**Gestión de identidades y accesos**

La seguridad va más allá de simplemente combinar procesos y tecnologías para proteger los activos: consiste en garantizar que estos procesos y tecnologías creen un entorno seguro que respalde una estrategia defensiva. Una clave para lograr esto es implementar dos principios fundamentales de seguridad que limiten el acceso a los recursos de las organizaciones:

* El **principio de mínimo privilegio**, según el cual a un usuario solo se le otorga el nivel mínimo de acceso y autorización requerido para completar una tarea o función.
* **La segregación de funciones**, que es el principio según el cual no se debe conceder a los usuarios niveles de autorización que les permitan hacer un uso indebido de un sistema.

Estos dos principios suelen funcionar en conjunto. El mínimo privilegio establece límites en cuanto al acceso y autorización que una persona recibe, mientras que la segregación de funciones divide las responsabilidades entre varias personas para evitar que recaiga demasiado control en una sola.

Anteriormente, aprendiste sobre el protocolo o marco de autenticación, autorización y trazabilidad (AAA, por sus siglas en inglés). Muchas empresas utilizan este modelo para implementar estos dos principios de seguridad y gestionar el acceso de los usuarios. En esta lectura, aprenderás sobre otro marco importante para gestionar el acceso de usuarios, **la gestión de identidades y accesos** (IAM, por sus siglas en inglés). Ampliarás tus conocimientos sobre las similitudes entre AAA e IAM y cómo se implementan habitualmente.

**Gestión de identidades y accesos (IAM)**

A medida que las organizaciones dependen cada vez más de la tecnología, los organismos reguladores aumentan su presión  para que demuestren que están haciendo todo lo posible por prevenir amenazas. La **gestión de identidades y accesos** (IAM) es un conjunto de procesos y tecnologías que ayuda a las empresas a administrar las identidades digitales en su entorno. Tanto los sistemas AAA como los IAM están diseñados para autenticar usuarios, determinar sus derechos de acceso y realizar un seguimiento de sus actividades dentro de un sistema.

Cualquiera de los dos modelos utilizados por tu organización es más que un solo sistema claramente definido. Cada uno de ellos consiste en una serie de controles de seguridad que garantizan que el *usuario adecuado* tenga acceso a los *recursos correctos* en el *momento oportuno* y por las *razones apropiadas*. Cada uno de estos cuatro factores es determinado por las políticas y procesos de la empresa para la que trabajas.

**Nota:** Un usuario puede ser una persona, un dispositivo o un software.

**Autenticación de usuarios**

Para garantizar que el usuario adecuado acceda a un recurso, se requiere algún tipo de prueba de que este es quien dice ser. En un [video sobre controles de autenticación](https://www.coursera.org/learn/activos-amenazas-y-vulnerabilidades/lecture/r6XuB/controles-de-acceso-y-sistemas-de-autenticacion), aprendiste que hay algunos factores que permiten confirmar la identidad de:

* **Conocimiento:** algo que el usuario sabe.
* **Posesión:** algo que el usuario posee.
* **Inherencia:** algo que el usuario es.

La autenticación se verifica principalmente mediante credenciales de inicio de sesión. El **inicio de sesión único** (SSO), una tecnología que combina varios inicios de sesión diferentes en uno solo, y la **autenticación de múltiples factores, o multifactor,** (MFA), una medida de seguridad que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red, son otras herramientas que las organizaciones utilizan para autenticar a personas y sistemas.

**Consejo profesional:** La siguiente es otra forma de recordar este modelo de autenticación: algo que sabes, algo que posees y algo que eres.

**Aprovisionamiento de cuentas de usuarios**

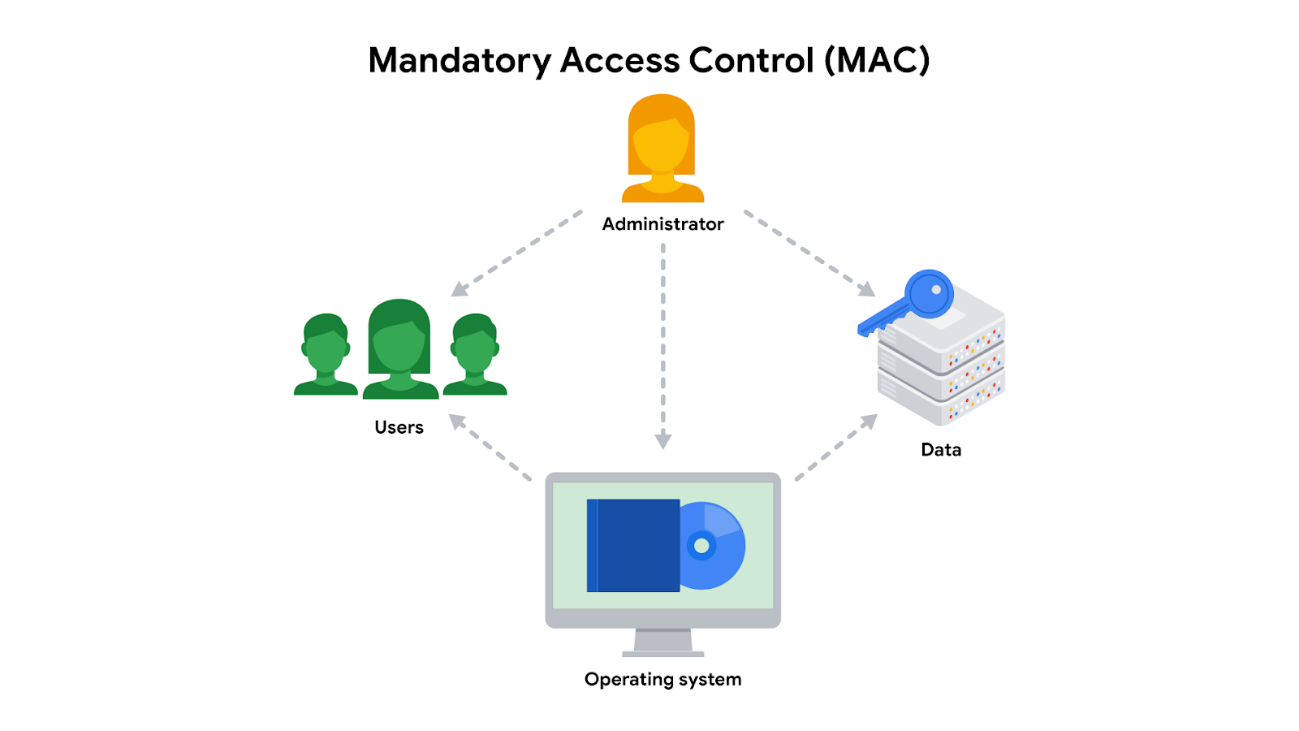
Los sistemas backend deben ser capaces de verificar si la precisión de la información proporcionada por los usuario. Para lograrlo, es necesario realizar un adecuado **aprovisionamiento de usuarios,** que consiste en el proceso de crear y mantener la identidad digital de cada usuario. Por ejemplo, cuando una universidad contrata a un nuevo profesor, se crea una nueva cuenta de usuario. Esta cuenta se configura para brindar acceso a recursos exclusivos destinados a los profesores durante el período en el que están dando clases. Los analistas de seguridad suelen participar habitualmente en el aprovisionamiento de usuarios y en la asignación de sus accesos.

**Consejo profesional:** Otra función de los analistas en IAM es la de desaprovisionar usuarios. Esta es una práctica importante que elimina los derechos de acceso de un usuario cuando ya no debería tenerlos.

**Concesión de autorización**

Si el usuario adecuado ha sido autenticado, la red debe garantizar que los recursos correctos estén a su disposición. Existen tres marcos comunes que las organizaciones utilizan para manejar esta etapa de IAM:

* Control de acceso obligatorio (MAC).
* Control de acceso discrecional (DAC).
* Control de acceso basado en roles (RBAC).



**Control de acceso obligatorio (MAC)**

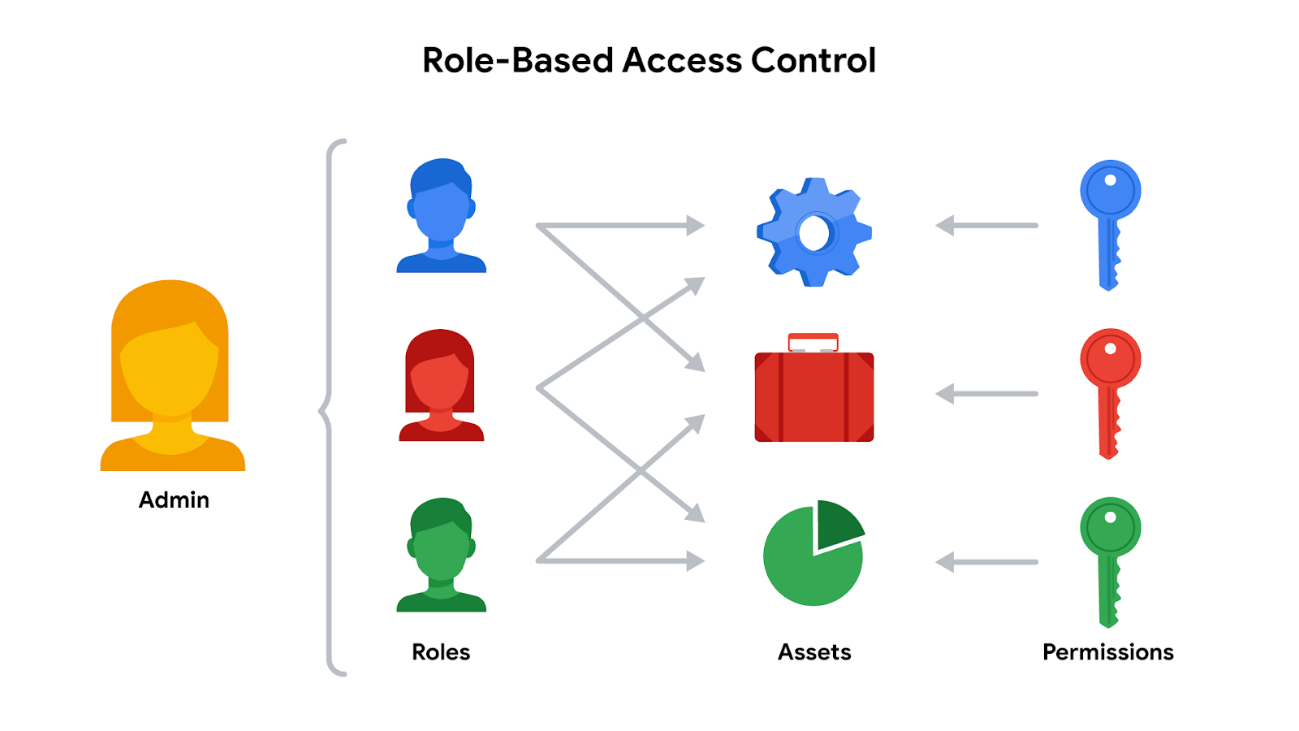
El control de acceso obligatorio (MAC) es el más estricto de los tres marcos. En este modelo, la autorización se basa en una estricta “necesidad de conocer”. El acceso a la información debe ser otorgado manualmente por una autoridad central o un administrador del sistema. Por ejemplo, MAC se aplica habitualmente en las fuerzas de seguridad, como el ejército, y otras agencias gubernamentales donde los usuarios deben solicitar acceso a través de una cadena de mando. MAC también se conoce como control no discrecional, ya que el acceso no se otorga a discreción del propietario de los datos.

Diagrama

Descripción generada automáticamente

**Control de acceso discrecional (DAC)**

El control de acceso discrecional (DAC) suele aplicarse cuando el propietario de los datos decide los niveles de acceso adecuados. Un ejemplo de DAC es cuando el propietario de una carpeta de Google Drive comparte acceso con modo de editor, lector o comentador con otra persona.



**Control de acceso basado en roles (RBAC)**

El control de acceso basado en roles (RBAC) se utiliza cuando la autorización se determina según la función que tiene una persona dentro de una organización. Por ejemplo, alguien que se desempeña en el departamento de marketing puede tener acceso al análisis de usuarios, pero no a la administración de la red.

**Tecnologías de control de acceso**

Los usuarios suelen percibir la autenticación y la autorización como una experiencia unificada y fluida, en gran medida gracias a la sinergia entre las tecnologías de control de acceso que se integran entre sí. Estas herramientas ofrecen la velocidad y automatización necesarias para que los administradores supervisen y modifiquen los derechos de acceso, al mismo tiempo que reducen errores y posibles riesgos.

Algunas organizaciones desarrollan y mantienen por sí mismas tecnologías de control de acceso a través de su departamento de TI. Un sistema IAM o AAA típico consta de un directorio de usuarios, un conjunto de herramientas para administrar datos en ese directorio, un sistema de autorización y un sistema de auditoría. Estas soluciones personalizadas se crean para adaptarse a las necesidades específicas de seguridad de la organización. Sin embargo, es importante tener en cuenta que la creación de una solución interna puede requerir un alto costo en términos de tiempo y otros recursos.

En lugar de eso, muchas organizaciones optan por adquirir licencias de soluciones de terceros que ofrecen una serie de herramientas para proteger rápidamente sus sistemas de información. Hay que tener en cuenta que la seguridad va más allá de simplemente combinar un conjunto de herramientas. Siempre es importante ajustar estas tecnologías para que contribuyan a proporcionar un entorno seguro.

**Conclusiones clave**

Controlar el acceso requiere un conjunto de sistemas y herramientas. IAM y AAA son dos protocolos o marcos ampliamente utilizados para implementar el principio de mínimo privilegio y la segregación de funciones. Como analista de seguridad, podrías ser responsable del aprovisionamiento de usuarios y colaborar con otros equipos de IAM o AAA. Familiarizarse con estos enfoques es valioso para ayudar a las organizaciones a alcanzar sus objetivos de seguridad, ya que ambos garantizan que los usuarios adecuados obtengan acceso a los recursos correctos en el momento oportuno y por las razones apropiadas.

**Recursos para obtener información adicional**

La industria de la gestión de identidades y accesos está creciendo a un ritmo vertiginoso. Al igual que en otros ámbitos de la seguridad, es importante mantenerse al día.

* [IDPro](https://idpro.org/)© es una organización profesional dedicada a compartir conocimientos esenciales del sector de IAM.