ManageEngine

ManageEngine solutions for Brazil's National Cybersecurity Policy

PNCiber at a glance

Decree № 11,856 (December 2023) established Brazil's National Cybersecurity Policy (PNCiber) for Critical Information Infrastructure (CII) operators across energy, telecom, finance, healthcare, transportation, water, and government sectors.

Applies to
CII operators and critical service providers

Enforced by
Sector regulators and National Cybersecurity Committee (CNCiber)

Core Focus
Prevention, CIA protection, cybercrime response, and resilience

How ManageEngine can help

Article, item	Description	Key controls	ManageEngine solutions
2, II	Guarantees fundamental rights and data protection	File integrity monitoring, USB/network share auditing, local account and privilege monitoring, adaptive MFA, approval-based access workflows	Log360, AD360
2, III	Prevents incidents and cyberattacks	Brute-force detection, Kerberos attack monitoring, MFA enforcement, strong password policies, and adaptive account lockout across VPN, Outlook on the web, IIS, and cloud	Log360, AD360
2, IV	Ensures organizational resilience to incidents	Log protection, backup monitoring, evidence preservation, 400+ threat rules, and automated AD backup and rapid recovery	Log360, AD360

3, III	Ensures CIA (Confidentiality, Integrity, and Availability)	Configuration change tracking, file integrity monitoring, registry changes tracking, database activity anomaly detection, real-time AD auditing, before/after snapshots, permission matrices for complete traceability, adaptive MFA across endpoints and apps, secure SSO and centralized access management, approval-based workflows and access governance, RBAC and delegated administration	Log360, AD360
3, IV	Fights cybercrime and malicious activity	Credential theft detection, AD enumeration, privilege escalation alerts (unauthorized user added to Local Administrators), suspicious account creation detection, account misuse and valid-account abuse control, automated dormant account cleanup, and identity life cycle management	Log360, AD360
3, V	Ensures risk management and cyber protection	Vulnerability scanning, ransomware detection, defence evasion, identity risk assessment, dormant account cleanup, privileged group audits, and access certification campaigns	Log360, AD360
3, VI	Enhances resilience through detection	Reconnaissance detection, lateral movement, incident management, automated provisioning and deprovisioning, RBAC with OU delegation, multiple point-in-time AD backups for rapid recovery	Log360, AD360
3, X	Develops regulatory oversight and control mechanisms	Compliance oversight and control dashboards, privileged access governance, access review, Zero Trust enforcement	Log360, AD360
6, III	Improves prevention, detection, analysis, and response	Incident management and SOAR automation, forensic analysis and before/after comparisons, cloud threat detection, automated provisioning and deprovisioning, approval workflows for admin changes, rapid search and filtering of identity events, and forensic AD change reports	Log360, AD360

For more information, contact us at sales@manageengine.com.

ManageEngine Log360

Personalized demo

ManageEngine AD360

Personalized demo