Política de Segurança Cibernética- BRB

NORMAS RELACIONADAS

Instrução Normativa BCB nº 511

Resolução CMN nº 4.893, de 26/02/2021.

Resolução BCB nº 85/2021

Resolução BCB nº 211, de 22 de março de 2022

Política de Segurança da Informação – BRB.

Manual de Gestão de Continuidade de Negócios - BRB.

INTRODUÇÃO

A informação é um ativo essencial para os negócios do Conglomerado BRB e deve ser adequadamente protegida. O Conglomerado BRB, alinhado com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos, tecnologia e demais normativos internos, de forma a proteger as informações do BRB, de seus clientes, fornecedores e parceiros de negócios.

OBJETIVOS

Nossa Política de Segurança Cibernética tem como objetivo estabelecer princípios, diretrizes, papéis e responsabilidades sobre os principais aspectos relacionados à segurança cibernética, visando: assegurar a confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade dos dados e dos sistemas de informação utilizados pelo Conglomerado BRB; assegurar o cumprimento da legislação vigente e fomentar uma cultura organizacional pautada na ética, integridade e conformidade. Esta política é revisada continuamente, considerando os desafios impostos pela dinâmica das atividades corporativas, bem como os apontamentos oriundos de auditorias internas, demandas do negócio e exigências de órgãos reguladores e auditorias externas.

PRINCÍPIOS

Confidencialidade: Asseguramos que as informações sejam acessadas apenas por pessoas devidamente autorizadas. Esse princípio protege dados sensíveis contra vazamentos, espionagem corporativa e uso indevido, preservando a privacidade e a vantagem competitiva da organização.

Integridade: Garantimos que as informações sejam precisas, completas e confiáveis, protegidas contra alterações não autorizadas. A integridade é essencial para a tomada de decisões baseada em dados corretos e para a manutenção da confiança nos sistemas e processos da organização.

Disponibilidade: Nossas informações e sistemas devem estar acessíveis sempre que necessário, garantindo a continuidade das operações. A indisponibilidade pode causar prejuízos financeiros, operacionais e reputacionais, sendo fundamental a adoção de medidas como redundância, backups e planos de contingência;

Autenticidade: Asseguramos que a identidade de usuários, sistemas e informações seja legítima e verificável. A autenticidade previne fraudes, acessos indevidos e garante que as comunicações e transações sejam realizadas por fontes confiáveis.

Irretratabilidade: Garantimos que uma ação ou comunicação não possa ser negada posteriormente por seu autor. Esse princípio é vital para a responsabilização, auditoria e conformidade legal, especialmente em ambientes digitais e transações eletrônicas.

DIRETRIZES

Estabelecemos critérios de avaliação de riscos e requisitos mínimos de segurança para adoção de novas tecnologias e arquitetura segura.

Executamos avaliações de risco para serviços críticos contratados em nuvem, considerando exigências regulatórias e aspectos técnicos.

Integramos cenários de ameaças cibernéticas em exercícios de Continuidade de Negócios para validar controles e planos de resposta.

Mantemos planos de contingência e comunicação para interrupções em serviços críticos contratados em nuvem.

Mantemos programa contínuo de aculturamento, capacitação e avaliação em segurança cibernética, privacidade e riscos de TI.

Participamos de fóruns e plataformas colaborativas de intercâmbio de informações sobre ameaças cibernéticas.

Monitoramos continuamente os normativos publicados por entes reguladores e adotamos ações para assegurar conformidade com temas relacionados à segurança cibernética.

Mantemos mecanismos de rastreabilidade e proteção de dados classificados como sensíveis, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e regulamentações do Banco Central do Brasil.

Adotamos política de classificação da informação com critérios objetivos e claros de sensibilidade e impacto ao negócio.

Estabelecemos diretrizes para o uso responsável da inteligência artificial (IA), com foco em segurança, ética e transparência.

Mantemos diretrizes para a proteção de identidades e gestão de acessos privilegiados (PAM), com foco em segregação de funções e trilha de auditoria.

Implementamos procedimentos e controles para prevenir, detectar e mitigar vulnerabilidades.

Estabelecemos critérios de segurança para o ciclo de vida de software, priorizando práticas seguras desde o desenvolvimento até a implantação.

Formalizamos diretrizes de segurança aplicáveis a terceiros e prestadores que lidam com dados sensíveis ou processos relevantes.

Disponibilizamos orientações periódicas aos clientes sobre segurança digital e proteção contra fraudes.

Adotamos diretrizes para proteção de endpoints e dispositivos móveis, com foco em monitoramento, prevenção e controle de acesso.

Classificamos os incidentes com base em critérios regulatórios e de impacto ao negócio, priorizando a resposta e a comunicação adequadas.

Documentamos causas, impactos e ações de resposta a incidentes cibernéticos, inclusive com informações de terceiros, quando aplicável.

GOVERNANÇA CORPORATIVA

Dispomos de estrutura pautada em normas e frameworks internacionais para manutenção dos processos que garantem a segurança cibernética do BRB, a conformidade com a Resolução CMN 4.893/21 e os demais normativos de entes reguladores, e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética.

ÂMBITO E VIGÊNCIA

As diretrizes e os princípios estabelecidos neste documento devem ser observados por todos os administradores, empregados, prestadores de serviço e demais colaboradores do Conglomerado BRB.

Esta política possui vigência a partir de sua publicação.