OpenText™ NetIQ™ IAM

Suite Integral de Gestión de Identidades y Accesos (Identity & Access Management)

RESUMEN EJECUTIVO

Suite integral de Gestión de Identidades y Accesos (IAM) diseñada para automatizar el ciclo de vida de usuarios, garantizar el principio de menor privilegio (Least Privilege Access) y proteger activos críticos en entornos híbridos y multi-cloud. Acelera los procesos de auditoría de accesos en más de un 50%, garantizando gobernanza, cumplimiento normativo y alineación estricta con el modelo de seguridad Zero Trust.

ESPECIFICACIONES CLAVE

Atributo	Detalle
Administración de Identidades	NetIQ Identity Manager: Aprovisionamiento/desaprovisionamiento automatizado y orquestación de flujos de trabajo.
Gobernanza y Auditoría	NetIQ Identity Governance: Certificación de accesos y análisis de Separación de Funciones (SoD).
Control de Acceso y SSO	NetIQ Access Manager: Single Sign-On (SSO) federado, políticas adaptativas y control por roles (RBAC).
Gestión de Cuentas Privilegiadas	NetIQ Privileged Access Manager (PAM): Monitoreo en tiempo real y grabación de sesiones.
Autenticación Avanzada	NetIQ Advanced Authentication: MFA adaptativo (biometría, tokens, notificaciones push).
Infraestructura de Directorio	NetIQ Identity Foundation: Repositorio de directorio escalable de alta disponibilidad.
Arquitectura de Seguridad	Verificación continua alineada a principios de Zero Trust (Least Privilege)
Modelos de Despliegue	Arquitectura híbrida flexible (On-Premises, Nube Privada y Multi-Cloud).

BENEFICIOS CLAVE Y RETORNO DE INVERSIÓN (ROI)

- **Reducción del Tiempo de Auditoría (+50%).**
  Acelera drásticamente la certificación y recertificación de permisos, reduciendo costos operativos y riesgos de penalizaciones normativas.
- **Eliminación de Procesos Manuales TI.**
  Automatiza las altas, modificaciones de rol y bajas de empleados o contratistas, evitando accesos huérfanos o brechas de seguridad tras la salida de personal.
- **Mitigación de Riesgos por Exceso de Privilegios.**
  Implementa control de Separación de Funciones (SoD) y acceso de menor privilegio (Least Privilege) para prevenir fraudes internos.
- **Arquitectura Unificada Zero Trust.**
  Evalúa continuamente la identidad y el contexto del usuario antes de conceder acceso a aplicaciones locales o en la nube.
- **Flexibilidad Operativa Híbrida.**
  Integra infraestructura existente en premisa con aplicaciones en nubes públicas o privadas en una sola plataforma de identidad.

NOTAS DE USO Y APLICACIONES RECOMENDADAS

Gestión del Ciclo de Vida de Empleados y Contratistas

Empresas con alta rotación o rápido crecimiento que requieren automatizar la asignación y revocación de accesos (Joiners, Movers, Leavers).

Entornos Altamente Regulados

Organizaciones que necesitan auditorías frecuentes de gobernanza, análisis SoD y control estricto de cuentas privilegiadas (PAM).

Ecosistemas Híbridos y Multi-Cloud

Empresas que buscan unificar el acceso de los usuarios (SSO y MFA) a través de servidores locales y múltiples proveedores de nube.

Confidencial — Uso comercial autorizado. Propiedad intelectual de Grupo CONSISA. Prohibida su reproducción sin autorización.