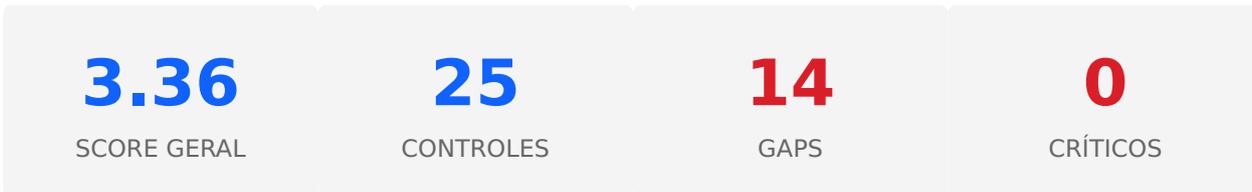


Relatório de Maturidade IAM

Assessment 2025 v0.7

Data da Avaliação: 17/12/2025

Resumo Executivo



Maturidade por Domínio

| Domínio | Score Médio | Nível |
|---------------------|-------------|-------|
| Autenticação | 3.29/5 | 3 |
| Ciclo de Vida (JML) | 3.5/5 | 3 |
| Privilégio (PAM) | 3.33/5 | 3 |
| Monitorização (MON) | 3.33/5 | 3 |

Conformidade por Padrão

| Padrão | Conformidade | Controles Conformes |
|-----------------|--------------|---------------------|
| ISO 27001:2022 | 90.9% | 40/44 |
| NIST CSF 2.0 | 92.6% | 25/27 |
| CIS Controls v8 | 92.9% | 26/28 |
| LGPD/GDPR | 92.0% | 23/25 |

| | | |
|----------------|--------|-------|
| IBGC 6ª Edição | 92.1% | 35/38 |
| PSI-CORP-001 | 100.0% | 15/15 |
| ISF SGP 2024 | 92.0% | 23/25 |

Gaps de Maturidade

| Controle | Domínio | Atual | Meta | Prioridade |
|----------|---------------------|-------|------|------------|
| AUTH-007 | Autenticação | 2 | 4 | High |
| MON-006 | Monitorização (MON) | 2 | 4 | High |
| AUTH-001 | Autenticação | 3 | 4 | Medium |
| AUTH-004 | Autenticação | 3 | 4 | Medium |
| AUTH-005 | Autenticação | 3 | 4 | Medium |
| JML-001 | Ciclo de Vida (JML) | 3 | 4 | Medium |
| JML-006 | Ciclo de Vida (JML) | 3 | 4 | Medium |
| PAM-003 | Privilégio (PAM) | 3 | 4 | Medium |
| MON-002 | Monitorização (MON) | 3 | 4 | Medium |
| MON-004 | Monitorização (MON) | 3 | 4 | Medium |
| JML-004 | Ciclo de Vida (JML) | 3 | 4 | Medium |
| PAM-001 | Privilégio (PAM) | 3 | 4 | Medium |
| PAM-005 | Privilégio (PAM) | 3 | 4 | Medium |
| PAM-006 | Privilégio (PAM) | 3 | 4 | Medium |

Recomendações

AUTH-007 [High]

Desabilitar protocolos legados (Basic Auth: POP3, IMAP, SMTP) globalmente....

Ação: Evoluir do nível 2 para 3 - Bloqueio parcial ou por exceção manual.

MON-006 [High]

Feedback do usuário ('Não fui eu') no MFA gera incidente de segurança imediato no SOC....

Ação: Evoluir do nível 2 para 3 - Feedback gera log para revisão.

AUTH-001 [Medium]

Relatório gerado automaticamente - IAM Security Maturity Assessment - 17/12/2025 06:04

Impor MFA Resistente a Phishing (FIDO2/CBA) para todas as contas administrativas, bloqueando SMS/Voz...

Ação: Evoluir do nível 3 para 4 - App + Number Matching obrigatório.

AUTH-004 [Medium]

Verificação de senhas banidas em tempo real contra listas globais (pwned) e dicionários da empresa....

Ação: Evoluir do nível 3 para 4 - Integração com listas globais (pwned).

AUTH-005 [Medium]

Bloquear login interativo e rotacionar segredos de Contas de Serviço a cada 90 dias (ou usar Managed...

Ação: Evoluir do nível 3 para 4 - Rotação automatizada via Scripts/DevOps.

JML-001 [Medium]

Automatizar provisionamento 'Birthright' via RH, criando contas desativadas até o dia de início....

Ação: Evoluir do nível 3 para 4 - Scriptado (Powershell) disparado por ticket.

JML-006 [Medium]

Prazo de validade (TTL) rígido para contas de convidados (B2B), exigindo renovação do sponsor....

Ação: Evoluir do nível 3 para 4 - TTL automático (90 dias) com renovação.

PAM-003 [Medium]

Remover Admin Local e usar LAPS para senhas únicas e rotacionadas por estação....

Ação: Evoluir do nível 3 para 4 - LAPS em 100% com auditoria de uso.

MON-002 [Medium]

Bloqueio automático baseado em Risco (User/Sign-in Risk) para eventos de alto risco....

Ação: Evoluir do nível 3 para 4 - Alerta integrado ao Ticket (SOAR).

MON-004 [Medium]

Alertas P1 para mudanças em grupos Tier 0 (Global/Domain Admins) com notificação fora de banda....

Ação: Evoluir do nível 3 para 4 - Alerta e-mail (Near real-time).