07/06/2024

ECONOMIST & JURIST

Redacción

Gestión de Identidades y Accesos (IAM): un pilar fundamental en la seguridad de la información

En un mundo donde la información es uno de los activos más valiosos de una organización, la seguridad de los datos se convierte en una prioridad crítica. Los abogados, que manejan información sensible y confidencial, deben estar especialmente atentos a las amenazas que **pueden comprometer la integridad y la confidencialidad** de los datos. La Gestión de Identidades y Accesos (IAM, por sus siglas en inglés) emerge como una herramienta esencial **para controlar quién tiene acceso a qué información y cuándo**, reduciendo así el riesgo de filtraciones de datos y ciberataques.

La Gestión de Identidades y Accesos (IAM) es un marco de políticas y tecnologías que garantizan que las personas adecuadas en una organización tengan **acceso a los recursos tecnológicos adecuados** en el momento adecuado. IAM abarca la administración de identidades digitales y sus **permisos asociados dentro de un sistema**. Esto incluye todo, desde la creación y eliminación de cuentas de usuario hasta la gestión de permisos y roles, la autenticación y el monitoreo continuo de las actividades de acceso.

Componentes clave del IAM

1. Identidad Digital: cada usuario tiene una identidad digital que incluye **información personal y credenciales de acceso**. Esto puede ser un empleado, un cliente, un proveedor o cualquier otra entidad que **interactúe con los sistem ...**