Relatório de Maturidade IAM

Assessment 2025 v0.1

Data da Avaliação: 17/12/2025

Resumo Executivo

1.0	25	25	25
SCORE GERAL	CONTROLES	GAPS	CRÍTICOS

Maturidade por Domínio

Domínio	Score Médio	Nível
Autenticação	1.0/5	1
Ciclo de Vida (JML)	1.0/5	1
Monitorização (MON)	1.0/5	1
Privilégio (PAM)	1.0/5	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
AUTH-001	Autenticação	1	4	Critical
AUTH-002	Autenticação	1	4	Critical
AUTH-003	Autenticação	1	4	Critical
AUTH-004	Autenticação	1	4	Critical
AUTH-005	Autenticação	1	4	Critical
AUTH-006	Autenticação	1	4	Critical
AUTH-007	Autenticação	1	4	Critical
JML-001	Ciclo de Vida (JML)	1	4	Critical
JML-002	Ciclo de Vida (JML)	1	4	Critical
JML-003	Ciclo de Vida (JML)	1	4	Critical
JML-004	Ciclo de Vida (JML)	1	4	Critical
JML-005	Ciclo de Vida (JML)	1	4	Critical
JML-006	Ciclo de Vida (JML)	1	4	Critical
MON-001	Monitorização (MON)	1	4	Critical
MON-002	Monitorização (MON)	1	4	Critical
MON-003	Monitorização (MON)	1	4	Critical
MON-004	Monitorização (MON)	1	4	Critical
MON-005	Monitorização (MON)	1	4	Critical
MON-006	Monitorização (MON)	1	4	Critical
PAM-001	Privilégio (PAM)	1	4	Critical
PAM-002	Privilégio (PAM)	1	4	Critical
PAM-003	Privilégio (PAM)	1	4	Critical
PAM-004	Privilégio (PAM)	1	4	Critical

PAM-005	Privilégio (PAM)	1	4	Critical
PAM-006	Privilégio (PAM)	1	4	Critical

Recomendações

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-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-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-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-005 [Critical]

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

Ação: Evoluir do nível 1 para 2 - Rotação manual ad-hoc (quando quebra).

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.

AUTH-007 [Critical]

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

Ação: Evoluir do nível 1 para 2 - Bloqueio apenas para novos usuários.

JML-001 **[Critical]**

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

Ação: Evoluir do nível 1 para 2 - Formulário padrão (E-mail), execução manual.

JML-002 **[Critical]**

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

Ação: Evoluir do nível 1 para 2 - Revisão manual ad-hoc pelo gestor.

JML-003 **[Critical]**

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

Ação: Evoluir do nível 1 para 2 - Manual (No mesmo dia - Best effort).