Direito,
Inovação
& Tecnologia

CYBERSECURITY AND CYBERCRIME

A VIEW OF BRAZIL

2ND EDITION, NEWLY RELEASED, INCLUDING:

- Global Risks Report 2026 – WEF
- United Nations Convention against Cybercrime
- National Cybersecurity Strategy (Brazil)
- CMN Resolution No. 5,274/2025 (Financial Sector)
- Use of AI in Criminal Investigations (Ordinance No. 961/2025 – Ministry of Justice and Public Security)

MARCH 2026

WWW.VLKLAW.COM.BR

SUMMARY

1. Contextualization of the Brazilian Landscape 3

2. General Rules 9

a) General Data Protection Law (LGPD – Law No. 13,709/18) 13

b) Brazilian Internet Civil Framework (Law No. 12,965/14) and its Regulatory Decree (Decree No. 8,771/16)

c) Consumer Protection Code

3. Sector-Specific Rules

a) Telecommunications Sector

b) Financial Sector

c) Energy Sector

d) Healthcare Sector

e) Insurance Sector

4. Essential Services and Critical Infrastructure 22

5. Cybercrimes 24

a) Criminal Classification of Conduct

Unauthorized Access to Computer Device (Art. 154-A of the Criminal Code)

Electronic Fraud (Art. 171, §2-A and §2-B of the Criminal Code)

Digital Theft (Art. 155, §4-B of the Criminal Code)

b) Use of Technology in Criminal Investigations

6. Federal Network for the Management of Cyber Incidents (Decree No. 10,748, of July 16, 2021)

7. Relevant Court Decisions 29

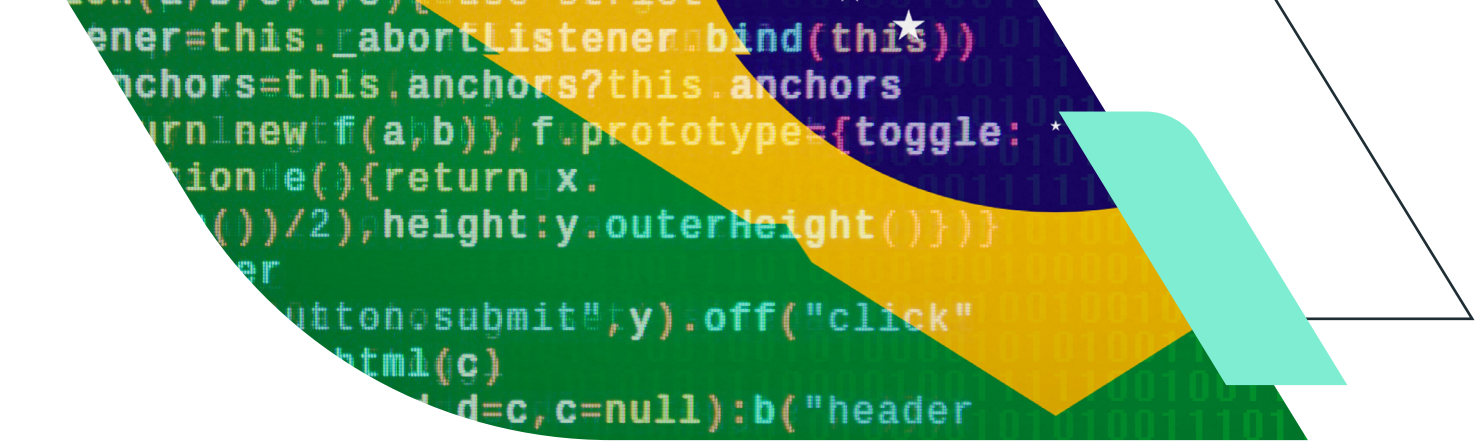
8. National Cybersecurity Policy (Decree No. 11,856/2023) and the National Cybersecurity Committee

9. New National Cybersecurity Strategy (Decree No. 12,573/25) 34

10. Next Steps in Brazil 36

Conclusion 38

About Us 39



1. Contextualization of the Brazilian Landscape

Cyber incidents emerge as a critical short- and long-term concern, according to the most recent reports from the World Economic Forum. The agenda goes far beyond fraud and data leaks: cyberattacks have the potential to paralyze companies, institutions, and even entire countries.

The Global Risks Report 2026 states that the world has entered an "Era of Competition", marked by institutional fragmentation and high uncertainty, in which technological risks assume strategic centrality. Disinformation is the 2nd largest risk in the short term (2 years) and the 4th in the long term (10 years), driven by generative AI, social networks and deepfakes, with a direct impact on social polarization and erosion of democratic trust. Artificial intelligence is the fastest growing risk in severity: it goes from 30th position in two years to 5th place in ten, with concerns linked to the massive replacement of administrative jobs, increasing inequality and military use in autonomous systems, raising the risk of unintended escalations. "Cyber insecurity" remains structural: 6th in the short term and 8th in the long term, with increasingly sophisticated attacks against critical infrastructure and the emerging threat of "Q-day", when quantum computing could break current encryption. The report concludes that digital literacy, transition to post-quantum cryptography and professional reskilling are urgent measures, and that the regulatory and technological governance choices made now will define whether technology will be a vector of prosperity or

systemic instability.

The financial impact is alarming. The direct and indirect cost of cyber incidents accounts for 14% of global GDP per year (World Economic Forum, 2024). In Brazil, this amount can reach 18% of GDP — the equivalent of R$ 2.3 trillion, according to the INCC. On average, each incident costs $4.48 million. In Brazil, the value is US$ 1.22 million, appearing in 16th position (IBM, 2025). When a publicly traded company suffers a successful attack, regardless of its past performance, its stock value tends to fall, on average, by 7.5% (Harvard Business Review, 2023).

Brazil is one of the main targets of cyberattacks and digital fraud in the world, experiencing a paradox in cybersecurity: while it leads in innovation and incorporates advanced digital solutions, such as PIX and Open Banking, it also becomes a target and is increasingly exposed to cyberattacks.

In terms of fraud, in March 2025, 38% of the Brazilian population was a victim of a banking scam (or attempted scam), according to Febraban, including credit card cloning (40%) social engineering on WhatsApp (28%); phishing by call (26%); and Pix scam, involving malicious link or QR Code (16%).

In the first quarter of 2025, Brazil registered, on average, more than 2.6 thousand weekly cyberattacks by companies (Check Point Research), an increase of 21% compared to the same period in 2024. The country suffered 60 billion attempted cyberattacks in 2023 (Fortinet).

Today, 40% of phishing attacks targeting businesses are already AI-generated (VIPRE Security Group) and up to 60% of recipients may fall for these scams

(Harvard Business Review), revealing a worrying success rate. It is the ,social engineering of high conversion: hyper-personalized, multi-language messages with voice cloning, for example.

On the criminal side, the use of AI reduces the costs of fraudulent campaigns by up to 95% (Harvard Business Review), making this vector even more attractive.

The impact also expands to deepfakes, which are expected to increase global losses by 32% by 2027, about US$ 40 billion annually (Deloitte).

The speed of attacks also reaches unprecedented levels: the average time for criminals to advance from an initial breach to lateral movemento has dropped to 48 minutes, with a record case of only 51 seconds (CrowdStrike, 2025).

The phenomenon of Shadow AI, in which employees use AI systems without corporate approval, has already been responsible for 20% of breaches and added, on average, $670,000 to the cost of incidents. In addition, 97% of incidents involving AI occurred in systems without adequate controls (IBM, 2025).

Given this scenario, several strategies have been pointed out as ways to mitigate risks. Among them, the following stand out:

» National cybersecurity coordination, as fragmentation between different stakeholders leads to slow and ineffective responses to the volume and complexity of threats;

» Regulatory harmonization, with the creation of a clear, balanced and risk-based legal framework, aligned with the best international practices and without imposing prohibitive operating costs; e

» The implementation of a national cybersecurity awareness program, aimed at companies and citizens, which also integrates the topic into educational curricula, from elementary to higher education.

On the international scene, the movement has already started decades ago. The Budapest Convention on Cybercrime was adopted in 2001. From the second decade of the 2000s, the European Union approved the NIS directive, obliging the 27 countries of the bloc to create national cybersecurity legislation and structures. More recently, the EU approved NIS2, raising the bar even higher. Countries such as China, Russia, Japan, and South Korea have also developed specific laws and bodies.

At the UN level, the United Nations Convention against Cybercrime, adopted by the General Assembly at the end of 2024 and formally signed in 2025, is going through the global ratification process to achieve the 40-country target and fully enter into force. It establishes the first universally binding legal framework and aims to standardize cross-border police cooperation and electronic evidence collection, seeking to balance state sovereignty and effectiveness in combating complex digital crimes, although it still faces intense debates on the protection of

privacy and human rights in the face of the surveillance power of states.

In Brazil, only in 2023 did the country enact its accession to the Budapest Convention, in addition to having signed the final text at the UN in 2025, which needs to go through the National Congress. The existing requirements are generally sectoral and non-harmonised. Laws such as the Civil Code, the Consumer Protection Code, the Civil Rights Framework for the Internet, the Industrial Property Law, and the LGPD, for example, contain provisions related to the subject, as well as specific regulations for sectors such as finance, telecommunications, insurance, and health. However, there is a lack of a common body of regulations, and other sectors do not even have minimum cybersecurity requirements.

In 2025, the new National Cybersecurity Strategy (E-Ciber - Decree No. 12,573/2025) was published. Formulated by the National Cybersecurity Committee (CNCiber), E-Ciber was structured in four thematic axes: protection and awareness of society; security and resilience of essential services and critical infrastructure; multisectoral cooperation; and digital sovereignty.

However, the absence of a national and intersectoral regulatory body compromises the implementation of cross-cutting standards, recommended by international good practices. This gap may help explain why Brazil is among the most attacked countries in the world. Without clear rules, cybersecurity is often neglected and the damage only becomes evident when it is too late.

Remembering that 98% of cyberattacks could be prevented with basic digital hygiene measures, such as the use of antimalware, updating systems, multi-factor authentication, access control, and credential governance (Microsoft Digital Defense Report, 2022). In other words, a central body guiding the awareness of companies and people would be enough to avoid most incidents.

Although the creation of a national cybersecurity governance structure represents a relevant investment, and should be analyzed with caution in light of the current fiscal scenario, — the numbers indicate that, if well designed and executed with a focus on efficiency and coordination, this measure can generate positive economic impacts. It is estimated that preventing just 10% of the damage caused by cyberattacks would already result in annual savings of between R$ 150 and R$ 230 billion. Even considering an estimated total cost of R$ 500 million per year from the fifth year onwards, the potential return would be very expressive, with gains in the order of 300 times higher than the investment. From the government's point of view, the tax collection derived from this economy would exceed R$ 50 billion, which would represent a fiscal return of more than 100 times the amount invested. Still, it is essential that any proposal moves forward based on intersectoral dialogue, transparency, and rationalization of resources.

In other words, cybersecurity is no longer a merely technical issue. It is a strategic and essential choice, of leaders, councils and, above all, of nations.

2. General Rules

A) GENERAL LAW FOR THE PROTECTION OF PERSONAL DATA (LGPD – Law 13.709/18)

Under the terms of the LGPD, the processing of personal data must observe good faith and be guided by principles (Art. 6), such as:

- **Secuurity,** with the adoption of technical and administrative measures to protect data against unauthorized access, as well as against accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;
- **Prevention,** through the implementation of actions that prevent the occurrence of damage as a result of treatment;
- **Accountability and accountability,** requiring the agent to demonstrate the adoption of effective measures that prove compliance with data protection regulations.

The processing will be considered **irregular** when it does not comply with the legislation or fails to guarantee the level of security that the holder can reasonably expect, considering the way it is carried out, the risks involved and the techniques available at the time (Art. 44).

Processing agents **must adopt security, technical and administrative**

measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or unlawful processing (Art. 46).

The **processing agents or any other person who intervenes in one of the phases of the processing undertakes to guarantee the security of the information** in relation to the personal data, even after its termination (Art. 47).

In addition, **in the event of a security incident with relevant risk or damage, the controller has the duty to notify both the National Data Protection Agency (ANPD) and the affected data subject** (Art. 48).

On the subject, the ANPD in 2024 issued Resolution 15, which approved the Security Incident Regulation, bringing with greater objectivity: i) relevant concepts (art. 3); ii) situations of high risk and relevant damage (art. 5); iii) accountability documents that must be prepared, especially the Security Incident Record (art. 10), among others.

Finally, it is also important to mention the ANPD Resolution 4/2023, which Approveor o Regulation on Dosimetry and Application of Administrative Sanctions of the National Data Protection Authority, Define going the criteria, methods and as circumstances to calculate and apply administrative sanctions for non-compliance with the LGPD, ensuring greater legal certainty and proportionality in punishments.

B) CIVIL RIGHTS FRAMEWORK FOR THE INTERNET (LAW 12.965/14) AND ITS REGULATORY DECREE (Decree 8.771/16)

The **Civil Rights Framework for the Internet** establishes, among its principles, the **preservation of the stability, security and functionality of the network**, through technical measures in line with international standards and the encouragement of good practices (art. 3, V).

In addition, it imposes duties of record keeping:

- The **autonomous system administrator** responsible for the connection must keep the connection records for a period of **1 year**, under **secrecy** and in a **controlled and secure environment** (art. 13).

- **Internet application providers**, when professionally organized and for economic purposes, must keep application access records for **6 months**, also under secrecy and in a **secure environment** (art. 15).

Decree No. 8,771/2016, in turn, regulates the security and confidentiality standards in the safekeeping, storage, and processing of personal data and private communications, requiring providers to adopt measures such as (Art. 13):

- **Strict control** of access to data, with clear definition of the responsibilities

and privileges of authorized users;

- **Robust authentication,** preferably with multiple factors, to individualize those responsible for access;

- **Detailed inventory of accesses,** including time, duration, identity of the person responsible and file accessed;

- **Data inviolability protection solutions**, such as encryption or equivalent security measures.

C) CONSUMER PROTECTION CODE

Under the terms of **the Consumer Protection Code**, it is considered an abusive practice to place products **or services on the market that do not comply with technical standards established by competent official bodies** or, in their absence, **by the Brazilian Association of Technical Standards (ABNT)** (art. 39, VIII).

This implies that **companies that neglect to comply with recognized technical standards for cybersecurity,** such as **ABNT NBR ISO/IEC 27001** and **ABNT NBR ISO/IEC 27701,** may be held **responsible for inappropriate or unsafe practices**, including in the field of consumer protection.

3. Sectoral Standards

A) TELECOMMUNICATIONS SECTOR

In the telecommunications sector, the **National Telecommunications Agency (Anatel)** is the entity responsible for defining cybersecurity guidelines applicable to service providers.

The topic is mainly governed by **Resolution No. 740/2020**, amended by **Resolution No. 767/2024**, which establishes the **Regulation on Cybersecurity Applied to the Telecommunications Sector**. Among its main requirements, the following stand out:

- **Establishment of a Cybersecurity Policy**, with incident response procedures (art. 14);
- **mandatory communication to Anatel** of security incidents considered relevant, such as: relevantes, tais como:
  - Those also reportable to the ANPD (art. 2-C);
  - Incidents that substantially affect the security of networks or user data (art. 9 and 17), requiring notification to users and inclusion of analysis of the

cause, impact, and mitigation actions.

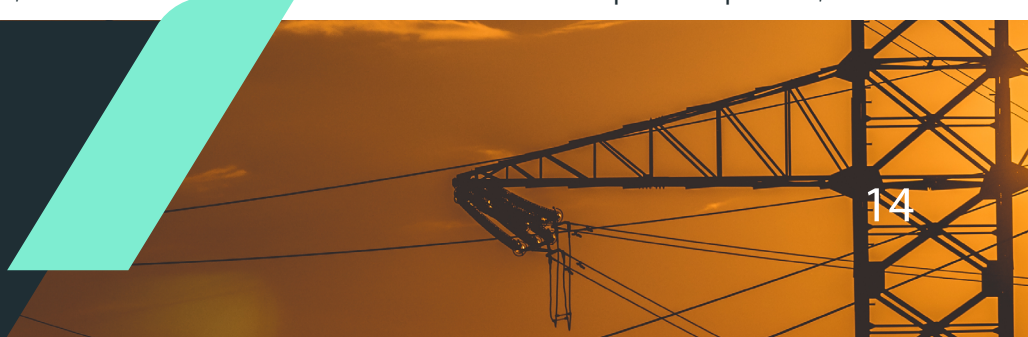
The form of communication must follow **guidelines from Anatel's GT-Ciber**, as established in **Decision Order 49/2021/COQL/SCO**: the incident must be reported by the SEI within 2 business days, even if preliminarily, with complementation within 60 days. Examples of relevant incidents are:

- Leaks of corporate or customer data;
- Successful ransomware attacks and advanced persistent threats (APT);
- Denial-of-service (DDoS) attacks with traffic equal to or greater than 50Gbps or 20Mpps;
- Routing issues impacting service delivery; and
- Unavailability of service caused by cyber incident.

The regulation also imposes **obligations for prior evaluation of suppliers,** including cloud services, regarding compliance with the rules, **requiring periodic independent audits** and documentation of the process, to be presented to Anatel upon request.

There is also a requirement to **share information on relevant incidents** between providers, in a confidential and non-discriminatory manner, including with the option of anonymity, for the purpose of coordination with other entities (art. 18).

In addition, in October 2023, Anatel published a **Cybersecurity Guide**, with practical recommendations, such as the creation of incident response plans,



specific contact channels for incident communication.

B) FINANCIAL SECTOR

In the financial sector, guidelines on cybersecurity and incident response are established by **regulatory entities such as the Central Bank of Brazil (BCB), the National Monetary Council (CMN)** and the **Securities and Exchange Commission (CVM).**

The Resolution CMN nº 5.274/2025 eraised the standard of governance by detailing the minimum mandatory content of cybersecurity policies, requiring specific mechanisms for authentication, encryption, prevention of information leakage and management of backups, partially updating the CMN Resolution nº 4.893/2021, that Establishes guidelines for the cybersecurity policy and requirements for the contracting of data processing and storage and cloud computing services by financial institutions, providing for the following obligations:

Cybersecurity Policy

- It must be designed, implemented and compatible with the size, risk profile and complexity of the institution;.

- It must contain specific objectives, controls, and procedures, such as authentication, encryption, intrusion detection, copy management, among others; and.
- Reviewed annually and approved by senior management.

Action Plan and Incident Response

- Establish preventive and reactive actions, with the area responsible for recording the effects of incidents.
- Prepare annual report, including incidents, tests and effectiveness.

Comunicação de Incidentes ao BCB

- Relevant incidents and disruptions of essential services must be reported in a timely manner.
- The measures adopted for the resumption of activities must also be informed.

Contracting Cloud Services and Data Processing

- Prior evaluation of the contracted company and adherence to regulation.
- Full responsibility of the institution for the contracted services.
- Communication to the BCB after contracting/changing relevant services.
- Additional requirements for services provided abroad.

Designation of Responsible Director

- The institution must appoint a **director responsible for** the cybersecurity policy and for the execution of the action plan and incident response.

Within the scope of **Pix, BCB Resolution No. 1/2020, BCB Resolution No. 402/2024** and **BCB Normative Instruction No. 412/2024**, determine that participants who offer accounts to holders must **communicate them directly about incidents with their personal data**, even when they are not directly responsible for the incident, and even if there is no relevant risk or damage.

The communication must follow the following operational criteria:

- Be carried out within the deadline defined by the BCB, via the official electronic mail system;
- Include clear, individualized language, and contain information about the incident, the data affected, and the risks involved;
- Be archived, being available to the BCB at any time.

In the capital market, **CVM Instruction No. 505/2011**, as amended by CVM Instruction No. 612/2019, imposes obligations on securities intermediaries regarding **information security and business continuity**. The rule requires the adoption of an **Information Security Policy**, covering:

- Processing and control of customer data;
- Assessment of the **relevance of security incidents**; and
- Communication to affected customers, when the incident involves **critical business processes** or **sensitive data**, with **significant impact.**

C) ENERGY SECTOR

NIn the electricity sector, the National Electric Energy Agency (ANEEL) establishes, through Resolutions No. 24/2021 and No. 964/2021, specific obligations related to cybersecurity.

According to article 4 of Resolution No. 964/2021, regulated agents must adopt incident prevention, detection, response, and recovery mechanisms as an integral part of their Cybersecurity Policy. This policy should also provide criteria for assessing the relevance of incidents and guide communication to the designated sectoral coordination team.

It is mandatory to report to ANEEL the incidents considered to have the greatest impact (article 6), which must be recorded, analyzed in terms of cause and impact, and accompanied by measures to control the effects, — including data provided by third-party service providers.

The standard defines a cyber incident as any event that compromises, actually or potentially, the availability, integrity, confidentiality or authenticity of information systems or the data processed therein, including attempts to exploit vulnerabilities that constitute a violation of internal rules or policies (art. 2, I).

The incidents with the greatest impact are those classified as high severity, according to the risk matrix of each agent (art. 2, II).

Já os incidentes de maior impacto são aqueles classificados como de **alta severidade**, conforme a matriz de risco de cada agente (art. 2º, II).
In addition, agents must keep detailed records and provide ANEEL, upon request, with information such as:

- Results of the maturity models applied, including extent and

impact of events, degree of threat, relevance, vulnerability, normalization effort and frequency;

- Identified cyber risks and respective forms of treatment; and

- Data from the teams responsible for preventing, handling, and responding to cyber incidents.

D) HEALTH SECTOR

In the health sector, the **National Health Surveillance Agency (Anvisa)** is the main regulatory entity with provisions aimed at information security, especially with regard to medical devices and personal data protection. The National Supplementary Health Agency (ANS), in turn, does not yet have specific regulations on the subject.

Anvisa Ordinance No. 1,184/2023 determines, among arts. 29 to 31, that information and communication technology service providers adopt procedures and a response plan **for security incidents**, and must prove the existence of security guarantees and immediately communicate any risk or incident that may affect personal data. The rule also provides that Anvisa must issue its own regulations for the management of incidents involving personal data, still pending publication.

Anvisa's **Guide No. 33/2020,** aimed at the **validation of computerized systems** applied in Good Manufacturing Practices, deals with **incident management** (Section 11.5), emphasizing the importance of rapid responses, clear notifications to the competent authorities, and staggered communication in case of relevant

impact. Section **11.6** addresses **corrective and preventive actions (CAPA)**, focusing on **rigorous documentation** of the measures adopted and **evaluation of effectiveness,** ensuring continuous improvement and robustness of the systems.

Guide No. 38/2020, which deals with **the principles and practices of cybersecurity in medical devices**, establishes guidelines for manufacturers to **develop solid processes for evaluating, responding to, and communicating cyber incidents**, in collaboration with Anvisa and health service providers, throughout the entire life cycle of devices (Section 6.5).

E) INSURANCE SECTOR

In the insurance sector, the **Superintendence of Private Insurance (Susep)** regulates cybersecurity requirements through **SUSEP Circular No. 638/2021,** applicable to insurers, open supplementary pension entities, capitalization companies, and local reinsurers.

The rule determines that supervised companies must maintain **updated processes, procedures and controls** to **identify and reduce vulnerabilities**, as well as **detect, respond to and recover from cyber incidents**, which must be formalized in the **company's Business Continuity Plan** (BCP) (article 5).

It is mandatory to implement an **Action and Incident Response Plan,** containing:

- AActions to adapt the organizational structure to the guidelines of the cybersecurity policy;
- Procedures, controls and technologies for incident prevention and response;

- Designation of the area responsible for recording and monitoring the effects of relevant incidents (articles 6 and following).

Relevant incidents are defined as adverse events (malicious or not) that substantially compromise the confidentiality, integrity, or availability of relevant data or services (art. 2, IV). Relevant data, on the other hand, includes personal data (according to the LGPD), customer information, critical processes, and any others defined as sensitive by the supervised companies themselves (art. 2, VI).

The communication of these incidents to **Susep must occur within 5 business days** (article 8) and must contain:

- The extent of the damage;

- The actions in progress for correction;

- The responsible parties and deadlines, when applicable.

In addition to Susep, there is also a duty to notify affected parties, including customers, although the rule does not stipulate a specific deadline or clearly define the types of incidents that require such communication (article 5, VII). In practice, the same period of 5 business days provided for submission to Susep has been adopted.

Finally, supervised companies must prepare an annual report on the effectiveness of incident prevention and response actions, based on the occurrences and measures adopted in the period.

4. Essential services and critical infrastructure

Critical infrastructure and essential services represent strategic areas for national security, the functioning of society, and the continuity of vital economic activities. The regulation on the subject is found in the following normative frameworks in Brazil:

The National Policy for the Security of Critical Infrastructures, established by **Decree nº 9.573/2018**, assigns to the Institutional Security Office of the Presidency of the Republic (GSI/PR) the competence to monitor issues related to critical infrastructures within the scope of the federal public administration (art. 2).

In addition, the National Strategy for the Security of Critical Infrastructures, provided for in **Decree nº 10.569/2020**, reinforces the strategic role of sectors such as communications, energy, transport, finance, and water, whose interruption or destruction can generate social, economic, political impacts, or impacts on national security and sovereignty itself. The strategy highlights the GSI's role in identifying and analyzing risks, in cooperation with public and private entities.

Law No. 7,783/1989, on the other hand, defines **essential services and activities**, which must be maintained even in strike contexts, given their importance for meeting the **urgent needs of the community**. The list includes, among others:

- Water, electricity, fuel and gas supply;
- Medical and hospital care;
- Distribution of medicines and food;
- Telecommunications and public transport;
- Processing of data related to essential services;
- Air traffic control, banking and port activities; and
- Medical-forensic and funeral activities.

The legislation determines that **unions and employers must keep minimum teams in operation during stoppages**, in order to avoid irreversible damage and ensure the continuity of essential services (articles 9 and 11).

5. Cybercrimes

A) CRIMINAL CLASSIFICATION OF CONDUCTS

Brazilian criminal legislation provides for specific sanctions for crimes committed in the digital environment, with a focus on **protecting computer devices, data, and systems** against intrusions and fraud.

INVASION OF A COMPUTER DEVICE (ART. 154-A OF THE PENAL CODE)

It is a crime **to invade a computer device for the use of others**, with or without a network connection, with the purpose of **obtaining, tampering, destroying data or installing vulnerabilities**, without the user's authorization.

- **Penalty:** imprisonment from 1 to 4 years, and fine
- Anyone who produces, sells or distributes programs or devices with the intention of allowing this practice incurs the same penalty.
- **The penalty** is increased from **1/3 to 2/3** if the invasion causes **economic loss**.
- If the invasion results in the obtaining of **private communications, commercial or industrial secrets, confidential information or remote control of the device**, the penalty is 2 to 5 years, and a fine.
- There will be **an increase of 1/3 to 2/3** if the data obtained is **disclosed,**

marketed or transmitted to third parties.

ELECTRONIC FRAUD (ART. 171, §2-A AND §2-B OF THE PENAL CODE)

It is the practice of **fraud to obtain an illicit advantage**, with the use of **social networks, calls, emails or other digital means** that induce the victim or third parties to error.

- **Penalty:** imprisonment from **4 to 8 years**, and fine.
- The penalty is increased from **1/3 to 2/3** if the crime is committed with the **use of servers abroad.**

DIGITAL THEFT (ART. 155, §4-B OF THE PENAL CODE)

It is characterized by **theft by fraud,** committed by means of **electronic or computer devices**, even without violation of security mechanisms or with the use of **malicious software.**

- **Penalty:** imprisonment from 4 to 8 years, and fine.

B) USE OF TECHNOLOGY IN CRIMINAL INVESTIGATIONS

Ordinance 961/2025, of the Ministry of Justice and Public Security (MJSP), establishes unprecedented standards for the use of technological solutions in criminal investigations and public security intelligence activities, with Three fundamental pillars:

- The strengthening of investigation and intelligence mechanisms through advanced technological solutions;
- The rigorous protection of personal data to prevent illicit use in fraud, financial scams and stalking; and
- The creation of clear parameters for the application of artificial intelligence (AI) in public security operations.

The ordinance applies to all federal security forces, such as the Federal Police, Federal Highway Police, Federal Criminal Police, National Public Security Force and National Criminal Force.

Among the main innovations, the ordinance authorizes the use of technologies in criminal investigations, provided that the principles of legality, necessity and purpose are respected.

For the first time in the country, a specific regulation establishes clear parameters for the use of artificial intelligence in public security, defining ethical and operational limits that ensure efficiency without compromising citizens' fundamental rights.

In the prison area, the measure authorizes the use of technology to locate and block cell phones and, with judicial authorization, access data stored on the devices. These actions aim to curb organized crime and expand control over illicit communications made from inside prisons.

The regulation establishes strict governance rules, including access control to systems, periodic reviews of user profiles, disaster response plans, regular audits, investigation of improper access, and detailed recording of all actions taken.

The contracting of technologies must follow specific bidding rules, with transparency and social control over investments in security technology.

6. Federal Cyber Incident Management Network

(DECREE NO. 10,748, OF JULY 16, 2021)

Decree No. 10,748/2021 establishes the **Federal Network for Cyber Incident Management,** based on Decree No. 9,637/2018, with the objective of **strengthening coordination between bodies and entities of the direct, autarchic and foundational federal public administration** in the face of cyber risks (art. 1 and 2).

The purpose of he Network is **to raise the level of resilience in cybersecurity** of the information assets of the federal public administration, through integrated actions of prevention, treatment and response to cyber incidents.

Among its **main objectives**, the following stand out (art. 3):

- **Disclosure of preventive and reactive measures** related to cybersecurity;
- **Sharing alerts** about threats and vulnerabilities;
- **Dissemination of information** about cyberattacks;
- **Promotion of institutional cooperation** among the participants of the Network; and
- **Agility in incident response**, ensuring efficiency in facing relevant cyber events.

7. Relevant court decisions

The Superior Court of Justice (STJ) has analyzed relevant cases on data breach and corporate liability, interpreting the LGPD:

- In 2023, the Second Panel understood that, **although data breach is an undesirable failure, it does not, by itself, generate the right to compensation for moral damages.** To do so, the holder must **prove the actual damage** caused by the exposure, as the leaked data was common and frequently provided in registries and consultation sites. However, the understanding could be different if the case involved sensitive data, such as health, racial or ethnic origin, religious conviction or biometrics, for example.
- Following the above premise, in 2025, the Third Panel of the STJ recognized that, in a life insurance contract, **the leakage of the insured's sensitive personal data generates strict liability of the insurer and characterizes presumed moral damage**, highlighting that sensitive data requires greater protection and that its leakage can compromise aspects of the insured's life, such as honor, image and personal security.
- In 2024, the same Third Panel of the STJ understood

that a financial institution is liable for the defect in the provision of the service consisting **of the improper treatment of bank data, when this information is used by fraudsters to scam consumers.**

- I n another case resulting from a hacker attack, the Third Panel of the STJ, in 2024, reinforced that the fact that the **invasion was caused by third parties does not remove the company's responsibility, as the organization needs to demonstrate that it has adopted good security practices**, including data governance, supervision tools, and risk mitigation policies. If it cannot prove its diligence (proactive liability), it may be held liable, and the allegation of "external fortuitousness" is not sufficient.

8. National Cybersecurity Policy and the National Cybersecurity Committee

(DECREE NO. 11,856/2023)

Decree No. 11,856/2023 instituted the **National Cybersecurity Policy (PNCiber)**, with the purpose of guiding the Brazilian State's actions on the subject. The policy is structured based on **fundamental principles,** such as:

- National sovereignty and prioritization of the country's interests;
- Prevention of incidents and cyber attacks, especially against critical infrastructure and essential services;
- Strengthening the resilience of public and private organizations;
- Promotion of education and technological development in cybersecurity;
- Cooperation between public and private entities; and
- Promotion of international technical cooperation.

PNCiber also establishes strategic objectives, among which the following stand out:

- DDevelopment of national products, services and technologies aimed at cybersecurity;
- Guarantee of the confidentiality, integrity, authenticity and availability of digital information;
- Enhanced protection for vulnerable groups in cyberspace, such as children, adolescents and the elderly;
- Combating cybercrime and malicious actions;
- Encouragement of the adoption of protection, risk management and organizational resilience measures;
- Strengthening of education and technical-professional training in cybersecurity;
- Encouragement of scientific research, innovation and articulation between different levels of government, powers, private sector and society;
- Creation of regulatory and control mechanisms to improve national security in the digital environment; and
- Structuring of coordinated actions for international cooperation.

As **implementation instruments,** the policy will be operationalized through:

- National Cybersecurity Strategy; and

- National Cybersecurity Plan.

To monitor and promote its execution, the decree creates the **National Cybersecurity Committee (CNCiber)**. Their duties include:

- Propose updates to PNCiber and its instruments;

- Evaluate and suggest measures to expand national cybersecurity;
- Formulate proposals to improve the prevention, detection and response to incidents;
- Propose cybersecurity training and international collaboration strategies;
- Act as an instance of dialogue with society and federative entities.

CNCiber is a collegiate chaired by the representative of the Institutional Security Office of the Presidency of the Republic, and composed of 14 representatives of federal public administration bodies, 1 representative of the Internet Steering Committee in Brazil and 9 representatives of civil society entities, including 3 entities with activities related to cybersecurity or the guarantee of fundamental rights in the digital environment. 3 scientific, technological and innovation institutions related to the area of cybersecurity and 3 entities representing the business sector related to the area of cybersecurity.

9. New National Cybersecurity Strategy (Decree 12,573/25)

E-Ciber has 3rd generation characteristics, compared to its counterparts in other countries, although it is the second document of its kind in Brazil. The strategy foresees that the approximately 40 strategic actions will be unfolded into initiatives described in National Cybersecurity Plans, updated periodically by CNCiber.

There are 4 thematic axes that are articulated and advanced in parallel:

- **1º AXIS:** ctions for greater protection and awareness of citizens and society, including formal and informal education actions at all levels and for audiences of different ages.
- **2º AXIS:** security and resilience of essential services and critical infrastructures, proposing actions that allow the accelerated digital transformation that Brazil is going through to continue while reducing the risk of incidents that destabilize society.
- **3º AXIS:** actions focused on cooperation and integration between national and international bodies and institutions.
- **4º AXIS:** focuses on initiatives to ensure national sovereignty and cybersecurity governance.

From thisques:

- it proposes centralized governance, promoting the development of regulation, inspection, coordination and control mechanisms;
- strengthens Brazil's sovereignty and independence by promoting national technological development and reducing dependence on foreign technologies;
- promotes inclusion and diversity, by encouraging the protection and awareness of vulnerable groups;
- promotes the structuring of cyber maturity, structurally evolving cybersecurity in Brazil;
- improves the protection of essential services and critical infrastructure by promoting preparedness and resilience of essential services and critical infrastructure, including minimum and secure standards and the certification of products and services;
- fosters innovation in Small, Microecompanies and Startups, including specific actions to create an innovation environment for smaller companies;
- proposes the increase of international cooperation activities for the joint strengthening of cyber capabilities;
- promotes education and awareness, by pursuing a sustainable cybersecurity culture rooted in society;
- favours incident communication and response by promoting risk management and cyber incident protection and response;
- emphasizes the adoption of emerging technologies, promoting the reduction of the country's technological debt in emergency and disruptive technologies; e
- it unlocks a period of validity (now indefinite), starting to consider short, medium and long-term objectives and actions, adjustable through annual plans.

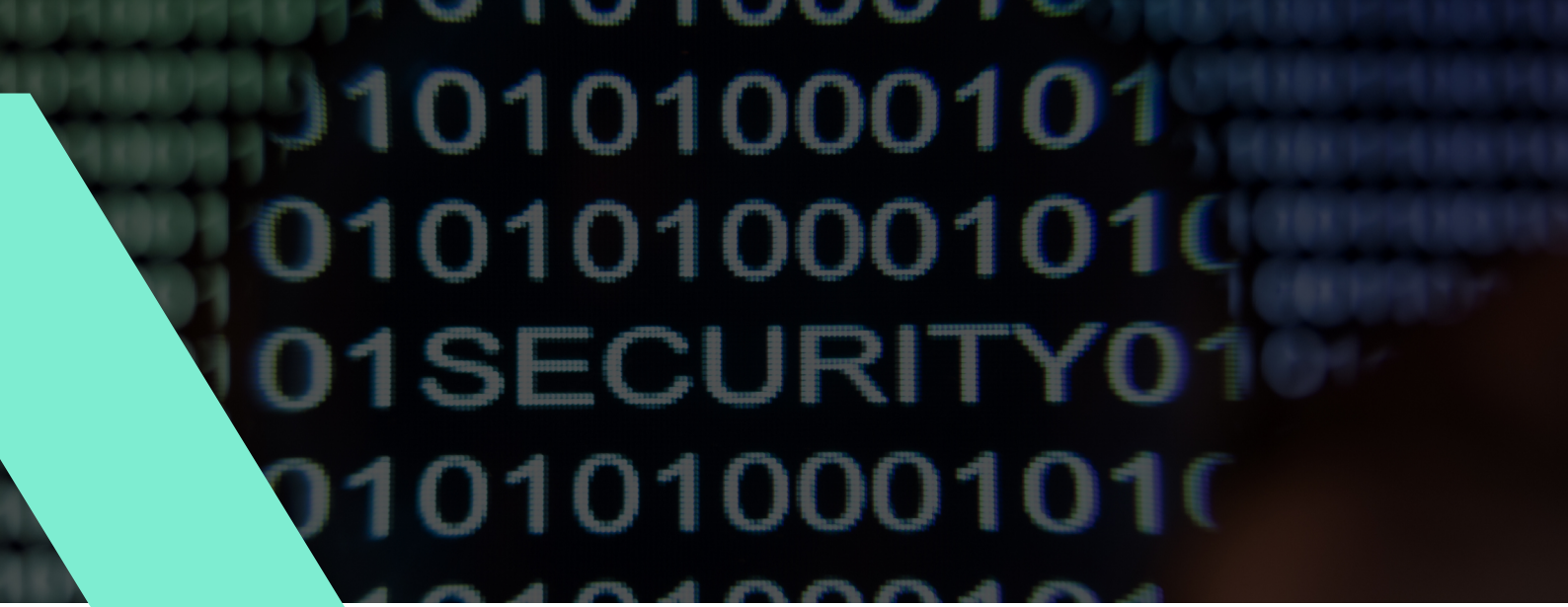
10. Next steps in Brazil

Brazil is moving forward with the consolidation of its cybersecurity governance, including the following assessments and measures:

- **Proposal for the creation of a Cybersecurity Activity Governance Body in Brazil:** the trend is for Brazil to advance in the institutionalization of a robust cybersecurity legal framework, accompanied by the formal definition of a central coordination body and national authority in this matter. Recent discussions at CNCiber indicated ANATEL as a possible central cybersecurity authority, reflecting the need for a structure capable of articulating incident responses, supervising critical sectors, and coordinating public policies**.**
- **The role of the ANPD and LGPD in Cybersecurity:** the LGPD, coordinated by the ANPD, tends to be increasingly integrated into cybersecurity policies, reinforcing the notion that data protection and information security are inseparable dimensions of digital governance. The ANPD should intensify technical guidelines, minimum security standards, and compliance expectations, especially in contexts of incidents involving personal data, in line with international initiatives that link data protection to cybersecurity operational requirements. In addition,

security, technical and administrative measures (including minimum technical security standards) are a priority item on the ANPD's Regulatory Agenda.

- **Cybereducation and Cyberhygiene:** awareness and good practices for individuals and companies, with a focus on risk prevention.
- **Mininum cybersecurity benchmarks:** development of pratical recommendations for operators of Essential Services and Critical Infrastructures, establishing mininum protecion parameters.
- **Guidelines for ISACs (Information Sharing and Analysis Centers)**: elaboration of Guide for the creation and operation of incident sharing and analysis centers, based on the GSI Ordinance No. 148, aiming at integration with the **Government Cyber Incident Management Network (REGIC).**
- **National Cybersecurity Plan:** construction of the operational plan that will support the **future National Strategy**, consolidating guidelines, goals and coordinated actions.



Conclusion

Cybersecurity is a fundamental pillar for digital transformation, the competitiveness of Brazilian companies and, consequently, the country's economic and social stability, which is why it is important for Brazil:

- Establish a balanced, flexible and efficient Legal Framework, in line with international best practices, restricting a greater regulatory burden to critical infrastructures and essential services for the Brazilian economy;
- Create a central entity for national cybersecurity coordination, with the function of organizing and coordinating regulatory actions and public policies related to the topic, as well as avoiding overlapping competences;
- Foster awareness, education and training in cybersecurity;
- It will insert SMEs in the cybersecurity governance treadmill;
- Encourage research, development and innovation in cybersecurity;
- Stimulate and create legal certainty for data sharing, intelligence, and the establishment of a national cyber incident response network; and
- Strengthen your international relationships to collaborate on global cybersecurity initiatives.

Direito,
Inovação
& Tecnologia

ABOUT US

At VLK, **the Law is not a barrier**. It is the momentum to **innovate, enable businesses**, and build a more prosperous and just society.

We are a **Digital Law boutique** driven by **results that make a difference.**

We reconcile:

» Risk and opportunity;

» Complexity and clarity; and

» Protection and progress.

No matter how bold the project: we will make it happen securely and by **breaking down unnecessary formalisms** in the following areas:

» Personal Data Protection

» Ethical and Responsible AI Governance

» Cybersecurity and Incident Response

» Legal Marketing and Intellectual Property

» Technology Regulation

» Strategic Litigation

AUTHORS

Rony Vainzof
rony@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Direito,
Inovação
& Tecnologia

The e-book: “Cybersecurity and Cybercrimes: A View from Brazil” – March 2026.

CC BY-ND – This license allows copying and distribution of the material in any medium or format, provided it is shared in its original, unadapted form and proper attribution is given to the creator. The license permits commercial use.