

# Relatório de Maturidade IAM

Assessment 2025 v0.2

Data da Avaliação: 17/12/2025

## Resumo Executivo

<b>1.48</b> SCORE GERAL	<b>25</b> CONTROLES	<b>25</b> GAPS	<b>11</b> CRÍTICOS
----------------------------	------------------------	-------------------	-----------------------

## Maturidade por Domínio

Domínio	Score Médio	Nível
Autenticação	1.57/5	1
Ciclo de Vida (JML)	1.33/5	1
Monitorização (MON)	1.83/5	1
Privilégio (PAM)	1.17/5	1

## Conformidade por Padrão

Padrão	Conformidade	Controles Conformes
ISO 27001:2022	0.0%	0/44
NIST CSF 2.0	0.0%	0/27
CIS Controls v8	0.0%	0/28
LGPD/GDPR	0.0%	0/25

IBGC 6ª Edição	0.0%	0/38
PSI-CORP-001	0.0%	0/15
ISF SGP 2024	0.0%	0/25

## Gaps de Maturidade

Controle	Domínio	Atual	Meta	Prioridade
JML-002	Ciclo de Vida (JML)	0	4	Critical
PAM-002	Privilegio (PAM)	0	4	Critical
AUTH-002	Autenticação	1	4	Critical
AUTH-004	Autenticação	1	4	Critical
AUTH-006	Autenticação	1	4	Critical
JML-004	Ciclo de Vida (JML)	1	4	Critical
JML-006	Ciclo de Vida (JML)	1	4	Critical
MON-002	Monitorização (MON)	1	4	Critical
PAM-003	Privilegio (PAM)	1	4	Critical
PAM-005	Privilegio (PAM)	1	4	Critical
PAM-006	Privilegio (PAM)	1	4	Critical
AUTH-001	Autenticação	2	4	High
AUTH-003	Autenticação	2	4	High
AUTH-005	Autenticação	2	4	High
AUTH-007	Autenticação	2	4	High
JML-001	Ciclo de Vida (JML)	2	4	High
JML-003	Ciclo de Vida (JML)	2	4	High
JML-005	Ciclo de Vida (JML)	2	4	High
MON-001	Monitorização (MON)	2	4	High
MON-003	Monitorização (MON)	2	4	High
MON-004	Monitorização (MON)	2	4	High
MON-005	Monitorização (MON)	2	4	High
MON-006	Monitorização (MON)	2	4	High

PAM-001	Privilégio (PAM)	2	4	High
PAM-004	Privilégio (PAM)	2	4	High

## Recomendações

### JML-002 [Critical]

Gatilho de revisão em transferências: Mudança de cargo no RH inicia recertificação de acesso....

**Ação:** Evoluir do nível 0 para 1 - Acessos acumulam (Privilege Creep).

### PAM-002 [Critical]

Separar contas: adm-user (sem email/web) para gestão e user para uso diário....

**Ação:** Evoluir do nível 0 para 1 - Mesma conta e-mail/admin.

### AUTH-002 [Critical]

Impor MFA para todos os usuários com Number Matching para mitigar fadiga de MFA....

**Ação:** Evoluir do nível 1 para 2 - 100% de cobertura, permite SMS.

### AUTH-004 [Critical]

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

**Ação:** Evoluir do nível 1 para 2 - Política de complexidade básica.

### AUTH-006 [Critical]

Forçar re-autenticação para ações críticas (ex: ver dados sensíveis) independente do token....

**Ação:** Evoluir do nível 1 para 2 - Re-autenticação apenas para reset de senha.

### JML-004 [Critical]

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

**Ação:** Evoluir do nível 1 para 2 - Revisão apenas de Admins (Manual).

### JML-006 [Critical]

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

**Ação:** Evoluir do nível 1 para 2 - Validade anual manual.

**MON-002 [Critical]**

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

**Ação:** Evoluir do nível 1 para 2 - Reativo (Check esporádico).

**PAM-003 [Critical]**

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

**Ação:** Evoluir do nível 1 para 2 - Senhas diferentes (Excel/KeePass).

**PAM-005 [Critical]**

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

**Ação:** Evoluir do nível 1 para 2 - 1 conta (uso diário se precisar).