Introducción al Control de Acceso Basado en Políticas (v2)

Por Mary McKee

Para información básica sobre el control de acceso, vea el artículo Introducción al Control de Acceso de André Koot.

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

Tabla de contenidos

Resumen

La natural evolución del control de acceso ha llevado a la implementación de modelos de administración de accesos que otorgan y deniegan el acceso basándose en reglas estructuradas y altamente reproducibles por muchas organizaciones.

El Control de Acceso Basado en Políticas (PBAC, por sus siglas en inglés) es uno de esos modelos y se caracteriza principalmente por dos aspectos clave:

1. Otros sistemas de control de accesos suelen centrarse en facilitar la otorgación de acceso de usuarios a todos los recursos relevantes; PBAC se centra en extender el acceso a recursos a todos los usuarios que aplican.

2. PBAC facilita la evaluación de contexto (hora del día, ubicación, etc.) en el cual se otorgó el acceso a un recurso protegido. El contexto se utiliza para determinar quién y bajo qué circunstancias puede acceder a un recurso.

Cambiar el foco del control de accesos del usuario a los recursos, permite que los sistemas PBAC sean particularmente resistentes a cambios en la estructura de una organización o en las obligaciones normativas. La inclusión de información de contexto (como una ubicación o dispositivo autorizado para el usuario) habilita la realización de controles de seguridad adicionales y garantiza que todos los aspectos del control de acceso estén contenidos y puedan ser auditados en una misma estructura.

PBAC es muy preciso para determinar quién y bajo qué circunstancias puede acceder a un recurso. Esto facilita la automatización del aprovisionamiento y desaprovisionamiento de accesos, lo cual simplifica su administración y aumenta la seguridad y adaptabilidad.

Introducción

Para garantizar una seguridad eficaz de los recursos, los sistemas de control de acceso deben diseñarse de manera que puedan adaptarse a cambios rápidos en la tecnología, obligaciones legales o normativas y en la estructura organizacional. A medida que las organizaciones adoptan tecnología cada vez más sofisticada buscando protección contra amenazas que son igualmente cada vez más sofisticadas, las estrategias de administración de control de acceso evolucionan para abordar los problemas actuales.

La mayoría de los sistemas de administración de acceso primitivos utilizan lo que ahora llamamos **Control de Acceso Discrecional** (**DAC**, por sus siglas en inglés). En los sistemas DAC (como listas de control de acceso), los administradores asignan manualmente los privilegios a los usuarios en función de su entendimiento sobre su necesidad, uso apropiado y cumplimiento de las reglas de la organización. A medida que los sistemas DAC crecen en número de usuarios, recursos, administradores, y/o envejecen, su dependencia en la administración ad hoc conduce a inconsistencias en la aplicación y entendimiento del acceso. Dado que en este tipo de sistema un acceso no autorizado o inapropiado suele pasar desapercibido a la vez que la otorgación de un

acceso insuficiente genera problemas visibles en un negocio, los administradores DAC tienden a ser cada vez más laxos con las autorizaciones y reacios a la limpieza/revisión de accesos. Como resultado, los sistemas DAC suelen ser demasiado costosos, inconsistentes e inflexibles como para adaptarse a las necesidades actuales.

Los sistemas de control de acceso actuales se enfocan en la consistencia y eficacia otorgando el acceso a recursos mediante reglas estructuradas. El modelo más conocido de control de acceso cuyos permisos se basan en reglas se llama **Control de Acceso Basado en Roles** (**RBAC**, por sus siglas en inglés). En RBAC los permisos están asociados a los "roles" asignados a los usuarios. Este modelo es eficaz para garantizar que se otorguen consistentemente los mismos permisos a todos los usuarios que comparten las mismas responsabilidades y, como requiere que los roles y sus permisos asociados se definan antes de ser puestos en práctica, facilita la gobernanza.

Más aún, RBAC es compatible con escenarios de autorización federada en los que los permisos a los recursos dependen de la información provista por una autoridad de usuario externa. Si bien RBAC implica una mejoría respecto a DAC, sus permisos no resisten a cambios en la estructura de responsabilidades de una organización y tienen limitaciones en cuanto a cómo pueden ser definidos. Estas desventajas en los sistemas RBAC, que abordaremos más adelante en el artículo, dificultan la garantía de que los usuarios tienen el acceso justo necesario para ejecutar sus funciones empresariales (esto se conoce también como el *principio del mínimo privilegio*[1]).

El **Control de Acceso Basado en Políticas (PBAC)** es un sistema más robusto para administrar permisos mediante reglas estructuradas en contextos federados y no federados.

Mientras que el modelo RBAC agrupa los permisos de manera intencional, PBAC crea un concepto llamado **Control de Acceso Basado en Atributos** (**ABAC**, por sus siglas en inglés) que permite automatizar la administración de permisos de forma separada y detallada. PBAC retoma el enfoque ABAC y calcula los permisos basándose en información del usuario como un código o estatus laboral y tiene en cuenta las circunstancias o contexto apropiados para permitir el acceso, ofreciendo una mayor precisión.

Terminología

- **Sistema de Control de Acceso** – es una estructura que controla y ejecuta decisiones sobre el acceso dentro de la organización.

[1] "Mínimo privilegio," https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege (consultado el 10 de febrero de 2020)

- **Usuario** o **Sujeto** – Una persona o entidad que puede recibir acceso dentro de determinado sistema de control de acceso.

- **Recurso** u **Objeto** – Es un valor protegido por los controles de acceso, como una aplicación, un sistema o puerta.

- **Acción** – Una operación protegida disponible para un recurso, como “Ver”, “Editar” o “Enviar”.

- **Permiso** – Es una declaración de autorización para uno o más sujetos para que realicen una o más acciones sobre uno o más objetos.

- **Contexto** – Condiciones bajo las cuales se autoriza una acción en un recurso a un sujeto, como por ejemplo el tiempo de acceso, la ubicación de acceso o determinados requisitos de cumplimiento.

- **Control de Acceso Federado** – Es una arquitectura de control de acceso que contempla la separación de la autoridad usuario/sujeto de la autoridad recurso/objeto.

- **Control de Acceso Discrecional** – Es un modelo de sistema de control de acceso que involucra definiciones manuales fijas sobre los permisos asignados directamente a los usuarios.

- **Control de Acceso Basado en Roles** – Es un modelo de sistema de control de acceso que involucra conjuntos de definiciones estáticas y manuales de permisos asignados a "roles", que se pueden asociar de manera consistente y repetible con usuarios con necesidades de acceso comunes

- **Control de Acceso Basado en Atributos (“ABAC”) / Control de Acceso Basado en Notificaciones (“CBAC”)** – Es un modelo de sistemas de control de acceso que involucra definiciones dinámicas de los permisos basados en información (como atributos o notificaciones), como por ejemplo códigos de trabajo, departamento o membresía a grupos.

- **Control de Acceso Basado en Políticas** – Es un modelo de sistema de control de acceso que tiene en cuenta las definiciones dinámicas sobre los permisos de acceso, basándose en los atributos del usuario (como en ABAC) y en las variables del contexto para permitir o denegar el acceso.

- **Principio de Mínimo Privilegio** – Es la mejor práctica de seguridad de la información para garantizar que dentro de un sistema de control de acceso, los usuarios no tengan acceso a recursos más que el estrictamente necesario para la realización de sus actividades.

- **Segmento** – Es una agrupación de sujetos que puede ser útil para autorizaciones, como empleados de tiempo completo, estudiantes de grado, administradores de TI o clínicos.

- **Abstracción** – La práctica de identificar y aislar los aspectos repetidos de operaciones o lógicas de negocio, para que se encuentren en un solo lugar y puedan ser referenciadas en muchos lugares.

PBAC vs. RBAC: Una comparativa

Explorar las diferencias entre PBAC y RBAC puede ser útil para comprender mejor las estructuras PBAC.

Mientras que en los permisos RBAC el foco principal está puesto en el usuario, en los permisos PBAC está puesto en el recurso.

RBAC pregunta "¿Qué tipos de usuarios tengo y qué pueden hacer en mi entorno?". Los mecanismos de control se construyen en base a **sujetos** (quién está accediendo), **permisos** (qué está siendo accedido o usado) y **roles** (qué permisos se pueden asignar a un sujeto)[2]:

Sujeto		**Rol**		**Permiso**
Ada	como	Editor	puede	Modificar Documentos

PBAC pregunta "¿Qué tipos de recursos tengo y quién/cómo pueden ser usados o administrados?". Los mecanismos de control se construyen en base a **sujetos** (quién está accediendo), **objetos** (qué recursos están siendo accedidos o usados), y el **contexto** (parámetros de entorno u otros que definen un acceso aceptable)[3]:

Objecto		**Acción**		**Sujeto**	**Contexto**
Documentos	pueden ser	Modificados	por	Quienes tengan el código laboral "Editor"	En dispositivos administrados

[2] "Control de Acceso Basado en Roles," https://en.wikipedia.org/wiki/Role-based_access_control (consultado el 10 de febrero de 2020)
[3] "Control de Acceso Basado en Atributos," https://en.wikipedia.org/wiki/Attribute-based_access_control (consultado el 10 de febrero de 2020)

En ambos ejemplos se abstraen los sujetos para garantizar que todos los editores tengan los permisos necesarios. En el ejemplo RABC, Ada recibe el permiso porque se le ha asignado por vía manual o automática el rol de “Editor”. En el ejemplo PBAC, Ada recibe el permiso porque la definición de sujeto se corresponde con su registro de empleado, aunque la definición de sujeto podría hacerse manualmente por ejemplo asignándole la pertenencia a un grupo.

Para comparar manzanas con manzanas, imagina que un sistema RBAC asigna a Ada el rol de “Editor” mientras que un sistema PBAC le asigna la pertenencia a un grupo de “Editor” que está referenciado en las políticas de acceso. Si bien estas acciones pueden parecer equivalentes, la arquitectura PBAC tiene los siguientes beneficios: la flexibilidad de respaldar diferentes situaciones (contexto), la habilidad de manejar cambios separadamente sin impactar en otros permisos (modularidad) y la capacidad de evaluar los permisos en tiempo real (simetría). Como se puede ver en los ejemplos a continuación, cada uno de estos factores conduce a un abordaje consistente y justificado del control de accesos de la organización.

Contexto

El empleador de Ada puede estar sujeto a asuntos legales o de conformidad que afectan cómo pueden ser accedidos los recursos. Por ejemplo, cuando una normativa de seguridad nacional (como el control de exportaciones) restringe el acceso de ciertos tipos de dispositivos, las políticas PBAC correspondientes pueden ser enmendadas para incluir este requisito.

En el caso que la empresa requiera algún tipo de formación o capacitación previa al acceso a recursos, este requisito puede articularse como contexto. Basándose en registros provenientes de la organización autorizadora o por fuera de ella, se puede atribuir y mantener un “estatus de certificación” de Ada. En lugar de tener que llevar a cabo procesos de auditoría laboriosos o manejar una infraestructura para revocar y reasignar permisos a medida que el estado de conformidad cambia, el acceso de Ada es automáticamente bloqueado cuando ella no cumple con la formación/capacitación necesaria y automáticamente restaurada cuando re-certifica su formación. De manera similar, en el caso que Ada deba consentir los términos y condiciones del acceso que se le ha otorgado, el contexto PBAC garantiza que esto se haya realizado previo a cualquier interacción con los recursos accedidos.

Por razones de seguridad, es posible que Ada solo pueda acceder a los recursos de la compañía desde determinadas ubicaciones de red que han sido clasificadas como seguras o mediante requisitos de autenticación de múltiples factores más estrictos que los de usuarios con menos permisos. Al codificar y ejecutar estos requisitos dentro del alcance del permiso, el empleador de Ada puede fácilmente referenciar, administrar y adaptar todos los requisitos de acceso en un solo lugar.

Modularidad

A diferencia de RBAC, los permisos otorgados por las políticas PBAC no están inherentemente interconectados y son por lo tanto altamente modulares y fáciles de administrar de forma segura. Cuando una organización necesita, agregar, remover o modificar los controles sobre un recurso, las políticas para ese recurso pueden adaptarse según la necesidad sin impactar en otros recursos.

Cuando los permisos están agrupados juntos, como es el caso en RBAC, incorporar nuevos escenarios de negocio requiere un vasto análisis de los conjuntos de permiso existentes. A menudo los administradores se ven forzados a elegir entre asociar un conjunto de permisos de acceso “suficientemente parecido” al necesario (que trae consigo permisos innecesarios), o ser los responsables de la proliferación de conjuntos de permisos que son cada vez más difíciles de comprender y administrar.

Por ejemplo, si los directivos de la compañía de Ada la seleccionan para editar los informes para inversores conteniendo información sensible, es posible que Ada necesite que se le otorgue un acceso atípico para un editor. Probablemente el administrador de sistemas RBAC encargado de otorgar este acceso considerará las siguientes soluciones:

- Otorgar a todos los editores el acceso que Ada necesita, aunque esto sobrepase los privilegios de otros editores.

- Asignar a Ada un cargo directivo que se sume a su rol de editor, concediéndole así privilegios que están por encima de su rol.

- Crear un rol nuevo con los permisos específicos para cubrir esta necesidad concreta, sentando el precedente de la creación ad hoc de roles temporales para cubrir necesidades.

- Rediseñar los roles para ofrecer una solución más limpia para este escenario de negocio, lo cual suele ser costoso.

Para las organizaciones cuyas necesidades de acceso están en constante cambio, no suele ser práctico tener que rediseñar los roles RBAC cada vez que un acceso no está representado por un rol preexistente. Las alternativas de sobre-privilegiar o complicar el escenario, conducen a un abordaje descuidado de la administración de accesos dentro de la organización.

Simetría

Cuando existen criterios diferentes para otorgar o denegar el acceso en un sistema, es habitual que el sistema acumule permisos que una vez fueron correctos pero que ya no lo son bajo la política actual. Los sistemas PBAC no tienen este problema porque las decisiones de control de acceso son realizadas en tiempo real basadas en atributos actuales y contexto.

Dado que PBAC es una extensión de ABAC, los controles PBAC pueden fácilmente incorporar la opción de ofrecer un acceso basado en atributos de forma parcial o totalmente automatizada. Una organización puede querer otorgar el acceso automáticamente a cualquier empleado actual de la empresa, o a cualquier empleado que trabaje en el Departamento X o en el Departamento Y, y que no esté de baja por motivos personales.

Automatizar la asignación del acceso simplifica las tareas de automatización del monitoreo continuo de la validez de los permisos y la revocación de los permisos que bajo determinadas normativas actuales ya no son válidos. Esto crea una simetría entre el aprovisionamiento y desaprovisionamiento de acceso, minimizando el mantenimiento del sistema y las acumulaciones de permisos.

PBAC es práctico

Por su versatilidad, PBAC es óptimamente escalable. Gracias a esta capacidad de adaptación, PBAC es una opción práctica para organizaciones de cualquier tamaño. El tiempo que se ahorra con los roles RBAC optimizados puede perderse rápidamente si no está claro el impacto que genera la modificación de un rol (o de sus permisos asociados) en la organización. Esto puede desincentivar una administración del control de acceso activa y responsable, y entorpecer el crecimiento de una organización de cualquier tamaño.

Consideremos el siguiente escenario para ilustrar porqué es preferible utilizar PBAC aún en organizaciones pequeñas:

La empresa *JE Plumbing* inicia sus actividades siendo un pequeño negocio conformado por cinco plomeros y un dueño que se encarga de la administración.

Gracias a una excelente reputación y una clientela cada vez mayor, el dueño decide expandir su personal a veinte plomeros que responden ante un gerente de negocio, tres vendedores y dos especialistas en finanzas.

Con el tiempo, *JE Plumbing* ve la oportunidad de expandir el área de cobertura y los servicios ofrecidos. Para concretar esto, establecen dos nuevos locales administrados por dos nuevos gerentes de negocio (uno de los cuales resulta de la promoción de un especialista en finanzas que asciende de cargo). Incrementan su personal de plomeros residenciales a setenta y cinco y contratan veinticinco plomeros comerciales. Los cargos de finanzas y ventas se replican en las dos nuevas oficinas, pasando de dos a seis personas. Un especialista de marketing es contratado para cubrir las necesidades de las tres oficinas.

En este escenario, un abordaje RBAC comenzaría con dos roles: un rol de administración para el dueño y un rol técnico para su personal. A medida que la empresa crece, un rol de administración puede ser otorgado a un gerente de negocio, pero en el caso de los especialistas en ventas y finanzas se deberán crear nuevos roles.

Luego de duplicar roles de dos a cuatro, la cantidad de roles se duplica nuevamente cuando la empresa separa los roles de ventas y marketing en dos roles diferenciados, formaliza roles para los gerentes de negocio y atención al cliente y mantiene los roles iniciales de administración y finanzas.

En este ejemplo mostramos el desarrollo de *JE Plumbing* deteniéndonos en tres momentos de su historia, pero es importante decir que cambios tan grandes como estos no se dan de la noche a la mañana. Si un pequeño negocio está llevando a cabo ajustes en su estrategia organizacional teniendo un capital de trabajo limitado mientras quiere preservar la seguridad a través de los cambios en las responsabilidades, debería incorporar a su equipo un rol que no estuvo incluido en el ejemplo: un profesional TI capaz de encargarse a tiempo completo de la re-ingeniería de las estructuras de administración de accesos y de adaptar cada sistema que las utilice.

En cambio, un abordaje PBAC comenzaría por analizar qué recursos necesita preservar *JE Plumbing*: órdenes de trabajo, información de clientes, facturas, inventario, información personal y de certificaciones de los empleados, información de nómina e informes de gastos. Si bien las responsabilidades de estas funciones cambian a medida que la empresa contrata personal, las funciones en sí mismas se mantienen iguales. Si además de crecer en escala, la empresa expande la naturaleza de su negocio, sería sencillo agregar nuevos permisos que den soporte a las nuevas funciones, sin interferir con las funciones existentes.

Este sencillo cambio en el enfoque del control de acceso, pasando de un enfoque de usuario a un enfoque de recurso, permite que la complejidad del control de accesos tenga un crecimiento lineal en lugar de exponencial. De esta manera, JE Plumbing puede adaptar los permisos a medida que ocurren los cambios en la organización sin tener que lidiar con una inflación en el número de roles.

Además de ser más adecuado a las necesidades, PBAC también permite minimizar los riesgos de la empresa mediante la configuración de contexto para el acceso. Por ejemplo:

- Si la información de los clientes es visible a los técnicos, se corre el riesgo de la violación de la privacidad del cliente y la empresa corre el riesgo de que un empleado filtre dicha información para, por ejemplo, iniciar su propia empresa que le haga competencia. Es posible que cierta información como el domicilio del cliente deba ser visible a los técnicos para que puedan trasladarse y cumplir con la tarea que se les ha asignado. A su vez, el servicio de atención al cliente puede necesitar ver los números de teléfono y direcciones de correo electrónico de todos los clientes, pero no necesariamente acceder a sus domicilios.

- Dado que únicamente los técnicos que realizan rondas de visitas a clientes necesitan acceder a información de la empresa por fuera de la oficina, la superficie de ataque cibernético de los sistemas de la empresa puede reducirse limitando el acceso de los demás empleados a la dirección IP interna de la

empresa.

- La sobreexposición de información relacionada con las órdenes de trabajo puede fomentar especulaciones entre los empleados sobre la forma en que se está manejando el negocio, lo cual puede resultar en malentendidos o en una divulgación indebida de las prácticas operativas.

- Cuando los trabajos son asignados a los técnicos de forma arbitraria por el gerente de negocio, existe el riesgo de que un técnico vaya a realizar su trabajo teniendo su certificación o licencia expirada. Los permisos basados en políticas permiten que el técnico deba poseer una licencia o certificación válida como requisito previo a la asignación del trabajo.

Si bien las organizaciones con necesidades de administración de acceso pequeñas pueden inicialmente prescindir de algunas funcionalidades PBAC como las limitaciones de contexto en las políticas de acceso, la adopción temprana de una arquitectura de control de acceso PBAC permite que las reglas de administración de accesos maduren de forma orgánica y natural a lo largo del tiempo - ya sea incorporando más usuarios, más recursos y/o una gestión de riesgos y seguridad más sofisticada.

¿Cuándo es preferible utilizar RBAC?

Dada la prominencia de RBAC como estrategia de control de acceso, este artículo se ha centrado fundamentalmente en la comparación entre los controles de acceso basados en políticas y los controles de acceso basados en roles.

Puede ocurrir que algunos profesionales IAM estén interesados en implementar controles PBAC pero que los sistemas en los que trabajan solo soporten RBAC. En estos casos es mejor repensar los roles institucionales en términos de recursos o de funciones laborales específicas que agrupar permisos que serán difíciles de adaptar con el paso del tiempo. Siempre y cuando un sistema RBAC habilite múltiples roles para un usuario, será viable la incorporación de algunas de las ventajas de PBAC (como la modularidad) en ese sistema.

A la hora de escoger entre RBAC y PBAC, es importante tener en cuenta que es más fiable construir PBAC para que se comporte como RBAC que a la inversa. Por ejemplo, una organización que prefiera pensar en términos de “roles” puede obtener el mismo resultado -es decir que una acción resulte en la aplicación de un conjunto definido de permisos-, asignando permisos de acceso a recursos a cada conjunto de roles. En cambio, las opciones de aplicación de una noción de contexto a los permisos RBAC suelen ser limitadas.

Si bien por su versatilidad y escalabilidad PBAC es una opción sólida para proteger recursos sensibles, es posible que no sea amigable para los usuarios ocasionales de sistemas de administración de acceso. En el caso de sistemas con controles de acceso directos y más bien estáticos, especialmente aquellos que delegan la administración de

acceso a usuarios finales en lugar de a administradores (como en el caso de creadores de contenido que pueden autorizar colaboradores) es posible que prefieran la intuición que ofrece un sistema RBAC a la versatilidad de un sistema PBAC.

Implementando PBAC

La clave para construir exitosamente un entorno de control de acceso reside en su capacidad de adaptación a los cambiantes requisitos de negocio. Para ofrecer una administración de acceso fácil y precisa, el sistema no debe ser demasiado concreto ni demasiado abstracto.

Para lograr este balance en una implementación PBAC ten en cuenta los siguientes principios rectores:

Construye componentes reutilizables

Administrar la abstracción en PBAC significa aislar las partes de tus políticas que pueden ser aplicables a otras políticas. Esto es muy útil, entre otros, en la segmentación de usuarios.

Por ejemplo, si estás construyendo una política para decir que:

Objecto		**Acción**		**Sujeto**	**Contexto**
(Los) Perfiles de usuario	pueden ser	Actualizados	por	Gerentes de negocio	Para empleados de tiempo completo

Es muy probable que los conceptos “gerentes de negocio” y “empleados de tiempo completo” aparezcan en otras políticas. Por eso es sensato crear definiciones para estos segmentos que serán utilizados en una o más políticas.

Para evitar que estas definiciones sean demasiado granulares y rígidas, es importante incorporar en el sistema de administración de accesos aquellas implementaciones que habiliten las lógicas de conjuntos, en particular las intersecciones (permitir la pertenencia al grupo A Y B), las uniones (permitir la pertenencia al grupo A O B) y los complementos (permitir la pertenencia al grupo A PERO NO al grupo B).

Es decir, si la política mencionada más arriba requiere la siguiente actualización:

Objeto		**Acción**		**Sujeto**	**Contexto**
(Los) Perfiles de usuario	pueden ser	Actualizados	por	Gerentes de negocio de la	Para empleados de tiempo completo ***de la oficina de Detroit***

				oficina de Detroit	

la mejor forma de resolverlo suele ser[4] mantener las definiciones de “gerentes de negocio” y “empleados de tiempo completo”, y agregar una tercera: “oficina de Detroit”. La definición “oficina de Detroit” puede usarse tanto para actualizar el sujeto de tu política (otorgando acceso a la intersección de “gerentes de negocio y “oficina de Detroit”) como como variable de contexto (con un acceso que abarque la intersección “empleados de tiempo completo” y “oficina de Detroit”).

Este abordaje hace que la asignación de un permiso a un grupo de individuos sea igualmente fácil que en RBAC, con el beneficio de que se evita la interdependencia entre permisos, permite segmentar de forma limpia los objetos y sujetos y habilita la especificidad a través de permisos de contexto (como grupos de usuarios, identificadores de dispositivos, rangos de direcciones IP o clasificación de documentos).

Facilita la gobernanza y las auditorías

Un buen sistema de control de acceso permitirá que los auditores y propietarios de negocio involucrados en la gobernanza de accesos entiendan los precedentes existentes en los controles de acceso de la organización, analicen cómo pueden llegar a necesitar ser extendidos o modificados y determinen el impacto de los cambios propuestos en el negocio.

A la hora de diseñar un sistema PBAC, es importante asegurarse de que los sujetos, acciones, objetos y contextos estén almacenados de forma tal que un acceso pueda ser reportado de forma directa desde cualquiera de estas perspectivas. Los propietarios del negocio y los auditores deben poder acceder fácilmente a los informes que respondan a preguntas sobre qué accesos tienen los usuarios, qué usuarios pueden acceder a recursos de interés y cuáles son los contextos permitidos para cualquiera de las acciones definidas para un recurso.

La versatilidad de los permisos PBAC hacen que sea realista definir todas las consideraciones de acceso en las políticas. Esta flexibilidad es más ventajosa que la implementación de medidas de seguridad adicionales (como restricciones IP) por fuera del sistema de control de acceso de una organización, ya que permite que haya una única fuente de verdad sobre las circunstancias en las cuales se debe otorgar el acceso.

[4] Los ejemplos de esta sección están pensados para ilustrar la optimización de la capacidad matemática existente en un contexto en el que tanto el proveedor de identidad (o almacén de atributos de usuario) como el proveedor de servicio (o recurso a ser protegido) existen en un entorno común pero no se extiende a contextos federados donde el proveedor de servicio puede estar interactuando con uno o más proveedores de identidad controlados externamente. Dicho esto, cabe mencionar que PBAC (/ABAC/CBAC) puede admitir fácilmente estas externalidades.

Reportar sobre los permisos de esta manera facilita el análisis de las reglas actuales para acceder a un recurso. Un buen informe puede también incluir a los usuarios que actualmente cumplen con los requisitos de acceso. Si bien PBAC suele utilizarse en contextos federados en los que la información de identidad (y otra información de contexto) no está disponible para el administrador del recurso, los informes de usuario pueden ser útiles para realizar controles puntuales especialmente en el contexto de un cambio propuesto. Los informes sobre quién ganaría o perdería acceso bajo una política propuesta permiten que los propietarios de negocio y auditores perfeccionen los controles para cubrir de la mejor manera las necesidades y la seguridad de la organización.

Prioriza los estados sobre los eventos

Los procesos de negocio suelen desarrollarse mediante diagramas de flujo que se enfocan en eventos. Por lo general esto conduce a sistemas de administración de accesos que se implementan basándose en eventos con forma de diagrama de flujo, como la asignación de un acceso cuando un nuevo empleado es contratado.

Al basarse en atributos visibles, las políticas PBAC tienden a enfocarse en los estados como el cargo actual de un empleado. Esto ofrece muchas ventajas:

- **Menos estados que eventos:** Cuando el aprovisionamiento de acceso se desencadena cuando un empleado ingresa por primera vez a su cargo, es necesario poder diferenciar entre contrataciones externas, traslados internos y ascensos. Los eventos inesperados como una rescisión cancelada también deben ser considerados.

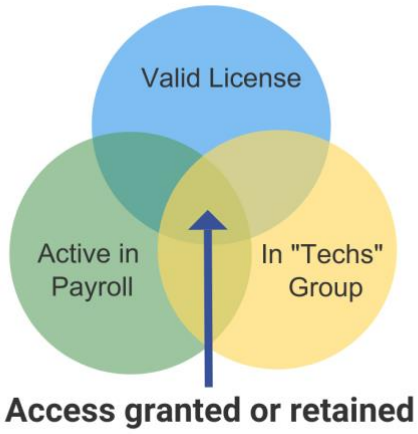
- **Cambios en los procesos locales:** Es mucho más probable que los equipos de administración de acceso sean informados sobre cambios en estados relevantes (por ej., empleo, políticas de la compañía, funciones de negocio) que sobre cambios en eventos (por ej. cuántos procesos pueden usarse para contratar personal, cambios en la red de la compañía, mejoras en la infraestructura, etc.).

  Cuando los procesos de departamentalización cambian de forma tal que afectan la detección de eventos que desencadenan accesos, los equipos de administración de acceso son responsables de investigar las inconsistencias resultantes y deberían evaluar el correcto funcionamiento de sus sistemas.

- **Los estados son reconciliables:** Los eventos ocurren en un momento determinado en el tiempo dificultando la evaluación de su pertinencia. Por ejemplo, alguien podría tener acceso mediante un proceso heredado que ha sido revisado (y cuyo acceso debe mantenerse) o porque quedó incompleto un proceso de desaprovisionamiento del acceso (en cuyo caso se debe revocar el acceso). Sin una política con la cual comparar, se hace muy difícil determinar si los permisos existentes son apropiados lo cual erosiona la confianza en el sistema.

Los estados pueden ser monitorizados continuamente habilitando que se lleve a cabo una reconciliación del acceso automática que garantiza que el acceso está permitido en la política actual y facilitan el análisis del impacto de los cambios propuestos en las políticas.

Para organizar reglas de acceso que construyan políticas PBAC robustas, considera dejar de lado las flechas de los diagramas de flujo y trabaja únicamente con círculos que representen condiciones. Organizar estos círculos como diagramas de Venn o de Euler[5] habilita el diálogo sobre qué condiciones de acceso son aceptables, resultando en políticas más claras y robustas.

Diseño de Permiso basado en Evento	**Diseño de Permiso basado en Estado**
Se ve como: Diagramas de flujo **Resulta en:** Diagramas de flujo rígidos y secuenciales, validación en tiempo real, una lógica de desaprovisionamiento complicada.	**Se ve como:** Círculos superpuestos **Resulta en:** Flujos de trabajo flexibles y paralelos, validación continua, una armonía entre el aprovisionamiento y el desaprovisionamiento.
	

Habilita la separación de intereses

Probablemente, una guía más avanzada sobre PBAC haga referencia a estándares como el Lenguaje eXtensible de Marcas de Acceso de Control de OASIS (XACML, por sus siglas en inglés)[6]. Estos estándares pueden ser particularmente útiles cuando se desea

[5] "Diagrama de Euler," https://es.wikipedia.org/wiki/Diagrama_de_Euler, (consultado el 25 de febrero de 2020)

[6] "Lenguaje eXtensible de Marcas de Acceso de Control (XACML) Version 3.0 Plus Errata 01," https://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os-complete.pdf (consultado el 20 de mayo de 2022)

mantener una separación entre los componentes de un sistema PBAC, como en el caso de sistemas federados o cuando las políticas se basan en información sensible.

A modo de ejemplo, consideremos el caso de un instrumento científico que está sujeto a leyes federales que requieren que todos sus usuarios sean ciudadanos o residentes permanentes legalizados y que se les haya realizado una verificación de antecedentes dentro de los últimos tres años. La separación de políticas sirve para hacer cumplir la política sin compartir con el instrumento información sobre la ciudadanía, situación migratoria y resultados de la verificación de antecedentes del usuario. Al mantener por separado la definición de las políticas, la evaluación de las políticas y el cumplimiento de las políticas, la organización puede cumplir con sus obligaciones legales sin propagar información sensible de los usuarios a lo largo de los recursos que administra (o, en contextos federados, por fuera del alcance de la organización).

Conclusión

Los sistemas de control de acceso promueven e implementan una estrategia de control de acceso de una organización a medida que ocurren cambios en los usuarios, personal, responsabilidades, estructura organizacional y obligaciones legales. La mayoría de las fallas en la administración de accesos ocurre cuando la implementación de un sistema es demasiado manual como para ser escalable, y demasiado precaria como para poder adaptarse a las cambiantes necesidades del negocio sin tener que llevar a cabo esfuerzos de reestructuración costosos y que consuman mucho tiempo.

Si bien es habitual medir la optimización de un sistema de control de acceso evaluando su eficacia para *otorgar* accesos, la verdadera medida para saber qué tan robusto es un sistema de control de acceso es su consistencia para *revocar* los mismos. Al ofrecer una lógica de simetría entre la asignación y revocación de accesos, los controles de acceso basados en políticas habilitan el principio de seguridad de mínimo privilegio. Definir políticas de acceso permite que los accesos sean evaluados dinámicamente y revocados o reportados automáticamente ni bien queden invalidados por la política actual.

Desarrollar los controles de acceso desde una perspectiva de recurso e incorporarles la noción de contexto permite que los sistemas PBAC maximicen la seguridad de los recursos, poniéndola por delante de la conveniencia de la asignación de accesos. Si bien al comienzo estos sistemas pueden ser más complejos que otros abordajes, la naturaleza indivisible de sus políticas y su relativa capacidad de adaptación de los permisos heredados hacen que el sistema sea más sostenible en el tiempo si se lo compara con sistemas de administración de acceso basados en reglas como el RBAC.

Biografía del Autor

Mary McKee se desempeña como directora adjunta de seguridad de la información y como directora sénior de servicios de administración de identidades y seguridad en la Universidad de Duke, donde fue estudiante de grado en ciencias de la computación y posteriormente contratada como desarrolladora de aplicaciones web. Su interés en la

abstracción e interoperabilidad la condujeron a la administración de identidades y accesos y, por consiguiente, a la seguridad de la información.

Agradecimientos

La autora quiere agradecer a André Koot y Andrew Hildle por sus meditadas respuestas a las versiones anteriores de este artículo, y a Heather Flanagan, Christienna Fryar, Dave Wible y Mary Ellen Wible por sus devoluciones y apoyo en su desarrollo.

Registro de cambios

Fecha	Cambio
03-06-2022	V2 publicada; se aclara el alcance del artículo indicando que se trata de un artículo introductorio, se reemplaza la sección sobre controles de acceso estáticos; se elimina la sección sobre privacidad
19-04-2021	V1 publicada