Tech Manager- ARGOS Identity Assessment

Relatório de Maturidade de Active Directory e Microsoft Entra ID

Empresa Avaliada: Empresa Demonstração S/A

Data do Relatório: 20 de Janeiro de 2026

Classificação Geral: Crítico

DOCUMENTO DE EXEMPLO – Dados fictícios para fins demonstrativos. O relatório real é gerado automaticamente após o preenchimento do formulário ARGOS AD Security

Sumário Executivo

Conteúdo:

O ambiente de Active Directory apresenta riscos estruturais relevantes, com impacto potencial em segurança e continuidade operacional. Recomenda-se plano imediato de remediação, priorizando controles de segurança, hardening de controladores de domínio e governança de privilégios.

Score Geral: 44/ 200
Nível de Maturidade: Crítico

Visão Geral por Pilar

Pilar	Pontuação	Interpretação
Governança	17 de 50	Avaliação estrutural
Segurança	9 de 50	Controles técnicos
Auditoria	9 de 50	Monitoramento
Cloud/Entra ID	9 de 50	Integração híbrida

Governança

Pontuação: 17/50

A governança do Active Directory reflete o nível de organização estrutural, delegação de privilégios e padronização de

objetos. Ambientes com baixa pontuação tendem a apresentar riscos de permissões excessivas e ausência de segregação

adequada.

Segurança

Pontuação: 9/50

Avalia hardening dos controladores de domínio, MFA, políticas de senha, controle de privilégios e proteção contra-ataques

conhecidos.

Auditoria

Pontuação: 9/50

Mede a capacidade de rastreabilidade, monitoramento e resposta a eventos suspeitos no ambiente.

Cloud / Entra ID

Pontuação: 9/50

Analisa integração híbrida, sincronização segura, Conditional Access e controles de identidade na nuvem.

Principais Riscos Identificados

• Segurança do Active Directory apresenta risco crítico devido à ausência de controles estruturais no(s) Controladores de Domínio.
• Governança do Active Directory está abaixo do esperado (estrutura, OU/Groups/Delegações), elevando risco de permissões inadequadas e administração não padronizada.
• Auditoria e monitoramento do Active Directory estão insuficientes, comprometendo rastreabilidade e resposta a incidentes.
• Integração com Microsoft Entra ID / ambiente Cloud apresenta lacunas que podem impactar autenticação híbrida e controle de identidades.

Roadmap Recomendado

Curto Prazo (0–30 dias):
• Revisão imediata de privilégios administrativos.
• Implementação obrigatória de MFA para contas críticas.
• Hardening básico dos Domain Controllers.

Médio Prazo (30–90 dias):
• Reestruturação de OUs e modelo de delegação.
• Implementação de auditoria estruturada.
• Monitoramento de eventos críticos de identidade.

Longo Prazo (90+ dias):

- Evolução para modelo Zero Trust.
- Revisões periódicas de permissões privilegiadas.
- Integração segura com Microsoft Entra ID.

Conclusão Estratégica

O ARGOS Identity Assessment fornece uma visão executiva clara sobre o nível atual de maturidade do ambiente de identidade corporativa.

A evolução contínua dos controles estruturais e técnicos é essencial para reduzir riscos operacionais, fortalecer governança e garantir resiliência diante de ameaças modernas.

A Tech Manager coloca-se como