#pública

Information and Cyber Security Policy

Pol600 V.13

BB Tecnologia e Serviços

INFORMATION AND CYBER SECURITY POLICY

1. AREA RESPONSIBLE

1.1. Digital Security and Information and Technology Governance Management - Geseg.

2. SCOPE

2.1. This policy guides the behavior of BB Tecnologia e Serviços, considering the specific needs and the legal and regulatory aspects to which BBTS is subject.

3. OBJECTIVE

3.1. The purpose of this policy is to establish principles and guidelines to be observed when handling and protecting corporate information and the company's cyber environment.

3.2. To provide input for the preparation of Internal Standards, Procedures, Processes and other documents to optimize the use of resources, improve the quality of services and enable successful responses to information and cyber security incidents, as well as disaster recovery.

4. REGULATIONS

4.1. CGPAR Resolution No. 11, of May 10, 2016.

4.2. ABNT NBR ISO/IEC 27001:2022 - Information security management systems - Requirements.

4.3. ABNT NBR ISO/IEC 27002:2022 - Code of practice for information security controls.

4.4. Complementary Standard 03/IN01/DSIC/GSIPR (Office of Institutional Security of the Presidency of the Republic) - Guidelines for drawing up an Information and Communications Security Policy in the bodies and entities of the Federal Public Administration.

4.5. Decree No. 9.637, of December 26, 2018 - National Information Security Policy.

4.6. Law No. 13.709, of August 14, 2018 - General Data Protection Law (LGPD).

4.7. Decree No. 10.222, of FEBRUARY 5, 2020 - National Cybersecurity Strategy - E-Cyber.

4.8. CMN Resolution 4.893/21 - Cyber security policy and requirements for contracting data processing, storage and cloud computing services to be observed by institutions authorized to operate by the Central Bank of Brazil.

5. REVIEW PERIODICITY

5.1. The Information Security Policy must be reviewed at least every one year, extraordinarily, at any time.

6. CONCEPTS

6.1. **Information attributes:** Confidentiality, Integrity, Availability and Authenticity.

6.2. **Authenticity:** Characteristic, particularity or state of what is authentic. Nature of what is real or true.

6.3. **Confidentiality:** ensuring that information is only accessible by those authorized to access it.

6.4. **Availability:** ensuring that authorized users have access to information and associated resources when required.

6.5. **Integrity:** ensuring that the information has not been altered during its transportation and storage process.

6.6. **Personal data:** information relating to an identified or identifiable natural person.

6.7. **Privacy:** Private life, intimacy, the right to personal information and privacy.

6.8. **Cybersecurity:** A set of actions that deals with aspects of the operationalization of information security resources to protect against cyberattacks.

7. ENUNCIATED

7.1. In business management, we treat information as an asset and, therefore, it must be comprehensively protected through practices and policies that guarantee its integrity, confidentiality and availability.

7.2. We align the management of information security and cyber security with the company's objectives, contributing to a secure, stable and reliable environment for doing business.

7.3. We preserve our information security and cyber security requirements when purchasing products, contracting services or people and in our relationship with employees, suppliers, third parties, partners, contractors and trainees and other individuals or legal entities that have a relationship with the company.

7.4. We process information ethically and responsibly, applying the rules, policies, legislation in force and good practices recognized by internal and external control bodies.

7.5. We control and identify access to information by individualizing the access authorization for each user, making them responsible for the security, confidentiality and privacy of the information in their custody, or that they may become aware of, and for all acts performed with their identifications.

7.6. We authorize and grant requesters access to and use of only the information necessary for the performance of their functions and duties or by legal determination.

7.7. We treat the information generated, acquired and/or held by BB Tecnologia e Serviços in such a way as to guarantee that the attributes of confidentiality, integrity and availability are present

throughout its entire life cycle: collection, production, handling, reproduction (copying), sharing, transportation, transmission, storage, disposal or restoration.

7.8. We classify information in terms of confidentiality, integrity and availability, applying protection in a way that is compatible with its criticality for our activities and affecting all processes, including those that deal with personal data, whether computerized or not.

7.9. We establish Information Security, Cyber Security and Business Continuity Risk Management, identifying and correcting vulnerabilities, threats and risks involving information assets and technological environments, including data communication networks and Cloud Computing.

7.10. We are committed to keeping the technology park preserved and protected, in accordance with the best physical and technological security practices. Access to the company's physical environments is controlled and granted only to authorized persons, with special attention to environments where information processing takes place.

7.11. We have adopted actions, mechanisms or measures aimed at reporting cyber attacks and malicious actions in accordance with the Incident Response Plan.

7.12. We disseminate the culture of information and cyber security through a permanent program of sensitization, awareness and training aimed at employees, collaborators, suppliers, third parties, partners, contractors and trainees and other individuals or companies that have a relationship with the company.

7.13. We analyze incidents of improper handling of corporate information under the legal and disciplinary aspects in force, and hold the company accountable. From a technical point of view, we use tools to protect against cyber threats.

7.14. We invest in mechanisms to protect, monitor, respond to and recover from cyber risks.

7.15. We are concerned with cyber resilience so that the appropriate measures can be taken in the event of a cyber incident or potential cyber threat.

8. APPROVAL

8.1. Through Technical Note 2023/0319, this policy was appraised by the Executive Board on June 22, 2023 and approved by the BBTS Board of Directors (Conad) on June 30, 2023.