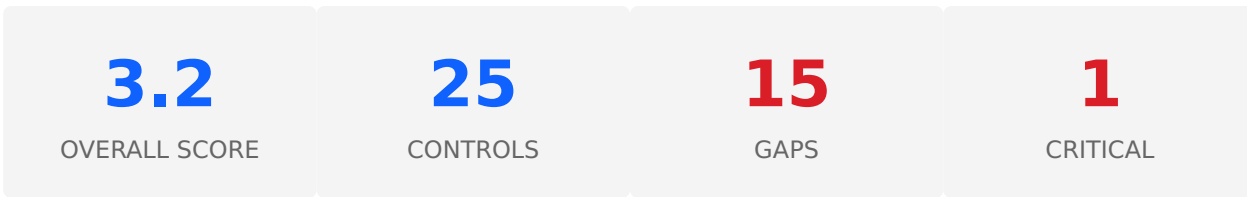


# IAM Maturity Report

Assessment 2026 v0.14

Assessment Date: 27/02/2026

## Executive Summary


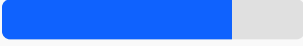


## Maturity by Domain

Domain	Average Score	Level
Autenticação	2.86/5	2
Ciclo de Vida (JML)	3.5/5	3
Privilégio (PAM)	3.67/5	3
Monitorização (MON)	2.83/5	2

## Compliance by Standard

Standard	Compliance	Compliant Controls
ISO 27001:2022	<div><div style="width: 77.3%;"></div></div> 77.3%	34/44
NIST CSF 2.0	<div><div style="width: 77.8%;"></div></div> 77.8%	21/27
CIS Controls v8	<div><div style="width: 71.4%;"></div></div> 71.4%	20/28
LGPD/GDPR	<div><div style="width: 76.0%;"></div></div> 76.0%	19/25

IBGC 6ª Edição	73.7%	28/38
PSI-CORP-001	 73.3%	11/15
ISF SGP 2024	 76.0%	19/25

## Maturity Gaps

Control	Domain	Current	Target	Priority
AUTH-006	Authentication	1	4	Critical
AUTH-005	Authentication	2	4	High
JML-004	Identity Lifecycle (JML)	2	4	High
MON-001	Monitoring (MON)	2	4	High
MON-002	Monitoring (MON)	2	4	High
MON-005	Monitoring (MON)	2	4	High
AUTH-001	Authentication	3	4	Medium
AUTH-002	Authentication	3	4	Medium
AUTH-004	Authentication	3	4	Medium
JML-001	Identity Lifecycle (JML)	3	4	Medium
JML-003	Identity Lifecycle (JML)	3	4	Medium
PAM-004	Privileged Access (PAM)	3	4	Medium
PAM-005	Privileged Access (PAM)	3	4	Medium
MON-004	Monitoring (MON)	3	4	Medium
MON-006	Monitoring (MON)	3	4	Medium

## Recommendations

### AUTH-006 [Critical]

Enforce re-authentication for critical actions (e.g., viewing sensitive data) regardless of token....

**Action:** Evolve from level 1 to 2 - Re-autenticação apenas para reset de senha.

### AUTH-005 [High]

Block interactive login and rotate Service Account secrets every 90 days (or use Managed Identity)....

**Action:** Evolve from level 2 to 3 - Rotação manual periódica (Planilha de controle).

**JML-004 [High]**

Quarterly Access Certification campaigns with automatic revocation if there is no response....

**Action:** Evolve from level 2 to 3 - Anual (Todos) via Planilha Excel.

**MON-001 [High]**

Centralize Audit/Sign-in Logs in a SIEM. Retention: 90 days (hot) / 365 days (cold)....

**Action:** Evolve from level 2 to 3 - Backup manual esporádico para Storage.

**MON-002 [High]**

Automatic blocking based on Risk (User/Sign-in Risk) for high-risk events....

**Action:** Evolve from level 2 to 3 - Alerta por e-mail (Investigação humana).

**MON-005 [High]**

Monitor anomalies in Service Principals (read volume, new IPs, atypical hours)....

**Action:** Evolve from level 2 to 3 - Baseline manual de comportamento.

**AUTH-001 [Medium]**

Enforce Phishing-resistant MFA (FIDO2/CBA) for all administrative accounts, blocking SMS/voice....

**Action:** Evolve from level 3 to 4 - App + Number Matching obrigatório.

**AUTH-002 [Medium]**

Enforce MFA for all users with Number Matching to mitigate MFA fatigue....

**Action:** Evolve from level 3 to 4 - 100% + Number Matching + Bloqueio SMS.

**AUTH-004 [Medium]**

Real-time checking of banned passwords against global (pwned) lists and company dictionaries....

**Action:** Evolve from level 3 to 4 - Integração com listas globais (pwned).

**JML-001 [Medium]**

Automate 'Birthright' provisioning via HR, creating accounts disabled until the start date....

**Action:** Evolve from level 3 to 4 - Scriptado (Powershell) disparado por ticket.