# Técnicas para abordar el mínimo privilegio

Por Matthew K. Carter



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

## Tabla de contenidos

## Resumen

Este artículo se enfoca en el ciclo de vida y las técnicas de control de acceso que los profesionales deben considerar al otorgar, validar y perfeccionar los permisos hacia el principio de mínimo privilegio. Comparamos los abordajes Justo-a-Tiempo (JIT, por sus siglas en inglés) con los permisos duraderos, equilibrando la productividad con la seguridad. El artículo también explora los riesgos del uso de datos históricos para perfeccionar los permisos. El lector aprenderá a perfeccionar el principio de mínimo privilegio en el contexto de un ciclo de vida de una identidad y para una actividad específica. Este artículo es escéptico en lo que respecta a las soluciones en la nube, híbridas y locales (*onprem*) así como a las herramientas.

## Introducción

Disminuir los permisos excesivos es un esfuerzo continuo. Los miembros de la fuerza laboral acumulan permisos a lo largo de sus trabajos a la vez que los requisitos laborales cambian con regularidad. Las personas asumen encargos o tareas temporales y las organizaciones suelen ser mejores para otorgar permisos que para quitarlos. Los proveedores SaaS e IaaS cambian constantemente el área de permisos que los clientes necesitan administrar. Otorgar un nivel suficiente de privilegios a los empleados, socios y clientes que acceden a un recurso digital sin poner en riesgo la organización, es desafiante. El principio de *mínimo privilegio* es el mejor escenario hipotético posible en el que un actor humano o no-humano solo tiene los permisos estrictamente necesarios para realizar una tarea en el momento en que debe ser realizada. Entender las técnicas para crear y perfeccionar permisos puede ayudarte a abordar el principio de mínimo privilegio y a reducir el riesgo de adoptar una postura excesivamente permisiva.

En este artículo hablaremos del mínimo privilegio en el contexto del ciclo de vida de la identidad y del desarrollo de políticas para actividades específicas. Revisaremos las ventajas de la otorgación de permisos a largo y corto plazo, teniendo en cuenta técnicas como los permisos Justo-a-Tiempo (JIT). Utilizaremos los roles como una forma de agrupar los permisos relacionados con la identidad y las actividades. Este uso es una extensión natural del Control de Acceso Basado en Roles (RBAC, por sus siglas en inglés), aunque no todas las organizaciones utilizan los roles para modelar permisos de la misma manera. A diferencia de la asignación de múltiples permisos a una entidad humana o no-humana, los roles son una forma natural de agrupar múltiples permisos con el fin de reducir su mantenimiento. Mostraremos las diferencias entre el principio de mínimo privilegio aplicado, RBAC y el Control de Acceso Basado en Políticas (PBAC, por sus siglas en inglés) pero, de cualquier forma, en este artículo los roles serán el mecanismo principal para agrupar permisos.

## Terminología

**Mínimo privilegio** - "Principio por el cual un recurso, como un usuario, puede acceder únicamente a los recursos (como aplicaciones, datos, etc.) que son necesarios para el cumplimiento de su función."[1]

**Usurpación de cuenta** - La usurpación de cuenta es una forma de robo de identidad y fraude, por la cual terceros maliciosos logran acceder exitosamente a las credenciales de la cuenta de un usuario.[2]

**Certificación de acceso** - La certificación es la revisión continua de quién tiene qué accesos (por ej., los procesos de negocio para verificar que los derechos de acceso son correctos). [2]

**Administración de Accesos Privilegiados** - Es un mecanismo para administrar el acceso temporal a cuentas con permisos de riesgo alto. A menudo, la PAM (por sus siglas en inglés) implica la entrega y devolución de una credencial generada para un solo uso.

**Acceso Justo-a-Tiempo** (JIT, por sus siglas en inglés) - Es una técnica mediante la cual una credencial o un permiso son otorgados temporalmente a una entidad principal por el lapso necesario para desarrollar una actividad determinada. El acceso es revocado una vez que la actividad es completada, limitando su uso.

**Eliminación Completa de Privilegios** (ZSP, por sus siglas en inglés) - Es un estado en el que un acceso JIT se utiliza en todos los permisos y en el que ningún permiso duradero es asignado a una entidad principal.

**Gestión de Derechos de Infraestructura en la Nube** (CIEM, por sus siglas en inglés) - Una clasificación de las tecnologías enfocada en gestionar la otorgación, verificación y perfeccionamiento de los permisos para las tecnologías en la nube o híbridas. CIEM es a menudo visto como un componente de la Gobernanza y Administración de Identidades (IGA, por sus siglas en inglés).

**Infraestructura como código** - Es un proceso de administración y aprovisionamiento de los centros de datos informáticos (*Data Centers*) mediante ficheros legibles por máquina en

---

[1] Laboratorio de Tecnología de la Información NIST, "Mínimo privilegio," glosario del Centro de Recursos de Seguridad Informática, https://csrc.nist.gov/glossary/term/least_privilege (consultado el 6 de septiembre de 2022).

[2] Flanagan (Editor), H., (2021) "Terminología en el Cuerpo de Conocimiento de IDPro", *Cuerpo de Conocimiento de IDPro* 1(8). doi: https://doi.org/10.55621/idpro.41.

lugar de configuraciones físicas de *hardware* o de herramientas interactivas de configuración.[3]

## El mínimo privilegio en el ciclo de vida de la identidad

El mínimo privilegio puede aplicarse a cada etapa del ciclo de vida de la identidad. Los derechos naturales deben perfeccionarse continuamente para ayudar a los nuevos empleados de la fuerza laboral (incorporaciones)[4] a ser más productivos desde el primer día, sin otorgar permisos excesivos que un empleado sin experiencia podría usar incorrectamente por accidente. Los empleados que cambian de trabajo (traslados) heredan nuevos permisos. Esto puede requerir la eliminación de los permisos de su trabajo anterior durante la transición, lo cual puede causar demoras en la revocación de permisos hasta que la transición se complete. En el caso que los permisos del nuevo trabajo generen una combinación tóxica con la función laboral anterior, estas demoras pueden poner en riesgo de violación del principio de segregación de tareas (SoD, por sus siglas en inglés) a las empresas. Los empleados salientes (bajas) aún pueden necesitar tener un acceso limitado a los recursos de la empresa, como a sus recibos de sueldo y formularios fiscales W-2. Garantizar que el credencial post-empleo del exempleado tenga permisos limitados puede evitar daños.

Es un error común pensar que el mínimo privilegio en la fuerza de trabajo se debe a la falta de confianza en los empleados. De hecho, el principio de mínimo privilegio protege a los empleados y empleadores limitando su exposición. A menudo, un conjunto de permisos naturales basados en su función laboral es otorgado a un nuevo empleado. Los permisos disponibles para ese empleado deberían ser continuamente perfeccionados, agregando o eliminando permisos para alinearse de mejor manera con las necesidades del empleado a medida que progresa en su ocupación. Los permisos excesivos pueden resultar en un aprovechamiento por parte de agentes maliciosos. Es más probable que un empleado advierta una *usurpación de cuenta* cuando está usando activamente un permiso que cuando no, ya que notará cambios en el recurso.

Para alinear los permisos otorgados con el objetivo siempre cambiante del mínimo privilegio, las organizaciones deben perfeccionar los permisos otorgados mediante derechos naturales y las solicitudes de acceso. Si estos permisos naturales son administrados mediante roles, los roles deben ser examinados en busca de permisos excesivos. Si los roles no aplican de manera consistente a los sujetos o entidades

---

[3] Contribuyentes de Wikipedia, "Infraestructura como código," *Wikipedia, La Enciclopedia Libre,* https://es.wikipedia.org/wiki/Infraestructura_como_c%C3%B3digo (consultado el 6 de septiembre de 2022).

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

principales a los cuales los roles son asignados, entonces estos roles deben ser modificados de forma que sean representativos de las actividades que el sujeto o entidad principal necesitan realizar. Un permiso insuficiente suele causar una baja en la productividad, así que para encontrar un equilibrio cada permiso debe ser evaluado.

Las solicitudes de acceso autogestionadas pueden incorporar un abordaje de mínimo privilegio para garantizar que la vida útil temporal de los privilegios sea utilizada para acciones de un solo uso. Los permisos de larga duración otorgados mediante solicitudes de acceso autogestionadas son evaluados durante la certificación de acceso junto con los permisos de derechos naturales para perfeccionar el permiso, sin importar cuándo fue otorgado el permiso. El acceso temporal puede involucrar la Administración de Accesos Privilegiados (PAM) o las técnicas de permiso JIT descritas más abajo.

Durante el proceso de *certificación de acceso*, los empleados revisan quién tiene acceso a los recursos. Un camino posible es la eliminación de los permisos innecesarios que puedan generar un riesgo para una organización. Este concepto es uno de los aspectos del principio de mínimo privilegio, donde se evalúa cada acceso que tienen las entidades humanas y no-humanas. Los administradores y propietarios de aplicaciones son responsables de perfeccionar los permisos para encontrar el equilibrio entre productividad y seguridad. Las soluciones de gobernanza de acceso son desarrolladas para realizar esta evaluación de riesgo. Las soluciones de *Gestión de Derechos de Infraestructura en la Nube* (CIEM) también proveen herramientas para perfeccionar los permisos de empleados de la fuerza laboral.

Los permisos inutilizados no equivalen a los permisos innecesarios. Algunas actividades son menos frecuentes que otras, como el acceso a documentos impositivos, así que evita perfeccionar el mínimo privilegio basándote en períodos estáticos. Algunas actividades pueden tener una frecuencia anual o menor, como la activación de un plan de contingencia (aunque ojalá tu empresa esté llevando a cabo tu planificación de continuidad de negocio y esto no sea necesario).

## El mínimo privilegio para actividades

En este contexto, una actividad debe pensarse como un conjunto de recursos y acciones para realizar una tarea. Por ejemplo, supongamos que tienes que administrar los permisos de un proceso de *Infraestructura como Código* (IaC, por sus siglas en inglés) el cual genera múltiples activos digitales de diferentes tipos de recursos para crear una aplicación. Supongamos que también tienes que administrar los permisos para operar esta nueva aplicación luego de su implementación. Es comprensible que te inclines a ejecutar los procesos IaC como “Admin”[5] ya que pensar y definir políticas de gobernanza para un

[5] “Admin” - es el término corto para referirse a un usuario con privilegios o a un rol que tiene control total de un entorno digital. El alcance de un “Admin” puede variar, pero representa un conjunto de

conjunto de recursos y acciones desconocido puede consumir mucho tiempo. Sin embargo, la tentación de operar continuamente como un usuario con privilegios puede resultar en permisos excesivos duraderos que pueden ser el blanco de una escalada de privilegios no autorizados.

Una actividad suele estar dividida en acciones más granulares y en recursos que son regulados por el sistema de autorización. En el caso de nuestro ejemplo IaC, el proceso puede incluir acciones de creación, modificación y eliminación de fuentes de computación y de datos para configurar y eliminar la aplicación. En este artículo, solo consideraremos los permisos acción-recurso de granularidad gruesa, por ejemplo: "crear-cómputo" o "modificar-basededatos".[6]

Dos técnicas para crear roles de mínimo privilegio para actividades son **falla-luego-agrega** y **registra-luego-reemplaza**. Cada técnica tiene un equilibrio diferente entre seguridad y productividad, limitando el uso de accesos privilegiados.

En la técnica **falla-luego-agrega**, inicialmente el proceso de Infraestructura como Código (Iac) no otorga permisos. El proceso IaC se ejecuta y luego, cuando falla la autorización, se decanta qué permiso debe ser otorgado y se habilita el acceso. Esta secuencia se repite hasta que el proceso IaC se completa. Si bien este abordaje de fuerza bruta puede parecer ineficaz, el artefacto de rol que produce puede usarse en posteriores ejecuciones de los procesos IaC, garantizando el principio de mínimo privilegio para esta actividad. Para que esta técnica sea viable debes tener un claro mecanismo de retroalimentación de los permisos necesarios y una capacidad de restauración transaccional. También es necesario que el profesional tenga una comprensión clara de las actividades requeridas. Otorgar permisos laxamente sin tener una buena comprensión de las actividades, conduce a una acumulación de privilegios innecesarios ya que una vez que todo está en funcionamiento, estos permisos superfluos rara vez son revocados.

La segunda técnica, y la más recomendable, toma un abordaje del tipo **registra-luego-reemplaza**. Inicialmente estos procesos IaC asignan un rol con privilegios como el de "Admin", el cual tiene permisos para realizar todas las acciones en todos los tipos de recursos en los procesos IaC. Para cada acción realizada por el proceso IaC se registra un evento mediante mecanismos como los registros de auditoría. Una vez que la actividad se completa, pueden extraer las acciones del registro de eventos y asignar los permisos necesarios a un nuevo rol de "mínimo privilegio". Con el nuevo rol de mínimo privilegio se

---

permisos que habilitan a una persona a controlar, manipular o dañar recursos y que por lo tanto debe ser estrictamente controlado.

[6] En términos de política, las restricciones de una organización para el aprovisionamiento de un recurso como "computar" pueden ser muy específicas. Por ejemplo, una organización puede querer permitir la creación de una base de datos únicamente en una región particular, con determinado tamaño y habilitando características específicas.

ejecutan posteriores procesos IaC, reemplazando el rol con privilegios “Admin”. Este nuevo rol de mínimo privilegio te da un rol de actividad específico que puede ser usado por otras entidades principales.

En el caso que una actividad no relacionada o no autorizada esté siendo ejecutada por la entidad principal durante el registro, basar el principio de mínimo privilegio en eventos históricos como los registros de auditoría, tiene la potencial desventaja de la incorporación de permisos no relacionados o no autorizados dentro del rol de mínimo privilegio. Revisa tus permisos registrados para verificar que no se hayan colado permisos superfluos o no autorizados en tu rol de mínimo privilegio.

Es importante separar las actividades de configuración y eliminación, de las actividades operativas. Las actividades de configuración y eliminación pueden involucrar permisos con privilegios que luego son excesivos para los actores humanos una vez que la actividad no-humana fue completada. En nuestro ejemplo IaC, la creación de soluciones de cómputo y de almacenamiento de datos, así como su posterior modificación son actividades de configuración, mientras que la ejecución de consultas y mutaciones son actividades operativas. Los permisos de configuración son limitados para los procesos IaC no-humanos. Cuando estés registrando operaciones en tu registro de auditoría, para definir el rol de configuración debes detener el registro enseguida después de la configuración. Esto evita que se incluyan permisos de modificación de la política en el rol operacional, dejando únicamente los datos de consultas y mutaciones. Un operador que tenga permisos de modificación de la política podría otorgarse permisos a sí mismo, violando así el principio de mínimo privilegio.

Para configurar las notificaciones de cambios en permisos, trabaja juntamente con tus proveedores de recursos digitales. Si tu rol tiene privilegios basados en expresiones como los comodines, que habilitan la incorporación automática de nuevos permisos, un cambio en los permisos de un recurso puede introducir nuevos riesgos y alejarte del principio de mínimo privilegio.

## Permisos Justo-a-Tiempo

Consideremos el factor tiempo del principio de mínimo privilegio. Por lo general, para un mismo permiso, es más seguro que un usuario principal tenga un acceso temporal que un acceso duradero. Podrás abordar el principio de mínimo privilegio simplemente permitiendo que una actividad se ejecute en el momento en que necesita ser ejecutada. La depuración paralela de permisos innecesarios junto a un abordaje JIT para otorgar permisos, nos acercan al principio de mínimo privilegio. Sin embargo, ten en cuenta que el JIT puede no ser adecuado para todas las organizaciones debido a la sobrecarga que genera la administración de accesos temporales y a la tasa de productividad que implica tener que realizar una consulta cada vez.

En un modelo de permisos duraderos, aun cuando los permisos de rol son perfeccionados con el tiempo, los permisos efectivos de la entidad principal se acumulan dentro de los permisos de rol. La entidad tiene el permiso en cualquier momento que lo necesite ya que el permiso persiste a través de la asignación de rol.

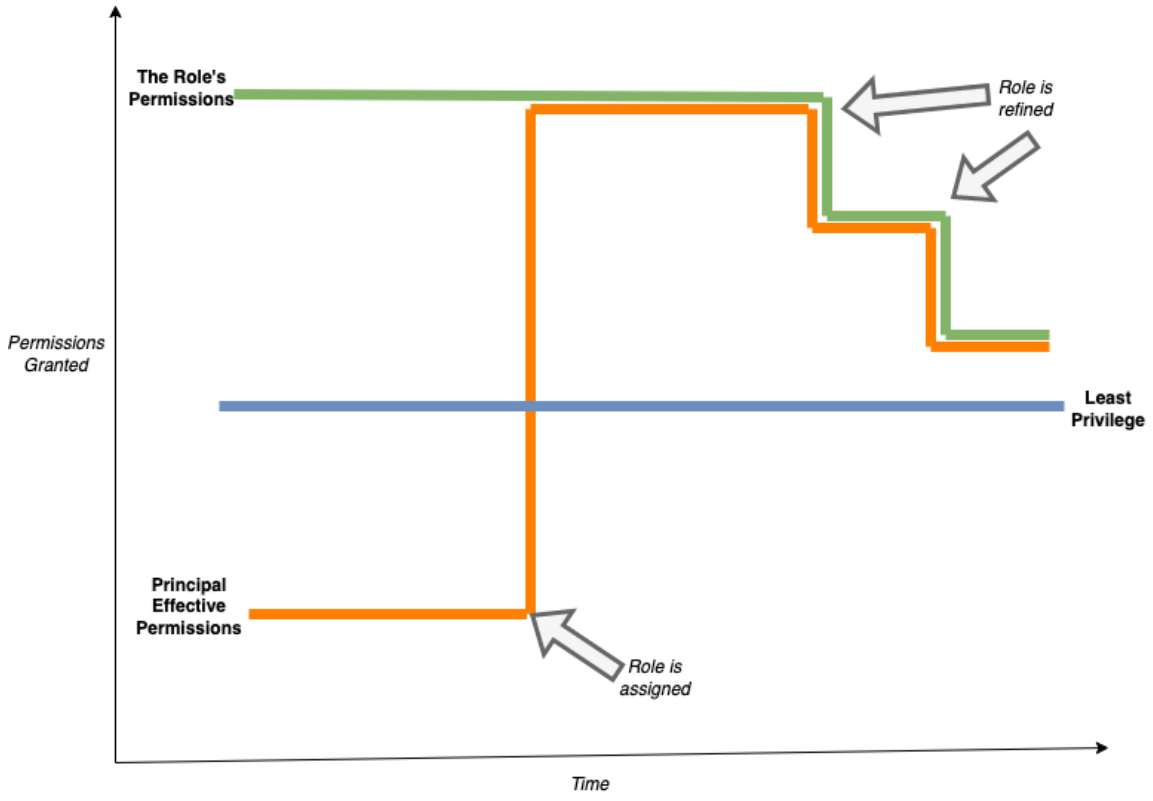


*Figura 1: Modelo de mínimo privilegio de permisos duraderos*

El mínimo privilegio es una actividad que debe ser evaluada en puntos específicos del tiempo, al momento en que una entidad principal debe realizar una acción o acceder a información protegida. En un modelo JIT, los permisos son otorgados únicamente por el periodo necesario, para realizar la actividad y luego son revocados. Al separar el acceso privilegiado temporal de las asignaciones de roles duraderos y de los permisos otorgados por los roles, hay una menor acumulación de permisos excesivos en esos roles duraderos.

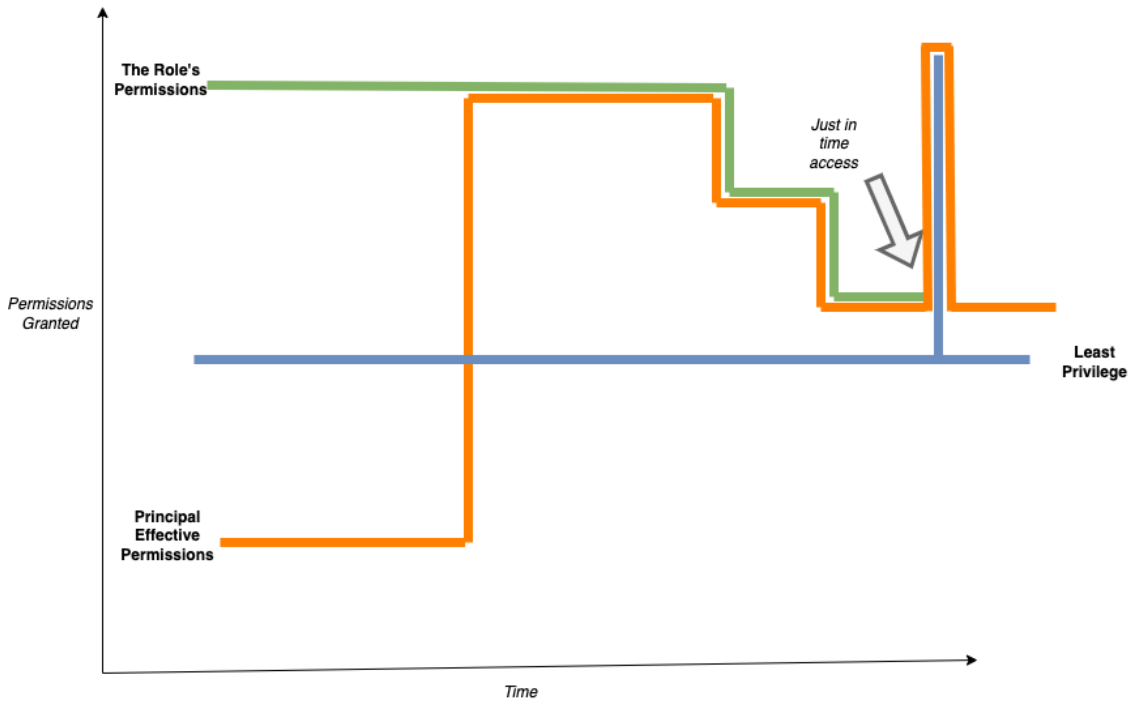


*Figura 2: Modelo de mínimo privilegio Justo-a-Tiempo*

El abordaje JIT es análogo a los sistemas de *Administración de Accesos Privilegiados* (PAM) y funciona con un sistema de "*check out*" y "*check in*" de la credencial utilizada para acceder a un sistema compartido (y generalmente también sensible). Los sistemas PAM se basan en hacer una copia de trabajo ("*check-out*" o "desproteger") para luego realizar cambios en la copia y volver a ingresar el recurso al repositorio ("*check-in*" o "proteger"). En cambio, en lugar de hacer *check out* de una credencial, el abordaje JIT habilita al actor a hacer *check out* de un permiso determinado para realizar una acción. Es decir que el abordaje JIT habilita a la entidad principal a hacer *check out* de su rol y de sus permisos necesarios para realizar la actividad. Los permisos otorgados para ese acceso JIT también deben ser continuamente perfeccionados.

Los riesgos asociados a los permisos duraderos o a la asignación de roles a largo plazo tienen que ver con una escalada de privilegios no autorizados. Si una credencial de una entidad principal está comprometida u otra entidad principal tiene permiso para asumir ese rol, una escalada de privilegios ocurre. Un abordaje JIT puede mitigar la escalada de privilegios ya que la entidad principal de la credencial comprometida no tiene un permiso duradero. Adicionalmente, la entidad principal debe hacer *check out* del rol o del permiso. Para que este proceso de mitigación de riesgos sea exitoso, la credencial comprometida no puede ser la misma que se usa para hacer *check out* del rol o de los permisos necesarios para la escalada de privilegios. Por todo lo anterior, la mejor práctica dicta que el sistema JIT debe requerir obligatoriamente un factor de autenticación adicional. Por ejemplo, si las operaciones habituales utilizan una biometría de huella digital, la escalada de privilegio podría requerir un *token* de *hardware*.

Al implementar el principio de mínimo privilegio se debe considerar un equilibrio entre seguridad, productividad y conveniencia. Si el costo de desarrollar y mantener un perfeccionamiento continuo del acceso JIT superan el impacto de la escalada de privilegios en tu sistema, es posible que prefieras aceptar el riesgo de la otorgación de permisos duraderos o innecesarios a entidades principales. Cuando se les da un tratamiento casi quirúrgico a los permisos, se compromete la productividad y hasta existe un riesgo de interrupción de las tareas habituales. Los empleados que estén obligados a hacer *check out* de permisos constantemente para poder realizar su trabajo pueden hartarse y buscar la manera de evitar el control.

## La relación del mínimo privilegio con el Control de Acceso Basado en Políticas

Por lo general, el Control de Acceso Basado en Políticas (PBAC)[7] implementa bien el principio de mínimo privilegio dado que sus reglas tienden a ser más granulares que las de RBAC, ya que provee especificaciones para recursos y acciones específicas. Por ejemplo, la siguiente instrucción natural es representativa de las reglas PBAC:

*Permite leer el contenido solo si el permiso del lector es más alto que la clasificación del contenido.*

Esta instrucción otorga el permiso de lectura del contenido basándose en una comparación condicional de un atributo de identidad (el permiso del lector) con un atributo de recurso (la clasificación del contenido). Para abordar el mínimo privilegio, esta regla podría actualizarse especificando una población menor de lectores o especificando en qué instancia del servidor de contenido es válida. Sin embargo, esto hace que PBAC pierda en parte su valor ya que tienes que tener reglas para cada instancia del servidor de contenido enlistada. El mínimo privilegio armoniza con la naturaleza centralizada de las decisiones de políticas de PBAC y con la mantenibilidad que surge de tener reglas que pueden aplicar a múltiples abstracciones.

De hecho, PBAC puede ser modelado siguiendo el principio de mínimo privilegio a varios niveles. Por ejemplo, para perfeccionar el caso mencionado más arriba sobre el servidor de contenido y llevarlo hacia el principio del mínimo privilegio, podrías agregar una expresión de red que incorpore límites adicionales sobre la ubicación en la que los lectores pueden acceder al contenido, o podrías incluir un motor de puntuación de riesgos en una regla que impida la anulación del permiso.

---

[7] Encuentra más información sobre el Control de Acceso Basado en Políticas en el artículo de Mary K McKee “Introducción al Control de Acceso Basado en Políticas (v2)” del Cuerpo de Conocimiento de IDPro 1(8). doi: https://bok.idpro.org/article/id/61/

*Permite leer contenido solo si el permiso del lector es más alto que la clasificación del contenido y dentro de un rango específico de ip.cliente*
*Y*
*Recházalo si el riesgo de lectura del contenido es más alto que bajo*

Perfeccionar el control de acceso basado en políticas con un abordaje JIT inherentemente requiere menos esfuerzo que hacerlo en un modelo RBAC. Sin embargo, implica realizar una auditoría rigurosa de las reglas PBAC en busca de aquellas que podrían otorgar accesos innecesarios a una población, o que tienen una ruta inaccesible.
La gobernanza de acceso es menos madura en PBAC que en RBAC, así que probablemente haya menos ofertas comerciales en esa área.

## Síntesis

El mínimo privilegio es un objetivo que cambia constantemente y que funciona como una zanahoria para los equipos de gobernanza que buscan reducir el riesgo de escalada del privilegio no autorizado. Perfeccionar continuamente los permisos asignados por derecho natural, habilitar las solicitudes de acceso autogestionadas y las actividades específicas pueden limitar la acumulación de accesos privilegiados que con el tiempo pueden conducir a un uso inapropiado de los mismos. Incorporar estrategias JIT para la otorgación de permisos de corta duración para realizar una tarea temporal, reduce la cantidad de permisos duraderos. Antes de invertir en herramientas o procedimientos, las organizaciones deben tener en cuenta el riesgo de productividad que implica un perfeccionamiento excesivo de los permisos o la sobrecarga que genera tener que solicitar permisos con demasiada frecuencia. Monitorea el modelo de permisos de tu proveedor para garantizar que los nuevos permisos introducidos no generen riesgos en tus políticas que usan comodines. En la medida que elijas un modelo de control de acceso basado en roles o en políticas, tus técnicas para alcanzar el mínimo privilegio variarán, pero los conceptos serán consistentes. La evaluación continua de estos factores a lo largo del ciclo de vida de todas las identidades y políticas reducirá la superficie de ataque.

## Biografía del autor

Matt Carter se ha desempeñado en la industria de la identidad y seguridad en la nube desde su incorporación a Netegrity en el año 2000. Carter ha ocupado varios cargos, incluyendo gestión de producto, pre-ventas e implementación en empresas como Oracle, AWS y Axiomatics. Actualmente, es especialista de ventas CIAM en Okta. Matt ha colaborado activamente con IDPro como redactor de preguntas en exámenes de certificación y forma parte del comité del Cuerpo de Conocimiento.

Matt Carter vive en el gran Boston con su esposa, dos perros, dos gatos y tiene tres hijos en la universidad. Le gusta el pickleball, hacer kayak en el río Charles y la ciencia ficción. Dato curioso: una vez Matt corrió con los toros en Pamplona...en chancletas.