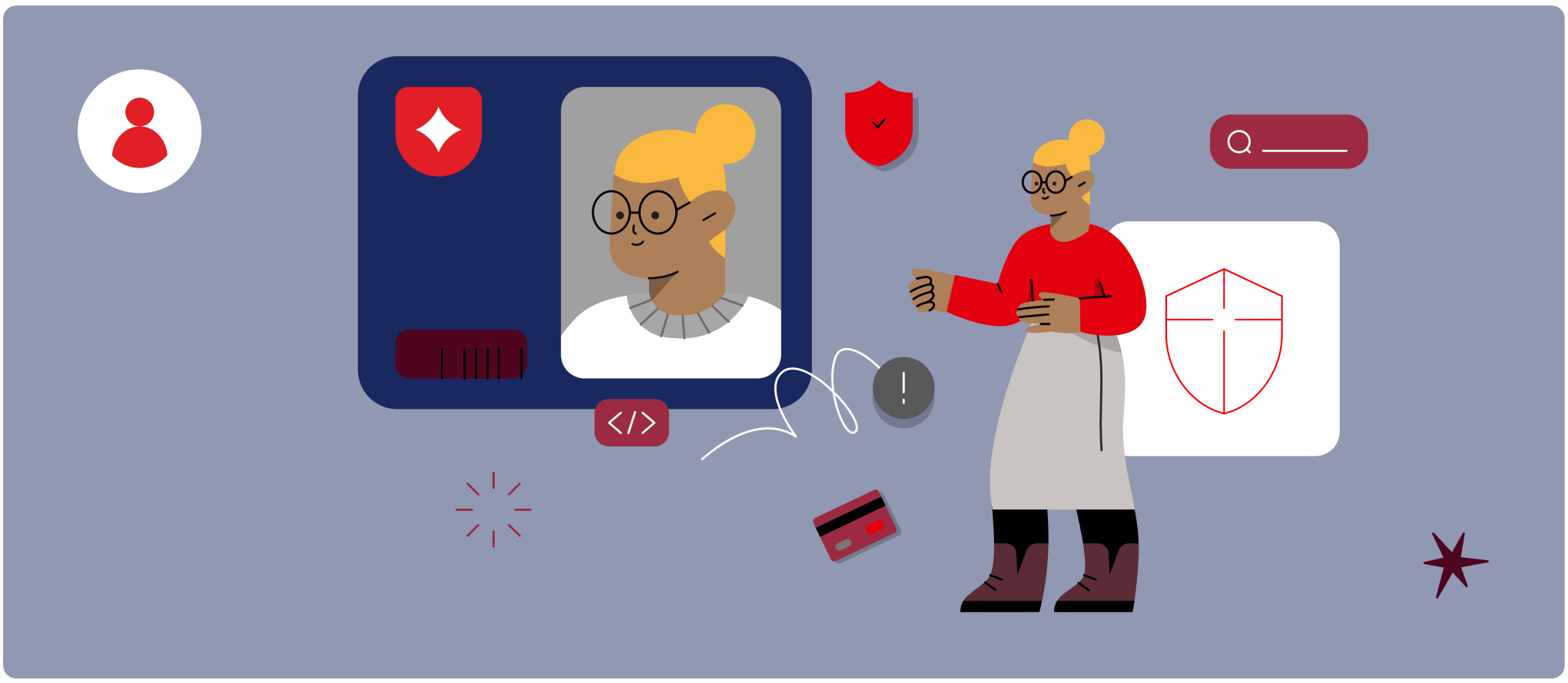
Gestión de identidades: ¿Qué debe saber?



Las brechas de seguridad de hoy en día, como los ataques a SolarWinds o T-Mobile, no son hechos aislados, sino ejemplos de cómo alguien puede robar las credenciales de su organización y utilizarlas para obtener un acceso privilegiado ilegítimo a activos sensibles. **Las violaciones de la seguridad de los datos ocurren a diario**, y en demasiados lugares a la vez como para llevar la cuenta. Nos recuerdan que, independientemente de nuestras inversiones en seguridad de la información, los recursos críticos para la empresa pueden verse comprometidos si no se protege el acceso.

Las organizaciones dependen de una gran variedad de sistemas, aplicaciones y dispositivos para llevar a cabo sus operaciones, y los usuarios necesitan acceder a estos recursos para realizar su trabajo con eficiencia. Gestionar todo esto puede ser un desafío, especialmente en grandes empresas con cientos o miles de usuarios que requieren un acceso personalizado. La gestión de identidades y accesos agrega una capa de seguridad mediante **el seguimiento, la gestión y la protección** de las identidades de las personas y sus datos asociados. Ayuda a realizar un seguimiento de quién es quién, para que las personas puedan acceder a la información que están autorizadas a ver y realizar las transacciones que tienen permitido hacer.

Índice

¿Qué es la gestión de identidades?

La gestión de identidades es el proceso de gestionar las identidades de los usuarios y los privilegios de acceso de forma centralizada. Implica el registro y control de las identidades dentro de una organización y la aplicación de políticas de gobernanza de identidades. En pocas palabras, su identidad en línea es el perfil que identifica quién es usted cuando utiliza una red, mientras que su acceso se refiere a qué permisos tiene una vez que ha iniciado sesión. Juntos, son un elemento importante de su modo de interactuar con la tecnología: es la forma en que las computadoras saben que es usted realmente quien intenta iniciar sesión en lugar de otra persona.

La gestión de identidades en acción

Mediante la gestión de identidades y accesos (IAM, por sus siglas en inglés), solo los usuarios especificados de una organización pueden acceder a información sensible y manejarla. He aquí algunos ejemplos de gestión de identidades en acción:

- **Creación y mantenimiento de identidades:**mediante la creación de flujos de trabajo automatizados para escenarios como una nueva contratación o una transición de funciones, la IAM centraliza el ciclo de vida de la gestión de identidades y accesos de la plantilla de una empresa. Supone una mejora en el tiempo de procesamiento de los cambios de acceso e identidad y una reducción de errores.
- **Administración de derechos:** los derechos del ciclo de vida se asignan a las personas y a sus roles. Por ejemplo, un operario de producción puede ver un procedimiento de trabajo en línea, pero no puede modificarlo. En cambio, un supervisor tendrá autoridad no solo para verlo, sino también para modificarlo o crear otros nuevos.
- **Verificación de identidades:** la identidad constituye el núcleo de las acciones cotidianas de la ciudadanía. Una vez que el Estado ha implementado un registro civil, la IAM permite a los gobiernos conceder a las personas el derecho a acceder a sus datos (certificado de nacimiento, permiso de conducir, etc.) y probar su identidad.

Varios sistemas de gestión de identidades y accesos utilizan el control de acceso basado en roles (RBAC, por sus siglas en inglés). Según este enfoque, existen roles de trabajo predefinidos con conjuntos específicos de privilegios de acceso. Por ejemplo, si se pone a un miembro de RR. HH. a cargo de la capacitación, no tiene mucho sentido darle también acceso a los archivos de funciones y salarios. Existen muchas otras formas de control automático del acceso, cada una de ellas con una variedad de características y tecnología.

Características comunes de la gestión de identidades

Existen muchas formas diferentes de software de gestión de identidades en el mercado y no hay una definición oficial de lo que deben y no deben incluir. Sin embargo, destacan un par de características esenciales:

- **Inicio de sesión único (SSO):** los usuarios pueden acceder a múltiples aplicaciones y servicios desde un único lugar, lo que evita tener que utilizar distintos nombres de usuario y contraseñas.
- **Autenticación de dos factores:** implica verificar la identidad de alguien no solo con su nombre de usuario y contraseña, sino también con otro dato, como un PIN o un token.

Otras características de la gestión de identidades pueden incluir el aprovisionamiento automático de cuentas de usuario, la gestión de contraseñas, el flujo de trabajo y los servicios de cumplimiento normativo y auditoría. En los últimos años, ha surgido una nueva generación de tecnologías de gestión de identidades, centrada en la **facilidad de uso además de en la seguridad**. Algunos ejemplos son la autenticación biométrica (como las huellas dactilares o el reconocimiento facial), la autenticación multifactor (que requiere varios factores de verificación) y la federación de identidades, por la que la responsabilidad de la autenticación de una persona o entidad se delega en una parte externa de confianza. SSO es un aspecto importante de la gestión federada de identidades.

Estas características clave de la gestión de identidades son comunes a casi todos los sistemas de gestión de identidades (IMS) actuales. Un IMS es una plataforma en línea que ayuda a las organizaciones a gestionar una serie de identidades de manera segura y eficiente. Se integra con otros sistemas de una organización, como los sistemas de RR. HH., las plataformas de comercio electrónico y el software de contabilidad.

¿Cómo funciona la gestión de identidades?

A grandes rasgos, los sistemas de gestión de identidades realizan tres tareas principales: **identificación, autenticación y autorización**. Permite que las personas adecuadas, dependiendo de sus funciones laborales, accedan a las herramientas que necesitan para desempeñar sus tareas asignadas, sin concederles acceso a aquellas que no necesitan.

Identidad y acceso: ¿cuál es la diferencia? Los términos «gestión de identidades» y «gestión de accesos» se utilizan a menudo indistintamente, pero son dos conceptos distintos. La diferencia crucial es que la gestión de identidades se ocupa de las **cuentas de usuario** (autenticación), mientras que la gestión de acceso se ocupa de los **permisos y privilegios** (autorización).

Pongamos un ejemplo. Cuando un usuario ingresa sus credenciales de acceso, se está comprobando su identidad en una base de datos para verificar si las credenciales introducidas coinciden con las almacenadas en la base de datos: esto es la autenticación. Una vez que se ha determinado la identidad del usuario, se le concede acceso a los recursos para los que su cuenta está autorizada: esto es la autorización.

Gestión de identidades: ¿en qué le beneficia?

Un sistema de gestión de identidades es una valiosa herramienta para proteger la información y los recursos de organizaciones de cualquier tamaño. Permite almacenar de forma segura los datos de los usuarios y gestionar sus privilegios de acceso, lo que

brinda una forma segura y confiable de mantener sus operaciones en perfecto funcionamiento.

Estos son algunos de los beneficios de la gestión de identidades:

- **Mayor seguridad:** un IMS ayuda a proteger a su organización del acceso no autorizado y del robo de datos de los usuarios.
- **Mayor eficiencia:** con un IMS, puede gestionar con eficiencia los procedimientos de inicio de sesión de los usuarios y realizar un seguimiento de la actividad de los usuarios en múltiples plataformas utilizando un único conjunto de credenciales.
- **Menor tiempo/costo de procesamiento:** los flujos de trabajo automatizados de un IMS le permiten gestionar y administrar fácilmente las cuentas de usuario, lo que le ahorra tiempo y dinero en tareas administrativas.
- **Mejor cumplimiento normativo:** con un IMS, puede garantizar fácilmente el cumplimiento de regulaciones y normas, como el RGPD y la HIPAA (véase más abajo).

Desplegar un sistema de gestión de identidades

La implementación de una solución de gestión de identidades sólida no garantiza una seguridad completa, pero la adopción de los siguientes principios puede hacerle menos vulnerable a las infracciones y a los ataques de agentes maliciosos. He aquí algunos consejos que debe tomar en cuenta:

- **Implemente métodos de autenticación fuertes** (como la autenticación multifactor) para reducir el riesgo de acceso no autorizado.
- **Revise periódicamente las políticas de control de acceso** para asegurarse de que solo los usuarios autorizados tienen acceso a la información y los recursos sensibles.
- **Supervise y audite el acceso** a la información y los recursos sensibles para detectar y evitar accesos no autorizados.
- **Actualice con frecuencia las cuentas de usuario** para asegurarse de que siguen siendo pertinentes y precisas.
- **Implemente una solución de gestión de contraseñas** para reducir el riesgo de incidentes de seguridad relacionados con las contraseñas, como la reutilización o el robo de contraseñas.

Implicaciones para el cumplimiento normativo

Si los procesos de gestión de identidades y accesos no se controlan eficazmente, es posible que incumpla las normas del sector o las regulaciones gubernamentales. El mundo avanza hacia **regulaciones y normas más estrictas** para la gestión de identidades, como el RGPD europeo (que exige el consentimiento explícito de los usuarios para la recogida de datos) y las Directrices de Identidad Digital NIST 800-63 en EE. UU. (una hoja de ruta para las buenas prácticas de IAM).

Existen varios protocolos que respaldan las políticas sólidas de IAM, al **asegurar los datos** y garantizar su **integridad durante la transferencia**. Generalmente conocidos como «autenticación, autorización y contabilidad» o AAA (por sus siglas en inglés), estos protocolos de gestión de identidades y accesos brindan normas de seguridad para simplificar la gestión de accesos, ayudar al cumplimiento normativo y crear un sistema uniforme para gestionar las interacciones entre usuarios y sistemas.

Aunque el cumplimiento de normas ISO no es un requisito legal, las normas ISO se alinean de forma natural con las regulaciones de diversos sectores. Así, el cumplimiento de la norma ISO/IEC 27001 para la seguridad de la información puede evitar que su organización se meta en problemas legales por aspectos cruciales de la gestión de identidades. Basada en la segregación de funciones y en la política de «un usuario, una identificación», demuestra que la información de su empresa está debidamente controlada.

> ISO/IEC 27001 Information security management systems
>
> ISO/IEC 24760-1 IT security and privacy — A framework for identity management

> ISO/IEC 27018 Protection of personally identifiable information (PII) in public clouds acting as PII processors

Hacia una gestión de identidades avanzada

Los complejos requisitos de seguridad y cumplimiento normativo están presionando más que nunca a las organizaciones para que protejan su información, y suponen un desafío para las formas convencionales de gestionar las identidades de los usuarios. Hace un lustro, las contraseñas eran lo más parecido a una identidad digital. No obstante, los **enfoques modernos de la autenticación** requieren algo más que una mera contraseña. La adopción generalizada de la computación en nube, cuyas escalabilidad y flexibilidad la convierten en una propuesta atractiva para la mayoría de organizaciones, ha sometido a la seguridad de la información a un nuevo nivel de tensión.

Hoy en día, los inicios de sesión sin contraseña mediante **biometría** o **autenticación multifactor** ofrecen una alternativa a la autenticación tradicional, pero con eso no basta. Cuando se trata de proteger los datos en entornos multinube, los profesionales de TI ven el cifrado como un control de seguridad crítico. El almacenamiento de identidades en una **cadena de bloques** ha emergido como una solución que puede aportar registros inmutables de un sistema determinado sin una autoridad centralizada que los gestione. Al contemplar nuestro futuro con la IAM, puede que no pase mucho tiempo antes de que los sistemas de identidad basados en cadenas de bloques se conviertan en la norma para mantener a salvo y seguros los datos de un usuario.