado en Contexto o Control de Acceso Basado en Notificaciones
- CIAM – Administración de Identidades y Accesos del Consumidor
- CRM – Gestión de Relación con el Cliente
- DAC – Control de Acceso Discrecional
- MAC – Control de Acceso Obligatorio
- PBAC – Control de Acceso Basado en Políticas
- PAP – Punto de Administración de Políticas
- PDP – Punto de Decisión de Políticas
- PEP – Punto de Aplicación de Políticas
- RBAC – Control de Acceso Basado en Roles o (menos frecuente) Control de Acceso Basado en Reglas

- ReBAC – Control de Acceso Basado en Relaciones
- SCIM – Sistema de Administración de Identidades entre Dominios
- SoD – Segregación de Funciones

AAA: Autenticación, Autorización, Responsabilidad

Como mostramos en el ejemplo del documento clasificado aquí arriba, la validación de la identidad es clave para permitir el acceso. Las ideas detrás de este modelo pueden resumirse en los conceptos de Autenticación, Autorización y Responsabilidad (AAA, por sus siglas en inglés).

Autenticación

La autenticación es el proceso de demostración de que el usuario propietario de la identidad digital que está solicitando el acceso, es el legítimo propietario de esa identidad. Esto puede hacerse de forma tan sencilla como mediante una contraseña o tan compleja como mediante la presentación de un certificado digital. Tanto el proveedor de acceso como el solicitante de acceso deben poder administrar y hacer uso de los resultados del proceso de autenticación.

Desafío - Respuesta

El usuario puede demostrar la legitimidad de su derecho de acceso proveyendo un secreto que solo el solicitante de acceso y el proveedor de acceso conocen, como una contraseña o código secreto. El mecanismo subyacente a este proceso se llama desafío-respuesta. El proveedor de acceso desafía al solicitante de acceso a que demuestre su identidad y el sujeto debe responder en la forma esperada por el proveedor de acceso. La manera más simple de llevar a cabo un desafío-respuesta es solicitando una contraseña o un PIN. El CAPTCHA, herramienta presente en muchos sitios web, es una forma de desafío-respuesta: debes demostrar que eres un ser humano.[4]

Conocimiento – Posesión - Inherencia

Dejando de lado el desafío CAPTCHA, un secreto conocido puede ser compartido. Es posible que un secreto no sea suficiente para garantizar un acceso legítimo ya sea porque la contraseña fue compartida con otros o porque se encuentra por ahí (por ejemplo, escrita en un papel): otros pueden fingir ser el legítimo propietario. Esta debilidad del modelo basado en un secreto conocido puede significar que el nivel de confianza de un solicitante de acceso que únicamente usa una contraseña no sea suficiente para algunas aplicaciones.

---

[4] Colaboradores de Wikipedia, "CAPTCHA," *Wikipedia, La Enciclopedia Libre,* https://es.wikipedia.org/wiki/Captcha (consultado el 24 de noviembre de 2022).

Luego de la identificación e incluso de la autenticación, perdura cierto nivel de desconfianza en la identificación del propietario legítimo lo cual normalmente se traduce en una mayor evaluación del nivel de acceso. Un nivel de confianza bajo puede ser suficiente para otorgar el acceso a información pública, pero será insuficiente para permitir el acceso a información clasificada.

A fin de agregar más pruebas de identidad pueden solicitarse identificadores más específicos y únicos. Estas formas de identificación más confiables no pueden ser fácilmente copiadas, compartidas o robadas (lo que no significa que sea imposible...pero el costo de copiar una ficha (en inglés un "token") de seguridad físico es demasiado elevado como para que sea económicamente redituable hacerlo). En la práctica, esto se hace incorporando factores adicionales como fichas , certificados y pruebas biométricas. Estas pruebas de identidad adicionales pueden solicitarse tanto en la primera autenticación al inicio de la sesión como durante la sesión cuando se decide que una autenticación de bajo nivel de confianza es insuficiente para otorgar el permiso de acceso a un recurso protegido. En este caso, el acceso de bajo nivel de confianza puede ser fortalecido llevando a cabo una autenticación incremental al solicitar factores adicionales: el primer paso en el inicio de sesión puede ser una contraseña cuya seguridad se incrementa con un segundo factor de mayor nivel de seguridad como una ficha o una demostración biométrica.

Autorización

A menudo utilizada como sinónimo de control de acceso, la autorización es el paso siguiente a la autenticación en un proceso de acceso. Es el acto de otorgar el acceso a un recurso específico, ya sea una aplicación informática o una función específica dentro de una aplicación.

El concepto de autorización está intrínsecamente ligado al de autoridad. Una persona, por ejemplo, un propietario, en su calidad de propietario, tiene el poder de autorizar a otros el acceso al recurso protegido y es, a su vez, responsable del mismo. Esto no implica que la otra persona se transforme en propietaria, pero sí que tendrá los permisos necesarios para ejecutar acciones como "leer" o "eliminar". El propietario seguirá siendo el responsable a lo largo de todo el ciclo de vida de la información. En ese sentido el propietario puede delegar, dentro de límites que el propetario defina, ciertas tareas a otros. Por ejemplo, puede autorizar a un gerente de línea para que pueda otorgar permisos de lectura a sus empleados.

Los métodos de Control de Acceso más utilizados

Hoy en día muchas organizaciones tienen políticas de seguridad embebidas en sus aplicaciones, sistemas operativos y componentes de red. Estos controles se implementan bajo la forma de Listas de Control de Acceso (ACL, por sus siglas en inglés), roles y reglas de negocio DAC. Dichos controles deben diseñarse de forma consistente e implementarse en

cada componente que corresponda. Por ejemplo, si se define una restricción de Segregación de Funciones (SoD, por sus siglas en inglés) para un proceso específico, cada sistema, programa, plataforma, aplicación y componente de red debe admitir la regla SoD. Basta con que solo uno de los muchos componentes carezca de control SoD para que toda la organización pierda el control.

Esta implementación descentralizada de las políticas de seguridad dificulta la implementación de controles administrados de forma centralizada por la organización. Es posible que no todos los controles sean similares, generando que las políticas de seguridad y conformidad deban ser verificadas para cada solicitud de acceso a sistemas o plataformas.

El Control de Acceso actual

Hoy en día, se utiliza un motor de políticas para evaluar las políticas de acceso de forma centralizada. El cumplimiento de las políticas debe incluir la evaluación de "nivel de riesgo". El propietario del negocio o de la información que esté encargado de administrar los riesgos de acceso definirá las políticas de las cuales son responsables. En algunos casos existen múltiples propietarios de negocio y cada uno es responsable de una parte de la política de seguridad corporativa, pero esto puede resultar en cambios constantes en las políticas de control de acceso.

Dado que muchas aplicaciones ya no admiten las Listas de Control de Acceso de usuarios, todavía queda mucho por hacer en esta área. En su lugar, confían en sistemas de administración de autorizaciones de identidades que basándose en una o más políticas de acceso, tomarán la decisión relacionada con la solicitud de acceso del usuario. Diferentes accionistas de una compañía son responsables de diferentes políticas. Todas las políticas aplicables deben ser evaluadas antes de otorgar un acceso. Este método de control de acceso detallado es un tipo de control de acceso obligado (MAC, por sus siglas en inglés).

Responsabilidad

La responsabilidad es clave en la gobernanza de acceso. Garantizar que cada decisión de acceso es responsabilidad de una persona autorizada implica que la propiedad debe ser abordada. A fin de ser responsable de la información que se encuentra bajo su protección, el propietario debe ser informado de todas las actividades que estén bajo su control.

Llevar un registro de todas las actividades de control de acceso es un requisito de calidad fundamental. La complejidad de este registro puede variar: desde el registro de cada solicitud de autorización (como la otorgación o revocación de autorizaciones o roles a personas) hasta el registro de cambios de autorizaciones dentro de los roles. Este registro es esencial para efectivamente tener un control del acceso. Lo mismo ocurre con los procesos de identificación y autenticación. Para garantizar la validación de cada solicitud

de acceso, el mecanismo de inicio de sesión, el sistema operativo y las soluciones IAM aplicadas deben ofrecer garantías.

Consideraciones específicas del control de acceso

El control de acceso no es únicamente una decisión de negocio. Otros elementos aportan información sobre la forma en que debe llevarse a cabo el control de acceso incluyendo cómo se relacionan los usuarios con los mecanismos de control, así como las implicaciones legales de lo que se está solicitando (o no se está solicitando) para administrar los permisos.

El factor humano

El propio usuario que está enfrentándose a los controles de seguridad puede ser en sí mismo un impedimento para llevar a cabo un control eficaz. La Experiencia de Usuario (UX, por sus siglas en inglés) es un elemento fundamental para concebir un proyecto de seguridad de la información exitoso. Si los controles de seguridad son demasiado estrictos, los usuarios pueden verse impedidos o desanimados de completar el control o incluso pueden intentar evitarlo. Este comportamiento de los usuarios suele verse principalmente en los casos de acceso de consumidor: si un portal de consumidor no está construido con el enfoque en el usuario, los consumidores tienden a irse a otro lado. Esto es una oportunidad perdida que resulta en tasas de conversión bajas. Las soluciones de Administración de Identidades y Accesos del Consumidor (CIAM) se implementan para evitar este tipo de comportamiento en los usuarios.

Las lecciones aprendidas en CIAM también se están implementando en la fuerza de trabajo IAM: la UX está comenzando a tener un impacto. Por ejemplo, si un usuario accede regularmente desde su casa a un portal intranet de la empresa usando un VPN, el sistema de control de acceso puede validar este comportamiento como un factor más del proceso de autenticación. En este caso, en el que se trata de un usuario conocido haciendo un uso conocido de los recursos desde una ubicación conocida y mediante una conexión confiable, se podría decidir que no es necesario someter al usuario al proceso de autenticación de múltiples factores a cada vez. Un contexto conocido resulta en un mejor control de acceso.

Implicaciones legales

Históricamente, el control de acceso ha sido considerado como una forma de dar soporte a los procesos de negocio, que conforma una política de seguridad y mitigación de riesgos más amplia. Las implicaciones legales asociadas a las prácticas de control de acceso varían de negocio a negocio, de sector a sector y de jurisdicción a jurisdicción. En lo que respecta a la pregunta sobre los requisitos legales concretos para llevar a cabo prácticas de control de acceso, solo hay respuestas ambiguas ya que estas políticas suelen conformar un programa más amplio que se rige por determinadas leyes, normativas o estándares. En parte, la función de un programa o sistema de control de acceso es garantizar que sea lo

suficientemente flexible como para dar soporte a los amplios programas de gestión de riesgos del negocio u organización. De este modo, las preguntas sobre los requisitos legales y las implicaciones del cumplimiento de los mismos pueden responderse de forma orgánica al permitir que la organización tenga la confianza necesaria para operar y proyectarse hacia el futuro.

Existen otros aspectos vinculados con las leyes y regulaciones. Los mismos son abordados en detalle en otros artículos del Cuerpo de Conocimiento de IDPro.

El estado actual del control de acceso

Los mecanismos de control de acceso más utilizados

Existen varios mecanismos para implementar un control de acceso. Aquí abordaremos los más utilizados o populares: las Listas de Control de Acceso (ACL), el Control de Acceso Basado en Roles (RBAC) y el Control de Acceso Basado en Atributos (ABAC).

Listas de Control de Acceso

El control de acceso de un recurso protegido se basa en el nivel de clasificación del recurso. Para definir el nivel de seguridad del recurso, cada recurso debe ser clasificado por su propietario (o persona delegada). Para garantizar un nivel de acceso correcto se deben implementar controles de seguridad basados en el nivel de seguridad. El acceso disponible, es decir los permisos que pueden ser otorgados, se conoce también como derechos (permisos específicos para acceder a recursos). Una de las primeras y más conocidas implementaciones de derechos son las ACL. En las ACL, el propietario del archivo define qué tipo de acceso pueden tener determinados usuarios: leer, escribir, actualizar, eliminar o cualquier otra forma de uso que el propietario acepte. Este concepto es fácil de comprender y administrar en el caso de objetos individuales. Por lo tanto, si el número de objetos es limitado, controlar el acceso con ACL puede ser suficiente pero cuando el número de usuarios y el número de objetos crecen, las ACL pueden resultar insuficientes.

Cada propietario de un archivo deberá definir la ACL para ese objeto. Este método de control distribuido implica necesariamente que no existe un control de acceso centralizado. Dicho esto, desde el punto de vista de las auditorías es relativamente sencillo encontrar quién tiene acceso a un recurso protegido ya que esa información está registrada en la ACL del recurso.

El concepto de ACL será explicado en un futuro artículo del Cuerpo de Conocimiento.

Control de Acceso Basado en Roles

Administrar ACL puede resultar una tarea tediosa. Administrar el acceso a recursos yendo usuario por usuario o derecho por derecho presenta problemas al futuro en la medida que la población crece. El problema de la falta de escalabilidad de este método dejó en

evidencia la necesidad de un nuevo abordaje de la administración de acceso. El abordaje RBAC habilita la otorgación de acceso a recursos a nivel grupal en lugar de individual. Para ello, es necesario establecer un componente intermediario: un controlador de accesos. Un rol de administración o de propietario debe poder mapear el rol de un usuario a su derecho de acceso a un recurso protegido. A simple vista, el mapeo parece sencillo, pero en la práctica implica que, para garantizar que las autorizaciones no entren en conflicto con los procesos de negocio y las estructuras organizacionales, esa persona de administración o propietario trabaje en conjunto con varias otras personas de la organización. Este concepto y la complejidad asociada al modelo de gobernanza se explican más a fondo en el artículo sobre gobernanza de acceso.

En el caso del sitio web interno de una empresa, cada empleado de la compañía es miembro de un grupo llamado “Empleados de la Empresa”. El recurso—en este caso la página principal del sitio web interno— está protegido de forma tal que el acceso es otorgado únicamente a los usuarios miembros de ese grupo. Otro ejemplo es un gerente de línea que asigna un rol de administración de cuentas a un nuevo empleado haciéndolo miembro del grupo asociado al rol, asegurando así que los permisos de acceso asociados al rol de administrador de cuentas estén disponibles para el nuevo empleado. Esta forma de otorgar el acceso de manera no individual simplifica la administración de accesos.

Un propietario de sistema también puede crear “roles” dentro de un sistema de información para evitar tener que administrar derechos de forma individual. El propietario de un sistema de Gestión de Relaciones con el Cliente (CRM, por sus siglas en inglés) puede definir un rol de “administrador de clientes” y agrupar las autorizaciones de sistema correspondientes (como leer el registro de un cliente de una base de datos o de un formulario) para luego asociarlas a ese rol.

En RBAC se puede identificar un modelo de roles de múltiples niveles. Por un lado, se identifican los grupos de identidades organizacionales o jerárquicas que definen los roles organizacionales o de empresa. Por otro lado, están los grupos de roles de sistema o de aplicación que agrupan las autorizaciones o permisos de una función de una aplicación o nivel de plataforma. Asociar los roles organizacionales a los roles de sistema o de aplicación es una manera muy eficaz de otorgar o revocar autorizaciones. Sin embargo, esta forma de administración de autorizaciones puede fácilmente complicarse al anidar grupos: por ejemplo, los empleados que trabajan en la “mesa de ayuda” serán miembros del grupo “MesadeAyuda”. Luego, ante una necesidad de acceso, podría decidirse que este grupo debe formar parte del grupo “Administradores de Windows”. Al anidar estos dos grupos, rápidamente se torna difícil saber quién tiene las autorizaciones de Administrador de Windows ya que no solo sería el grupo de personas miembro del rol Administrador de Windows sino también los empleados que son miembros del rol Mesa de Ayuda. Esta anidación puede acarrear grandes problemas. Muchos proyectos IAM fallan justamente por no ofrecer la opción de desanidar. La anidación también limita la auditabilidad de los

entornos RBAC ya que, para evaluar las autorizaciones y las autorizaciones potencialmente conflictivas, los grupos deben ser desanidados.

Las implementaciones RBAC así como sus pros y sus contras se explican en el artículo del Cuerpo de Conocimiento exclusivamente enfocado en el tema.

Control de Acceso Basado en Atributos

ABAC se construye sobre el modelo RBAC e introduce controles adicionales basados en la lógica de negocio. Una de las fallas más grandes del modelo RBAC reside en su naturaleza estática: una vez que un derecho ha sido otorgado seguirá estando asociado al usuario final hasta que sea revocado manualmente. A menos que se lleven a cabo acciones de limpieza, esta longevidad del permiso otorgado acarrea situaciones como usuarios que llevan consigo todos los permisos que le fueron históricamente otorgados en cada uno de los roles por los que pasó. Para lidiar con este problema, ABAC expande el modelo incorporando la evaluación de otras características y atributos del usuario para determinar si un acceso debe ser otorgado. Esto significa que un sistema de control de acceso ABAC puede tomar una decisión de acceso basándose no solo en los derechos otorgados al usuario sino también en la hora del día del acceso, la ubicación del usuario (por ej., mediante geolocalización basada en una dirección IP de red o remota), el tipo de dispositivo (por ej., personal, de la organización, de escritorio o tablet) y otros metadatos del trabajador. ABAC puede usarse para controlar el acceso en tiempo real durante la transacción o para controlar pasivamente los roles asignados y derechos otorgados basándose en metadatos del usuario. Para entender y definir las necesidades del usuario, ambos abordajes requieren de una fuerte participación y apoyo por parte de los propietarios de recursos, administradores de roles y gerentes de la organización, así como de analistas que colaboren en la definición de la lógica de negocio.

Por ejemplo, el Administrador de Relaciones de Cliente propietario del proceso podría definir que todos aquellos que tengan el atributo “Rol Empresarial = Administrador de Cuentas” pueden acceder al recurso pero solo si el atributo “Tiempo Permitido = Horario de Oficina Definido”. Ahondaremos sobre las múltiples opciones que ofrece este abordaje dinámico del control de acceso en un futuro artículo del Cuerpo de Conocimiento de IDPro.

¿Hacia dónde se dirige el futuro del Control de Acceso?

El Control de Acceso llevado a cabo mediante ACL y RBAC es relativamente estático; la agrupación de un usuario con sus autorizaciones es fija y no puede ser modificada fácilmente. Es decir que en la medida que surja la necesidad de otorgar otras autorizaciones a ese usuario, será inevitable realizar cambios. Las personas cambian de trabajo, de dispositivo, de ubicación y/o de tareas en un contexto nuevo. A su vez, el nivel de riesgo asociado a un recurso protegido puede cambiar en función del contexto o de modificaciones en las leyes y regulaciones aplicables.
Algunos cambios relevantes incluyen:

- Escenarios en los que personas por fuera del alcance de las funciones de recursos humanos necesiten tener acceso a recursos diariamente, como es el caso en organizaciones extendidas, internacionalización, colaboración y federación y/o una fuerza de trabajo flexible.
- Trasladar el procesamiento de datos a la nube, forzando el desarrollo de nuevos protocolos como SCIM (Sistema de Administración de Identidades entre Dominios; la primera vez que se utilizó este acrónimo se lo llamó Administración Simple de la Identidad en la Nube, pero supongo que consideraron que el nombre era demasiado simple o limitado☺).[5]
- La aparición de nuevas regulaciones de privacidad, como RGPD.[6]
- La utilización de aplicaciones móviles que usan protocolos modernos como *OpenID Connect* y que requieren una topología de control de acceso flexible.
- La aplicación del consentimiento y control administrado por el usuario final - como mediante la implementación de una solución de Acceso Administrado por el Usuario (UMA, por sus siglas en inglés). [7]
- Pasarse a un acceso basado en API (Interfaz de Programación de Aplicaciones, por sus siglas en inglés) para microservicios - conduciendo a nuevas arquitecturas de administración de acceso basadas en protocolos como OAuth2.

Se hace evidente que para lidiar con las limitaciones y los cambios que mencionamos es necesario tener un método de administración de acceso dinámico. Y hacia allí parece dirigirse el futuro del control de acceso: hacia los desarrollos necesarios para ofrecer un eficaz control de acceso dinámico.

Autenticación dinámica

El control de acceso no es un evento estático. Cuando un usuario inicia sesión y accede a servicios de bajo riesgo de seguridad, la combinación de un nombre de usuario y contraseña puede ser suficiente. Más adelante en la sesión, puede ocurrir que se requiera otro nivel de seguridad. Por ejemplo, al realizar una transferencia bancaria, es posible que se solicite una identificación adicional como una ficha .

---

[5] "*SCIM: System for Cross-domain Identity Management*," http://www.simplecloud.info/ (consultado el 23 de noviembre de 2022).

[6] "Reglamento General de Protección de Datos de la UE (RGPD): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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 el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)." OJ 2016 L 119/1.

[7] *Kantara Initiative, "UMA Specifications,"* página wiki, actualizada por última vez el 27 de julio de 2022, https://kantara.atlassian.net/wiki/spaces/uma/pages/29229182/UMA+Specifications (consultada el 23 de noviembre de 2022).

Para adaptarse a estas dinámicas dentro de una sesión, la autenticación en sí misma también debe ser un proceso continuo, como es el caso del nuevo concepto de biometría del comportamiento.
A continuación, encontrará algunos ejemplos de cambios en el nivel de confianza requerido a una identidad:

- Cambios en el contexto del usuario (como su ubicación). La sesión debe ser re-evaluada para definir si la nueva ubicación también es confiable.
- Un usuario recibe un documento -adjunto en un correo electrónico- que requiere de un nivel de confianza más alto que el proporcionado por sus credenciales de inicio de sesión. Abrirlo debería desencadenar una autenticación adicional como una Autenticación de Múltiples Factores.

La autenticación adaptativa es una forma de autenticación segura, dinámica y flexible. Permite determinar la legitimidad de una solicitud de inicio de sesión mediante la validación de múltiples factores antes de otorgar el acceso a un recurso. Los factores usados para validación del usuario pueden depender del riesgo asociado a la otorgación concreta de ese acceso lo cual suele implicar que se ajuste la fortaleza de la autenticación requerida, basándose en el contexto actual.

Control de Acceso Basado en Políticas (PBAC)

Para tener un control de acceso eficaz y efectivo, las organizaciones extendidas que trabajan con entornos de fuerza laboral flexible necesitan un método dinámico y flexible. El modelo capaz de proveer esta flexibilidad es el Control de Acceso Basado en Políticas (PBAC). PBAC, también conocido como Control de Acceso Basado en Notificaciones o Control de Acceso Basado en Contenido, recupera algunas de las lógicas de negocio introducidas en el modelo ABAC y las mejora incorporando la evaluación del contexto y una capacidad de adaptación dinámica.

El contexto de un solicitante de acceso puede cambiar dinámicamente. Si los controles de riesgo definidos lo requieren, gracias a la naturaleza dinámica de la administración y cumplimiento de políticas es posible llevar a cabo una autenticación incremental dentro de una misma sesión, alcanzando así un mayor nivel de garantía. Un motor de políticas se encarga de verificar que los atributos y la información de contexto del usuario al momento de solicitar el acceso estén en conformidad con las políticas de acceso definidas por los propietarios de las políticas de seguridad. La información de contexto puede incluir una hora del día, una ubicación geográfica o el tipo de dispositivo desde el que se accede. Posibilitar la recolección de atributos de diferentes proveedores de atributos confiables y predefinidos habilita la escalabilidad del acceso. Por ejemplo, se podría definir que x persona puede acceder a los informes de gestión de riesgos, pero únicamente si x persona tiene el certificado CRISC. Dado que ISACA otorga este certificado, una búsqueda en el registro ISACA podría responder a la pregunta sobre el certificado CRISC (el mapeo entre el

solicitante de acceso y la categoría de miembro ISACA está por fuera del alcance del tema que estamos abordando).[8]

El componente central de esta arquitectura es el Punto de Decisión de Políticas que evalúa las políticas de acceso y da una respuesta al solicitante de acceso. El Punto de Decisión de Políticas ejecuta la respuesta ya sea mediante un código embebido en la aplicación o de forma incremental mediante un *API gateway*. El Motor de Cumplimiento de las Políticas es un componente opcional del flujo de solicitud de acceso.

Habiendo dicho todo esto, si vamos a hablar del futuro de la administración de acceso, no podemos dejar de mencionar los modelos AIAC y ReBAC.

Control de Acceso Basado en Relaciones

ReBAC, o el Control de Acceso Basado en Relaciones, es un nuevo concepto de control de acceso. ReBAC habilita la posibilidad de tomar decisiones de control de acceso en función de la relación entre el solicitante de acceso y otras identidades que potencialmente puedan verse afectadas por esta decisión de control de acceso. Estas decisiones de acceso pueden deducirse de las relaciones del solicitante de acceso en redes sociales (u otros servicios). Un atributo como la "reputación" puede ser considerado y evaluado. La implementación del modelo ReBAC depende de la disponibilidad de grandes y diferentes conjuntos de datos (ya que incorpora información proveniente de recursos humanos así como información de acceso/derechos/comportamiento) y de una Inteligencia Artificial que evalúe las decisiones de acceso y emita recomendaciones.

El camino futuro que tomará ReBAC no está aún del todo claro y su desarrollo no está lo suficientemente maduro como para implementarlo de forma masiva pero su implementación en tecnologías predictivas de la minería de roles en implementaciones ABAC dinámicas, tiene potencial.[9]

Control de Acceso Basado en Inteligencia Artificial (AIAC)

Al incorporar la Inteligencia Artificial (IA) en el control de acceso podemos esperar grandes avances en esta área. Un entorno robusto que clasifica los recursos sensibles permite un abordaje sofisticado de la gestión de riesgos y un control de acceso dinámico donde la solución de administración de identidades alertará sobre solicitudes de acceso que excedan los niveles de riesgo normales. La IA también monitorea las solicitudes de control de acceso y alerta sobre actividades fuera de lo común. Por ello, podría ser incorporado a las implementaciones actuales RBAC y ABAC. Si bien este modelo no es masivo aún y

---

[8] Página de inicio de ISACA, https://www.isaca.org/ (consultada el 23 de noviembre de 2022).

[9] "*Data Mining and Predictive Analytics: Things We should Care About*," Inside Big Data, 24 de noviembre de 2018, https://insidebigdata.com/2018/11/24/data-mining-predictive-analytics-things-care/.

predecir su futuro es difícil, podemos afirmar que la IA y el aprendizaje automático pueden añadir valor al sistema.

Control y consentimiento administrado por el usuario

Las leyes y regulaciones sobre privacidad crearon una nueva conciencia del acceso a la información personal de identificación (PII, por sus siglas en inglés). Estas leyes y regulaciones impulsaron el concepto de propiedad de la información y consentimiento de los clientes, empleados o pacientes. Los propietarios de información esperan estar en control de su información personal y en muchos casos las leyes y regulaciones así lo exigen. Varias plataformas tecnológicas emergieron con el fin de cubrir esta brecha en la propiedad. Soluciones como el A cceso A dministrado por el U suario (UMA) de *Kantara Initiative* se abrieron paso entre los nuevos modelos de acceso. El amplio desarrollo de protocolos como OAuth simplificó la implementación de estos conceptos.[10]

Conclusión

Los mecanismos de control de acceso más populares como RBAC y ACL vienen de larga data y seguirán teniendo casos de uso válidos en muchas organizaciones. No obstante, en la medida en que las empresas, gobiernos y organizaciones requieran llevar a cabo comunicaciones y colaboraciones por fuera de las tradicionales cuatro paredes, otras formas de controlar el acceso son necesarias.

Los métodos de control de acceso más utilizados actualmente no son capaces de ofrecer las soluciones de control de acceso flexibles necesarias en un mundo en constante cambio. La gobernanza de acceso moderna requiere métodos de control de acceso modernos. Existe una evidente necesidad de un control de acceso dinámico. Afortunadamente, las herramientas necesarias están apareciendo en escena y su implementación, aunque implica cierta planificación basada en una hoja de ruta, no interfiere con las mejores prácticas actuales: la autenticación adaptativa y PBAC pueden incorporarse a una arquitectura de identidad y acceso existente. Por supuesto, también requiere la implementación de elementos de gobernanza de acceso.

[10] Contribuyentes de Wikipedia, "Información clasificada."

Biografía del Autor

 André Koot es Consultor IAM y de Seguridad en SonicBee. Su experiencia IAM proviene de sus antecedentes en contaduría y auditoría financiera. Este pasado en el sector de la detección antifraude y prevención de procesos de negocio lo condujo a investigar el área de los principios de autorización y control de acceso.

Registro de cambios

Fecha	Cambio
17-06-2020	V1 publicada
19-04-2021	Cambio en la afiliación del autor
30-09-2021	Actualización de la definición de autenticación
15-12-2022	V4 publicada: aclaración en la definición de Motor de Políticas; actualizaciones editoriales menores