ManageEngine

A guide to

Complying with Brazil's National Cybersecurity Policy (PNCiber)

Table of contents

Introduction

Brazil's National Cybersecurity Policy (PNCiber), formalized in December 2023, represents a transformative step in establishing comprehensive cybersecurity governance frameworks across critical infrastructure, government agencies, and essential services. As digital threats escalate and adversaries target critical systems with increasing sophistication, PNCiber sets clear strategic and operational expectations for how organizations must protect national digital assets, ensure business continuity, and maintain resilience in the face of cyber incidents. The policy mandates that these organizations implement comprehensive security controls, establish incident response capabilities, collaborate on threat intelligence sharing, and build organizational resilience against cyberattacks.

By adopting PNCiber-aligned security practices, organizations strengthen their ability to withstand attacks, protect sensitive information, maintain operational continuity, and demonstrate accountability to regulators and stakeholders.This guide provides a practical roadmap for understanding PNCiber's requirements and leveraging ManageEngine's comprehensive security solutions to achieve and maintain compliance.

What is PNCiber compliance

PNCiber was enacted through Decree № 11,856 and establishes a comprehensive framework for cybersecurity governance across the nation's critical infrastructure and essential services. Unlike single-sector regulations, PNCiber applies to a broad spectrum of organizations designated as Critical Information Infrastructure (CII) operators, including energy utilities, telecommunications providers, financial institutions, healthcare systems, transportation networks, water systems, and government agencies.

Purpose and scope

PNCiber was developed in response to the escalating sophistication and frequency of cyberattacks targeting critical systems. The policy aims to:

- Establish unified cybersecurity principles across all critical infrastructure sectors, reducing fragmentation and strengthening national resilience.
- Mandate risk-based security controls tailored to the criticality of systems and data.
- Enable rapid incident detection and response through monitoring, alerting, and coordination mechanisms.
- Promote information sharing about threats and vulnerabilities among infrastructure operators and government agencies.
- Ensure continuity of essential services even in the face of significant cyber incidents.
- Support national security objectives by protecting critical systems from foreign and domestic threat actors.

Key stakeholders

The policy establishes roles and responsibilities across multiple layers.

Operators of Critical Information Infrastructure (CII): Organizations designated as critical by their sector regulator must comply with PNCiber's technical, operational, and governance requirements.

The National Center for Cybersecurity (Centro Nacional de Inteligência – CNI): Serves as a central coordinating body for threat intelligence and national cybersecurity strategy.

Regulatory bodies: Federal agencies (such as ABNT, ANATEL, ANP, ANVISA, and others) supervise compliance within their respective sectors and report to central coordinating authorities.

Service providers and third parties: Organizations that provide crucial services to CII operators must also adhere to security standards proportionate to their role.

Challenges with PNCiber compliance implementation

Organizations might face challenges while adhering with the PNCiber compliance such as:

1. **Translating broad principles into concrete controls**
PNCiber articles describe high-level objectives (sovereignty, fundamental rights, cybercrime fighting, resilience) rather than prescriptive technical checklists. Many organizations struggle to map these abstract goals into specific logging, monitoring, and identity-governance controls they can actually implement and evidence.

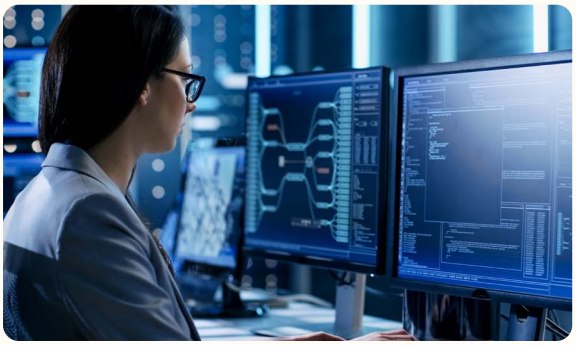
2. **Fragmented visibility across hybrid environments**
Most environments span on-premises AD, SaaS, cloud, and legacy systems, but PNCiber expects consistent protection, traceability, and incident handling across all of them. Without a unified monitoring layer, events remain siloed, making it difficult to demonstrate end-to-end visibility for principles like prevention, resilience, and coordinated incident response.

3. **Proving traceability and incident records**
Requirements linked to confidentiality, integrity, availability, and cybercrime fighting demand detailed records of access, changes, and incidents across systems. Many teams find it challenging to maintain complete, searchable audit trails and structured incident timelines that regulators or auditors can easily review.

4. **Managing privileged access and identity risk**
Articles focused on confidentiality, integrity, and availability (the CIA Triad), risk management, and cybercrime mean institutions must tightly control privileged accounts, local admin rights, and the account life cycle. In complex AD and hybrid identity setups, identifying risky privilege chains, dormant accounts, and valid-account abuse paths is non-trivial without specialized IAM tools.

5. **Sustaining continuous monitoring and improvement**
PNCiber emphasizes ongoing prevention, detection, and resilience rather than one-time projects. Organizations often lack defined KPIs (mean time to detect, mean time to respond, failed logon trends, configuration drift), making it hard to show continuous improvement and to align CNCiber-style responsibilities (better prevention, detection, analysis, and response) with day-to-day SOC operations.

Role of SIEM and IAM in PNCiber compliance



SIEM—Monitoring, detection, and traceability backbone

A SIEM tool helps organizations centralizes logs from AD, servers, applications, cloud services, and network devices, turning PNCiber's principles and objectives into concrete, monitorable signals. Correlation rules and threat analytics detect brute-force attempts, ransomware behavior, exfiltration patterns, cybercrime techniques, and configuration tampering. At the same time, predefined reports (failed logons, policy changes, backup status, incident timelines, audit trails) provide the traceability and incident records needed to evidence compliance with CIA, resilience, and incident-response obligations.

IAM—Identity, access, and privilege governance layer

IAM capabilities address the identity-centric side of PNCiber by governing who can access what, under which conditions, and with which level of privilege. Automated provisioning/deprovisioning, MFA, password-policy enforcement, privileged-group monitoring, and access-review campaigns support objectives around CIA, risk management, and fighting cybercrime by shrinking the attack surface for valid-account abuse, privilege escalation, and insider threats.

Together, SIEM and IAM give institutions both the continuous monitoring and the strong access control foundation that PNCiber expects.

Compliance levels and requirements

The National Cybersecurity Policy (PNCiber) defines Brazil's strategic, operational, and governance expectations for cybersecurity across public and private sectors. Rather than a single checklist, it combines high-level principles, concrete objectives, implementation instruments, and a national governance structure to coordinate cybersecurity actions over time.

From a compliance standpoint, organizations need to understand both the strategic articles (which define principles, objectives, and governance) and the technical and operational articles (which drive concrete controls, monitoring, and incident-response expectations).

ARTICLE 1

Purpose and scope of PNCiber

Article 1 formally establishes PNCiber as the national policy that will guide all cybersecurity activities in Brazil. It sets the expectation that cybersecurity is a matter of national interest and that both public and private entities must align their strategies and practices with this policy.

For organizations, this article frames cybersecurity as a long-term, state-level agenda rather than a set of isolated IT projects, and it underscores that compliance involves continuous alignment with national policy direction.

ARTICLE 2

Principles of PNCiber

Article 2 defines seven guiding principles that underpin all cybersecurity activities:

- I – **National sovereignty and national interest:** Cybersecurity decisions must preserve national sovereignty and prioritize Brazil's strategic interests.
- II – **Guarantee of fundamental rights:** Protection of freedom of expression, personal data, privacy, and access to information is central, making cybersecurity inseparable from digital rights.
- III – **Prevention of incidents and cyberattacks:** Emphasis on anticipating and preventing incidents, especially those targeting critical infrastructures and essential services.
- IV – **Organizational resilience:** Public and private organizations must be capable of withstanding and recovering from cyber incidents.
- V – **Education and technological development:** Continuous investment in cybersecurity education, awareness, and local technology development is required.
- VI – **Cooperation among actors:** Collaboration among government branches, private sector, and civil society is a core expectation.
- VII – **International technical cooperation:** Brazil aims to strengthen international cooperation on cybersecurity, including information sharing and joint initiatives.

These principles define the compliance mindset that should guide all internal policies, governance forums, and technical control decisions.

ARTICLE 3

Objectives of PNCiber

Article 3 operationalizes the principles as 11 concrete objectives that organizations and the national ecosystem must pursue:

- **I – National cybersecurity industry:** Promote development of nationally produced cybersecurity products, services, and technologies.
- **II – Confidentiality, integrity, authenticity, and availability (CIAA):** Ensure CIAA of solutions and data used for electronic or digital processing, storage, and transmission.
- **III – Responsible behavior in cyberspace:** Encourage safe and responsible behavior, including for vulnerable groups such as children, adolescents, and the elderly.
- **IV – Fight against cybercrime:** Contribute to combating cybercrime and other malicious activities in cyberspace.
- **V – Cyber protection and risk management:** Promote adoption of cyber protection and risk-management measures to prevent, avoid, mitigate, reduce, and neutralize vulnerabilities, incidents, and attacks.
- **VI – Organizational resilience:** Enhance resilience of public and private organizations to incidents and cyberattacks, going beyond mere prevention.
- **VII–VIII – Education, training, research, and innovation:** Develop cybersecurity education and professional training and foster research, technological development, and innovation.
- **IX–XI – Coordination, regulation, and international cooperation:** Improve coordinated actions and information sharing; develop regulatory, supervisory, and control mechanisms; and implement collaborative strategies for international cooperation.
  obligations for the above mentioned supervised entities under one regulatory standard.

From a compliance levels perspective, these objectives span:

- Strategic governance (for example, objectives I, IX–XI);
- Technical and operational security (for example, objectives II, IV, V, VI);
- Societal capacity-building (for example, objectives III, VII, VIII).

ARTICLES 4–5

Instruments and governance body (PNCiber and CNCiber)

Article 4 specifies that PNCiber will be implemented through two core instruments: the National Cybersecurity Strategy and the National Cybersecurity Plan, which provide concrete programs, milestones, and indicators for execution. These instruments translate the high-level principles and objectives into actionable initiatives for government and, indirectly, for regulated organizations.

Article 5 creates the National Cybersecurity Committee (CNCiber) within the Chamber of Foreign Affairs and National Defense of the Government Council, assigning it the role of monitoring the implementation and evolution of PNCiber. CNCiber is effectively the governance and coordination hub for national-level cybersecurity policy execution.

ARTICLES 6–13

CNCiber responsibilities, composition, and operation

Articles 6 through 13 detail how CNCiber will function in practice.

- **Article 6** defines CNCiber's responsibilities, which include proposing updates to PNCiber, evaluating measures to strengthen national cybersecurity, improving prevention/detection/response capabilities, promoting cybersecurity education, and fostering international technical cooperation.
- **Articles 7–11** define CNCiber's composition (multiple ministries, Central Bank, Anatel, civil society, academia, and private sector) and how it operates (quorum, voting, meetings, participation via videoconference).
- **Article 10** allows CNCiber to establish temporary thematic working groups with specific mandates and time-bound objectives.
- **Articles 12–13** clarify that participation is a relevant public service without remuneration and assign the Institutional Security Office as CNCiber's executive secretariat.

These provisions define the regulatory and oversight layer of PNCiber. While individual organizations do not "implement" these articles directly, they operate under the policies, guidance, and coordination that CNCiber produces.

ARTICLES 14–16

Transitional provisions, revocations, and entry into force

Article 14 describes the initial, transitional composition of CNCiber members from civil society, academia, and the private sector, until the regular selection processes defined in Article 7 are completed. Article 15 revokes specific provisions of Decree № 9,637/2018 to avoid overlap and conflict, consolidating cybersecurity governance under the new framework.

Article 16 states that Decree № 11,856 enters into force on the date of its publication, making PNCiber immediately effective as the overarching reference for national cybersecurity policy. For organizations, this confirms the expectation that strategies, risk programs, and technical controls should now be aligned with PNCiber's principles and objectives.

Technical and operational focus areas for organizations

Although PNCiber is primarily a strategic and governance-oriented policy, several objectives translate directly into technical and operational requirements that impact security architectures, SOC processes, and control landscapes:

- **Protection of fundamental rights and data (Article 2-II; Article 3-II):** Requires strong data protection, access control, logging, and auditability to safeguard privacy and personal data.
- **Prevention of incidents and cyberattacks (Article 2-III; Article 3-V):** Implies continuous monitoring, threat detection, vulnerability management, and robust configuration/change controls.

- **Organizational resilience and incident response (Article 2-IV; Article 3-VI):** Demands resilient infrastructure, backup and recovery, incident-management processes, and evidence-rich audit trails for analysis and recovery.
- **Implementation of incident response plans (Article 6, as mapped in the solution matrix):** Requires concrete procedures, timelines, and reporting capabilities when responding to cyber incidents.

How ManageEngine can help

ManageEngine provides a comprehensive portfolio of security solutions that directly address PNCiber's technical and operational requirements. By integrating Log360 (SIEM/threat detection) and AD360 (identity governance), organizations can build a unified security posture that achieves and maintains compliance.

Article, item	Description	How Log360 can help?	How AD360 can help?
2, II	Guarantees fundamental rights and data protection	Comprehensive IAM capabilities including user provisioning, deprovisioning, and group management.	Comprehensive IAM capabilities including user provisioning, deprovisioning, and group management.
2, III	Prevents incidents and cyberattacks	Real-time brute-force detection (failed logon reports and Kerbrute rules), Kerberos attack monitoring (TGT ticket requests), and over 400 threat rules	MFA enforcement (over 20 methods, including SMS, TOTP, push notifications, and biometrics); strong password policies; and adaptive account lockout across VPNs, Outlook on the web, IIS servers, and the cloud
2, IV	Ensures organizational resilience to incidents	Log protection, backup monitoring, evidence preservation, 400+ threat rules	Automated AD backup and rapid recovery
3, II	Ensures CIA (Confidentiality, Integrity, and Availability)	File integrity monitoring (for files created, modified, or deleted), real-time AD auditing (of user, group, GPO, and computer changes), registry change tracking, database activity anomaly detection, and Windows backup monitoring, defense evasion monitoring, ransomware detection and containment, configuration change tracking	Adaptive MFA across endpoints and apps, secure SSO and centralized access management, approval-based workflows and access governance, RBAC and delegated administration

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, identity life cycle management
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
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
3, X	Develops regulatory oversight and control mechanisms	Compliance oversight and control dashboards	Privileged access governance, access review, Zero Trust enforcement
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

Conclusion

PNCiber establishes clear, comprehensive requirements for critical infrastructure operators to strengthen cybersecurity governance, enhance incident detection capabilities, and build organizational resilience. Compliance is not a one-time effort, but a continuous process of monitoring, detecting, responding, and improving.

ManageEngine's integrated security portfolio—combining Log360 SIEM, AD360 identity governance, provides critical infrastructure operators with the visibility, control, and automation required to meet PNCiber's technical and operational requirements. From real-time threat detection and forensic analysis to identity risk management and automated incident response, ManageEngine enables organizations to:

- Detect threats in real-time before they cause operational impact
- Respond rapidly and consistently with automated playbooks and centralized coordination
- Maintain forensic evidence for investigations and regulatory reporting
- Reduce identity risks through privilege management and access governance
- Protect critical data through file monitoring and access controls
- Maintain operational resilience through backup, recovery, and continuity planning

By implementing ManageEngine solutions aligned, organizations strengthen their ability to protect national critical infrastructure, maintain business continuity, preserve customer trust, and demonstrate accountability to regulators and stakeholders.

ManageEngine
AD360

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download

ManageEngine
Log360

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download