POLÍTICA DE SEGURANÇA CIBERNETICA

1. OBJETIVO

Em atendimento a resolução CMN nº4.893/2021, o Banco CCB Brasil mantém em sua estrutura uma política de Segurança da Informação que engloba a segurança cibernética e plano de resposta a incidentes. Este documento tem por objetivo registrar e direcionar numa visão geral e macro os principais aspectos de Segurança da Informação a serem observados para o CCB Brasil. Todas as diretrizes expressam de maneira geral a posição da Instituição sobre a Política de Segurança da Informação adotada, as premissas, valores, atuação e direcionamentos determinados pela alta direção para minimizar os riscos sobre seus ativos de informação.

1. OBJECTIVE

In accordance with CMN Resolution No. 4893/2021, CCB Brasil bank maintains in its structure an Information Security policy that includes cyber security and an incident response plan. The goal of this document is to register and direct in a general and macro vision the main aspects of Information Security to be observed to CCB Brasil. All directives generally express the position of the Institution about the adopted Information Security Policy, its premises, values, acting e directions demanded by the board to mitigate risks over information assets.

2. ALCANCE

Aplica-se ao público em geral, clientes, prestadores de serviços, usuários de websites e aplicativos do Conglomerado CCB Brasil.

2. SCOPE

It applies to the public, customers, services providers, users of Conglomerate CCB Brasil websites and applications

3. PRINCIPIOS

O CCB Brasil tem o compromisso de garantir a segurança e tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

Confidencialidade – garantia de que a informação somente será acessada por pessoas efetivamente autorizadas a terem acesso.

Disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessário, nos períodos e ambientes aprovados pela empresa.

Integridade – garantia de que a informação somente será modificada por pessoas efetivamente autorizadas a fazê-la e dentro dos métodos aprovados para estas ações.

3. PRINCIPLES

CCB Brasil is committed to ensuring the security and proper handling of information. To this end, our activities are based on the following principles:

Confidentiality – The guarantee that only authorized personal can access the information

Availability – The guarantee that authorized personal can have access to the information and systems always that it is needed, in periods and environment approved by the company.

Integrity – The guarantee that only authorized personal can modify information and using approved methods.

4. TERMOS GERAIS

- Toda informação deve ser classificada, protegida e controlada de acordo com sua importância, sensibilidade e requisitos de negócios.
- Seguindo as boas práticas de Segurança da Informação, o Banco CCB Brasil deve:
  - Identificar, proteger, detectar, investigar e responder às ameaças que possam afetar as informações tratadas;
  - Efetuar o monitoramento e prevenção ao vazamento de informações;
  - Promover a conscientização, treinamento e a cultura de Segurança da Informação;
- Funcionários e prestadores de serviços devem utilizar a informação de forma legítima, legal, respeitosa e responsável, seguindo os preceitos da Política de Segurança da informação;
- O acesso a informação deve ser restrito, permitindo que colaboradores acessem apenas a informação estritamente necessária para desempenhar sua função.
- O fluxo de informação deve ser limitado e protegido pelas barreiras de informação interdepartamentais;
- Todo tratamento de informação deve assegurar a privacidade, autenticidade, confidencialidade, integridade e disponibilidade da informação;
- A responsabilidade sobre a informação deve ser estabelecida e revisada periodicamente;
- Os tratamentos de informações sensíveis devem ser auditáveis e devem estar disponíveis para consulta pelo período determinado na legislação vigente;
- Os controles de segurança da informação e segurança cibernética devem ser testados regularmente e auditados para assegurar eficácia.

4. GENERAL TERMS

• All information must be classified, protected and controlled according to its importance, sensitivity and business requirements.

• Following good Information Security practices, Banco CCB Brasil must:

- Identify, protect, detect, investigate and respond to threats that may affect the information processed;
- Monitor and prevent information leakage;
- Promote awareness, training and a culture of Information Security;

• Employees and service providers must use the information in a legitimate, legal, respectful and responsible manner, following the precepts of the Information Security Policy;

• Access to information must be restricted, allowing employees to access only the information strictly necessary to perform their duties.

• The flow of information must be limited and protected by interdepartmental information barriers;

• All information processing must ensure privacy, authenticity, confidentiality, integrity and availability of information;

• Accountability for information must be established and periodically reviewed;

• Treatments of sensitive information must be auditable and must be available to consultation for the period determined in the legislation in force;

• Information security and cybersecurity controls must be regularly tested and audited to ensure effectiveness.

Emissão/Issue	Validade/Expiration
10/11/2022	10/11/2023