Deloitte.

Gestión de accesos e identidades en tecnología de información

Estrategia y Road Map

Implementación

Operación y Mantenimiento

Definición y valor del concepto

La integridad del negocio y su información se ve amenazada cuando la administración de accesos e identidades en la tecnología de información, falla.

Verificar de manera efectiva el acceso a la información nunca antes había sido tan importante.

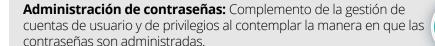
El rápido crecimiento en número de usuarios que requieren acceso a múltiples fuentes de datos y con distintos niveles de privilegios, representa un reto en:

- O1. Otorgar acceso a múltiples recursos en tiempos razonables.
- Ofrecer los accesos con privilegios adecuados.
- **03.** Evitar conflictos de segregación de funciones.
- Habilitar la operación, protegerla y así gestionar riesgos.
- O5. Auditar y certificar el acceso de usuarios.
- O6. Dar cumplimiento a leyes y regulaciones.

Diagnóstico básico ¿Su empresa lo necesita?

- ¿Existen usuarios que ya no laboran en la organización y aun tienen acceso a los sistemas?
- ¿La asignación de accesos y segregación de funciones es una observación recurrente de auditoría?
- ¿Cuenta con proceso de asignación de acceso manuales, tardados y propensos a error humano?
- ¿Le inquietan las acciones que un usuario privilegiado puede efectuar en sus sistemas?

Administración de Identidades: Procesos y actividades para la gestión de usuarios en todos los sistemas, así como la asignación granular de privilegios. El aprovisionamiento y des-aprovisionamiento de las cuentas es un factor clave.



Certificación de accesos: Analiza los procesos para determinar y confirmar si el acceso otorgado a los usuarios es apropiado o no respecto de sus funciones, incluyendo si existen programas formalizados y estandarizados.

Integración de datos: Analiza la factibilidad de integración con el sistema final considerando: homologación de User ID, administración de cuentas, gestión de privilegios, administración de contraseñas y federación.



Gobierno IAM (Identity & Access Management): Definición e implementación de los elementos necesarios (áreas y procesos) para lograr eficazmente la visión del programa IAM mediante la alineación y coordinación de equipos y actividades.



Administración de accesos: Evaluación de los procesos y soluciones tecnológicas utilizadas para permitir o limitar el acceso a sistemas y aplicaciones.



Control de accesos basado en roles (RBAC): Considera la definición de roles empresariales y procesos para administrar el ciclo de vida de los roles.



Administración de accesos privilegiado: Se evalúan los procesos para la administración de cuentas de acceso con privilegios extendidos.

Beneficios y Valor

Cumplimiento Regulatorio

Mejora en el servicio

Reducción de costos

Automatización de procesos

Reducción de riesgos

Reportes y trazabilidad de accesos para auditoría

Prevención de fraude

Gobierno IAM (Identity & Access Management)

Santiago Gutiérrez

Socio Líder de Riesgo Cibernético sangutierrez@deloittemx.com

Iván Campos

Socio de Riesgo Cibernético icampos@deloittemx.com

Fernando Bojorges

Socio de Riesgo Cibernético fbojorges@deloittemx.com

Erick Robles

Socio de Riesgo Cibernético errobles@deloittemx.com

Sergio Solis

Socio de Riesgo Cibernético sesolis@deloittemx.com

