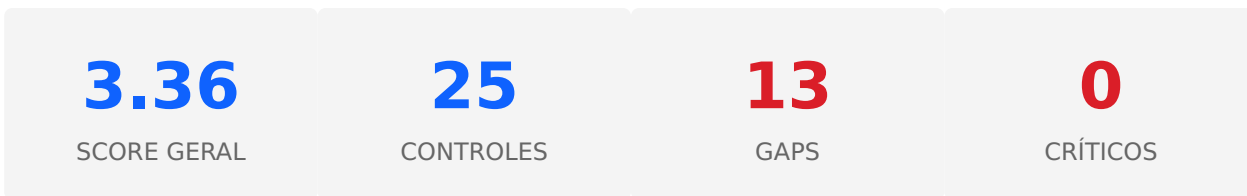


# Relatório de Maturidade IAM

Assessment 2026 v0.13

Data da Avaliação: 26/02/2026

## Resumo Executivo


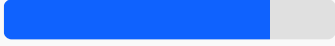


## Maturidade por Domínio

Domínio	Score Médio	Nível
Autenticação	3.43/5	3
Ciclo de Vida (JML)	3.5/5	3
Privilégio (PAM)	3.67/5	3
Monitorização (MON)	2.83/5	2

## Conformidade por Padrão

Padrão	Conformidade	Controles Conformes
ISO 27001:2022	<div><div style="width: 79.5%;"></div></div> 79.5%	35/44
NIST CSF 2.0	<div><div style="width: 81.5%;"></div></div> 81.5%	22/27
CIS Controls v8	<div><div style="width: 75.0%;"></div></div> 75.0%	21/28
LGPD/GDPR	<div><div style="width: 80.0%;"></div></div> 80.0%	20/25

IBGC 6ª Edição	76.3%	29/38
PSI-CORP-001	 73.3%	11/15
ISF SGP 2024	 80.0%	20/25

## Gaps de Maturidade

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

## Recomendações

### JML-004 [High]

Campanhas trimestrais de Certificação de Acesso com revogação automática se não houver resposta....

**Ação:** Evoluir do nível 2 para 3 - Anual (Todos) via Planilha Excel.

### MON-001 [High]

Centralizar Logs de Auditoria/Sign-in em SIEM. Retenção: 90 dias (quente) / 365 dias (fria)....

**Ação:** Evoluir do nível 2 para 3 - Backup manual esporádico para Storage.

### MON-002 [High]

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

**Ação:** Evoluir do nível 2 para 3 - Alerta por e-mail (Investigação humana).

**MON-005 [High]**

Monitorizar anomalias em Service Principals (volume de leitura, IPs novos, horários atípicos)...

**Ação:** Evoluir do nível 2 para 3 - Baseline manual de comportamento.

**AUTH-005 [High]**

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

**Ação:** Evoluir do nível 2 para 3 - Rotação manual periódica (Planilha de controle).

**JML-001 [Medium]**

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

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

**JML-003 [Medium]**

Automatizar 'Kill Switch' de saída: Bloqueio e revogação de tokens em <15 min após baixa no RH...

**Ação:** Evoluir do nível 3 para 4 - Scriptado (Batch noturno).

**PAM-004 [Medium]**

Implementar Modelo de Camadas (Tiering/Red Forest): Admins Tier 0 nunca logan em Tier 1/2...

**Ação:** Evoluir do nível 3 para 4 - Bloqueio Técnico (GPO) parcial/learning.

**PAM-005 [Medium]**

2 contas de Emergência (Break Glass) monitoradas, cloud-only, fora do MFA e com senha longa em cofre...

**Ação:** Evoluir do nível 3 para 4 - 2 contas cloud-only, alertas configurados.

**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).