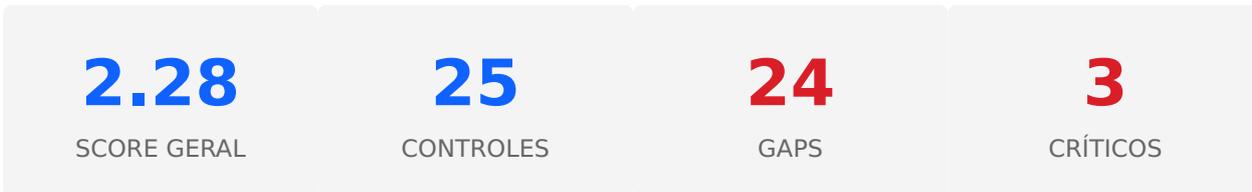


Relatório de Maturidade IAM

Assessment 2025 v0.8

Data da Avaliação: 17/12/2025

Resumo Executivo

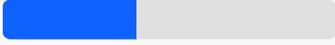


Maturidade por Domínio

Domínio	Score Médio	Nível
Autenticação	2.0/5	2
Privilégio (PAM)	2.17/5	2
Ciclo de Vida (JML)	2.67/5	2
Monitorização (MON)	2.33/5	2

Conformidade por Padrão

Padrão	Conformidade	Controles Conformes
ISO 27001:2022	<div><div style="width: 45.5%;"></div></div> 45.5%	20/44
NIST CSF 2.0	<div><div style="width: 40.7%;"></div></div> 40.7%	11/27
CIS Controls v8	<div><div style="width: 42.9%;"></div></div> 42.9%	12/28
LGPD/GDPR	<div><div style="width: 40.0%;"></div></div> 40.0%	10/25

IBGC 6ª Edição	39.5%	15/38
PSI-CORP-001	 33.3%	5/15
ISF SGP 2024	 40.0%	10/25

Gaps de Maturidade

Controle	Domínio	Atual	Meta	Prioridade
PAM-006	Privilégio (PAM)	0	4	Critical
AUTH-001	Autenticação	1	4	Critical
AUTH-003	Autenticação	1	4	Critical
AUTH-002	Autenticação	2	4	High
AUTH-004	Autenticação	2	4	High
AUTH-006	Autenticação	2	4	High
JML-002	Ciclo de Vida (JML)	2	4	High
JML-004	Ciclo de Vida (JML)	2	4	High
JML-005	Ciclo de Vida (JML)	2	4	High
MON-001	Monitorização (MON)	2	4	High
MON-002	Monitorização (MON)	2	4	High
MON-003	Monitorização (MON)	2	4	High
MON-005	Monitorização (MON)	2	4	High
PAM-001	Privilégio (PAM)	2	4	High
PAM-002	Privilégio (PAM)	2	4	High
AUTH-005	Autenticação	3	4	Medium
AUTH-007	Autenticação	3	4	Medium
JML-001	Ciclo de Vida (JML)	3	4	Medium
JML-003	Ciclo de Vida (JML)	3	4	Medium
MON-004	Monitorização (MON)	3	4	Medium
MON-006	Monitorização (MON)	3	4	Medium
PAM-003	Privilégio (PAM)	3	4	Medium
PAM-004	Privilégio (PAM)	3	4	Medium

Recomendações

PAM-006 [Critical]

Exigir Estações de Acesso Privilegiado (PAW) dedicadas para acessar consoles de gestão (Azure/AWS)....

Ação: Evoluir do nível 0 para 1 - PC padrão corporativo.

AUTH-001 [Critical]

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

Ação: Evoluir do nível 1 para 2 - MFA obrigatório, mas permite SMS/Voz.

AUTH-003 [Critical]

Configurar Smart Lockout: Bloquear ator da ameaça (IP), não a conta do usuário (AD), após 10 falhas....

Ação: Evoluir do nível 1 para 2 - Política de bloqueio definida, desbloqueio manual.

AUTH-002 [High]

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

Ação: Evoluir do nível 2 para 3 - 100% cobertura (App/Push).

AUTH-004 [High]

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

Ação: Evoluir do nível 2 para 3 - Lista de senhas banidas personalizada.

AUTH-006 [High]

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

Ação: Evoluir do nível 2 para 3 - Re-autenticação para algumas ações críticas.

JML-002 [High]

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

Ação: Evoluir do nível 2 para 3 - Revisão manual obrigatória via Ticket.

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.

JML-005 [High]

Deteção de contas órfãs (Reconciliação): Comparar AD vs. RH semanalmente para achar contas sem dono....

Ação: Evoluir do nível 2 para 3 - Comparação manual mensal (Vlookup).

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.