TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3-UNIDAD 2

Universidad Tecnológica de Pereira

faceIT

Definición de Identity and Access Management (IAM)

La gestión de identidades y acceso (IAM, por sus siglas en inglés) es un conjunto de procesos, herramientas y políticas diseñadas para gestionar las identidades digitales y regular el acceso a recursos empresariales, tanto en centros de datos locales como en servicios en la nube. IAM autentica a los usuarios, gestiona sus identidades y controla el acceso a sistemas, redes y datos sensibles, asegurando que solo las personas autorizadas puedan interactuar con los recursos adecuados.
Ejemplos de IAM

- **Autenticación de empleados:** Un empleado accede al sistema corporativo utilizando inicio de sesión único (SSO), que le permite trabajar en diferentes plataformas sin tener que recordar varias contraseñas.

- **Control de acceso basado en roles:** Los desarrolladores tienen acceso al repositorio de código fuente, pero no a los datos financieros, reduciendo el riesgo de errores o fugas de información.

- **Seguridad en trabajo remoto:** Un empleado remoto utiliza la autenticación multifactor (MFA) para conectarse a un servidor corporativo, protegiendo la empresa de accesos no autorizados.

Características clave de IAM

1. **Autenticación de usuarios:** Verifica la identidad del usuario utilizando contraseñas, sistemas biométricos o MFA.
2. **Control de acceso:** Aplica principios como el de mínimo privilegio, regulando qué recursos puede utilizar cada usuario.
3. **Supervisión y auditoría:** Rastrea actividades y genera informes para garantizar el cumplimiento de las políticas de seguridad y normativas.

¿Qué es la gestión de identidades?

La gestión de identidades se centra en la creación, mantenimiento y eliminación de identidades digitales. Este proceso asegura que cada usuario tenga un perfil único con derechos y roles claros.
Ejemplo:

Cuando un nuevo empleado es contratado, se le crea una identidad digital que le otorga acceso a las herramientas necesarias para su puesto. Si el empleado cambia de rol o deja la empresa, sus permisos se ajustan o eliminan automáticamente

¿Qué es la gobernanza de identidades?

La gobernanza de identidades asegura que los derechos de acceso sean coherentes con las políticas de la organización y las normativas legales. Incluye:

- Aprovisionamiento: Creación de cuentas de usuario en diferentes sistemas.
- Desaprovisionamiento: Revocación automática de accesos.
- Evaluaciones de conformidad: Revisiones periódicas para verificar que los usuarios tienen solo los permisos necesarios.

Ejemplo:
Una institución financiera revisa trimestralmente los permisos de sus empleados para asegurarse de que solo las personas adecuadas pueden acceder a datos sensibles, cumpliendo con normativas como SOX.

¿Qué es la gestión del acceso?

La gestión del acceso regula la manera en que los usuarios interactúan con los recursos. Las principales herramientas incluyen:

- **Autenticación multifactor (MFA):** Combina varios métodos de verificación para garantizar la seguridad.
- **Inicio de sesión único (SSO):** Permite a los usuarios autenticarse una sola vez para acceder a varios sistemas.

Ejemplo:
Una universidad implementa SSO para que estudiantes y profesores puedan acceder a bibliotecas digitales, correo electrónico y plataformas de aprendizaje con una única credencial.

¿Qué son los servicios de directorio?

Los servicios de directorio son bases de datos jerárquicas que almacenan y sincronizan información sobre usuarios, dispositivos y recursos.
Ejemplo:
Una empresa utiliza Microsoft Active Directory para centralizar la gestión de cuentas y aplicar políticas de seguridad de manera uniforme, como la expiración automática de contraseñas.

¿Por qué es importante IAM?

IAM es crucial para proteger los activos empresariales de amenazas internas y externas, así como para garantizar el cumplimiento normativo. Los beneficios principales incluyen:

1. Seguridad mejorada: Minimiza los riesgos de accesos no autorizados.
2. Cumplimiento normativo: Facilita el cumplimiento de regulaciones como GDPR, HIPAA o ISO 27001.
3. Eficiencia operativa: Automatiza procesos de gestión de identidades y accesos, reduciendo costos y errores humanos.

Ejemplo:
Un hospital implementa IAM para proteger historiales clínicos, asegurando que solo el personal autorizado pueda ver o modificar los datos de los pacientes.

Ventajas de IAM

- Automatización: Agiliza procesos como el aprovisionamiento y desaprovisionamiento de cuentas.
- Colaboración segura: Facilita el trabajo en equipo, especialmente en entornos distribuidos.
- Reducción de riesgos: Limita los privilegios excesivos, previniendo errores o filtraciones de datos.

Ejemplo:
Una multinacional utiliza IAM para permitir que sus empleados trabajen desde cualquier ubicación con acceso seguro y sin interrupciones, manteniendo la seguridad de los datos corporativos.